



Kentucky Cybersecurity Industry Study June 2017

for Kentucky Commission on
Military Affairs

by Simon Everett, Ltd.



simon
everett
an analytic design firm

This study was prepared under contract with the Commonwealth of Kentucky, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Kentucky, and does not necessarily reflect the views of the Office of Economic Adjustment.

Table of Contents

Executive Summary	1
Key findings	4
Recommendations	8
Introduction	13
Chapter 1 Economic Impact.....	16
Understanding the data	17
Defining the cybersecurity sector	18
Assessing the sector’s economic impact	18
Characterizing the cybersecurity sector	28
Recommendations	34
Chapter 2 Economic Incentives	35
The economics of cybersecurity	36
Incentives for organizations to improve their cybersecurity	37
Incentives for attracting cybersecurity companies	49
Recommendations	55
Chapter 3 Workforce.....	57
Defining the cybersecurity workforce	58
Characterizing Kentucky’s cybersecurity workforce	61
Recommendations	66
Chapter 4 Education	68
Cybersecurity education in Kentucky today	69
Connecting education and workforce	78
Cybersecurity education initiatives around the country	80
Recommendations	83
Chapter 5 Governance	84
Critical infrastructure risk management	85
A framework for CCI risk assessment	91
Information sharing	99
Laws	102
The Commonwealth Cybersecurity Committee	106
Recommendations	108
Chapter 6 Defense Partnerships + Emergency Management.....	109
Emergency management in the cyber context	110
Key emergency management resources	112
Department of Defense installations in Kentucky	113
Recommendations	117
Chapter 7 Capability + Awareness	118
Capability adoption	119
User awareness	123
Recommendations	129
Chapter 8 Risk Management.....	130
Why every organization should have a risk management strategy	131
Frameworks for risk management	132
Cybersecurity planning	134
Recommendations	141
Chapter 9 Privacy	142
What is a Chief Privacy Officer?	143
Why is privacy so important?	144
Enter the CPO	144
Case Study: Washington Office of Privacy and Data Protection	146
Case Study: South Carolina Enterprise Privacy Office	147
Case Study: West Virginia State Privacy Office	148
Recommendations	149
Chapter 10 Cybersecurity Initiative	151
What is a cybersecurity initiative?	152
State-by-state comparison	153
Case Study: Virginia Cyber Security Commission	159
Case Study: Michigan Cyber Initiative	161
The Kentucky Cybersecurity Council	163
Recommendations	165
Acknowledgments	166
Appendices	169
Appendix A: Key terms	170
Appendix B: Acronyms	172
Appendix C: Educational institutions and degrees	178
Appendix D: Sources	183

The image is a landscape photograph of a rural scene at sunset. A wooden fence with wire mesh runs from the foreground into the distance, leading the eye towards a single, bare tree on the horizon. The sky is a gradient of colors from deep blue at the top to bright orange and yellow near the horizon. The foreground is filled with green grass and yellow wildflowers. The entire image is split vertically by a dark blue gradient that is darkest on the left side, where the text is located.

EXECUTIVE SUMMARY

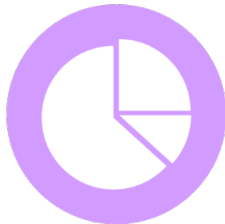
Executive Summary

In September 2016, the Commonwealth of Kentucky commissioned a team of analysts led by Simon Everett, Ltd., and its partner kglobal, LLC, to conduct the first-ever statewide study of cybersecurity in Kentucky. This study was made possible by a grant awarded to the Kentucky Commission on Military Affairs (KCMA) by the Department of Defense (DoD) Office of Economic Adjustment (OEA). Through grants like this one, OEA helps communities adjust to the economic impacts of fluctuations in defense spending.

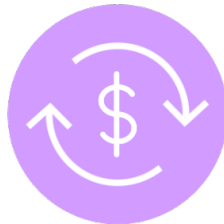
Through independent research, stakeholder interviews, and an industry survey, our team sought to understand, assess, and make actionable recommendations to improve the state of cybersecurity in the Commonwealth. In particular, the study is designed to help Kentucky’s policymakers devise strategies to meet three objectives:

- **make the defense industrial base more resilient** by helping defense companies better assess opportunities for growth and diversification in the cybersecurity sector;
- **strengthen the economy** by creating an environment conducive to the growth of the cybersecurity industry; and
- **protect critical infrastructure** by empowering government agencies, businesses, and citizens to create a healthy cybersecurity ecosystem.

The study addresses ten topic areas, as shown below. In this executive summary, we will recap the study’s major findings and key recommendations.



Economic Impact



Economic Incentives



Workforce



Education



Governance



Defense Partnerships +
Emergency Management



Capability +
Awareness



Risk Management



Privacy



Cybersecurity Initiative

About the Office of Economic Adjustment

OEA is the Department of Defense's field organization responsible for supporting state and local government's response to defense program changes, such as base closures, base restructuring or realignment, growth issues surrounding compatible land and air use for military base and community, and other issues that can impact the economy of a region.

About the Kentucky Commission on Military Affairs

The Kentucky Commission on Military Affairs (KCMA) is an independent agency attached to the office of the governor. It is the lead advocate for military installations and the related defense economy in Kentucky. KCMA has directly managed Base Re-alignment and Closure (BRAC), set conditions for economic growth near Kentucky military installations, and provided insight to all levels of government regarding the military and veterans.

About the study team

Simon Everett is an analytic design firm that conducts objective research and analysis to support strategic planning efforts on issues like defense diversification and cybersecurity. kglobal is a strategy and communications firm that works with public and private sector clients on a range of economic development programs. Together, we have supported three states and over 20 individual defense companies under OEA-supported initiatives to strengthen economic and workforce resilience.

Contact information

For more information about this study, please contact:

- Simon Everett // inquiries@simon-everett.com
- Kentucky Commission on Military Affairs // 502.564.2611, extension 302

Key findings

Although it represents a small portion of the economy, Kentucky’s cybersecurity sector is rife with opportunity. Cybersecurity workers earn more than the average worker, and cybersecurity companies can spur innovation, investment, and additional economic activity. Moreover, the Commonwealth has key infrastructure in place to enable the growth of the sector: an educational system with broad-based computer science programs, advanced research and development institutions, tax incentive programs for business attraction and retention, and a growing information technology hub in Louisville.

Kentucky has also taken significant strides in bolstering the state’s cybersecurity posture. It has partially centralized the state government’s information technology infrastructure within the Commonwealth Office of Technology (COT); the Kentucky Office of Homeland Security (KOHS) is planning to increase its focus on cybersecurity information sharing; and the Kentucky Army National Guard (KYARNG) is a leader among its peers in the cybersecurity field. Moreover, the state government has adopted two laws to help protect the data of Kentucky’s citizens.

The Kentucky Cybersecurity Industry Study yielded dozens of insights into the cybersecurity landscape in the Commonwealth, covering a range of economic and security issues. The table below highlights 22 of the most salient findings.

Table 1 // Key findings of the Kentucky Cybersecurity Industry Study

#	Finding
1	<p>The cybersecurity industry has an estimated economic impact of \$730,277,977 in Kentucky.</p> <p>When compared against Kentucky’s Gross State Product for 2015, this figure represents 0.37% of the total. The bulk of the cybersecurity industry’s impact (92%) results from economic effects induced by the spending of cybersecurity workers, rather than direct (6%) or indirect (2%) effects.</p>
2	<p>Kentucky’s cybersecurity sector is small.</p> <p>There are 54 companies in Kentucky that sell cybersecurity goods and services, but only a handful are “pure play” cybersecurity companies. Most are managed services companies that provide cybersecurity as part of a larger information technology capability suite. Kentucky lacks a critical mass of disruptive, cutting-edge cybersecurity companies that generate the buzz required to attract innovators and investors.</p>
3	<p>Most of Kentucky’s cybersecurity workers do not work at cybersecurity companies.</p> <p>Approximately 9,516 people work in Kentucky’s cybersecurity sector, 9,383 of whom are performing cybersecurity functions. Of that group, 8,825 are supporting the internal cybersecurity needs of companies in non-cybersecurity sectors – like manufacturing and healthcare.</p>
4	<p>Louisville is the epicenter of Kentucky’s cybersecurity sector.</p> <p>Louisville is home to about half of the state’s cybersecurity companies, as well as industry associations and conferences focused on the information technology industry. Many of the ingredients needed to create a geographic hub for the cybersecurity sector are already resident in Louisville.</p>

#	Finding
5	<p>There is a state-level precedent for designing and implementing a tax incentive program to attract cybersecurity companies.</p> <p>Maryland’s Cybersecurity Investment Incentive Tax Credit encourages investments in qualified cybersecurity companies. Two or three companies have participated in the program every year since 2014.</p>
6	<p>Approximately 60% of Kentucky’s total cybersecurity workforce is comprised of three job categories.</p> <p>Computer systems administrators, computer and information systems managers, and computer systems analysts are the most common cybersecurity occupations in the Commonwealth.</p>
7	<p>Cybersecurity workers earn far more than the average Kentuckian.</p> <p>Workers in every cybersecurity occupation earn more – on average – than Kentucky’s annual mean wage of \$41,760. Some workers, like computer and information systems managers, earn more than double that figure. Knowledge economy skillsets command higher wages, and the cybersecurity sector in Kentucky is no exception.</p>
8	<p>Demand for cybersecurity workers in Kentucky is relatively low.</p> <p>Kentucky’s demand for workers in nearly every cybersecurity occupation is lower than the national average for that occupation, reflecting a greater need (from an economic development perspective) for information technology companies generally and cybersecurity companies specifically.ⁱ</p>
9	<p>Kentucky universities offer broad IT education options, but fewer cybersecurity-specific programs.</p> <p>24 public, independent, and for-profit universities, along with 16 community and technical colleges, offered 79 degrees, diplomas, and certificates relevant to cybersecurity in 2016. Most such programs concerned IT, computer science, or homeland security generally, with just a handful focusing on cybersecurity specifically. Broadly speaking, these programs are geographically well dispersed throughout Kentucky.</p>
10	<p>The number of cybersecurity-relevant degrees, diplomas, and certificates spiked in 2014 and again in 2016.</p> <p>At the undergraduate level, approximately 2,500 Kentuckians completed such programs in 2015; the next year, that number had more than doubled.</p>
11	<p>Kentucky has three Centers for Academic Excellence in Cyber Defense.</p> <p>The National Security Agency and the Department of Homeland Security have designated Northern Kentucky University, the University of Louisville, and (most recently) the University of the Cumberlands as Centers for Academic Excellent in Cyber Defense (CAE-CDs). With only three CAE-CDs, Kentucky trails the country’s leading cybersecurity states: Maryland (16), Florida (13), Texas (13), New York (12), and Virginia (11). Kentucky’s three CAE institutions are also only for cyber defense education; none are designated for research or for two-year programs. Other states have a mix of all three CAE-CD programs, which gives them a more balanced impact on the cybersecurity workforce. And although CAEs for Cyber Operations are less common, Kentucky has none.</p>

#	Finding
12	<p>Kentucky has at least four institutions that can enable cybersecurity research and development.</p> <p>The Center for Applied Informatics at Northern Kentucky University, the Center for Computational Sciences at the University of Kentucky, the Center for Research and Development at Western Kentucky University, and the Cardinal Research Cluster Supercomputer at the University of Louisville all represent infrastructure that can support cybersecurity innovation.</p>
13	<p>There are 8 organizations that provide cybersecurity-related training at 13 locations in Kentucky.</p> <p>Even though training is available online for each of the 19 certifications that we reviewed, there is a lack of brick-and-mortar training locations in the eastern and southeastern parts of Kentucky. CompTIA Security+ and the (ISC)² Certified Information Systems Security Professional (CISSP) certifications are most often regarded as the most important certifications by respondents to our industry survey.</p>
14	<p>Thousands of people who received a cybersecurity-relevant education in Kentucky are also currently employed in Kentucky.</p> <p>Of those individuals who were issued a relevant degree, diploma, or certificate in Kentucky in the eleven-year period between 2006 and 2016, there were a total of 12,027 individuals employed in Kentucky in the 2015-16 fiscal year. The technology and education sectors are two of the leading employers of these individuals. However, many work for employers that naturally have low demand for information technology expertise – such as supermarkets, restaurants, and temp agencies.</p>
15	<p>Just 18% of Kentucky workers who received a cybersecurity-relevant education in Kentucky are female.</p> <p>This stark gender gap in the technology industry is not Kentucky’s challenge alone, but it is one that should be addressed directly in order to realize the full economic benefits of the cybersecurity economy.</p>
16	<p>Kentucky is taking a leadership role on elementary and secondary cybersecurity education.</p> <p>Following Louisiana, Kentucky became – in early 2017 – the second state to adopt National Integrated Cyber Education Research Center curricula for elementary and secondary school educators.ⁱⁱ The Kentucky Department of Education has made the curricula available to all school districts, and Jefferson County Public Schools will be first to put the curricula into effect at the high school level.ⁱⁱⁱ</p>

#	Finding
17	<p>Kentucky's state government has taken significant steps towards improving its own cybersecurity posture.</p> <p>Kentucky has established a Chief Information Security Officer; centralized cybersecurity for state agencies through the Commonwealth Office of Technology; created a Financial Cybercrime Task Force; held at least two cybersecurity-focused exercises; recognized cybersecurity in homeland security, law enforcement, and emergency strategic and operational plans; and formed fundamental homeland security and information sharing partnerships. The Kentucky Intelligence Fusion Center is also ramping up its cybersecurity program.</p>
18	<p>Kentucky has two state laws that address key cybersecurity issues.</p> <p>House Bill 5, among other directives, compels the state government to develop a framework for the protection of personally identifiable information (PII) and establishes requirements for what must happen if such information is compromised. House Bill 232 requires non-government holders of PII (like businesses and individuals) to notify any individual whose PII was compromised. However, Kentucky does not require businesses and individuals to notify the state government of such a compromise. As a result, there is no mechanism for the state to track these incidents. Some other states require businesses and individuals to notify the Attorney General.</p>
19	<p>The Kentucky Army National Guard is a national leader in cybersecurity.</p> <p>Kentucky is home to a nationally competitive National Guard cybersecurity unit. The National Guard has announced plans to establish an Army National Guard Cyber Protection Team in the Commonwealth by FY19.^{iv} This new unit has the potential to add immense value in defining and maturing cybersecurity assessment, protection, response, and recovery processes.</p>
20	<p>Kentucky lacks a comprehensive public awareness program for cybersecurity.</p> <p>COT and the Office of the Attorney General both host cybersecurity resource pages on their websites, which provide a starting point for the state's public awareness effort. However, the state lacks a comprehensive program for businesses (to help them establish baseline capabilities, user awareness, and risk management processes) and residents (to improve cybersecurity habits and awareness).</p>
21	<p>Six states have established Chief Privacy Officer (CPO) positions.</p> <p>While CPOs typically serve as the state government's lead resource on privacy issues, some also have a public-facing function designed to increase citizen awareness of privacy considerations. CPO roles also include best practice promotion, policy recommendation, training and education, technology regulation advice, and stakeholder engagement.</p>
22	<p>More than 20 states have established a multi-stakeholder cybersecurity initiative.</p> <p>Variable factors include structure, purpose, type, authority, method of establishment, and number and responsibilities of participants. While some states focused primarily on improving the state government's cybersecurity posture, other initiatives addressed education, workforce, economic development, information sharing, and a host of issues that concern the private sector and individual residents, as well.</p>

Recommendations

Kentucky already has many of the key ingredients it needs to realize the economic and security benefits of a vibrant cybersecurity sector. With purposeful action tied to strategic direction, it can put those ingredients to work. Kentucky can become a recognized hub for cybersecurity companies and talent, and it can be a national leader in protecting citizens, businesses, and infrastructure from cyber risk.

Guided by our findings, our report makes dozens of specific, actionable, and practical recommendations. Here, we highlight the most salient 22 recommendations identified in the study.

#	Recommendation
1	<p>Establish the Kentucky Cybersecurity Council (KCC).</p> <p>Kentucky should establish a comprehensive cybersecurity initiative that serves as the vehicle for implementing most of the recommendations in this report. The KCC should be forward-leaning, action-oriented, and collaborative. The KCC should be a permanent organizational unit attached to the Office of the Governor, and it should be co-chaired by the Governor or Lieutenant Governor and an industry executive. It should have three permanent government staff members and six committees comprised of both public and private sector members. The committees should cover: economy and innovation; workforce and education; critical infrastructure; military and veterans affairs; public awareness; and privacy. If the state government opts to create a Chief Privacy Officer position within the Commonwealth Office of Technology, that individual should lead the privacy committee.</p>
2	<p>Develop a statewide cybersecurity strategy.</p> <p>The Kentucky Cybersecurity Council should build on the findings of this study to develop a comprehensive statewide cybersecurity strategy. The strategy should be sweeping in scope but practical in design, and it should have achievable goals tied to measurable objectives that yield clearly defined outcomes.</p>
3	<p>Develop and promote a cybersecurity brand for Kentucky.</p> <p>Kentucky will need to brand its cybersecurity niche and promote it in order to appeal to the workers and companies that will build the cybersecurity economy. Focus on Kentucky’s assets – both in terms of industry and in terms of lifestyle – and contextualize them for innovators and investors. We recommend a comprehensive communications effort that includes strategic planning, stakeholder engagement, and marketing.</p>

#	Recommendation
4	<p>Launch a public awareness campaign.</p> <p>The cybersecurity planning guidelines we outline in this report should be validated, consolidated, and promoted in order to encourage business and citizen awareness of cybersecurity best practices. The campaign would include several discrete components, including (but not limited to):</p> <ul style="list-style-type: none"> • Cybersecurity resource website. A “one-stop shop” for businesses and citizens to access cybersecurity resources, and to learn about the latest risks and best practices, and to report incidents on their networks. While not endorsing a specific methodology or product, the website should include available government resources, non-commercial assessment tools, standards, information sharing organizations, and community best practices. The website should also have a specific section dedicated to privacy resources, to include tips and best practices and white papers. • Cybersecurity and privacy guidebooks. Clear, simple, and visually appealing guides to cybersecurity and privacy fundamentals for businesses and citizens, endorsed by the KCC. • Marketing support. Even though it’s a public policy issue, cybersecurity should be the subject of a marketing campaign not unlike ones brands use to market their products.
5	<p>Establish a cybersecurity hub.</p> <p>Investors and innovators need a dot on the map. They are drawn to thriving hubs of activity that are already attracting other investors and innovators. Louisville has organically become the center of Kentucky’s information technology industry. With a strong foundation of technology associations, conferences, and academic institutions, Louisville is well positioned to be the focus of attention. State and local leaders should work collaboratively on initiatives to bolster cybersecurity on the city’s economic agenda.</p>
6	<p>Invest in research and development.</p> <p>With excellent R&D infrastructure at universities throughout the Commonwealth, state government leaders should encourage investments in discrete cybersecurity initiatives. Specific attention should be given to commercializing technologies so that the results of R&D efforts can be brought to market by Kentucky companies. Additionally, another avenue for R&D investment could be a statewide competition for innovative cybersecurity research. The idea creates additional opportunities – like corporate sponsorship, incentivizing companies to establish a location in Kentucky, and so on.</p>
7	<p>Establish targeted economic incentives to cultivate the cybersecurity sector.</p> <p>Kentucky needs to create and attract cybersecurity companies – particularly the cutting-edge businesses that will create “buzz” for the Commonwealth. An economic incentive program designed to specifically attract a small but critical mass of such companies will provide the momentum needed to attract others to the state. If Kentucky chooses to become one of the first states in the nation to develop such a program, Maryland’s Cybersecurity Investment Incentive Tax Credit should be used as a frame of reference. The Kentucky Enterprise Fund and the Kentucky Business Investment Program represent existing frameworks that can be readily repurposed for attracting cybersecurity companies. The Commonwealth should ensure that additional focus be given to entrepreneurs who are looking for a place to launch their business.</p>

#	Recommendation
8	<p>Help existing companies pivot to the cybersecurity sector.</p> <p>For certain companies in adjacent industries (like defense), the cybersecurity sector represents an opportunity to grow their businesses and diversify their revenue streams. Kentucky should consider making business consulting services (like strategic planning and communications) available to qualified companies that want to pursue growth opportunities in the cybersecurity industry.</p>
9	<p>Invest in incentives for Kentucky-based organizations to improve their cybersecurity.</p> <p>Consider hosting a conference on cyber insurance; funding risk assessments for critical infrastructure assets; piloting new technologies for critical infrastructure protection; and investing in processes to help critical infrastructure operators mitigate cyber risk.</p>
10	<p>Host cybersecurity planning workshops.</p> <p>We recommend making training, technical assistance, and guidance available to businesses. If businesses better understand the cybersecurity challenges that they face on the potential costs associated with cyber risks, they will be more inclined to make the necessary investments in cybersecurity expertise. Workshops could be held monthly or bimonthly in different regions of the Commonwealth. They would be designed to help businesses develop cybersecurity plans by drawing on the guidelines we provide for capability adoption, user awareness, and risk management.</p>
11	<p>Increase cybersecurity education opportunities at the university level.</p> <p>A diversified and sophisticated cybersecurity education system is vital to a competitive cybersecurity workforce. The Commonwealth must take concrete steps, such as establishing university scholarships and expanding cybersecurity programs at universities. Particular attention should be paid to increasing access to cybersecurity education among females (to address the stark gender gap), residents of eastern Kentucky (where cybersecurity education opportunities lag behind other parts of the state), and other underrepresented groups.</p>
12	<p>Bring cybersecurity education to elementary and middle schools.</p> <p>While the adoption of the Cyber Engineering Pathway Curricula is an excellent first step, its near-term rollout is limited to the high school level. Cybersecurity education should begin earlier; children interact with technology every day, and the concepts of proper cyber hygiene should be taught at an early age. While the primary purpose would be to cultivate a cyber-savvy population, this effort would have the ancillary benefit of widening the funnel for the future cybersecurity workforce.</p>
13	<p>Establish the Commonwealth Cybersecurity Committee (C3).</p> <p>Building on existing cybersecurity efforts within the Commonwealth Office of Technology and across state government, Kentucky should establish the C3. Led by Kentucky’s Chief Information Security Officer, the C3 would conduct risk assessments for state government assets; oversee compliance with technical control programs; and oversee a training program for all government employees, among other functions.</p>

#	Recommendation
14	<p>Formalize a concept of operations for the cybersecurity mission of the Kentucky Intelligence Fusion Center (KIFC).</p> <p>The KIFC is well-positioned to be the “one-stop shop” for the sharing of cybersecurity information between government and industry. This expansion of KIFC’s role should be met with sufficient resourcing to ensure it can fulfill this vital function.</p>
15	<p>Adopt the proposed Kentucky Cyber Critical Infrastructure (CCI) Risk Management Process.</p> <p>Following a validation process by KIFC and key stakeholders, we recommend that the process become KIFC’s approach to identifying and managing risk across the Commonwealth’s CCI. For the first iteration of this process, KIFC should host a full-day workshop for key stakeholders from KOHS and Kentucky’s sector-specific agencies. The purpose will be to educate stakeholders on the CCI Risk Management process and to generate a comprehensive list of assets in question (AIQs). Stakeholders should nominate AIQs on an annual basis, although a refresher workshop may be necessary on a biennial basis.</p>
16	<p>Designate state-level sector-specific agencies.</p> <p>While the responsibility for coordinating critical infrastructure protection efforts in Kentucky falls to KOHS, we recommend that Kentucky mirror the Federal framework of assigning a sector-specific agency for each of the 16 critical infrastructure sectors.</p>
17	<p>Expand the data breach notification law.</p> <p>When a business or individual experiences a security breach that results in the loss of PII, they are required to notify the citizens whose PII was affected, but not the government. The Kentucky legislature should require those individuals and businesses to also notify the Office of Attorney General of the breach and PII loss.</p>
18	<p>Integrate cybersecurity into the Emergency Operations Plan.</p> <p>The EOP does address the threat of cyber terrorism, and it has a well-documented concept of operations for Emergency Support Function (ESF) 2: Communications. Moreover, COT has a cyber incident response plan for state government functions. However, the EOP should document the Commonwealth’s processes for managing a cyber disruption event that affects cyber critical infrastructure outside of the public sector.</p>
19	<p>Capitalize on the cybersecurity capability of the KYARNG.</p> <p>The KYARNG is rapidly establishing itself as a cybersecurity leader among its peers in other states. Currently a primary agency for ESF 2, the J6 is already one of the state’s foremost cybersecurity centers of excellence. The Commonwealth should consider expanding its cybersecurity roles and authorities in the case of an emergency, provided it is allocated appropriate resources and staff to fulfill additional obligations. As an example, the cyber annex to Washington State’s Emergency Management Plan specifically highlights the Governor’s authority to activate the National Guard.</p>

#	Recommendation
20	<p>Formalize Kentucky’s cybersecurity exercise program.</p> <p>The cybersecurity exercises conducted in Kentucky are an excellent starting point for a formal exercise program under the leadership of KOHS. Exercises can be held two or three times per year, with one strategic-level exercise and one or two with an operational focus. To ensure that progress is made in the intervals, each exercise should build on the findings of the previous one, and they should all be deliberately designed to identify gaps in plans and capabilities. Exercises provide an excellent opportunity to understand and strengthen partnerships, so it is critical that Kentucky’s military installations are included. Exercise management should include the Homeland Security Exercise and Evaluation Program (HSEEP) phases of foundation, design and development, conduct, evaluation, and improvement planning, as well as necessary coordination and after-action reporting.</p>
21	<p>Organize a government and military CISO roundtable.</p> <p>Because they are funded by taxpayer dollars and serve the public interest, government and military agencies at the federal and state levels share common concerns and constraints. We suggest that an informal roundtable of major government and military chief information security officers (CISOs) in Kentucky meet on a quarterly basis to discuss best practices and lessons learned. Although their authorities and scopes of responsibility vary significantly, CISOs from COT, the Kentucky National Guard, the Fort Knox NEC, the RNEC-Bluegrass, and major local jurisdictions (like Louisville and Lexington) could work together to address challenges shared by the enterprises they oversee.</p>
22	<p>Conduct another cybersecurity industry study in two years.</p> <p>We recommend conducting portions of this study (especially economic impact, education, and workforce) again in 2019. This “update” will allow policymakers to assess the progress of the cybersecurity economy over the previous two-year period and allow them to make adjustments as necessary.</p>

INTRODUCTION



Introduction

In September 2016, the Commonwealth of Kentucky commissioned a team led by Simon Everett, Ltd., and its partner kglobal, LLC, to conduct the first-ever statewide study of cybersecurity in Kentucky. This study was made possible by a grant awarded to the Kentucky Commission on Military Affairs (KCMA) by the Department of Defense (DoD) Office of Economic Adjustment (OEA). Through grants like this one, OEA helps communities adjust to the economic impacts of fluctuations in defense spending.

Through independent research, stakeholder interviews, and an industry survey, our team sought to understand, assess, and make actionable recommendations to improve the state of cybersecurity in the Commonwealth. In particular, the study is designed to help Kentucky's policymakers devise strategies to meet three objectives:

- **make the defense industrial base more resilient** by helping defense companies better assess opportunities for growth and diversification in the cybersecurity sector;
- **strengthen the economy** by creating an environment conducive to the growth of the cybersecurity industry; and
- **protect critical infrastructure** by empowering government agencies, businesses, and citizens to create a healthy cybersecurity ecosystem.

How this document is organized

The study is divided into ten chapters. Each chapter is designed to be read as a stand-alone study, and each one closes with practical recommendations to improve Kentucky's position relative to the issues analyzed therein. However, the chapters also work together, as the findings in one will impact the recommendations in another.

We have attempted to organize the chapters thematically: we start with the economy before we move on to security issues. We close with our recommendation for a statewide multi-stakeholder initiative that can put the recommendations in this study into practice.

- **Chapter 1 / Economic Impact** defines, assesses, and characterizes the cybersecurity sector in Kentucky. It also assesses the economic impact of the industry, including its direct, indirect, and induced effects.
- **Chapter 2 / Economic Incentives** discusses the economics of cybersecurity and then considers incentives for organizations to improve their cybersecurity posture. It also explores incentives for attracting cybersecurity companies to locate in the Commonwealth.
- **Chapter 3 / Workforce** discusses cybersecurity workforce categorization efforts at the Federal level and in California, and it analyzes the current and projected cybersecurity workforce within Kentucky.
- **Chapter 4 / Education** reviews the cybersecurity education and training landscape in the Commonwealth, and it highlights cybersecurity education initiatives in other parts of the country.
- **Chapter 5 / Governance** explores three sets of issues critical to the state government's cybersecurity challenge: critical infrastructure (and management of risks thereto), information sharing, and cybersecurity laws. It also discusses ways the Commonwealth can strengthen its existing internal cybersecurity infrastructure.

- **Chapter 6 / Defense Partnerships + Emergency Management** discusses key emergency management resources and military installations in Kentucky, as well as ways the Commonwealth can strengthen partnerships between them.
- **Chapter 7 / Capability + Awareness** explores ways Kentucky organizations can adopt enhanced capabilities and improve user awareness to strengthen their cybersecurity posture.
- **Chapter 8 / Risk Management** provides a roadmap for any Kentucky organization – whether a business, a government agency, or a non-profit organization – to adopt a risk management strategy and a cybersecurity plan.
- **Chapter 9 / Privacy** discusses the criticality of privacy in the context of cybersecurity, and it assesses how other states have approached the position of a Chief Privacy Officer.
- **Chapter 10 / Cybersecurity Initiative** analyzes the approaches taken by more than 20 states towards establishing a comprehensive, multi-stakeholder cybersecurity initiative. It also presents a structure for such an initiative in Kentucky.

About the Office of Economic Adjustment

OEA is the Department of Defense's field organization responsible for supporting state and local government's response to defense program changes, such as base closures, base restructuring or realignment, growth issues surrounding compatible land and air use for military base and community, and other issues that can impact the economy of a region.

About the Kentucky Commission on Military Affairs

The Kentucky Commission on Military Affairs (KCMA) is an independent agency attached to the office of the governor. It is the lead advocate for military installations and the related defense economy in Kentucky. KCMA has directly managed Base Re-alignment and Closure (BRAC), set conditions for economic growth near Kentucky military installations, and provided insight to all levels of government regarding the military and veterans.

About the study team

Simon Everett is an analytic design firm that conducts objective research and analysis to support strategic planning efforts on issues like defense diversification and cybersecurity. kglobal is a strategy and communications firm that works with public and private sector clients on a range of economic development programs. Together, we have supported three states and over 20 individual defense companies under OEA-supported initiatives to strengthen economic and workforce resilience.

Contact information

For more information about this study, please contact:

- Simon Everett // inquiries@simon-everett.com
- Kentucky Commission on Military Affairs // 502.564.2611, extension 302

An aerial photograph of a city, likely Knoxville, Tennessee, showing a mix of residential and commercial buildings. The left side of the image is covered by a dark, semi-transparent overlay. The text 'CHAPTER 1' is overlaid on this dark area in white, and 'Economic Impact' is overlaid in purple. The right side of the image shows the city in more detail, including a large stadium, a university campus, and surrounding hills under a cloudy sky.

CHAPTER

1

**Economic
Impact**

Chapter 1 | Economic Impact

Characterized by high wages, innovation, and long-term projected workforce demand, the cybersecurity industry is a rapidly growing segment of the American economy. Across the country, state and local government leaders are looking for ways to attract cybersecurity employers and workers. In this section, we'll define the cybersecurity sector for the purposes of our analysis, and then we'll assess its economic impact in Kentucky. We'll also characterize the cybersecurity sector by assessing the number, capabilities, and geographic profile of Kentucky's cybersecurity companies and by reviewing other enabling factors within the sector. Finally, we'll make recommendations for Kentucky to further develop and advance its cybersecurity economy.

Understanding the data

Before we begin, we'd like to explain two important data taxonomies that we used in building our analysis: NAICS and SOC codes. They are essential to performing any type of workforce or economic assessment, but they also have their limitations – especially in the context of this study.

To gather and organize data about companies and industries, government agencies primarily rely on the North American Industrial Classification System (NAICS). For the workforce, the standard is the Standard Occupational Classification (SOC) system. So, an analysis would be able to reveal how many retail salespersons (SOC code 41-2030) were employed by furniture stores (NAICS code 4421) in a given jurisdiction in a given year. Although these systems are not perfect, they work well for conventional industries that have been studied for decades and are relatively static.

But because it takes time to update these systems to reflect the changing nature of the economy, NAICS and SOC codes have limitations when studying a young or dynamic industry like the cybersecurity sector. In the most recent NAICS revision (published in 2017), there is no NAICS code for cybersecurity, nor are there codes for sub-categories like encryption or application security. Likewise, there is only one SOC code that would always map to a cybersecurity occupation; others would only sometimes represent cybersecurity occupations.

Throughout this section, you will see references to NAICS and SOC codes. We have identified the ones that we assess to be most relevant to cybersecurity, but they should not be interpreted as perfect matches.

Defining the cybersecurity sector

Cybersecurity is a broad term. Even within the U.S. Government, there is no consensus definition. Federal agencies that deal with cybersecurity, like the Department of Homeland Security, approach the term from their own vantage points, and they set parameters according to their respective missions. So, for the purposes of this study, we did the same in order to allow us to provide meaningful analysis.

In establishing a definition, we took care to avoid being overly detailed or technical; adding more specificity would unnecessarily complicate our assessments. On the other hand, we did want to set parameters that are clear and meaningful – but broad enough to encompass the range of people and organizations that play a role in cybersecurity. Following a thorough review of public and private sector definitions of cybersecurity, we arrived at the following:

Cybersecurity refers to the protection of electronic information and the devices, applications, and networks used to generate, access, transfer, or store electronic information.

Likewise, the cybersecurity *sector* encompasses a broad diversity of **cybersecurity companies**. It includes large software providers that sell event monitoring systems, consultancies that advise on cybersecurity strategy, and non-profits that produce cutting-edge encryption technologies. Some companies sell products, some companies sell services, and some companies sell both. But it also includes **cybersecurity workers** at non-cybersecurity companies. For example, the sector would include network security analysts at a manufacturer or a health care provider.

Assessing the sector's economic impact

To assess the cybersecurity sector's economic impact, we organized the sector into those two broad categories: **cybersecurity companies** and **cybersecurity workers**. In order to enable the necessary economic impact analysis (explained later in this chapter), we first had to derive the necessary inputs for each of the two categories. They are as follows:

- **Cybersecurity companies** – To account for the impact of these companies, we had to arrive at an estimated number of total workers employed by them (including employees who do not directly perform cybersecurity work, since their efforts still contribute to the health of the company and, in turn, the health of the state's economy). This number of employees is then used to estimate the economic impact of cybersecurity goods and services delivered by these companies.
- **Cybersecurity workers** – To account for the impact of these workers (at *non*-cybersecurity companies), we had to arrive at an estimate of their total income. This is then used to assess the impact of their spending as it flows through the state's economy.

Category 1: Identifying and characterizing cybersecurity companies

For the purpose of this study, we consider a *cybersecurity company* to be a **for-profit Kentucky-based company that sells cybersecurity capabilities (products, services, or both) as either part of, or the entirety of, its business offerings**. Some of these companies are “pure play” – meaning that they sell *only* cybersecurity products and services – while others sell cybersecurity capabilities among others. For the latter group, we attempted to only consider the portion of their business focused on cybersecurity. So, if an organization has two divisions – one for data storage and one for data security – only the data security division would be considered in our analysis, wherever possible. Thus, we will use

the term “cybersecurity company” to refer to either the entirety of a “pure play” company or to the cybersecurity portion of a diversified company.

To identify cybersecurity companies in Kentucky, we reviewed several different sources of data, in addition to those available through online research.

State government data. We reviewed data provided by the Cabinet for Economic Development (CED). CED conducts an annual survey of companies in Kentucky to gather information about the facilities they operate; the types of work performed at each facility (categorized by NAICS code), and the number of employees at each facility. We reviewed the reports for facilities associated with the three NAICS codes that are most relevant to the cybersecurity sector (represented in Table 1). While many companies associated with these NAICS codes do not sell cybersecurity capabilities, we identified the ones that do based on their corporate descriptions and additional online research.

Table 2 // NAICS codes most relevant to cybersecurity

5415	Computer Systems Design and Related Services
5182	Data Processing, Hosting, and Related Services
5416	Management, Scientific, and Technical Consulting

Industry survey. We designed a comprehensive industry survey to identify, characterize, and solicit inputs from the cybersecurity sector in the Commonwealth. We invited representatives of nearly 70 companies (including cybersecurity companies and companies in other sectors), universities, and government entities to respond. We encouraged them to forward the survey to their contacts, and we also asked more than a dozen industry associations in Kentucky for help in promoting the survey. The survey window was open from April 3 through April 28, 2017. In total, we received 25 responses.

Federal contracting data. We also reviewed federal contracting data that is publicly available, courtesy of USAspending.gov. We flagged any contract or grant issued to a Kentucky company in Government Fiscal Years 2015, 2016, or 2017 that appeared to be related to cybersecurity. This allowed us to identify several Kentucky companies that provide cybersecurity products or services to the Department of Defense or other federal agencies.

Our research indicates that there are 54 cybersecurity companies operating in Kentucky as of May 2017. Those 54 companies perform cybersecurity services at 63 facilities, and they employ nearly 700 people as part of their cybersecurity lines of business. We divided the cybersecurity sector into three industry codes. The results of our review of cybersecurity companies are represented in Table 2, and the narrative explanation follows.

Table 2 // Kentucky cybersecurity companies

NAICS	Description	Companies	Facilities	Employees
5182	Data Processing, Hosting, and Related Services	10	11	29
5411	Legal Services	1	2	14
5415	Computer Systems Design and Related Services	37	42	574
5416	Management, Scientific, and Technical Consulting	5	7	71
6114	Business Schools and Computer and Management Training	1	1	3
Totals		54	63	691

In the table above, **NAICS** and **Description** represent the industry classification that either a company voluntarily self-identified or our team assigned based on our assessment of that company’s capabilities. For those companies for which we determined a code, we selected only one code even if multiple codes may have been relevant.

Companies represents the number of cybersecurity companies, whereas **Facilities** represents the total number of facilities or locations at which those companies perform relevant services in Kentucky. Some companies perform cybersecurity work at more than one office, which is why there are slightly more facilities than companies. The “companies” category does not include academic institutions or non-profit organizations. Note that several institutions that offer cybersecurity training in Kentucky were omitted from this list because we could not make a determination or reasonable assumption about the number of cybersecurity staff they employ in Kentucky.

Employees represents an estimated number of people employed at those companies. Again, this number includes employees who are not directly performing cybersecurity work (e.g., business development and human resources personnel) because their efforts contribute to the health of the company, and therefore to the company’s economic impact. The figure is a very rough estimate. For companies that provided such data via the industry survey, we included that figure in our tally. But we did not have an estimated number of either total company employees or cybersecurity employees for most companies included in our tally. Through online research, we first attempted to estimate the total number of people employed at each company. We then assigned a percentage to each company, based on our assessment of how large a role cybersecurity played in its business portfolio. For a company that provides only cybersecurity capabilities, we included 100% of its employees. For other companies, we assigned a figure of 50%, 20%, 10%, or 5%.

Category 2: Identifying and characterizing cybersecurity workers

Because Category 1, detailed above, includes only employees who work at cybersecurity companies, we then had to account for workers who perform cybersecurity work at *non*-cybersecurity companies; i.e., people whose cybersecurity work is internal-facing to support companies in various industries. As a first step, we determined who would constitute a “cybersecurity worker” for the purpose of our analysis. As mentioned above, there is no set of SOC codes for cybersecurity, so we must make assumptions about the existing set of SOC codes. After a comprehensive review of the SOC list, we determined that there are 13 SOC codes that would normally be assigned to cybersecurity workers. We can only assume that one SOC code – 15-1122, Information Security Analysts – is comprised entirely of cybersecurity workers. For the other 12, we assigned a percentage, based on our understanding of the cybersecurity workforce. All subsequent data in this section is prorated based on the percentages represented in Table 3.

Table 3 // Cybersecurity workers, as a percentage of relevant SOC codes

SOC	Description	Estimated proportion of workers performing cybersecurity functions
11-3021	Computer and Information Systems Managers	50%
15-1111	Computer and Information Research Scientists	10%
15-1121	Computer Systems Analysts	20%
15-1122	Information Security Analysts	100%
15-1131	Computer Programmers	10%
15-1132	Software Developers, Applications	10%
15-1133	Software Developers, Systems Software	10%
15-1141	Database Administrators	10%
15-1142	Network and Computer Systems Administrators	60%
15-1143	Computer Network Architects	60%
15-1152	Computer Network Support Specialists	10%
17-2061	Computer Hardware Engineers	10%
25-1021	Computer Science Teachers, Postsecondary	20%

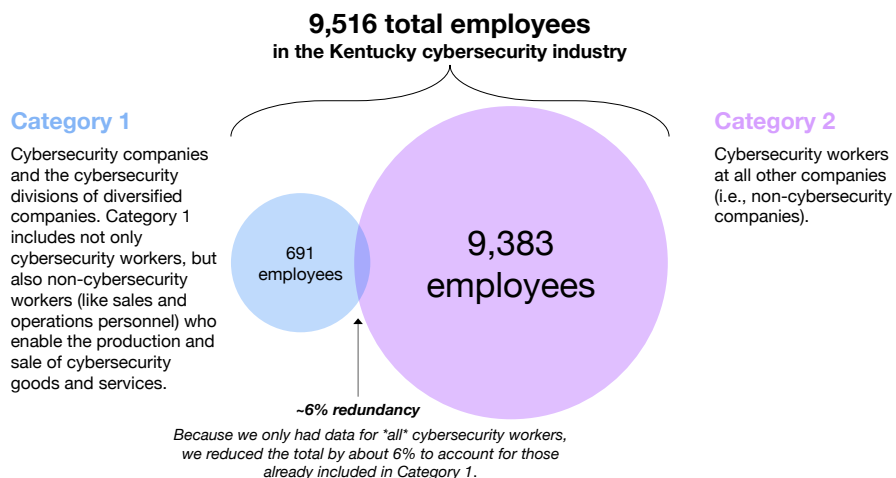
We then used data provided by the Cabinet for Economic Development and the JobsEQ® platform to determine how many cybersecurity workers were employed in Kentucky in 2016.^v Because some of these cybersecurity workers are already accounted for in our tally of Category 1 employees (and their economic impact will be accounted for in the Category 1 analysis), we reduced relevant SOC codes by a reasonable figure (6%) to achieve a total “exclusive” number of Category 2 cybersecurity workers for Category 2 (see Table 4). Note that workers in the *Computer Science Teachers, Postsecondary* category were not included in this reduction because none of the Category 1 cybersecurity companies was likely to employ an individual with this occupation.

Table 4 // Calculating the number of cybersecurity workers

SOC	Description	Cyber Workers	Reduction %	Cat 2 cyber workers
11-3021	Computer and Information Systems Managers	1,813	6%	1,704
15-1111	Computer and Information Research Scientists	20	6%	19
15-1121	Computer Systems Analysts	1,251	6%	1,176
15-1122	Information Security Analysts	947	6%	890
15-1131	Computer Programmers	300	6%	282
15-1132	Software Developers, Applications	695	6%	654
15-1133	Software Developers, Systems Software	353	6%	331
15-1141	Database Administrators	132	6%	124
15-1142	Network and Computer Systems Administrators	2,594	6%	2,438
15-1143	Computer Network Architects	923	6%	8667
15-1152	Computer Network Support Specialists	207	6%	195
17-2061	Computer Hardware Engineers	60	6%	56
25-1021	Computer Science Teachers, Postsecondary	88	--	88
Cyber workforce (including some Category 1)		9,383	Cat 2 workers	8,825

Although the combined total of Category 1 (691) and Category 2 (8,825) workers is not relevant to the subsequent economic impact analysis (because they serve as separate inputs to that analysis), it is worth pointing out that this figure – **9,516 workers** – represents total cybersecurity industry employment in Kentucky. Again, this includes both the cybersecurity and non-cybersecurity workers employed by cybersecurity companies (Category 1), as well as the cybersecurity workers we estimate to be employed by non-cybersecurity companies (Category 2). Figure 1 depicts the division between the two categories.

Figure 1 // How Category 1 and Category 2 are divided



For the purpose of representing Category 2 in our economic impact analysis, we determined the average wage of workers in each occupational category, based on data provided to us by CED via the JobsEQ® platform. We then multiplied the number Category 2 workers in each occupation code by the corresponding average wage in order to determine total wages for Category 2, as shown in Table 5.

Table 5 // Wages for Category 2 cybersecurity workers

SOC	Description	Cat 2 Workers	Average Wage	Total Wages
11-3021	Computer and Information Systems Managers	1,704	\$106,400	\$181,279,000
15-1111	Computer and Information Research Scientists	19	\$93,100	\$1,776,534
15-1121	Computer Systems Analysts	1,176	\$74,900	\$88,106,068
15-1122	Information Security Analysts	890	\$73,200	\$65,161,176
15-1131	Computer Programmers	282	\$69,400	\$19,590,371
15-1132	Software Developers, Applications	654	\$73,100	\$47,776,844
15-1133	Software Developers, Systems Software	331	\$84,800	\$28,098,480
15-1141	Database Administrators	124	\$71,900	\$8,928,111
15-1142	Network and Computer Systems Administrators	2,438	\$63,400	\$154,580,105
15-1143	Computer Network Architects	8667	\$77,300	\$67,052,494
15-1152	Computer Network Support Specialists	195	\$55,400	\$10,779,732
17-2061	Computer Hardware Engineers	56	\$97,700	\$5,482,729
25-1021	Computer Science Teachers, Postsecondary	88	\$82,100	\$7,241,220
Category 2 workers		8,825	Wages	\$685,852,863

Assessing economic impact

To assess the economic impact of the cybersecurity industry, we applied an input-output model using IMPLAN software, a tool designed by economists specifically for conducting such assessments. IMPLAN’s economic model accounts for all the unique characteristics and interdependencies of a geographic region’s economic profile, using industry and labor data.^{vi} Analysts run relevant industry and workforce figures (inputs) against the model, which then generates different types of figures to measure economic impact (outputs). In this case, the region is the entire state of Kentucky, and the inputs are the employment figures for Category 1 and the wage figures for Category 2.

Creating inputs for Category 1

IMPLAN’s model is organized around industries. In lieu of NAICS codes, IMPLAN uses its own industry code structure. IMPLAN provides a helpful mapping tool, which we used to assign the 54 cybersecurity companies in Category 1 to six different IMPLAN codes, as shown in Table 6.

Table 6 // IMPLAN mapping for cybersecurity companies

NAICS	Description	Companies	Employees	IMPLAN
5182	Data Processing, Hosting, and Related Services	10	29	430
5411	Legal Services	1	14	447
5415	Computer Systems Design and Related Services	1	2	451
5415	Computer Systems Design and Related Services	36	572	452
5416	Management, Scientific, and Technical Consulting	5	71	454
6114	Business Schools & Computer & Mgmt Training	1	3	474
Totals		54	691	

These six groups of employees represent the change the cybersecurity industry brings to the economy, so we entered each group into the model as a discrete industry change “activity.” Because we can assume that Kentucky cybersecurity companies are acquiring some goods and services from outside of the Commonwealth, we allowed the IMPLAN model to estimate – using a feature called the Social Accounting Matrix (SAM) – what percentage of the Category 1 inputs to apply to the outputs in Kentucky.^{vii}

Creating inputs for Category 2

Category 2 does not represent an industry change activity, because the workers it represents are not contributing cybersecurity goods and services to the economy. They are, however, receiving compensation for their cybersecurity skills and spending that money in the economy. In other words, without Category 2 workers, Kentucky’s economy would lack the compensation these workers are receiving. So, to represent Category 2 input, we created what is called a “labor income change” activity for the IMPLAN model.

But first, we had to convert the wage data shown in Table 4 to total employee compensation so that we can include benefits in our input. IMPLAN provides a conversion chart that is organized around industries, but because our Category 2 workers are not organized by industry, we averaged the conversion across all industries to achieve a multiplier of 1.239873289. We then multiplied our Category 2 wage data (\$685,852,863) by that figure to achieve a total employee compensation amount of

\$850,370,645.³² This was served as our labor income change input for the economic model. Note that we set Local Purchase Percentage to 100%, on the assumption that Kentucky workers were spending their income within Kentucky.

Outputs of our analysis

Our analysis estimates the total economic impact of the cybersecurity industry in Kentucky to be \$730,277,977.^{viii} Table 7 provides a breakdown of that figure.

Table 7 // Economic impact of the cybersecurity industry

Impact Type	Employment	Labor Income	Value Added	Output
Direct Effect	376	\$27,238,341	\$24,133,260	\$45,016,604
Indirect Effect	152	\$6,623,053	\$9,533,567	\$17,100,451
Induced Effect	5,145	\$210,298,508	\$370,631,630	\$668,160,922
Total Effect	5,673	\$244,159,902	\$404,298,457	\$730,277,977

The model organizes economic impact into three categories: direct, indirect, and induced effects. *Direct effect* represents the economic activity of the cybersecurity industry itself; i.e., the expenditures made by cybersecurity companies. *Indirect effect* represents the economic activity of industries that supply the cybersecurity industry; e.g., when a cybersecurity company needs to buy a telephone system, indirect effects would include the expenditures made by the telephone manufacturer. Finally, *induced effect* represents the economic activity added to the region by workers spending their income – on groceries, restaurants, property, and so on.

Each of these effects is represented in four categories: employment, labor income, value added, and output. *Employment* includes full and part-time annual wage and salary workers, as well as self-employed and sole proprietors. It does not refer to people or full-time equivalent hires; it refers to jobs, and an individual can hold multiple jobs. *Labor income* does not refer to take-home pay; it includes all employee compensation (wages and benefits) plus sole proprietor income. *Value added* includes labor income plus property income and indirect business taxes. *Output* is the sum of value added plus the cost of what are called intermediate expenditures (goods and services needed to make the product). Output represents the total value of the industry’s economic impact.

We observe that the cybersecurity sector creates about 376 jobs within the industry; another 152 in adjacent industries; and another 5,145 jobs as a result of increased household spending. The industry also adds nearly a quarter of a billion dollars to the total employment income of Kentucky’s workers, and just over \$400 million when we factor in property income and indirect business taxes.

However, as a percentage of Kentucky’s economy, the cybersecurity industry is still a very small factor. When compared to total employment and Kentucky’s Gross Regional Product in 2015, the cybersecurity industry represents less than 0.4% of both economic measures (see Table 8).

Table 8 // Cybersecurity industry as a percentage of Kentucky's economy

Impact Type	Employment Impact	Output Impact
Cybersecurity industry	5,673	\$730,277,977
Kentucky economy (2015)	2,448,150	\$200,016,826,375
% of total	0.23%	0.37%

As Figure 2 shows, induced effect represents (by far) the greatest economic impact of the cybersecurity industry in Kentucky. Approximately 92% of the industry's economic effects result from workers spending their income in the economy. The effects of this imbalance become more apparent when we look at the economic impact of the cybersecurity sector on specific industries. Table 9 shows the top ten industries that are affected by the cybersecurity sector. The industry representing the greatest impact isn't actually an industry at all – IMPLAN's 441 code (owner-occupied buildings) represents home ownership. Likewise, the third most affected industry is real estate. Increased property purchases are a natural outgrowth of the rise in household income that the cybersecurity industry introduces into Kentucky's economy. Hospitals, as well, benefit substantially. The first cybersecurity-related industry to make the list – computer systems design services – comes in at number 4.

Figure 2 // Proportional view of direct, indirect, and induced effects of the cybersecurity industry

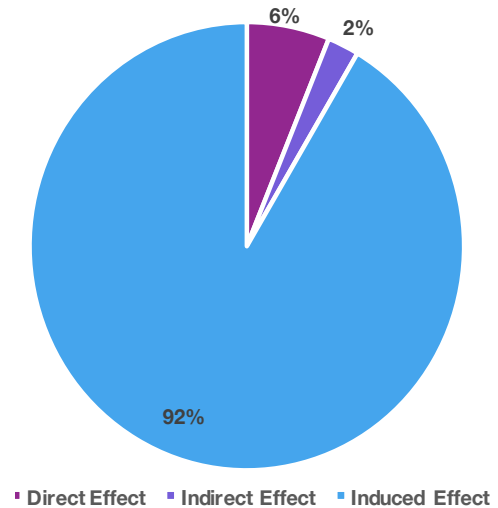


Table 9 // Top ten industries affected by the cybersecurity sector

Code	Industry	Direct	Indirect	Induced	Total
441	Owner-occupied dwellings	\$0	\$0	\$89,854,688	\$89,854,688
482	Hospitals	\$0	\$0	\$45,183,249	\$45,183,249
440	Real estate	\$0	\$1,305,649	\$37,780,321	\$39,085,971
452	Computer systems design services	\$34,036,287	\$222,242	\$766,261	\$35,024,790
395	Wholesale trade	\$0	\$331,725	\$27,175,527	\$27,507,253
475	Offices of physicians	\$0	\$0	\$24,406,689	\$24,406,689
502	Limited-service restaurants	\$0	\$519,555	\$22,976,506	\$23,496,060
437	Insurance carriers	\$0	\$284,746	\$19,181,536	\$19,466,283
433	Monetary authorities and depository credit intermediation	\$0	\$754,103	\$15,203,250	\$15,957,353
501	Full-service restaurants	\$0	\$521,862	\$12,683,271	\$13,205,132

Based on our inputs into the model, these findings are expected. By our estimates, the vast majority of workers in Kentucky’s cybersecurity industry are employed by companies that don’t sell cybersecurity goods and services. While induced effects are an important economic outcome, Kentucky’s cybersecurity sector would have a greater economic impact if more cybersecurity companies – and therefore more cybersecurity goods and services – were located in Kentucky. Cybersecurity companies (Category 1) have induced effects on the economy, but they also have direct and indirect effects. If Kentucky is going to realize the economic benefits of a vibrant and productive cybersecurity sector, it must attract more cybersecurity companies.

Impacts on tax revenue

The IMPLAN model also estimates the impacts the cybersecurity sector has on tax revenue at the federal, state, and local levels. Kentucky’s cybersecurity sector generates \$55,964,959 in federal taxes, and \$37,959,812 in state and local taxes.

Table 10 // The cybersecurity sector’s impacts on federal, state, and local tax revenue

Tax Category	Employee Compensation	Proprietor Income	Tax on Production & Imports	Households	Corporations	Totals
Federal	\$25,614,319	\$1,331,812	\$5,214,958	\$13,866,267	\$9,937,603	\$55,964,959
State & local	\$472,012	\$0	\$28,834,139	\$6,731,459	\$1,922,202	\$37,959,812
State	\$468,281	\$0	\$19,071,593	\$5,203,952	\$1,602,842	\$26,346,668
County	\$0	\$0	\$1,087,577	\$287,410	\$24,154	\$1,399,141
Sub-County General	\$3,731	\$0	\$2,216,777	\$978,534	\$284,950	\$3,483,992
Sub-County Special	\$0	\$0	\$6,458,191	\$261,563	\$10,255	\$6,730,009

Table 10 shows a complete breakdown of the taxes yielded by the cybersecurity industry. The *Federal*, *State*, and *County* rows represent all revenue collected at the federal, state, and county levels, respectively. *Sub-County General* refers to municipalities and *Sub-County Special* refers to school districts and other “special” governmental entities. Finally, the *State & local* row adds all four rows beneath it together, representing the total tax revenue collected by state and local government entities.

Employee Compensation and *Proprietor Income* refers to taxes paid by employees (and their employers) and sole proprietors (and unincorporated business owners) to social insurance funds, like retirement plans, workers’ compensation insurance, and temporary disability insurance. *Tax on Production & Imports* refers to sales and other taxes that are not derived from payroll or income. *Households* refers to income taxes, as well as certain fees and personal licenses (like fishing licenses). And *Corporations* refers to corporate taxes.

Characterizing the cybersecurity sector

Now that we understand the cybersecurity sector’s economic impact, let’s analyze its discrete elements to put the sector into context. Here, we analyze the capabilities and distribution of Kentucky’s cybersecurity companies, as well as the research and development institutions, industry associations, and incubators and accelerators that serve as “enabling factors” for the cybersecurity industry. In Chapter 3, we delve into greater detail on Kentucky’s cybersecurity workforce.

Cybersecurity companies

The number of cybersecurity companies in Kentucky – 54 – is relatively low. Although not a state, San Diego County – whose population and Gross Domestic Product are in the same ballpark as Kentucky’s – provides a useful reference point for putting this figure in context. According to an industry study completed in 2016, San Diego County is home to 104 cybersecurity companies – nearly double Kentucky’s count.^{ix}

Our analysis shows that the vast majority of Kentucky’s cybersecurity companies are primarily *managed services* businesses. Managed services businesses provide day-to-day operation of information technology (IT) services to other companies. Nearly all organizations rely on managed services for some IT function (your e-mail service provider is providing you with a managed service), and some organizations outsource all their IT to a managed services business. For comprehensive managed services providers, cybersecurity is usually part of the capability suite – because most organizations want to store their data with a provider that can also protect their data. Managed services companies are common in the IT sector, and they’re a vital part of the economy. They’re also how organizations of all sizes meet their cybersecurity needs, so the presence of several dozen such companies throughout Kentucky is encouraging.

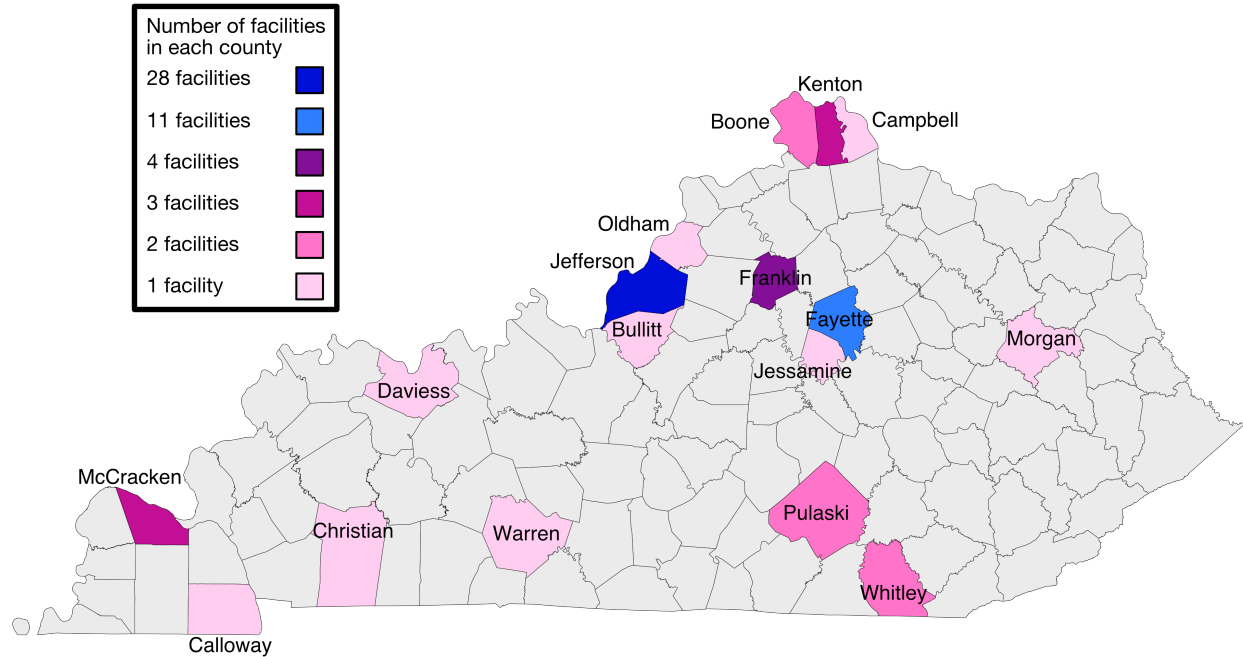
On the other hand, our research reveals that Kentucky has few “pure play” cybersecurity companies. Once we exclude what appear to be independent consultants from our tally in Table 2, we estimate that just five Kentucky companies provide *only* cybersecurity services or products. While a company does not need to be a pure play cybersecurity company to innovate or stand out in the field, they tend to be the ones to break new ground.

This leads us to a broader point – Kentucky lacks a critical mass of companies that are organized to develop niche, specialized, or advanced cybersecurity products or services. There are some notable exceptions, like one company dedicated to securing the industrial control systems of critical infrastructure assets. But it is telling that no company headquartered in Kentucky is featured on the most recent Cybersecurity Ventures list of 500 “hot cybersecurity companies to watch”.^x Conversely, states with strong cybersecurity name recognition – California, Maryland, Colorado, Texas, and New York – feature prominently.

So while Kentucky’s cybersecurity sector has a strong and practical foundation, it lacks the additional layer of disruptive, cutting-edge cybersecurity companies that generate buzz and recognition; attract innovators and investors; and accelerate economic growth. To be recognized nationally for its cybersecurity sector, Kentucky will need to make the attraction of these types of businesses a strategic priority.

To understand the cybersecurity sector another way, we organized its 63 facilities according to the counties in which they operate. Figure 3 shows the results of our analysis.

Figure 3 // Map of Kentucky's cybersecurity companies



The cybersecurity industry broadly mirrors Kentucky's population map and its economic activity. The epicenter of the cybersecurity sector is Jefferson County, home to Louisville and more than half of the Commonwealth's cybersecurity companies. That there is such a high concentration of companies in one area is an asset: vibrant industries like cybersecurity need a geographic focus to create an ecosystem that attracts innovators and investors. Louisville is already in the best position to be that ecosystem for Kentucky.

Beyond Jefferson County, the cybersecurity picture becomes more fragmented. There are smaller pockets of activity in Fayette County (Lexington), Franklin County (Frankfort), and in the northern Kentucky counties closest to Cincinnati. But broadly speaking, there is little cybersecurity industry activity outside of the Bluegrass region in the north central part of the state.

All three of Kentucky's National Centers of Academic Excellence in Cyber Defense (CAE-CD) are located in areas of cybersecurity industry activity: the University of Louisville (Jefferson County), Northern Kentucky University (Campbell County), and the University of the Cumberlands (Whitley County). Except for Fort Campbell, the Commonwealth's major military installations are geographically well-positioned with respect to Kentucky's cybersecurity industry. Fort Knox is near Jefferson County; Bluegrass Army Depot is near Fayette County; and the Boone National Guard Center is between the two in Franklin County.

Research and development institutions

Research and development (R&D) institutions can play a significant role in long-term economic growth. A team of researchers at Pepperdine University studying total factor productivity (TFP) found that “R&D performed within a state has a positive, significant effect on GDP through TFP in the long run,” estimating a “contemporaneous marginal return [on investment] within the state” at 82%.^{xi} In Table 11, we highlight R&D institutions that do or could play a role in accelerating the cybersecurity ecosystem. While none is specifically dedicated to cybersecurity, they provide infrastructure that can be used for cybersecurity research.

Table 11 // R&D Institutions relevant to cybersecurity

Institution	Role and Relevance to Cybersecurity
<p>Center for Applied Informatics Northern Kentucky University Newport</p>	<p>Northern Kentucky University’s Center for Applied Informatics puts the principles of informatics into practice. Informatics, or information science, considers the interaction between humans and information^{xii}; subspecialties include aspects of computer science, information technology, and statistics.^{xiii} The Center for Applied Informatics employs a co-op program that builds students’ skills while designing interfaces between technology users and information, including designing websites, creating mobile platform applications, and analyzing data.^{xiv}</p>
<p>Center for Computational Sciences University of Kentucky Lexington</p>	<p>The University of Kentucky’s Center for Computational Sciences houses the university’s supercomputer, which is used to build students’ skillsets and support various types of interdisciplinary research throughout the university. The center evaluates “big data” systems and software, providing a useful tool to data owners. The supercomputer is also used to perform complex computational calculations relating to pharmaceutical and chemical projects.^{xv}</p>
<p>Center for Research and Development Western Kentucky University Bowling Green</p>	<p>Western Kentucky University’s Center for Research and Development^{xvi} is home to the High-Performance Computing Center, which, like other centers with high-powered computers, supports the university’s research projects and goals and develops students’ cyber-related skills. Bioinformatics, or the development of software and tools to understand biological data^{xvii}, is a particularly focus of the center and could have an impact on cybersecurity protocols and access controls in the future.</p>
<p>Cardinal Research Cluster Supercomputer University of Louisville Louisville</p>	<p>The University of Louisville’s Cardinal Research Cluster Supercomputer, like those discussed above, provides a computing infrastructure that supports the university’s research priorities.^{xviii} Like WKU’s center, the Cardinal Research Cluster Supercomputer enables research into bioinformatics.^{xix}</p>

These R&D institutions should be viewed as assets for stimulating economic growth. Funding should be increased for discrete cybersecurity initiatives – particularly those that study differentiating technologies that can be commercialized. The introduction of commercially viable technologies will spur creation of the new businesses – particularly the types of businesses Kentucky needs to create name recognition and attract investment.

Industry associations, accelerators and incubators, and conferences

These organizations and events are critical to the creation of a strong and sustainable cybersecurity ecosystem. They make a particular geographic area more attractive for entrepreneurs – both professionally (in that there is a structure for generating new business ideas and opportunities) and personally (in that there is a community of like-minded individuals). They also serve as labs of new ideas and mechanisms for establishing a common voice on industry-specific issues. In Tables 12, 13, and 14, we have highlighted several Kentucky associations, accelerators and incubators, and events that are or could be relevant to the cybersecurity sector; the list is by no means exhaustive.

Table 12 // Select technology industry associations in Kentucky

Association	Location	Role and Relevance to Cybersecurity
Louisville CIO Series	Louisville	Louisville CIO Series is a quarterly invitation-only meeting of Louisville IT Executives to discuss IT and security trends and topics. The meetings also serve as networking functions. ^{xx}
Code Louisville	Louisville	Code Louisville offers free classes in software development, helping to grow the cyber workforce in Kentucky. ^{xxi}
Louisville Digital Association (LDA)	Louisville	LDA aims to bring together viewpoints from engineering and development, design and user experience, sales and marketing, and business and leadership to further the tech conversation in Louisville. LDA focuses on organizations from startups to Fortune 500 companies. ^{xxii}
Technology Association of Louisville Kentucky (TALK)	Louisville	TALK aims to uses its growing network of technologists to identify and develop talent, advocate for new technology applications, and educate its membership. ^{xxiii}
Lexington Tech Forum	Lexington	The Lexington Tech Forum covers aspects of IT from security and virtualization to cloud services and disaster recovery. The forum meets monthly to exchange experience and learn about the IT space. ^{xxiv}

Table 13 // Select accelerators and incubators in Kentucky

Organization	Location	Role and Relevance to Cybersecurity
Nucleus iHub	Louisville	Nucleus provides business management and consulting services to entrepreneurs in new and high-tech market sectors. Nucleus aims to facilitate research and incubate start-ups. Its iHub facility is a co-working space for startups. ^{xxv}
Awesome Inc.	Lexington	Awesome Inc. aims to grow startups by hosting community events and educational seminars, and managing a co-working space. ^{xxvi}
Advanced Science & Technology Commercialization Center (ASTeCC)	Lexington	ASTeCC is the business incubator at the University of Kentucky (UK), and it caters to technology-focused startups and businesses. Startups in ASTeCC use licensed UK intellectual property or have some connection to UK faculty or staff. ^{xxvii}
Eastern Kentucky University Biz-Accelerator	Richmond	This university-based incubator provides coaching, resources, and office space to help startups grow and realize their goals. ^{xxviii}
UpTech	Covington	UpTech is an accelerator specifically for startups that focus on tech-enabled data solutions. The accelerator has a standard pipeline and path to get startups spun up and operational. ^{xxix}
WKU Small Business Accelerator	Bowling Green	The WKU Small Business Accelerator provides startups with office space and an information-sharing network consisting of regional entities that can help startups grow. It is collocated with WKU’s Center for Research and Development, linking businesses to R&D initiatives. The accelerator also provides business support services, such as business development consulting and IT support. ^{xxx}

Table 14 // Select technology events in Kentucky

Event	Location	Role and Relevance to Cybersecurity
Louisville Startup Weekend	Louisville	Louisville Startup Weekend brings together designers, programmers, and others to turn innovative new ideas into real-world applications. Participants benefit from the Louisville entrepreneur community and their experience and guidance. ^{xxxix}
DerbyCon	Louisville	Founded in 2010, DerbyCon is a conference that focuses on the computer security industry. The conference includes presentations on topics such as software security and cybersecurity, security product vendors, and training. ^{xxxix}
Techfest Lou and Cybersecurity Summit	Louisville	Hosted by TALK, TechFest Lou is a biannual gathering of technology professionals for networking and education. Attendees include coders, CIOs, and IT managers, and presentations include IT, advanced manufacturing, and cybersecurity. ^{xxxix} TALK is also hosting a one-day Cybersecurity Summit in June 2017.
NKU Cybersecurity Symposium	Covington	NKU's Cybersecurity Symposium covers multiple aspects of cybersecurity, including information security governance and compliance, emerging topics, and legal and privacy issues in security. ^{xxxix}

As reflected in Tables 12, 13, and 14, Louisville is the center of gravity for the technology community in Kentucky. When considering where to focus energies on cultivating a vibrant cybersecurity ecosystem, the Commonwealth already has the ingredients for that ecosystem in Louisville. That ecosystem developed organically, but it can be accelerated by state government attention.

Recommendations

Kentucky's cybersecurity sector is small both in absolute terms and relative to Kentucky's economy. This is consistent with analysis of Kentucky's broader technology industry. CompTIA's most recent Cyberstates report notes that the technology sector accounted for only 3.4% of Kentucky's Gross State Product in 2016 – that's 43rd in the nation.^{xxxv} The same report finds that Kentucky ranks 34th for the number of new technology establishments; 36th for technology patents granted; and 46th for innovation per capita.^{xxxvi}

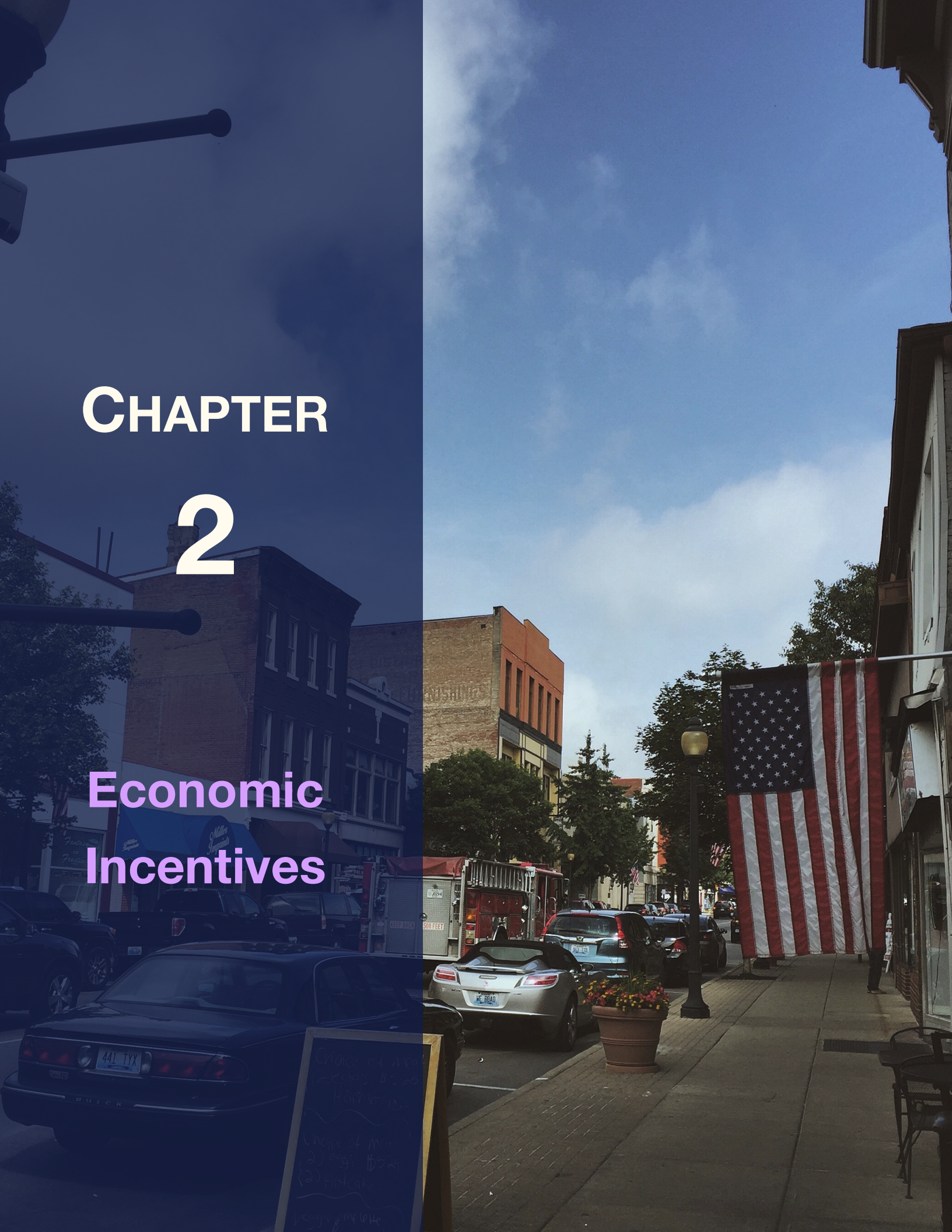
The cybersecurity sector represents an opportunity for Kentucky to move higher on these lists and to increase the economic benefits of this high-wage knowledge sector. When considering the following recommendations, keep in mind the two primary categories of people the Commonwealth will need to catalyze growth in this sector: investors and innovators.

- **Establish targeted economic incentives.** Kentucky needs to create and attract cybersecurity companies – particularly the cutting-edge businesses that will create “buzz” for the Commonwealth. An economic incentive program designed to specifically attract a small but critical mass of such companies will provide the momentum needed to attract others to the state. Additional focus should be given to entrepreneurs who are looking for a place to launch their business.
- **Establish a cybersecurity hub.** Investors and innovators need a dot on the map. They are drawn to thriving hubs of activity that are already attracting other investors and innovators. Louisville has organically become the center of Kentucky's information technology industry. With a strong foundation of technology associations, conferences, and academic institutions, Louisville is well-positioned to be the focus of attention. State and local leaders should work collaboratively on initiatives to bolster cybersecurity on the city's economic agenda.
- **Invest in R&D.** With excellent R&D infrastructure at universities throughout the Commonwealth, state government leaders should encourage investments in discrete cybersecurity initiatives. Specific attention should be given to commercializing technologies so that the results of R&D efforts can be brought to market by Kentucky companies.
- **Develop and promote a cybersecurity brand for Kentucky.** Kentucky will need to brand its cybersecurity niche and promote it in order to appeal to the workers and companies that will build the cybersecurity economy. Focus on Kentucky's assets – both in terms of industry and in terms of lifestyle – and contextualize them for your key audiences: innovators and investors. We recommend a comprehensive communications effort that includes strategic planning, stakeholder engagement, and marketing.

CHAPTER

2

Economic
Incentives



Chapter 2 | Economic Incentives

This section discusses the economics of cybersecurity, then addresses two sides of the economics coin. First, it addresses how individual organizations – especially those in the private sector – can be incentivized to improve their cybersecurity posture. Second, it discusses how the Commonwealth can create economic incentives for the creation of a vibrant cybersecurity economy.

The economics of cybersecurity

Cybercrime is costly. But just how costly has been a point of contention among researchers for several years. Multiple efforts have attempted to characterize the global economic impact of data theft and other malicious cyber activity, often resulting in astronomical figures. Juniper Research estimated that the cost of cybercrime would exceed \$2 trillion worldwide by 2019. That would mean that more than 2% of the world's economic activity is being siphoned off to criminals via cyber means alone.^{xxxvii} A report published by the Center for Strategic and International Studies (CSIS) and McAfee put the annual figure in the more conservative range of \$375B to \$575B^{xxxviii}. Even on the low end of this spectrum, the global cost of cybercrime would be approximately equivalent to the total economic output of Thailand in 2014, the year the report was published.

These top-line numbers help us understand and contextualize the scale of the problem – and why cybersecurity must garner the urgent attention of economic policymakers. If 2% of the water in your bathtub were leaking onto the floor, you'd want to fix the leak. But we have to dig beneath the surface to understand the economic risks to businesses and individuals, who are the ones who directly incur the costs of a cybercrime. At this level, cybercrime's impact is less uniform than the collective numbers imply; aside from the indirect effect of the macroeconomic impacts, many people will feel no hit to their pocketbooks unless they themselves (or a business they use) are victims of a cybercrime. But when they are, the costs can be punishing.

A 2017 study published by Hiscox, a British insurer, surveyed more than 1,000 businesses in the United States on a range of cybersecurity-related issues. The report determined that the average cybersecurity incident affecting U.S. businesses with 1,000 or more employees cost just over \$100,000. That's a significant figure, but most large businesses are sufficiently well-capitalized to weather that type of cost.

The story is not the same further down the food chain. The Hiscox study assessed that U.S. businesses with 99 or fewer employees suffered losses of nearly \$36,000 per cybersecurity incident. That figure is an estimate based on survey responses, and it includes soft costs like loss of productive time and hard costs like payment for incident response services. Nevertheless, a sudden \$36,000 cost can put a small company out of business overnight.

More than 90% of Kentucky's businesses employ fewer than 100 people, and those companies are responsible for employing about a third of Kentucky's entire workforce^{xxxix}. They are the engine of Kentucky's economic growth – and they are especially vulnerable to cybersecurity risk. Nearly two thirds of smaller U.S. companies surveyed in the Hiscox study reported having at least one cybersecurity incident in the previous 12 months. Cybercrime not only imposes a massive macroeconomic cost, but it presents stark microeconomic risks – especially for small businesses.

Investing in cybersecurity capabilities has been shown to reduce costs in the case of a breach. For example, IBM estimates that using an incident response team can save a company approximately *\$16 per lost record* if their data has been stolen^{xl}. So, why are companies still so reluctant to make that type of

investment? For one, many business leaders simply don't know what they need to do – or even what resources are available to them. But more fundamentally, many executives still view cybersecurity as a cost that doesn't yield an obvious return. Like an investment in physical security, an investment in cybersecurity doesn't seem necessary – until, of course, a breach has already occurred.

Incentives for organizations to improve their cybersecurity

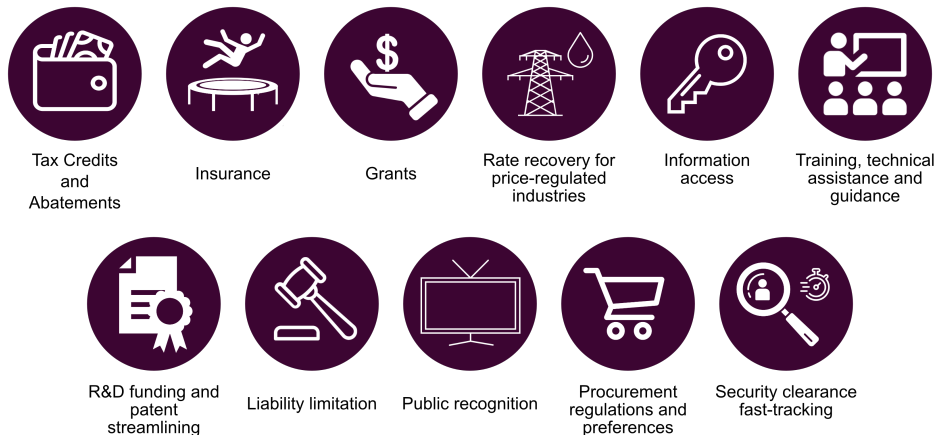
Why consider economic incentives?

Government leaders are left with a dilemma: how to address a matter of public interest (cybercrime's drag on the economy) when the responsibility for cybersecurity lies predominantly with the private sector. Broadly speaking, policymakers have two categories of options to address this challenge: they can compel companies through regulation, or they can encourage companies through incentive programs. The tension between regulations and incentives is not a new one – it colors many other public policy issues. But in the context of cybersecurity, it is infinitely more complex.

The debate becomes more important in the context of critical infrastructure. Because so much of the nation's critical infrastructure is operated by private companies, an investment in cybersecurity isn't optional. Government agencies have worked to craft policies and laws that will compel companies to conform to minimum cybersecurity standards – especially if they operate in certain sectors like defense. But industry has been resistant to new regulations, and – regardless – regulations will not suffice. Businesses must be positively incentivized to pursue robust cyber hygiene.

Recognizing this challenge, President Obama issued *Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity* along with *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience* in 2013. Among other outcomes, these actions tasked the National Institute for Standards and Technology (NIST) to create a “recipe book” for managing cyber risk. Through a participatory public process that directly involved the private sector, NIST developed a cybersecurity framework (CSF) that reflects the realities and concerns of business leaders. It should be considered a useful guide for any type of company seeking to manage cyber risk – whether or not they own or operate critical infrastructure.

But a challenge remained: how to impel companies to use the NIST CSF. So, the White House tasked the Treasury Department to review ways to incentivize its adoption. Separately, the White House, the Department of Homeland Security, and the Department of Commerce have all studied ways to incentivize improved cybersecurity more generally. This subsection consolidates the findings of these reviews, and it includes our analysis of each specific incentive category, represented here:





Tax credits and abatements^{xli}	
Definition	This category of incentives refers to policies that exempt, exclude, or otherwise limit an organization or individual from certain tax liabilities during a period in which the participant engages in certain eligible activities or meets certain requirements.
Examples	The tax code has long been used by the government to advance public policy objectives. For example, the Renewable Electricity Production Tax Credit (PTC) provides a federal tax credit to energy producers based on the amount of renewable electricity they generate ^{xlii} . Likewise, Kentucky offers 24 types of business tax credits and 8 types of individual tax credits, incentivizing a range of outcomes from increased education enrollment to investment in scientific research. However, neither the federal government nor any state government (by our assessment) has used tax credits to incentivize improved cybersecurity.
Pros	While every business leader has different needs and concerns, the one aspect common to every executive’s decision process is the bottom line. That’s why tax credits are so appealing: they are the most direct way of providing companies with a financial benefit in exchange for improving their cybersecurity posture. And unlike other types of tax credits that are targeted towards certain types of businesses (like energy producers, in the example above), cybersecurity tax credits could be structured to help any type of business. Kentucky could lower tax rates for companies that meet certain cybersecurity standards, demonstrate they have adopted the NIST Cybersecurity Framework, or spend a certain percentage of revenue on cybersecurity services or products. Kentucky could also allow accelerated depreciation for investments in cybersecurity hardware ^{xliii} .
Cons	Tax credits are expensive – especially when policymakers are attempting to incentivize behavior across the entire business community. Even a small tax credit for companies that adopt improved cybersecurity would cut the state’s revenues significantly, possibly impacting the delivery of public services in an already-constrained budget environment. Additionally, the state must be able to tier cybersecurity incentives appropriately; it may be difficult to design a program that is as relevant to a large energy critical infrastructure operator as it is to a small medical clinic. These are among the reasons that led DHS, the Department of Commerce, and the Treasury Department to recommend against tax credits as a method for incentivizing adoption of the NIST Cybersecurity Framework.



Insurance^{xliv}	
Definition	Cybersecurity insurance, or “cyberinsurance,” is effectively a risk management strategy. It refers to the transfer of financial risk tied to network and computer incidents (cyber-attacks) to a third party (the insurance agency) in exchange for the payment of a premium. These policies usually cover conditions not included in more “traditional” insurance policies, such as liability arising from loss or theft of electronic data, as well as regulatory fines.
Examples	Although cybersecurity insurance is a relatively new discipline, there are many providers in the market today. American International Group (AIG) has a “CyberEdge” insurance solution that protects policy holders from the following: third-party loss resulting from a security or data breach; direct first-party costs of responding to a breach; lost income and operating expense resulting from a security breach; threats to disclose data or attack a system to extort money; and online defamation and copyright and trademark infringement. It also works with the client to devise personalized strategies for mitigating a variety of cyber incidents.
Pros	Insurance is a free-market construct for managing cyber risks – just as it is for managing health risks, auto risks, and flood risks. In a cybersecurity context, any company could take out an insurance policy based on its cybersecurity profile, and it would pay a premium based on its risk level. The company would then be protected from sudden economic liabilities in the case of a cybersecurity incident. Both the insurer and the policyholder are incentivized to lower cyber risk; the insurer is incentivized because it would be less likely to cover losses during a breach, and the policyholder can be incentivized to lower risk by paying a lower premium. Over time, insurers’ cyber risk models will become more sophisticated, allowing them to better price the risks associated with data losses and ultimately offer the market a comprehensive set of tailored insurance products. At some point, insurance providers could even serve as a source of threat intelligence for homeland security agencies and as a reference point for economic policymakers in state government.
Cons	Although it is rapidly becoming more sophisticated, the cybersecurity insurance market is still immature. This market immaturity creates an information asymmetry between the insurer and the policyholder; the policyholder may have a better understanding of its cybersecurity posture than the insurer will. As such, the insurance rates may not accurately reflect the level of cybersecurity risk a company has. Another disadvantage to cybersecurity insurance is that it can lull companies into a false sense of security, as it offers a financial safety net without the need to invest properly to address cybersecurity requirements. Though the company may be covered financially, cyber insurance cannot adequately remedy reputational damage, lost data, or stolen IP – for small businesses, in particular, these risks may still result in business closure. Cybersecurity insurance should not be considered a substitute for a holistic security program.



Grants^{xiv}

Definition	Public grant programs could be used to give private businesses the resources they need to improve their cybersecurity posture, provided those organizations meet certain eligibility criteria.
Examples	Newly introduced legislation in the U.S. House of Representatives and the U.S. Senate (called the State Cyber Resiliency Act) would create a cyber grant program for the states. It would first establish funding for resiliency planning, and then establish funding for the acquisition of technology, services and implementation of cybersecurity best practices.
Pros	Among other benefits, grant programs could encourage Framework adoption. A grant program could be designed to give critical infrastructure owners and operators the resources they need to implement the NIST CSF, although rigorous criteria would need to be established to ensure that such a direct application of funds is being applied only in the highest-priority cases.
Cons	Grants that provide funding directly to individual companies can be costly, and they would therefore need to be applied in a limited fashion with strict criteria. Grants would also need to be “pushed” to eligible organizations to make sure the government reaches fulfills the most urgent needs.



Rate recovery for price-regulated industries^{xlvi}

Definition	This incentive would allow regulated utilities to recover the cost of their cybersecurity investments (e.g., in adopting and implementing the NIST CSF). The government would set a price cap, allowing the utility to charge a fee (up to a ceiling amount) that is independent of the real cost of the service.
Examples	At the federal level, an incentive could be applied to prices of transportation services provided by interstate natural gas pipeline companies using Federal Energy Regulatory Commission (FERC) authorities.
Pros	Existing legal authorities may be sufficient to enable rate recovery. Also, most price-controlled industries are regulated at the state and local levels.
Cons	Rate recovery passes the cost of public utilities' investment in cybersecurity directly on to the consumer. We recognize that citizens ultimately pay for such an investment one way or another and that rate recovery may result in only a fractional increase in individual utility bills. But the conversation over dinner tables may not play out that way, as families already struggling to make ends meet may not be open to the idea of paying more money for cybersecurity protections that they already expect from their utilities.



Information access^{xlvii}	
Definition	This incentive refers to sharing cybersecurity information with companies in exchange for them meeting baseline cybersecurity standards (or adopting the NIST CSF). The information – which may include attack signatures, vulnerabilities, or general threat observations – may be “owned” by government organizations or other private companies.
Examples	Information Sharing and Analysis Centers (ISACs), most of which are organized by private companies within individual sectors (like aviation or financial services) offer excellent examples of coherent information sharing. Fusion Centers, which are run by State and local governments to enable the sharing of information within government but also with the private sector, are prominent examples of public-private cybersecurity information sharing.
Pros	Because information critical to helping Company A prevent or manage a cyber attack is often owned by Agency B and Organization C, seamless information sharing is vital to enabling informed and prepared decision-making in the private sector. When Company A’s CEO knows she can receive that information in a structured, efficient, and predictable way, she will be much more likely to adopt the security protocols necessary to have access to that information. Moreover, once she has that information, she can prevent an attack (and all its attendant costs and consequences), better manage an attack in progress, or better recover from an attack that has occurred. With a structured information sharing framework in place, she will then be able to share her company’s lessons learned (and technical information) with government agencies and other companies, improving the health of the overall ecosystem.
Cons	<p>As described in the “Pros” section, information sharing sounds ideal – but it is very difficult to create a system that works that seamlessly. Cybersecurity information comes in many different flavors – different sensitivity levels, distribution restrictions, and owners. Accordingly, organizations have legitimate regulatory and reputational concerns about sharing sensitive information – and the protection of that information once it leaves their control. Organizations are also concerned about liability – what happens if they share information that implies their own negligence in preventing a cyber attack? Organizations want to know who is liable and responsible for information they share, how it will be used, and how it will be protected.</p> <p>Because most are focused on individual industrial sectors (and because they often don’t have government members), ISACs have managed to address these problems and the associated trust issues that fuel a reluctance to share sensitive information. They are an essential component of the information sharing landscape, but companies are typically not required to participate in an ISAC – and ISACs don’t always share information with each other.</p>



Training, technical assistance, and guidance^{xlviii}

Definition	This incentive refers to services provided directly by the government to assist businesses (and critical infrastructure owners and operators) to adequately configure their computer networks, address system vulnerabilities, or handle other potential threats.
Examples	The federal government already provides technical assistance, training, and guidance to critical infrastructure operators in many forms, mostly related to emergency response. For example, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works with law enforcement agencies and the intelligence community to coordinate efforts between all levels of government during a cybersecurity emergency. DHS also provides cyber risk planning services through its Cyber Security Advisor program. At the state level, the government could set up a program to provide these services directly to critical infrastructure operators in exchange for adoption of the NIST CSF.
Pros	This was one of the only incentives to gain recommendation from all reviewing organizations (Treasury, Commerce, and DHS). Treasury has said in their review of the incentive, “critical infrastructure organizations’ access to prioritized and enhanced levels of assistance, both regularly and during incidents, could improve computer network security and reduce the likelihood of a successful cyber incident.” One advantage to this incentive is that the assistance given could be specially tailored for each critical infrastructure organization’s circumstances. Secondly, assistance could be provided quickly, giving the receiving organization an immediate and flexible response and quicker adaptation to cybersecurity threats.
Cons	Building a technical assistance program is very expensive, even if the assistance were restricted to critical infrastructure organizations. The Treasury notes this is because the government “bears all of the costs and may not have sufficient personnel or other resources in place to provide one-on-one consultation on a widespread basis.” As with cyberinsurance, there is a possibility that the critical infrastructure organization becomes complacent, effectively transferring cyber risk to the third party (in this case, the government technical assistance body) altogether, limiting its ability to develop its own capacity.



R&D funding, patent streamlining ^{xlix}	
Definition	These incentives refer to increased or dedicated funding for research and development (R&D) of cybersecurity measures, and to streamlining the examination and costs of cybersecurity patent applications. These incentives would create a “fast lane” for protecting inventions and processes that would strengthen our nation’s cybersecurity.
Examples	Presently, the federal government provides direct support for basic R&D relating to cybersecurity, with research grants and other support administered by several agencies, including the National Science Foundation, DHS’s Science and Technology Directorate and its Homeland Security Advanced Research Projects Agency, and the Intelligence Advanced Research Projects Activity.
Pros	If grants are used to fund R&D initiatives, the return on taxpayer investment could be high – especially if they are focused on technologies that make cybersecurity more affordable and accessible to small businesses. R&D also enables the generation of intellectual capital and property, which has secondary and tertiary economic benefits.
Cons	Investments in R&D are not guaranteed to yield results – so while the reward may be high, the risk may be, as well. Also, R&D initiatives may not bear fruit for a long time. (Fortunately, many of the urgent cybersecurity problems relate more to people and process than to the technology challenges that R&D would primarily address.)



Liability limitation¹	
Definition	This incentive refers to liability protections afforded to an organization in the case that it is the victim of a cyber attack. The government would afford those protections if the organization meets a minimum standard of cybersecurity.
Examples	Consider a scenario where Organization A is breached, and the data of its client – Organization B – is stolen. In certain circumstances, Organization B could sue Organization A for damages. This incentive would protect Organization A from certain liabilities if it could demonstrate that it had adopted and faithfully implemented a minimum cybersecurity standard (like those identified in the NIST Cybersecurity Framework). This would also incentivize organizations to participate in information sharing frameworks.
Pros	Companies have serious concerns about being sued for improperly protecting third-party data. Firms will be more likely to adopt the Framework if they know their liability for damages associated with the loss of that data is limited (under certain circumstances). Though it directly encourages adoption of the Framework, it would still leave the implementation decision up to the individual critical infrastructure organizations.
Cons	Liability protections for organizations need to be carefully crafted in order to be effective. If the protections are too broad, companies may (ironically) be discouraged from taking sufficient action to protect third-party data.



Public recognition^{li}	
Definition	This incentive refers to any type of program (whether run by the government or a non-profit organization) that issues a credential, seal, or certification to any company that meets a certain cybersecurity protection threshold (or adopts the NIST Cybersecurity Framework).
Examples	The Ohio Environmental Protection Agency’s Encouraging Environmental Excellence (E3) Program “recognizes an organization’s exceptional achievements in environmental stewardship. Any business, industry, trade association, professional organization or local government of Ohio can be recognized for their commitment to environmental excellence.” While this is not a cybersecurity example, it demonstrates how the government can use its authority to highlight companies that take steps to advance the public interest.
Pros	A “seal of approval” from the government – or even a trusted independent agency – can give consumers the confidence that a particular business maintains a certain cybersecurity standard or operates under the rubric of a particular risk management framework.
Cons	There is concern amongst critics that – if such a program were implemented – companies <i>without</i> such recognition would be more vulnerable to malicious actors. In the same way that burglars might be more inclined to skip over the house with the home security alarm placard on the front lawn, a public recognition program could point malicious actors to the ostensibly easier targets. And although a “seal of approval” program sounds like it might be inexpensive, implementing an effective one could be very costly. Establishing objective and meaningful criteria, vetting highly technical applications, monitoring compliance, and marketing the program are all expensive pursuits.



Procurement regulations and preferences^{lii}

Definition	Government agencies can establish minimum cybersecurity standards as a requirement of (or advantage in) winning public contracts.
Examples	In 2016, the federal Government amended the Federal Acquisition Regulation to require government contractors that process, store, or transmit certain types of information to adopt basic information safeguarding protocols ^{liii} . While this example speaks to a minimum requirement, the government could also award evaluation points to contract bidders that meet higher standards of cybersecurity.
Pros	Procurement preferences help the government better protect its information systems, while at the same time compelling a segment of the private sector to increase its own security standards. Moreover, regulations for government contractors are numerous and regularly updated; implementation of cybersecurity regulations (or preferences) in the procurement system would be relatively seamless and it would not require allocation of any new funds.
Cons	As with other regulations, validating contractor compliance with these regulations could prove difficult and costly. Procurement preferences also affect only those companies that do (or want to do) business with the government. State government procurement regulations or preferences will only affect a small slice of the economy.



Security clearance fast-tracking^{liv}	
Definition	While this is not technically an incentive, the expedited processing of security clearances for appropriate private sector individuals (especially those representing critical infrastructure organizations) should be considered a tool in the government’s toolset.
Examples	An individual employed by an eligible organization would have his application moved forward in the queue, taking what is normally a long process (6 months to a year) down to a more manageable period of weeks or a few months.
Pros	Because certain types of cybersecurity threat information are particularly sensitive, it is helpful to issue security clearances to certain individuals in the private sector. This would facilitate the flow of information between government agencies and – for example – critical infrastructure owners and operators, allowing them to collaborate on preventing or mitigating attacks on key assets. But the security clearance process is cumbersome and lengthy, and many businesses do not have the resources to navigate that process. Shortening and streamlining the clearance process for such firms would strengthen the cybersecurity ecosystem and encourage companies to take appropriate measures to improve their cybersecurity posture. And because the actions needed to streamline the process are mostly administrative in nature, implementation should not be particularly costly.
Cons	From a state government perspective, it is important that certain critical infrastructure owners and operators within the state have active security clearances. But the issuance of clearances is not controlled by state government; all the state government can do is help identify high-priority individuals and then lean on the federal government to expedite their clearance applications.

Incentives for attracting cybersecurity companies

Kentucky already has several programs that incentivize companies to locate in Kentucky. Operating on the assumption that it will be easier for policymakers to work within the existing economic development structure, we reviewed those programs and identified several that could be purposed or repurposed for cybersecurity companies.

Kentucky Business Investment (KBI) program^{lv}

What is it?

The KBI program provides “income tax credits and wage assessments to new and existing agribusinesses, regional and national headquarters, manufacturing companies, and non-retail service or technology-related companies that locate or expand operations in Kentucky.” The tax credit can be taken as up to 100% of the Kentucky income tax imposed on income arising from the project, and the credit is in effect for 10 years. The wage assessment is up to 4% of the gross wages of each employee of the company.

Companies located in certain designated “enhanced counties” may apply for enhanced incentives (longer tax credit duration and an increase in the wage assessment percentage). These enhanced counties are those that the state has determined are struggling and are in a state of economic distress, and thus are in especial need of program assistance.

Eligible projects are those that meet the following minimum requirements: 1) create a minimum of 10 new, full-time jobs for Kentucky residents and maintain an annual average of at least 10 new, full-time jobs for Kentucky residents; 2) incur at least \$100,000 in eligible costs; and 3) meet a minimum level of wages and benefits.

What would Kentucky need to do to repurpose this for cybersecurity companies?

Repurposing this program for cybersecurity companies could be as easy as adding cybersecurity to the list of eligible activities.

If Kentucky had to start a new program from scratch, then it could implement similar eligibility requirements tailored specifically to cybersecurity (designate which activities are eligible and which are not), and offer similar incentives strictly for those companies that offer cybersecurity goods and services. The minimum for eligible costs may need to be lowered, as cybersecurity companies may be able to introduce a new technology or service offering with (relatively) low start-up costs. The project eligibility requirements would also need mending, as the current stipulation of 10 required new full-time jobs in Kentucky may be too high for the cybersecurity industry, where small businesses are an important segment.

A program like this designed for cybersecurity would incentivize companies to expand or relocate to Kentucky, and cyber companies that meet the requirements could take on projects that advance their own capabilities.

Kentucky Economic Development Finance Authority (KEDFA) Direct Loan Program^{lvi}

What is it?

The Direct Loan Program provides eligible companies with loans and mortgages at below-market interest rates. With easier access to such loans, the program supports economic development, business expansion, and job creation to impacted Kentucky businesses and communities.

Projects financed must be in the agribusiness, tourism, industrial ventures, or service sectors. No retail projects are eligible. The amount of KEDFA participation is dependent on the project fixed asset cost, based on the following: 1) KEDFA participation of 50% for project costs up to \$200,000; 2) 40% for project costs of \$200,000 to \$500,000; and 3) 30% for project costs exceeding \$500,000.

The loans are available “for fixed asset financing (land, buildings, and equipment) for business startup, locations, and expansions that create new jobs in Kentucky or have a significant impact on the economic growth of a community,”

The interest rate is fixed and is tied to the term of the loan. Rates are as follows: 1.0% interest rate if the term is 3 years, 2.0% interest rate if the term is 5 years, 3.5% interest rate if the term is 7 years, and a 5.0% interest rate if the term is 10 years. KEDFA funds are not disbursed until the entire project, as outlined in the application, is complete.

What would Kentucky need to do to repurpose this for cybersecurity companies?

Accommodating cybersecurity companies could be as easy as amending the eligible projects to include cybersecurity. If Kentucky were to create a new program from scratch, it would look very similar to the one in place. However, the differences could lie in the project cost, interest rates, and other financing terms – all of which would need to be assessed in relation to the cybersecurity market.

Kentucky Enterprise Fund (KEF)^{lvii}

What is it?

The Kentucky Enterprise Fund offers sources of capital and financing to seed and early-stage Kentucky-based companies that are commercializing a technology product or process. The goal of the fund is to stimulate private investment in Kentucky technology companies that have high growth potential, and that will further develop entrepreneurial technology coming out of Kentucky. The Kentucky Science and Technology Corporation administers the funds. Companies may apply for a grant of \$30,000 or an initial investment of up to \$250,000.

Eligible companies are those that are in their early stages of development and develop a product, process, or service in the following industries: bioscience, environmental and energy technologies, human health and development, information technology and communications, and materials science and advanced manufacturing. These companies must be based in Kentucky (or have at least 50% of its property and payroll in Kentucky).

Currently, about 10% of companies that apply receive funding.

What would we need to do to repurpose this for cybersecurity companies?

Cybersecurity companies are likely to already be eligible for investment from this fund, as they could meet the high-growth technology firm requirement.

If Kentucky were to create a new program from scratch, then having an investment fund designated specifically for developing the cybersecurity sector would make it easier for cybersecurity companies to acquire capital, as they would not be competing with companies in other high-growth industries. Additional, cyber-specific requirements may be needed to properly assess applying firms.

Kentucky Enterprise Initiative Act (KEIA)^{lviii}

What is it?

Companies that are KEIA-approved can receive a refund of the sales & use tax paid for eligible costs associated with a “new or expanded service or technology, manufacturing, or tourism attraction project in Kentucky.” Such costs include purchasing building and construction materials, research and development equipment, and electronic processing equipment (totaling a minimum of \$50,000).

Eligible companies include those that specialize in manufacturing, service, or technology activities, or in operating or developing a tourism attraction in Kentucky. This does not include companies primarily engaged in retail sales. Also, in order to qualify, the eligible company must make a minimum investment of \$500,000 in the economic development project undertaken.

What would we need to do to repurpose this for cybersecurity companies?

In order to repurpose this for cybersecurity companies, the list of eligible equipment should be expanded to include all information technology infrastructure, not just data processing equipment. Kentucky could also create a similar program that refunds the sales and use tax for construction and materials costs for cybersecurity companies moving to (or expanding their operations in) Kentucky. Such eligible costs would include the servers and infrastructure requirements needed to create a secure facility, amongst other construction, materials, and equipment costs. The minimum investment of \$500,000 would need to be lowered substantially, as this would be far too expensive a project for innovative startup companies and other small businesses in the cybersecurity field.

Case Study: Maryland's Cybersecurity Investment Incentive Tax Credit (CIITC)^{lix}

Maryland is the first (and, by our assessment, only) state to have created a program specifically designed to attract cybersecurity companies. Here, we profile the incentive program and discuss its advantages and disadvantages.

Background

Adjacent to the nation's capital and home to the National Security Agency, Defense Information Systems Agency, and thousands of government contractors, the State of Maryland has long been considered a hub for the cybersecurity industry.

To secure and advance this national leadership position, Governor Martin O'Malley signed the Cybersecurity Investment Incentive Tax Credit (CIITC) into effect on May 2, 2013. Maryland views the cybersecurity sector as an economic asset, and the CIITC was launched to accelerate its growth and benefit from an influx of high-wage, high-skill workers. The program is designed to incentivize cybersecurity companies to launch in (or move to) Maryland by making it easier for them to raise capital.

CIITC provides a refundable tax credit equal to 33% of an investment (not to exceed \$250,000) in qualified Maryland cybersecurity companies (QMCCs). Montgomery County – which borders Washington, DC, and considers government contracting to be a strategic industry – provides further incentives for QMCCs located there. As of July 1, 2016, investments in QMCCs located in four of Maryland's lowest-income counties would qualify for a credit equal to 50% of the invested amount (not to exceed \$500,000).

Qualification requirements

A QMCC must be a for-profit enterprise that is headquartered in Maryland and "engaged primarily in the development of innovative and proprietary cybersecurity technology," Cybersecurity technology is defined as "products or goods intended to detect or prevent activity intended to result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system," To qualify, a QMCC must be in good standing with the state, and it cannot employ more than 50 people; be more than 5 years old; be publicly traded; be in default on any state contracts; or be behind on its tax obligations.

A qualified investor (whether a person or an organization) must invest at least \$25,000 in a QMCC. The investor is limited to a 25% stake in the QMCC, and the investor must meet the same basic requirements (in terms of good standing, currency on all tax obligations, and the like) as the QMCC itself.

Each QMCC is limited to the benefit of 15% of the total program appropriation for each fiscal year, and the QMCCs and investors must retain the investment for a minimum of three years. QMCC participation is limited to just two years.

Case Study (continued): Maryland's Cybersecurity Investment Incentive Tax Credit (CIITC)

Program Status

Eight companies have benefited from the incentive program, with two or three companies supported each year since 2014. While data for the entire history of the program is not readily available, a 2015 report provides a window into the program's efficacy. In 2015, two QMCCs received \$620,625 in tax credits, representing 33% of \$1.86M private investment in the state. That investment created eight direct jobs and 11 indirect jobs, resulting in \$61,280 in state revenue. If those figures stay the same year over year, it would take Maryland ten years to recuperate its investment. But the state recognizes that the cybersecurity workforce will yield ancillary benefits (like generation of intellectual property, attraction of educated workers) not captured in an economic impact analysis. Maryland is also betting that cybersecurity companies are likely to grow quickly, meaning that the state should "break even" much sooner. To date, only one of the eight companies has broken out of startup status, but the program is still young.






Another helpful way to look at the program's efficacy is to compare it to a similar program. The CIITC was modeled after Maryland's biotechnology investment incentive tax credit (BIITC), which has been wildly successful. In effect since 2007, the BIITC is constantly flooded with eligible companies, with 30 to 40 participating on an annual basis. Participants include companies that moved to Maryland specifically to take advantage of the credit.

It is unclear why the BIITC has generated so much more interest than the CIITC, but it could be because of an important distinction between the two programs. Under the BIITC program, the *investor* in the qualified company receives the tax credit. But under CIITC, the *qualified company* receives the tax credit. This was designed to ensure the credits were spent in Maryland as opposed to on an out-of-state investor (which was often the case under the BIITC). But cybersecurity companies themselves have indicated that the credit would be better spent on investors; perhaps this is because investors are laser-focused on the bottom line, while cybersecurity company founders are focused on the capability.

Whatever the rationale, lawmakers have responded. Senate Bill 318, which takes effect June 1, 2017, now gives the credit to the investor instead of the qualified company. It also extends the CIITC program through fiscal year 2023, ensuring the program's long-term viability and creating another advantage for Maryland's cybersecurity sector.

Recommendations

Our review of economic incentives has yielded a number of insights that can be considered by Kentucky’s policymakers. Having assessed the advantages and pitfalls of different types of approaches, we can offer a series of recommendations – both for incentivizing Kentucky-based organizations to strengthen their internal cybersecurity posture and for incentivizing a cybersecurity economy in the Commonwealth.

Incentives for organizations to improve their cybersecurity	
	<p>Cyber insurance is the free market’s solution to cyber risk management. The cyber insurance market is rapidly maturing as actuarial models become more sophisticated. The insurance industry in Kentucky is already offering cybersecurity plans, and we expect that providers will continue to enter this market. Kentucky’s government should gently encourage this trend, and it may consider convening a conference of leading cyber insurance experts to discuss the state’s role in the market.</p>
	<p>Grants should be designed to meet focused high-priority needs or to achieve broad-based outcomes. For example, Kentucky could organize a program designed specifically to enhance the cybersecurity posture of critical infrastructure operators within the state. Such a program would fund risk assessments for discrete critical infrastructure assets; the piloting of new cybersecurity technologies for critical infrastructure protection; or the investments required by critical infrastructure operators to mitigate their cyber risk in accordance with the NIST CSF.</p>
	<p>Information access for businesses is a vital component of the cybersecurity ecosystem, and we describe (in Chapter 5) how it should be enabled. But KOHS, which would be the gatekeeper for sharing cybersecurity information with the private sector, could limit information access to companies that have demonstrated a certain degree of cyber hygiene (or to those that have adopted the NIST CSF).</p>
	<p>Training, technical assistance, and guidance can be high-impact investments if applied correctly. There are numerous options for pursuing specific programs under this category, but here’s one example: the state could organize a series of expert-led workshops targeted at helping businesses build a cybersecurity plan that maps to the NIST CSF. The workshops would be short, executive-level instructional sessions that empower companies to make immediate changes in the way they handle cyber risk. Moreover, Kentucky’s government should be seen as an expert resource for businesses to improve their own cybersecurity. That expertise should be approachable, clear, and easy-to-access; the Commonwealth should consider establishing a one-stop shop for cybersecurity resources at a ky.gov domain.</p>
	<p>R&D funding directly advances both security (by developing new game-changing technologies) and economic (by cultivating Kentucky’s intellectual capital) objectives. The Commonwealth is already home to multiple R&D centers that focus on areas adjacent to cybersecurity, including: the Center for Applied Informatics, the Center for Computational Sciences, the Center for Research and Development, the Center for Visualization and Virtual Environments, the HIVE High-Performance Computing Center, and the University of Louisville Cardinal Research Cluster Supercomputer. Although the Commonwealth could create a new R&D center for cybersecurity, some of these centers already offer researchers advanced IT infrastructure for their studies. The more cost-efficient route would be to fund (through public or private financing) a specific cybersecurity program at one of these existing centers.</p>

Incentives for attracting cybersecurity companies

Kentucky has several tools in its toolset for incentivizing growth in its nascent cybersecurity sector. First, any of the existing incentive programs profiled in this chapter could be readily modified to attract and retain cybersecurity companies.

The most appealing is the **Kentucky Enterprise Fund (KEF)**, which is geared towards innovative, high-growth industries like cybersecurity. Because startup costs in the cybersecurity industry *can* be relatively low, and because there is such a high demand for cybersecurity goods and services, it is particularly attractive to entrepreneurs. KEF financing allows entrepreneurs to bring their idea to market; without it, some cybersecurity companies may never take root in Kentucky.

The **Kentucky Business Investment (KBI) Program** is a direct incentive that could be attractive to younger cybersecurity companies, in particular. As discussed in our analysis, the eligibility requirements would need to be amended, and – even though many cybersecurity companies would be eligible based on the type of activity they perform – it would be helpful from a marketing perspective to carve out a specific set of cybersecurity activities to generate interest in the program. Tax incentives could be costly, and a cost-benefit analysis should be performed before initiating any cybersecurity carve-out.

The **Kentucky Economic Development Finance Authority (KEDFA) Direct Loan Program** is of limited relevance to the cybersecurity sector. Because they operate in an information industry, cybersecurity companies tend to have fewer fixed assets than, say, manufacturers or aerospace companies. Particularly for a cybersecurity startup, an office and a server farm may constitute the bulk of its fixed assets. The KEDFA Direct Loan Program could be helpful in attracting more established cybersecurity companies to a new location (e.g., an operations center) in Kentucky, but – even then – the program alone would not offer a compelling reason for a larger company to relocate.

The **Kentucky Enterprise Initiative Act (KEIA)** is perhaps the least relevant to cybersecurity companies. Only cybersecurity companies that sell products would be liable for Kentucky's sales and use tax in the first place. Moreover, only larger, well-capitalized cybersecurity companies would be able to make a \$500,000 investment in a Kentucky location, further limiting its applicability to the cybersecurity sector. If Kentucky wants to attract larger cybersecurity product companies – such as those that might want to invest in an R&D facility, for example – then KEIA would be a useful tool.

Maryland's experience with its **Cybersecurity Investment Incentive Tax Credit (CIITC)** offers both promise and caution. If Kentucky were to develop a similar program, it would be the second state in the nation to carve out a tax incentive specifically for cybersecurity companies. This would be a tremendous opportunity for the state to put itself on the cybersecurity map, and it should be marketed aggressively. But it is important to remember that Maryland is already well known as a cybersecurity hub, and still only eight companies subscribed to the incentive program in its first three years. Maryland's move to an investor-directed credit is likely to increase subscription rates, and we would recommend that Kentucky structure any similar program accordingly. Finally, Maryland's treasury is estimated to have received only 10 cents for every dollar it has invested in this program. Kentucky must carefully consider the financial terms of the incentive program before making a decision to create it.

CHAPTER 3

Workforce



Chapter 3 | Workforce

Understanding the cybersecurity workforce is key to unlocking the benefits of a vibrant cybersecurity economy. This chapter will first address existing efforts – one at the federal level and one in California – to define and categorize cybersecurity workers in general. It will then present our analysis of Kentucky’s current and projected cybersecurity workforce, and it will provide recommendations for the Commonwealth to meet its cybersecurity workforce needs.

Defining the cybersecurity workforce

In Chapter 1, we explained the limitations presented by conventional labor and economic datasets in quantitatively characterizing the cybersecurity workforce. But from a qualitative perspective, government and industry leaders have undertaken a number of efforts to characterize the occupations and skill sets of the cybersecurity workforce. In this section, we’ll explain the federal effort (the NICE Cybersecurity Workforce Framework), as well as California’s comprehensive workforce definition initiative.

The NICE Cybersecurity Workforce Framework

The NICE Cybersecurity Workforce Framework (NCWF, or the “Framework”) was developed by the National Initiative for Cybersecurity Education (NICE), an interagency effort led by the National Institute of Standards and Technology (NIST). The NCWF categorizes and defines cybersecurity work into specialty areas, tasks, and knowledge, skills, and abilities. Revised and updated through a rigorous three-year process with many iterations, the current Framework has been refined to provide cybersecurity stakeholders “with a common language to define cybersecurity work, as well as a common set of tasks and skills required to perform cybersecurity work.”^{ix} This allows businesses to improve recruitment and training; professionals to improve career planning; and educators to refine curriculum development.

The NCWF comprises seven categories that describe major cybersecurity worker functions and specialty areas. The categories group workers together regardless of their occupational titles and terms, and they are composed of specialty areas that further detail the competencies and functions that best describe the jobs included in each particular category. The categories are shown in Table 1.^{lxi}

Table 1 // NCWF workforce categories

Category	Specialty areas responsible for...
Analyze	"...specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence."
Collect and Operate	"...specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence."
Investigate	"...investigation of cyber events and/or crimes of IT systems, networks, and digital evidence."
Operate and Maintain	"...providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security."
Oversight and Development	"...leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work."
Protect and Defend	"...the identification, analysis, and mitigation of threats to internal IT systems or networks."
Securely Provision	"...conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development."

Of these seven functions, laypeople may be quick to recognize the *protect and defend* category as a set of cybersecurity functions, but they may not readily identify other categories as being critical components of the cybersecurity workforce. The Framework makes cybersecurity functions accessible to organizations outside the cybersecurity sector, such as manufacturers who need to build an internal cybersecurity team or college administrators who need to design a new academic program. Moreover, when businesses and academic institutions actively use the Framework’s lexicon, they are speaking the language of prospective cybersecurity employees and students, in turn making them more attractive options for work and education.

California’s workforce development initiative

In 2015, the California Cybersecurity Task Force produced a report on workforce development and training. With its high concentration of technology companies, it is no surprise that California is particularly invested in the continuing development of its cybersecurity workers. Even though the California cybersecurity workforce has experienced double-digit growth in recent years, there remains a gap between demand and supply – particularly when it comes to filling state government cybersecurity positions. To remedy this problem, the report recommended (among other actions) that the state create a new classification system for cybersecurity professionals.^{lxii} Under the new system, there are eight roles that filter the many job titles with the current cyber workforce into functional groups:^{lxiii}

1. Chief Information Security Officer
2. Privacy Officer
3. Information Security Officer or Manager
4. Compliance Officer
5. Cybersecurity Engineer
6. Cybersecurity Professional
7. Cybersecurity Operations & Maintenance Professional

8. Cybersecurity System Administration Professional

Each of the eight roles can be placed into functional categories that further describe the role, as shown in Table 2:^{lxiv}

Table 2 // California cybersecurity workforce development initiative job categories

Category	Functions that encompass...
Manage	“...overseeing a program or technical aspect of a security program at a high-level and ensuring currency with changing risk and threat environments.”
Design	“...scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.”
Implement	“...putting programs, processes, or policies into action with an organization.”
Evaluate	“...assessing the effectiveness of a program, policy, process or security service in achieving its objectives.”

As one of the country’s major technology hubs, California recognized the need for a highly skilled cybersecurity workforce that protects the data of its citizens, securely maintains the technology systems of the state, and protects the state’s information technology infrastructure. California also understood that competition to hire these highly skilled cybersecurity professionals is intense, not only amongst other state and local governments, but also the federal government and private sector (both nationally and internationally). Beyond recruiting, there is a real challenge in retaining highly skilled cybersecurity professionals, in part due to the state government’s inadequate compensation structure.

One way California is combatting this problem is through the definition of career pathways and better organized workforce solutions. The previous IT professional classification in California did not adequately align with the highly specialized skills of cybersecurity professionals. The new cybersecurity classification system should help California incentivize professionals to not only work in the state government, but also to remain there and move up the career ladder in California.

Although it may be the first state to undertake such a massive workforce categorization effort, California’s problem is not unique at all. Kentucky government agencies are struggling with the same recruitment and retention problems for cybersecurity professionals. Clarification of career pathways for state government employees – ideally aligned to the NCWF – and separate pay structures for specialized positions would go a long way to making public sector positions attractive for cybersecurity professionals.

Characterizing Kentucky’s cybersecurity workforce

Cybersecurity workers by occupation

As explained in Chapter 1, the systems used to gather economic and labor data do not yet reflect the realities of today’s cybersecurity workforce, nor are they aligned with purpose-built frameworks like the NCWF. Imperfect though they are, the economic and labor datasets do allow us to conduct meaningful analysis, provided we make certain analytic assumptions about the numbers. The complete discussion of those assumptions is included in Chapter 1, but we repeat here (in Table 3) our assigned apportionment of cybersecurity workers for each Standard Occupational Classification (SOC) code. These allocations form the basis of the calculations we present throughout the rest of this chapter. In Table 3, we also include – after factoring in the assigned percentage – the number of cybersecurity workers in each SOC code employed in Kentucky in 2016.

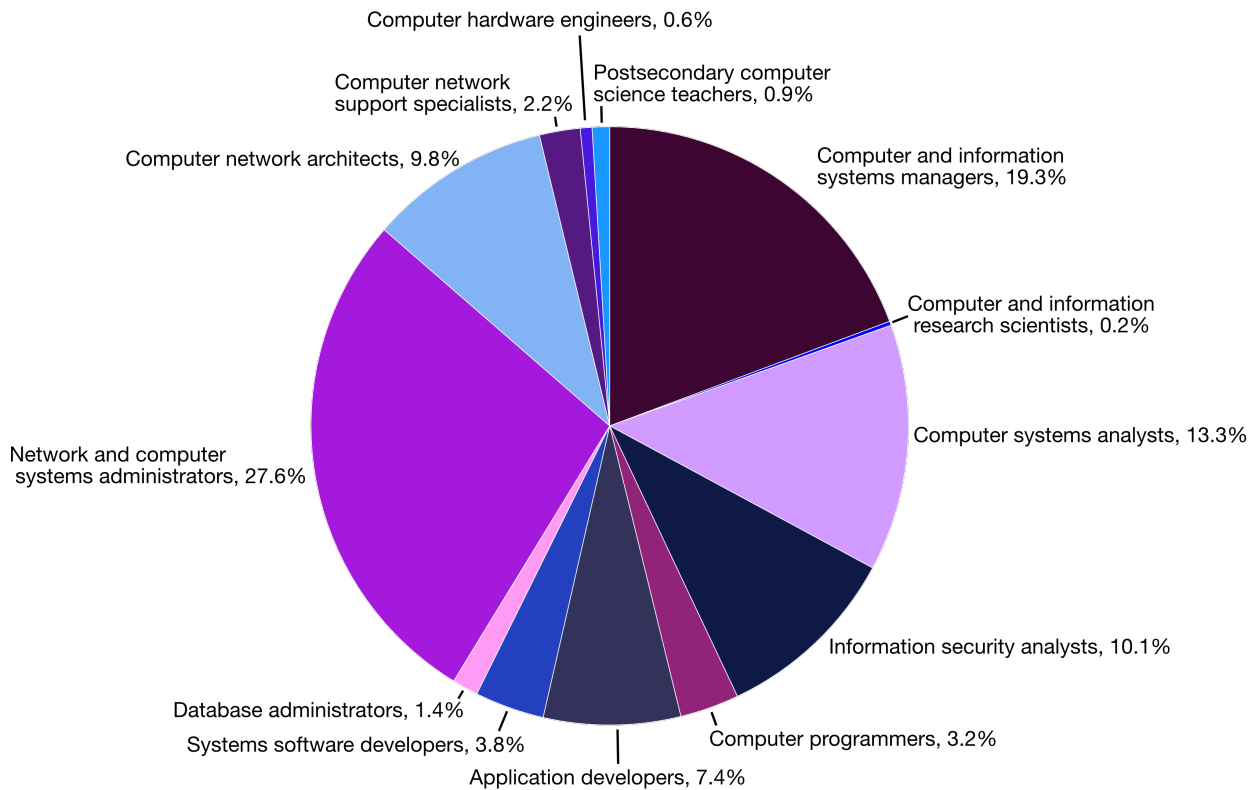
Table 3 // Kentucky cybersecurity workforce in 2016, organized by occupation

SOC	Description	Estimated % of workers in cyber roles	Estimated number of cyber workers
11-3021	Computer and Information Systems Managers	50%	1,813
15-1111	Computer and Information Research Scientists	10%	20
15-1121	Computer Systems Analysts	20%	1,251
15-1122	Information Security Analysts	100%	947
15-1131	Computer Programmers	10%	300
15-1132	Software Developers, Applications	10%	695
15-1133	Software Developers, Systems Software	10%	353
15-1141	Database Administrators	10%	132
15-1142	Network and Computer Systems Administrators	60%	2,594
15-1143	Computer Network Architects	60%	923
15-1152	Computer Network Support Specialists	10%	207
17-2061	Computer Hardware Engineers	10%	60
25-1021	Computer Science Teachers, Postsecondary	20%	88
Total cybersecurity workforce			9,383

Figure 1 displays the cybersecurity workforce’s percentage breakdown by occupation. Just three categories – computer systems administrators, computer and information systems managers, and computer systems analysts – comprise approximately 60% of the total cybersecurity workforce. The only position that is by definition *always* a cybersecurity occupation – information security analysts – constitutes about a tenth of the workforce.

Figure 1 is also helpful in determining who is *not* part of the workforce. In particular, computer and information research scientists and postsecondary computer science teachers are in short supply; they would play an important role in creating “bleeding-edge” cyber activity and in educating the future cybersecurity workforce, respectively.

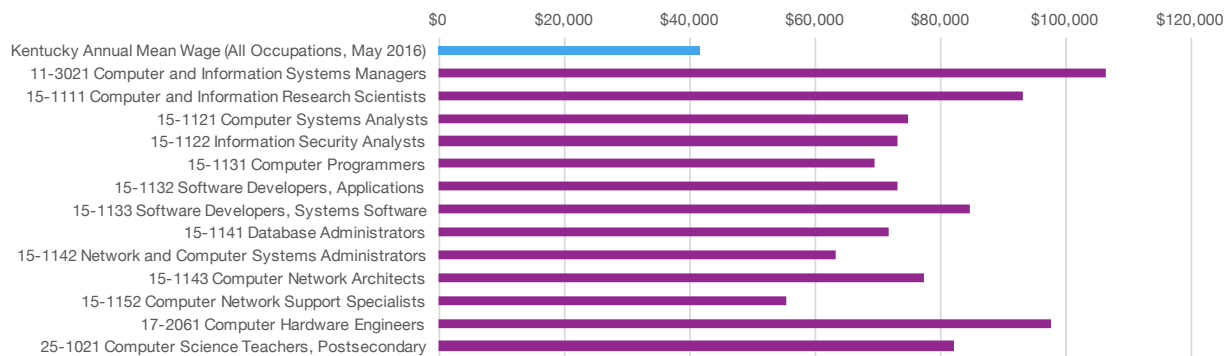
Figure 1 // Cybersecurity workers by occupation



Wages and employment

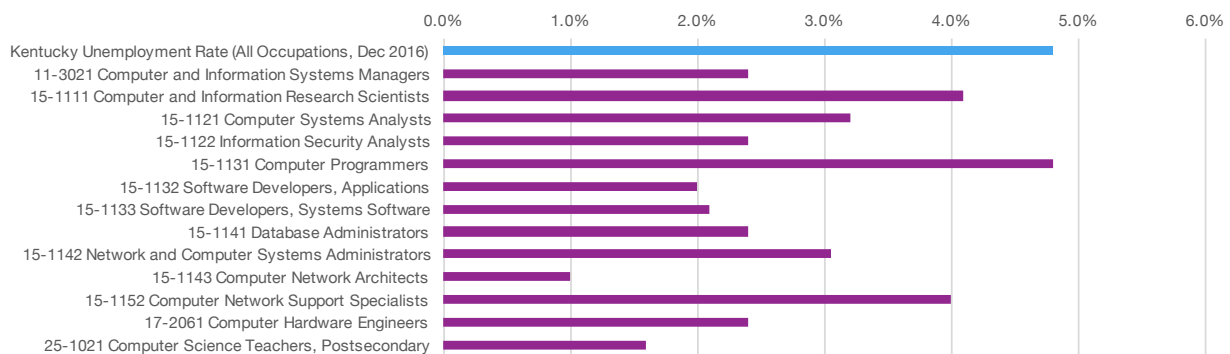
To get a better sense of the cybersecurity workforce, we analyzed labor statistics provided by the Cabinet for Economic Development and the JobsEQ® platform.^{lxv} About 1.9 million people were employed in Kentucky in December 2016, so the cybersecurity workforce represents a very small fraction of the total: about 0.5%. But within these occupations, the story is mostly encouraging. As shown in Figure 2, workers assigned to every single cybersecurity SOC earned far more on average than Kentucky’s annual mean wage of \$41,760 (calculated as of May 2016). Knowledge economy skillsets command higher wages, and the cybersecurity sector in Kentucky is no exception.

Figure 2 // Average annual wage of Kentucky cybersecurity workers



Unemployment rates for relevant occupations are also positive, as reflected in Figure 3. In the fourth quarter of 2016, the unemployment rates for every SOC code were lower than Kentucky’s December 2016 average of 4.8% – with the single exception of computer programmers, who were unemployed at the same rate. While this suggests high current demand for individuals to fill cybersecurity occupations, these low unemployment rates may be indicative of low supply, which may challenge industry growth efforts.

Figure 3 // Unemployment rates for cybersecurity workers



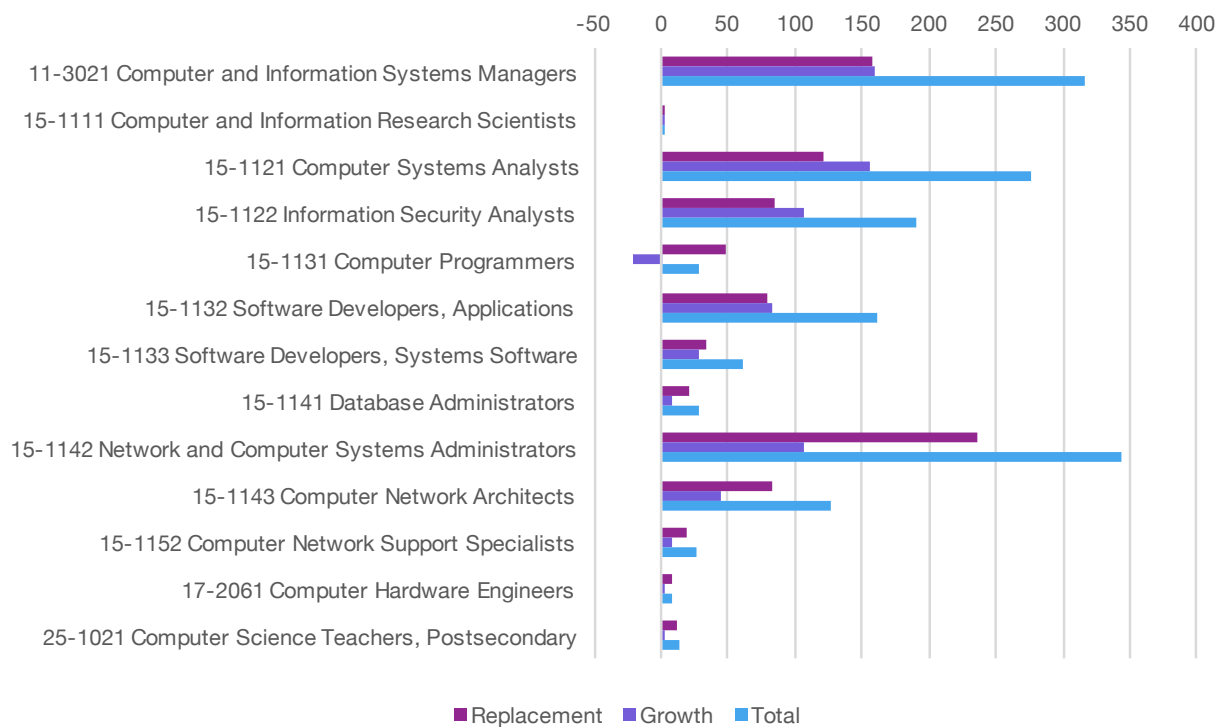
Forecasted demand

While the current state of the cybersecurity workforce looks positive, we can look at forecasted demand for cybersecurity positions to gain insight as to the workforce’s future. There are three categories of forecasted demand: replacement, growth, and total. *Replacement demand* refers to the number of positions required to backfill workers who leave the workforce or switch occupations. *Growth demand* refers to the number of positions that need to be filled due to an overall increase (or decrease) in the number of jobs. *Total demand* is the combination of the two, giving workforce developers a sense of how many total individuals need to be hired into the workforce over time.

Based on the JobsEQ® model, we estimate that the cybersecurity workforce will require 1,584 new hires over the course of the next seven years, given current projected total demand. That number is broken down into 902 replacements and 682 growth hires. Growth demand is projected at about 1% year over year for the next seven years. For the cybersecurity industry, which one market assessment estimates will grow globally at a rate of 9.8% per year from 2015 to 2020, this is a very low figure – even if we assume our calculations are conservative.^{lxvi}

Figure 4 breaks down the forecasted demand by category. There is significant demand for positions such as network and computer systems administrators, computer and information systems managers, and computer systems analysts. Collectively, these three positions constitute three-fifths of the current cybersecurity workforce. Other categories show weaker demand – some to the point of being almost negligible; computer programmers are actually forecasted to have negative growth. No occupation is forecasted to exceed 1.7% annual growth demand over the next seven years.

Figure 4 // Replacement, growth, and total demand by cybersecurity occupation, forecasted over 7 years



Another way to view the demand for cybersecurity workers in Kentucky is to compare it to the rest of the country. Figure 5 presents the Kentucky *location quotient* for each occupation. A location quotient of 1.0 represents the national average demand for that occupation. As Figure 5 shows, the demand in Kentucky is lower across the board – with the one exception of postsecondary computer science teachers, for whom there is a near-average need in the Commonwealth. Figure 5 underscores the need for Kentucky to stimulate the development of its cybersecurity economy in order to generate more demand for the cybersecurity workforce, and, in turn, better compete with other states.

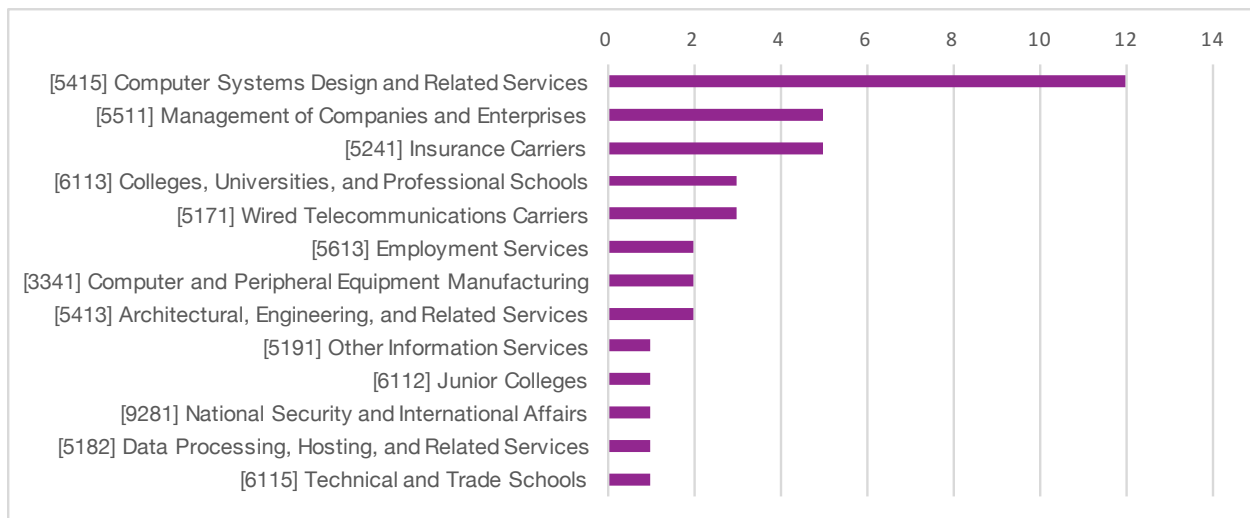
Figure 5 // Location quotient for cybersecurity workers



Key industries

To understand which industries are employing Kentucky’s cybersecurity workers, we reviewed the top three industries that employ workers assigned to each of the 13 SOC codes. Every time an industry featured as one of the top three employers of a particular type of cybersecurity worker, we assigned it a point, and we plotted those points on the bar graph in Figure 6. We see that – unsurprisingly – Computer Systems Design and Related Services is by far the most important industry for cybersecurity workers. Not only does it feature in the top three employers for 12 of the 13 SOC codes, it is actually the largest employer for each of those 12 occupations. The remaining key industries include computer-oriented fields, education, and a diversity of other sectors.

Figure 6 // Number of times an industry was one of the top three employers of a cybersecurity occupation



Recommendations

Development of a cybersecurity workforce does not happen overnight. A successful effort will require broad-based planning, stakeholder input, and a long-term commitment to meeting the needs of the state government and the private sector. There are many hurdles to overcome when fostering a cybersecurity workforce, including ambiguously defined skill-sets and varying requirements, outdated compensation structures, and a competition between the public and private sectors for talent.

Our workforce analysis reveals that those challenges are even more acute in Kentucky. Relative to other states, Kentucky has low demand for cybersecurity workers. At the same time, there is low unemployment among the cybersecurity workforce, potentially indicating a shortage of supply. And finally, the cybersecurity sector is not yet large enough to sustain the regular flow of workers between Kentucky's employers – and between Kentucky and other states. This last issue creates a cyclical problem: it is difficult to attract cybersecurity workers if there isn't a robust cybersecurity sector in Kentucky, but it's difficult to attract companies without a ready supply of cybersecurity workers.

In order for the Commonwealth to successfully develop and support its cybersecurity workforce, we recommend the following:

- **Establish a workforce-education committee.** In Chapter 10, we recommend that the Kentucky Cybersecurity Council designate a committee for workforce and education. This is in line with the way leading cybersecurity states – such as Virginia, Michigan, and California^{lxvii} – have approached this same challenge (see Chapter 10 for more on this topic). The collaboration of universities, school district administrators, business leaders, and government agencies is essential to common understanding of workforce needs and how educators can design curricula to meet those needs. Such collaboration should be ongoing, purposeful, and iterative, and it should consider public engagement mechanisms like conferences and competitions.
- **Increase cybersecurity education opportunities in schools and universities.** A diversified and sophisticated cybersecurity education system is vital to a competitive cybersecurity workforce. The Commonwealth must take concrete steps, such as establishing university scholarships, introducing cyber curricula to more secondary and primary schools, and expanding cybersecurity programming at universities. Chapter 4 provides further analysis and more detailed recommendations on how to strengthen cybersecurity education in Kentucky.
- **Educate businesses on their cybersecurity needs.** Kentucky's businesses are not hiring enough cybersecurity workers. If businesses better understand the cybersecurity challenges that they face and the potential costs associated with cyber risks, they will be more inclined to make the necessary investments in cybersecurity expertise. In this way, public awareness can have a direct economic impact. Chapter 7 provides further guidance on methods to enhance public awareness throughout Kentucky.
- **Apply the NCWF to categorize state cybersecurity jobs.** The state should implement a system that aligns cybersecurity position descriptions, job duties, and job competencies to the NCWF in order to develop a uniform career pathway. While the effort does not need to be as comprehensive as California's, a basic system aligned with the NCWF would empower the state government to improve recruitment and retention of cybersecurity professionals. The NCWF creates a structure for professional development, and it could also empower the state government to establish a more competitive pay scale for cybersecurity workers.

- **Brand Kentucky as an attractive home for cybersecurity workers.** In Chapter 1, we recommend developing and promoting a cybersecurity brand for Kentucky. This should not just be directed at businesses, but at workers, as well. The Commonwealth should encourage events like cybersecurity competitions, hackathons, conferences, workshops and training exercises, and job fairs. The proposed cybersecurity initiative, detailed in Chapter 10, would be an ideal vehicle for implementing this recommendation.

CHAPTER

4

Education

```
1 * Link https://development.wordpress.org/packages/
2 * @package _s
3 */
4 function_exists( 'incode_starter_setup' ) );
5
6 /**
7  * Sets up theme defaults and registers support for various WordPress features.
8  * Note that this function is hooked into the after_setup_theme hook, which
9  * runs before the init hook. The init hook is too late for some features, such
10 * as indicating support for post thumbnails.
11 */
12 function incode_starter_setup() {
13     // Make theme available for translation.
14     // Translations can be filed in the /languages/ directory.
15     // For more information on this, see the WordPress Codex page on
16     // Internationalization at https://codex.wordpress.org/Internationalization
17     add_theme_support( 'translations' );
18
19     // Enable support for Post Thumbnails.
20     add_theme_support( 'post-thumbnails' );
21
22     // Add default posts and pages unless we're using the WordPress.com atomic theme.
23     if ( ! is_customize_preview() ) {
24         wp_installer();
25     }
26 }
27
28 add_action( 'after_setup_theme', 'incode_starter_setup' );
```



Chapter 4 | Education

This chapter addresses the current state of Kentucky’s cybersecurity education and training landscapes, and it highlights cybersecurity education initiatives in other parts of the country. We will also provide recommendations on how Kentucky policymakers can strengthen the state’s cybersecurity education infrastructure.

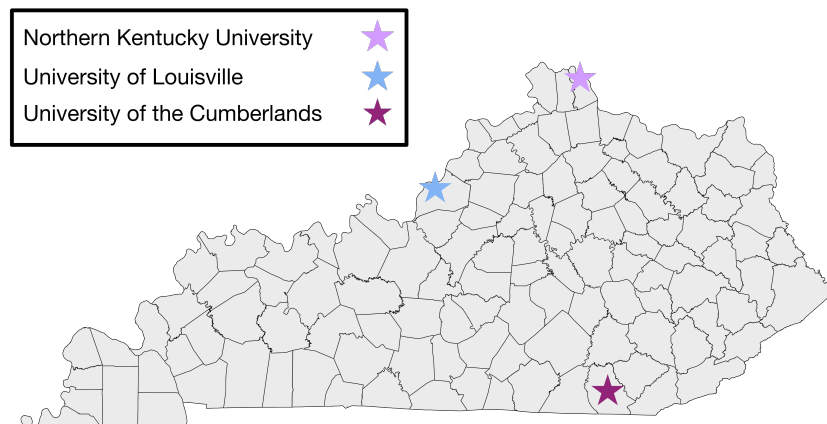
Cybersecurity education in Kentucky today

Conversations about cybersecurity education at the university level typically begin with the Centers for Academic Excellence (CAE) program, which is jointly administered by the National Security Agency and the Department of Homeland Security. Created in response to the need for enhanced education that meets the nation’s long-term cybersecurity workforce demands, the program allows NSA and DHS to certify qualifying academic institutions or programs as CAEs.

There are two types of CAE: those that specialize in cyber defense (CD) and those that specialize in cyber operations (CO). CAE-CDs are designated as a four-year cyber defense education program (CAE-CDE); a two-year cyber defense education program (CAE-2Y); or a cyber defense research program (CAE-R). CAE-COs focus on more technical disciplines critical to intelligence, military, and law enforcement organizations. The designation as a CAE lasts for five academic years, after which the institution or program must reapply.

Nationally, there are 213 institutions designated as a CAE-CD (137 CAE-CDE, 46 CAE-2Y, and 68 CAE-R). Of the 213, three are located in Kentucky: Northern Kentucky University (NKU), the University of Louisville, and the University of the Cumberlands (see Figure 1).

Figure 1 // Kentucky Centers for Academic Excellence in Cyber Defense Education



In 2015, NKU became the first university in Kentucky to earn a CAE-CD designation. For undergraduates, NKU offers two minors (computer forensics and information security) and a certificate in cybersecurity. Graduate students have an option of two information security certificates. The Center for Information Security (CIS) is the focal point of the university’s cybersecurity efforts, directing research and housing the nationally competitive Cyber Defense Team.^{lxviii} NKU’s team placed first at the 2014 Midwest Collegiate Cyber Defense Competition and 6th in the National Collegiate Cyber Defense Competition the same year.

The University of Louisville’s primary cybersecurity effort is housed in its Cyber Security Initiative (CSI). The CSI is a joint program across the department of Computer Engineering and Computer Science (CECS) in the J.B. Speed School of Engineering^{lxix}, and the department of Computer Information Systems (CIS) in the College of Business.^{lxx} By tying the two programs together, the university is reflecting the increased need for integration between business and technical minds to address critical cybersecurity issues. In the National Collegiate Cyber Defense Competition, the University of Louisville placed third in 2007, 2008, 2011, and second in 2010. Louisville offers a graduate certificate in Network and Information Security and an undergraduate certificate in Information Security.

Kentucky’s newest CAE is the University of the Cumberlands, which received its designation in early 2017. The Center for Cyber Security is home to cybersecurity research at the university. The university’s Master of Science in Information Security Systems is one of the only graduate-level programs in Kentucky dedicated specifically to cybersecurity.

The CAE program is setting the pace for advanced cybersecurity education. With only three CAE-CDs, Kentucky trails the country’s leading cybersecurity states: Maryland (16), Florida (13), Texas (13), New York (12), and Virginia (11). Kentucky’s three CAE institutions are also only for cyber defense education; none are designated for research or for two-year programs. Many other states have a mix of all three CAE-CD programs, which gives them a more balanced impact on the cybersecurity workforce. And although CAE-COs are less common, Kentucky has none. To bolster Kentucky’s profile, the Commonwealth should consider encouraging other local academic institutions to pursue the certification process.

Number of programs available

While Kentucky’s universities offer plenty of classes that deal with cybersecurity as part of a broader computer science program, there are only a handful of cybersecurity-specific degrees, like the Master of Science in Information Security Systems at the University of the Cumberlands. Other examples include those issued by Sullivan University, a for-profit university in Louisville, which offers both a Bachelor of Science in Network Security and a Master of Science in Cyber Security. But a degree does not need to be cybersecurity-specific to prepare an individual for the cybersecurity workforce. We expanded the scope of our analysis to include academic programs that we deemed relevant to a cybersecurity career.

Table 1 presents a tally of relevant undergraduate and graduate programs that are or have been offered in Kentucky since 2006. Most programs are related to computer science, although some deal with homeland security. **Public universities** refers to state-operated institutions that issue four-year undergraduate degrees; **independent universities and colleges** are privately operated, not-for-profit institutions; and **community and technical colleges** issue two-year undergraduate degrees and belong to the Kentucky Community and Technical College System (KCTCS). Data on public, independent, and community and technical colleges are derived from the Kentucky Center for Education and Workforce Statistics (KCEWS), while data on for-profit universities was derived from our research.

In Table 1, the two blue columns reflect the number of programs that issued a degree, certificate, or diploma in 2016. “U” refers to undergraduate programs, which include bachelor’s degrees, as well as associate’s degrees, and postsecondary certificates and diplomas. “G” refers to graduate programs, which includes both master’s and doctoral degrees.

Table 1 // Cybersecurity-relevant academic programs

	U (2016)	G (2016)
Public Universities	25	11
Eastern Kentucky University	3	2
Kentucky State University	2	1
Morehead State University	1	
Murray State University	3	2
Northern Kentucky University	6	2
University of Kentucky	3	2
University of Louisville	3	1
Western Kentucky University	4	1
Independent Universities and Colleges	15	2
Bellarmino University	2	1
Berea College	1	
Brescia University	1	
Campbellsville University	1	
Centre College	1	
Georgetown College	2	
Kentucky Wesleyan College	1	
Lindsey Wilson College	1	
Midway University		
Spalding University		
St. Catharine College		
Thomas More College	2	
Transylvania University	1	
Union College	1	
University of the Cumberlands		1
University of Pikeville	1	
Community & Technical Colleges	18	
Ashland C&TC	1	
Big Sandy C&TC	1	
Bluegrass C&TC	2	
Elizabethtown C&TC	1	
Gateway C&TC	1	
Hazard C&TC	1	
Henderson CC	1	
Hopkinsville CC	1	
Jefferson C&TC	1	
Madisonville CC	1	
Maysville C&TC	1	
Owensboro C&TC	1	
Somerset CC	1	
Southcentral Kentucky C&TC	1	
Southeast Kentucky C&TC	1	
West Kentucky C&TC	2	
For-profit Universities and Colleges	6	2
Daymar College	1	
Sullivan University	3	1
University of Phoenix	2	1

Table 1 reveals that 8 **public universities** offer a total of 36 relevant degrees, diplomas, or certificates: 11 at the graduate level and 25 at the undergraduate level. The average public university is likely to offer multiple programs at both levels, and they offer by far the most options for students seeking graduate-level education. The university with the most offerings is Northern Kentucky University (8 total); Eastern Kentucky University, Murray State University, the University of Kentucky, and Western Kentucky University each offers 5.

There are 13 **independent universities** that offer a total of 17 relevant programs: 2 are graduate degrees and 15 are undergraduate degrees. There are also 16 **community and technical colleges** that offer 18 relevant two-year programs. Finally, there are 3 **for-profit universities and colleges** that offer 6 undergraduate and 2 graduate programs. Although there are many independent universities, community and technical colleges, and for-profit institutions available for students to choose from, there are limited course options at each individual institution.

Number of degrees, diplomas, and certificates issued

As indicated above, the datasets from KCEWS do not include for-profit institutions, so – for the rest of this chapter, unless otherwise noted – Daymar College, Sullivan University, and the University of Phoenix will be excluded from our analysis.

Our analysis of KCEWS data found that over the eleven-year period from 2006 to 2016, a total of 21,740 degrees, diplomas, and certificates were issued by cybersecurity-relevant programs. (A complete list of the degrees, diplomas, and certificates in this dataset can be found in Appendix C.) We have organized that information into two categories: level of institution and type of institution, as displayed in Table 2 and 3, respectively.

Table 2 // Degrees, diplomas, and certificates issued by level

Level	Number issued
Graduate or post-graduate degrees	3,123
Undergraduate degrees, diplomas, and certificates	18,617

Table 3 // Degrees, diplomas, and certificates issued by institution

Type of institution	Degrees issued
Public Universities	7,581
Independent Universities	831
Community & Technical Colleges	13,333

Looking at historical KCEWS data, we can analyze the growth in the number of degrees, diplomas, and certificates issued over time. The number of degrees, diplomas, and certificates issued was relatively flat until 2014, when there was a marked uptick in undergraduate programs, followed by a similar uptick in

2015 in graduate degrees. Shown in Figures 2 and 3, these upticks are encouraging for the information technology sector in general and the cybersecurity sector specifically.

Figure 2 // Number of relevant degrees, diplomas, and certificates issued by level over time (2006 – 2016)

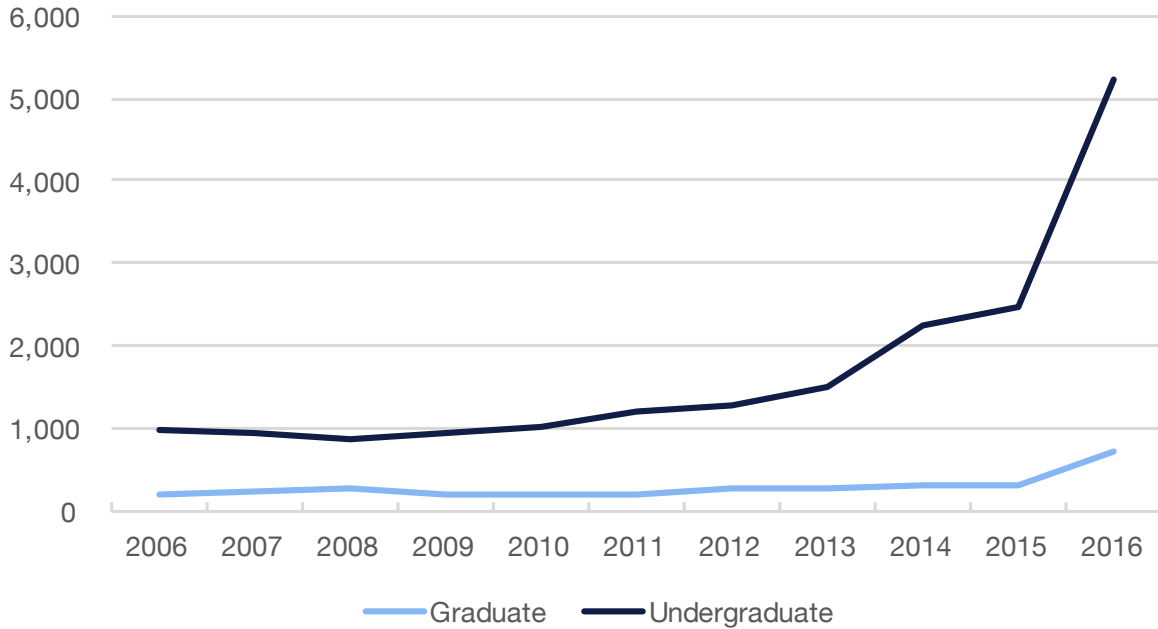
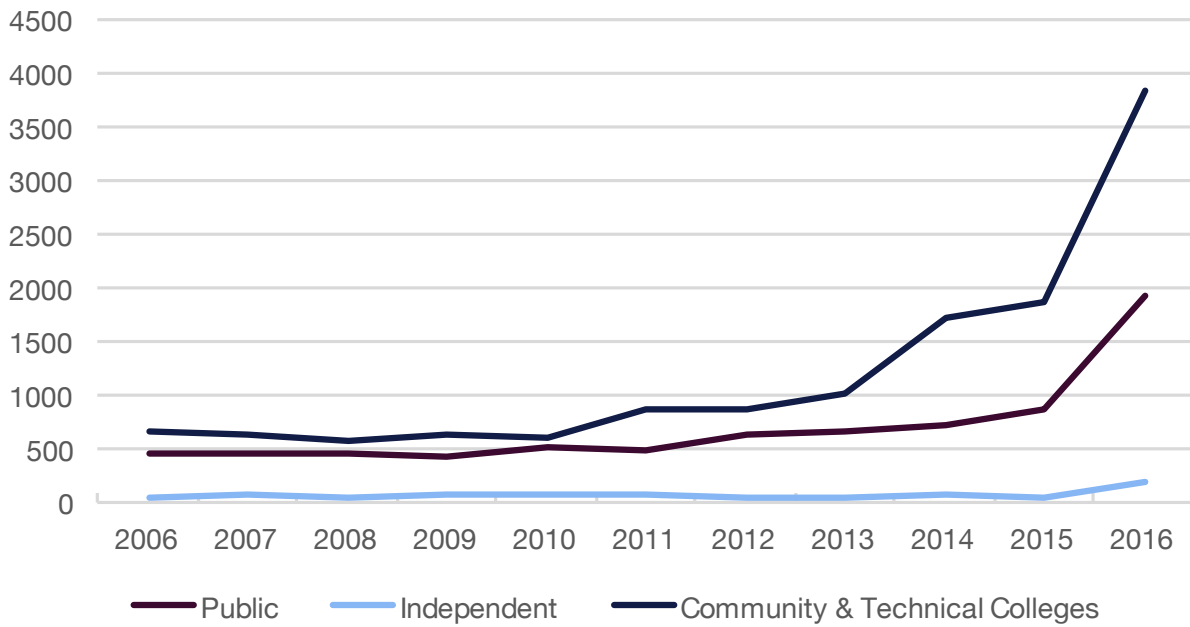


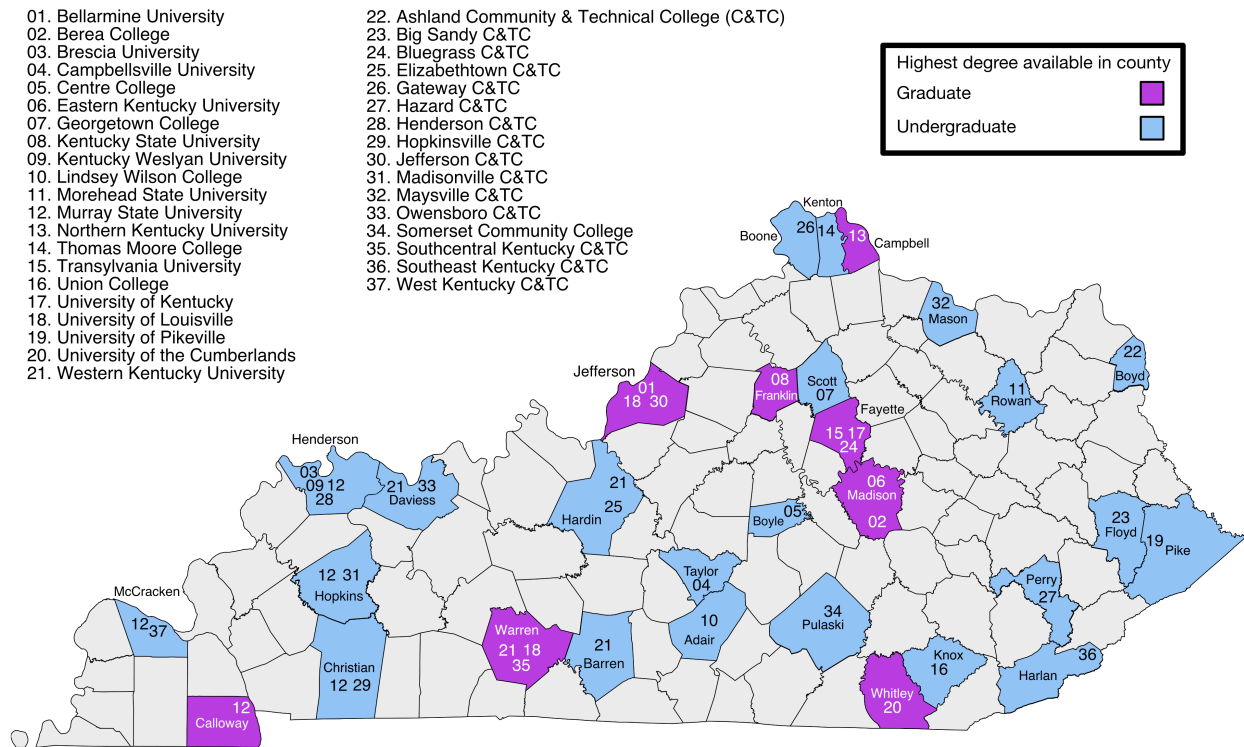
Figure 3 // Number of relevant degrees issued by institution over time (2006 – 2016)



Academic programs by geography

We plotted the information from Table 1 (the set of institutions that issued degrees in 2016) on a county map of Kentucky to understand where relevant programs are being offered. Figure 4 shows the highest relevant program offered at a brick-and-mortar institution in each county in Kentucky. (Note that for-profit institutions are not included here.)

Figure 4 // Geographic footprint of relevant degrees, diplomas, and certificates



This map is encouraging; it shows that cybersecurity-relevant education has been relatively accessible to Kentucky residents, regardless of where they live. The only noticeable gap is that residents of eastern Kentucky would need to travel or move to another part of the state to receive a graduate or post-graduate degree.

Cybersecurity training and certification in Kentucky today

Professionals seeking a competitive advantage in the workforce may elect to receive cybersecurity-specific certifications. Employers responding to our industry survey tended to cite on-the-job experience as more important than a specific cybersecurity certification. But for an individual who is new to the labor force, ready to change careers, or keen to become a more marketable professional, a certification can prove an important asset in landing a cybersecurity position.

There are two components to a certification: the **training** on the relevant subject matter and the **test** that one must pass to receive the certification. Training and testing are usually provided at different locations; training is usually offered by an organization that specializes in the content, while testing is usually performed by an organization that specializes in administering exams (regardless of the content). There are many cybersecurity-related certifications; here, we identified a list of 19 certifications that we deemed relevant to a cybersecurity career and that our research suggested are among the most common and commonly-required certifications. Of note, industry survey respondents most often regarded two certifications as important: Security+ and CISSP. As Table 4 shows, training for all 19 certifications is available online, but some certifications require testing at a physical location.

Table 4 // Key cybersecurity certifications

Certification	Training Online?	Test Online?
Cisco Certified Entry Network Technician (CCENT)	Yes	No
Cisco Certified Network Associate (CCNA)	Yes	No
Cisco Certified Network Professional (CCNP)	Yes	No
CompTIA Advanced Security Practitioner (CASP)	Yes	Yes
CompTIA A+	Yes	Yes
CompTIA Network+	Yes	Yes
CompTIA Security+	Yes	Yes
EC-Council Certified Ethical Hacker (CEH)	Yes	Yes
GIAC Certified Incident Handler (GCIH)	Yes	No
GIAC Certified Intrusion Analyst (GCIA)	Yes	No
GIAC Industrial Cyber Security Professional (GICSP)	Yes	No
GIAC Penetration Tester (GPEN)	Yes	No
GIAC Security Essentials Certification (GSEC)	Yes	No
GIAC Security Expert (GSE)	Yes	No
GIAC Security Leadership Certification (GSLC)	Yes	No
ISACA Certified Information Security Manager (CISM)	Yes	Yes
ISACA Certified Information Systems Auditor (CISA)	Yes	Yes
(ISC)² Certified Cyber Forensics Professional (CCFP)	Yes	No
(ISC)² Certified Information Systems Security Professional (CISSP)	Yes	No

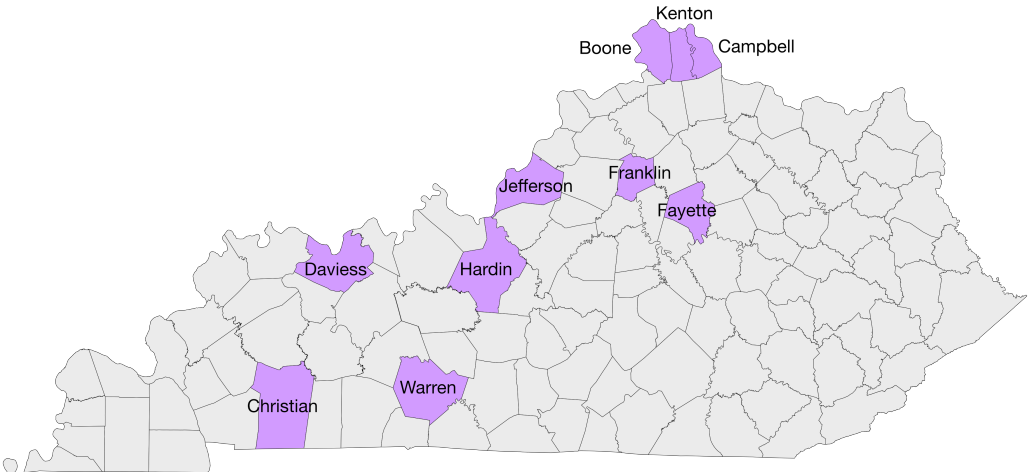
Although training for all 19 certifications is available online from a variety of providers, some students prefer to learn in person. As reflected in Table 5, there are a total of eight institutions that provide training for one or more of these certifications, and they do so at 13 different brick-and-mortar locations in Kentucky. Among the 19 listed certifications, there is only category for which training is not available in person: the GIAC category, which is offered only online by the SANS Institute.

Table 5 // Organizations that offer in-person training in Kentucky

	Sunset Learning Institute, Louisville	New Horizons, Lexington	ONLC Training Center, Lexington	ONLC Training Center, Florence	CED Solutions, Bowling Green	CED Solutions, Fort Knox	CED Solutions, Louisville	CED Solutions, Covington	CED Solutions, Frankfort	CED Solutions, Owensboro	Certified Staffing Solutions, Lexington	ExecuTrain, Lexington	ExecuTrain, Louisville	TrainUp, Louisville	NKU, Highland Heights
Cisco Certified Entry Network Technician (CCENT)															
Cisco Certified Network Associate (CCNA)															
Cisco Certified Network Professional (CCNP)															
CompTIA Advanced Security Practitioner (CASP)															
CompTIA A+															
CompTIA Network+															
CompTIA Security+															
EC-Council Certified Ethical Hacker (CEH)															
ISACA Certified Information Security Manager (CISM)															
ISACA Certified Information Systems Auditor (CISA)															
ISC(2) Certified Information Systems Security Professional (CISSP)															

Figure 5 shows the counties in Kentucky with brick-and-mortar training locations. Even though training is available online, the lack of physical locations in the eastern and southeastern parts of the state may deter residents in these regions from pursuing careers in cybersecurity.

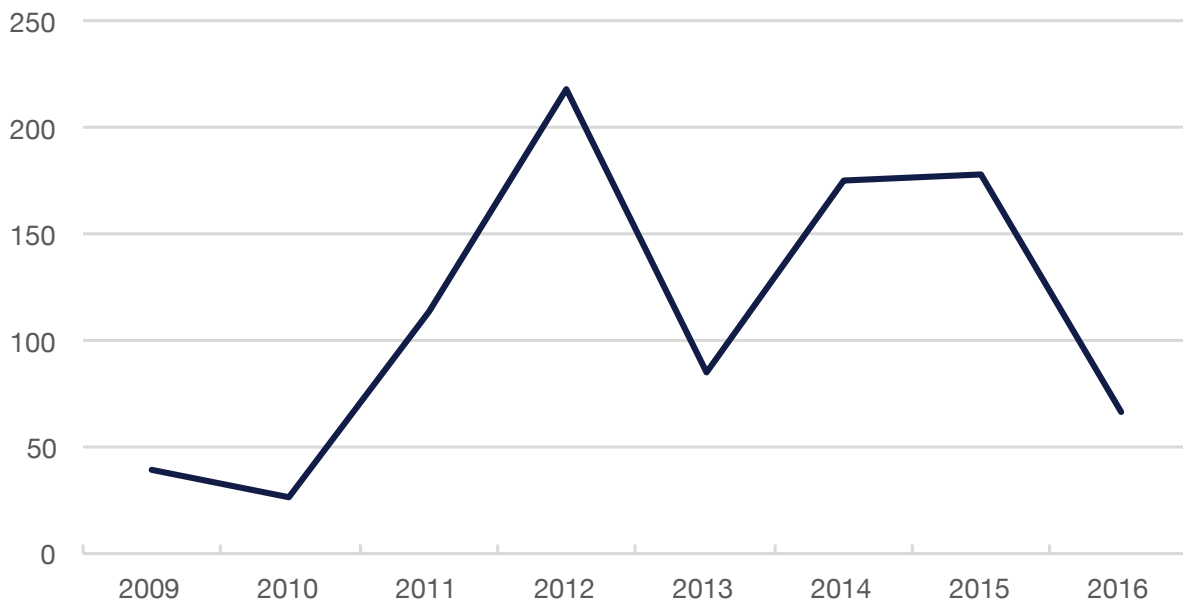
Figure 5 // Counties with training locations



For most of the 19 certifications, there are ample testing centers across the Commonwealth. The ISC(2) certifications are the exception: not only is testing not available online, one can only take the certification test at a PearsonVUE center in Louisville or Lexington – although military personnel are able to take the exam at either Fort Knox or Fort Campbell.

While we were unable to access reliable data on most of these certifications, KCEWS provided data on the number of certifications issued in Kentucky for five among our list of 19: CCENT, CCNA, Network+, Security+, and A+. In total, 325 residents – mostly at the high school level – received one of these certifications between 2009 and 2016; and of that group, approximately 223 were employed in Kentucky in the 2015-2016 fiscal year. As shown in Figure 6, the number of certifications issued spiked in 2011 and 2012, then fell substantially in 2013. It is unclear what caused this drop, which is surprising considering the growing demand for cybersecurity professionals.

Figure 6 // CCENT, CCNA, Network+, Security+, and A+ certifications issued in Kentucky (2009-16)



Connecting education and workforce

A critical question for Kentucky policymakers is whether the Commonwealth’s academic institutions are adequately preparing Kentucky’s workforce to meet future employment demand. Fortunately, KCEWS is an institution designed to help answer that question, and their datasets help us shed light on this issue in the context of cybersecurity.

Of those individuals who were issued a relevant degree, diploma, or certificate in Kentucky in the eleven-year period between 2006 and 2016, there were a total of 12,027 individuals employed in Kentucky in the 2015-16 fiscal year. (Note that this figure excludes industries that employed fewer than 10 individuals, so the real number is marginally higher.) Of that employed group, 94% of the received a degree, diploma, or certificate at the undergraduate level, and only 6% received a graduate or post-graduate degree (see Figure 7). Those receiving graduate or post-graduate degrees were far more likely to remain in academia than to pursue careers in any one other industry. Approximately 40% (168 people) of individuals in this category are employed by Colleges, Universities, and Professionals Schools; no other industry employs even 50 graduate-level degree holders.

Figure 7 // Kentucky workers by level of cybersecurity degree earned

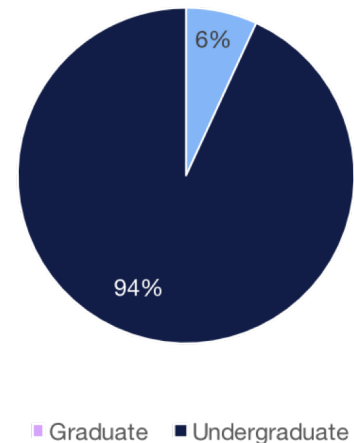


Figure 8 shows a breakdown of the top 15 industries of employment for people who a) received an undergraduate-level cyber-relevant education in Kentucky, and b) are currently employed in Kentucky. Not surprisingly, the leading industry is Computer Systems Design and Related Services. But of note is the number of graduates who have gone on to work in education – if tertiary, secondary, and primary educational institutions were treated as one industry, it would be the leading employer. Another interesting finding is that many people who received a cyber-relevant education in Kentucky went on to work in industries that would naturally have low demand for such workers – such as supermarkets, limited-service restaurants, and temporary help services. While it is possible that Kentucky-based employers in these industries have an unusually high need for computer science and homeland security graduates, it is more likely that these graduates are not being matched to jobs that fit their credentials.

Figure 8 // Kentucky workers who received undergraduate cyber-relevant education by 2015-2016 industry

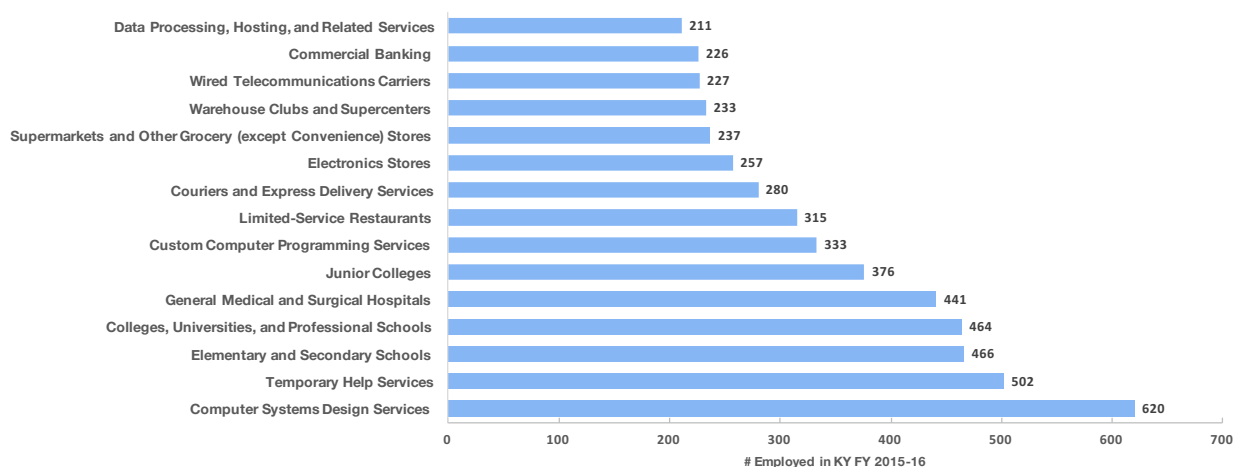


Figure 9 reveals a significant gender disparity among this population. Among people who a) received a cyber-relevant education in Kentucky between 2006 and 2016 and b) were employed in Kentucky in the 2015-2016 fiscal year, only 18% are female. This stark gender gap in the technology industry is not Kentucky's challenge alone, but it is one that should be addressed directly in order to realize the full economic benefits of the cybersecurity economy.

Figure 10 reflects an important finding: the vast majority of employed individuals who received a cyber-relevant education in Kentucky did so through the Kentucky Community and Technical College System (KCTCS), underscoring the vital role community and technical colleges play in the educating Kentucky's workforce. However, the disparity between community and technical colleges (72%) and other types of institutions (28%) implies that KCTCS computer science graduates are not going on to complete four-year degree programs in ample numbers (at least not in Kentucky). Moreover, the high number of people who appear to have pursued roles in unrelated industries implies that an associate's degree in computer science is not necessarily leading individuals to careers in cybersecurity. For Kentuckians who hold an associate's degree in computer science, the pathway to a cybersecurity job (whether that involves a four-year degree or not) must be strengthened and clarified.

Figure 9 // Gender breakdown among cyber-relevant graduates employed in Kentucky

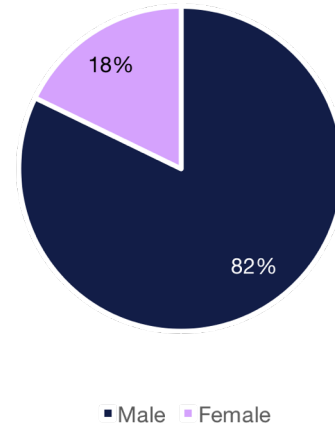
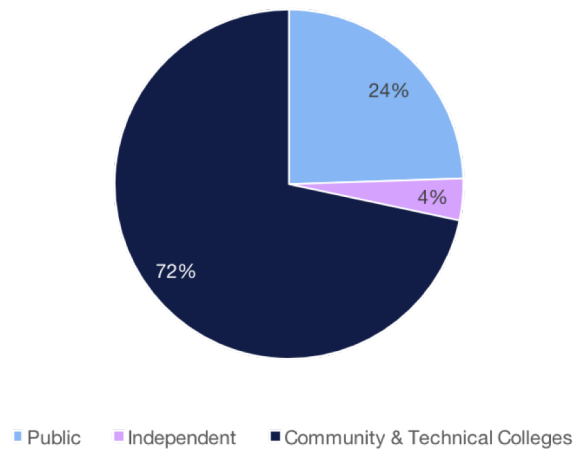


Figure 10 // Employed graduates by type of institution



Cybersecurity education initiatives around the country

To put the above analysis into context, we conducted a review of cybersecurity education efforts at the federal level and in other parts of the country. There are countless initiatives focused on cybersecurity education, so we elected to highlight a few examples – namely those in Maryland, Michigan, and San Antonio.

National Initiative for Cybersecurity Education (NICE)

NICE is an interagency initiative coordinated by the National Institute of Standards and Technology (NIST). With a mission “to energize ...cybersecurity education, training, and workforce development,” NICE is the main federal effort designed to bridge the gap between educational institutions at all levels and the growing cybersecurity needs of the national workforce. NICE has developed a Cybersecurity Workforce Framework to give educators and businesses a common lexicon and professional development construct for the cybersecurity workforce. The initiative makes available a host of resources, including conferences, competitions, webinars, and educational materials.

RAMPS Cybersecurity Education and Workforce Development

Managed by NICE, Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development (RAMPS) grants are awarded competitively to state and local organizations that develop programs to connect employers with academic institutions. Educators can collaborate with employers in a structured context to confront current and anticipated cybersecurity skill shortages.^{lxxi} In 2016, NICE awarded five RAMPS grants to the Arizona Statewide Cyber Workforce Consortium; the Pikes Peak Community College Cyber Prep Program (Colorado); the Cincinnati-Dayton Cyber Corridor (Ohio); the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (Virginia); and the Partnership to Advance Cybersecurity Education and Training (New York).^{lxxii}

National Initiative for Cybersecurity Careers and Studies (NICCS)

Managed by DHS, NICCS is a national resource for education, workforce, and training as they relate to cybersecurity. NICCS connects students, government agencies, and industry stakeholders with cybersecurity training and education providers across the country. NICCS disseminates the NICE Cybersecurity Workforce Framework (NCWF) and applies it to the development of its own education and training programming.^{lxxiii}

Cyber Engineering Pathway Curricula

Recognizing the urgent need to integrate cybersecurity education into all levels of schooling in the United States, DHS funded the establishment of the National Integrated Cyber Education Research Center (NICERC) at the Cyber Innovation Center in Bossier City, Louisiana. NICERC develops cybersecurity education curricula that elementary and secondary school educators can integrate into their classroom instruction, free of charge. The curricula are designed to increase cybersecurity awareness and ultimately help prepare students for careers in the cybersecurity field.^{lxxiv} Following Louisiana, Kentucky became the second state to adopt the NICERC curricula in early 2017. The Kentucky Department of Education has made the curricula available to all school districts, and Jefferson County Public Schools will be first to put the curricula into effect at the high school level.^{lxxv}

Maryland

At the state and local levels, Maryland is proactively pursuing a bold cybersecurity education and workforce development agenda. For example, Governor Hogan has committed \$3 million to provide job training for cybersecurity-specific occupations.^{lxxvi} Backed by a \$14.9 million Department of Labor grant, the Cyber Pathways Across Maryland program puts 14 community colleges at the helm of a multi-layered workforce development initiative targeted specifically at filling the cybersecurity skills gap.^{lxxvii} The University System of Maryland and Business-Higher Education Forum created the Undergraduate Cybersecurity Network to attract college students – particularly women and minority students – to cybersecurity career paths.^{lxxviii} Through the Maryland Cybersecurity Center, the University of Maryland draws on its resources and federal partnerships to recruit middle and high school students to the cybersecurity field through seminars, events, and cybersecurity camps.^{lxxix}

Michigan

Similarly, Michigan has launched a number of initiatives related to cybersecurity education, including the Michigan Cyber Range. Operated by Merit Network, Inc., an organization run by Michigan's public universities, the Cyber Range is a secure platform for research, training, and testing related to cybersecurity. It focuses on the higher end of the skill spectrum, allowing both professionals and students to learn and to test cybersecurity concepts in its Secure Sandbox – which safely simulates a real-world networked environment. The Cyber Range offers a broad array of certifications and classes, and is aligned with the NICE Cybersecurity Workforce Framework.^{lxxx}

San Antonio: a case study in cybersecurity education

San Antonio is leaning forward in its efforts to be one of the nation's leading hubs for cybersecurity. The city's cybersecurity strengths stem from its longstanding relationship with the military. In fact, San Antonio's growing cyber industry, talent pool, and education infrastructure are some of the reasons why the 24th Air Force (Cyber Command), the Navy's Fleet Cyber Command / Tenth Fleet, and cyber components of other military and federal organizations are located there.^{lxxxii}

With such high demand for cybersecurity workers from the military, the government, and industry, San Antonio has had to develop an education infrastructure that can keep pace; San Antonio has five regional colleges that are designated as CAE-CDs: the University of Texas at San Antonio (UTSA), Our Lady of the Lake University, St. Philip's College, San Antonio College, and Texas A&M University – San Antonio. In 2014, *Computerworld* crowned UTSA the leading cybersecurity institution in the country, following an HP survey of approximately 2,000 certified IT security professionals. The survey considered UTSA's 14 undergraduate and graduate programs – in areas such as digital forensics, secure design and intrusion detection and response – to be the best in the nation for academic excellence and practical relevance.^{lxxxiii}

UTSA's prominence did not materialize overnight. Back in 2005, USTA created the National Collegiate Cyber Defense Competition, the nation's largest cybersecurity contest for college students. It has three research centers – the Institute for Cyber Security, the Center for Infrastructure Assurance and Security, and the Center for Education and Research in Information and Infrastructure Assurance and Security – focused on solving critical cybersecurity challenges.^{lxxxiii} And in 2015, UTSA was selected by the Department of Homeland Security to develop national cybersecurity standards for information sharing to support President Obama's cybersecurity strategy.

San Antonio is also home to the Alamo Academies, which guide students into cybersecurity and other STEM career pathways. Its Information Technology and Security Academy allows students to earn college credits at no cost and helps place them in IT internships with local industry.^{lxxxiv}

The support for cybersecurity comes from all corners of the community. The San Antonio Chamber of Commerce established a Cybersecurity Industry Council to support the growth of the cybersecurity sector. The Council promotes a friendly environment for cyber startups and ensures universities strengthen cyber curricula and issue degrees in related fields.^{lxxxv} San Antonio is also home to the annual CyberTexas conference, which reinforces the city's importance in the field.^{lxxxvi}

There are two keys to San Antonio's success as a leader in cybersecurity education. The first is the presence of an anchor for the cybersecurity economy: military and other federal government agencies. The second is the community's degree of vertical and horizontal alignment. From high schools through to universities, from business across to government, San Antonio has made cybersecurity a priority. In turn, the leaders of area academic institutions have worked with industry, local organizations, and the government to understand and respond to the community's critical needs.

Recommendations

Kentucky's cybersecurity education infrastructure has a broad foundation with plenty of room to grow. Kentucky's universities offer a range of two-year and four-year computer science programs, and cybersecurity-specific programs are increasing in number. With the recent addition of the University of the Cumberlands, Kentucky now has three CAEs. At the high school level, the Kentucky Department of Education's recent adoption of the Cyber Engineering Pathway Curricula is a significant accomplishment that will advance Kentucky's long-term cybersecurity workforce needs. But much more work needs to be done, and the Commonwealth should seize this momentum. State leaders should look at each of these recommendations through an integrated lens, both vertically (from elementary school curricula through to post-graduate programming) and horizontally (across government, business, and the education and training communities).

- **Establish a cybersecurity workforce-education body.** In Chapter 5, we recommend that the Kentucky Cybersecurity Council designate a committee for education and workforce development. As demonstrated in other states, the collaboration of universities, school district administrators, business leaders, and government agencies is essential to common understanding of workforce needs and how educators can design curricula to meet those needs. Such collaboration should be ongoing, purposeful, and iterative, and it should consider public engagement mechanisms like conferences and competitions. Once it has established its key priorities, the committee should consider applying for a NICE RAMPS grant to facilitate implementation.
- **Bring cybersecurity education to elementary and middle schools.** While the adoption of the Cyber Engineering Pathway Curricula is an excellent first step, its near-term rollout is limited to the high school level. Cybersecurity education should begin earlier; children interact with technology every day, and the concepts of proper cyber hygiene should be taught at an early age. While the primary purpose would be to cultivate a cyber-savvy population, this effort would have the ancillary benefit of widening the funnel for the future cybersecurity workforce.
- **Increase the number and variety of cybersecurity university programs.** Kentucky's universities should broaden the scope of their programming, offering more cybersecurity-specific degrees with an increased variety of specializations. While not every institution needs to be *the* national cybersecurity leader, Kentucky's most prominent cybersecurity institutions can look to leading universities like USTA as models.
- **Pursue more CAE designations.** The Commonwealth should increase the number of CAE-CDEs and it should also be home to at least one of each type of other CAE: CAE2Y for two year-institutions; CAE-R for research programs; and CAE-CO for specialized cyber operations. A diversity of CAE types will increase the options available to students entering cybersecurity careers, and it will raise the national profile of Kentucky within the cybersecurity community.
- **Fund cybersecurity scholarships.** The state government – perhaps in collaboration with corporate sponsors – should encourage the establishment of cybersecurity scholarships to incentivize high achievers to pursue a cybersecurity education and career in Kentucky. Particular attention should be paid to increasing access to cybersecurity education among females (to address the stark gender gap), residents of eastern Kentucky (where cybersecurity education opportunities lag behind other parts of the state), and other underrepresented groups.

CHAPTER 5

Governance



Chapter 5 | Governance

Cybersecurity is a complex web of issues that requires holistic, all-hands-on-deck problem solving. For state governments like Kentucky's, the challenge is broad: how do we cover all aspects of the cybersecurity challenge with limited resources? And how do we make sure our government is appropriately integrated with Federal and local government agencies, the private sector, and our citizens? There are three key elements of this problem set: critical infrastructure (and managing risks thereto), information sharing, and cybersecurity laws. This chapter explains those three elements in the Kentucky context, and it provides recommendations for the establishment of a committee for state government cybersecurity functions.

Critical infrastructure risk management

Critical infrastructure in 60 seconds

The President's Commission on Critical Infrastructure Protection (PCCIP) was the first formal body to define critical infrastructure (CI) in 1998. The PCCIP definition was adopted with little modification and codified into law by the USA Patriot Act of 2001. It reads:

"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

These systems and assets are diverse, stretching across industries, functions, and geographies. The protection of critical infrastructure is therefore a complex challenge requiring interaction across all levels of government and industry. The federal government has taken many steps to bring order and alignment to this complex picture, but – for the purposes of this report – we will only skim the surface.

One of those steps is the organization of CI into 16 discrete industrial sectors, as defined by *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience*. Those 16 sectors (like energy and financial services) are the lenses through which CI professionals – planners and analysts, owners and operators, government and industry – view the world. The guiding document for protecting those sectors is the National Infrastructure Protection Plan (NIPP), the most recent version of which was published by the Department of Homeland Security (DHS) in 2013.

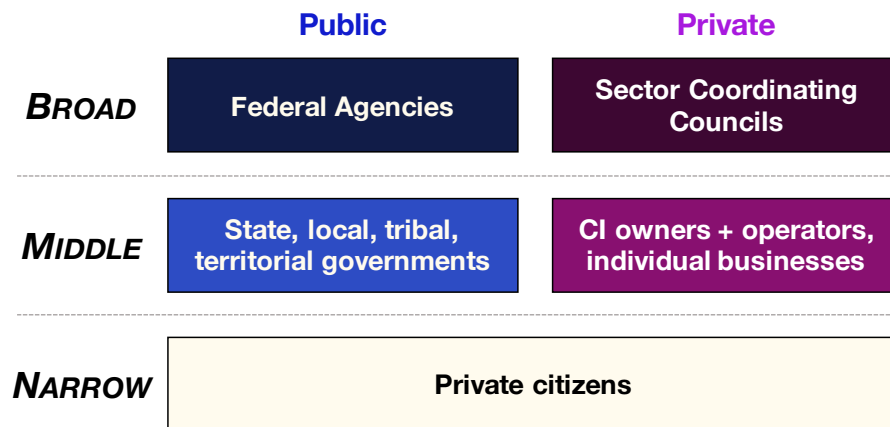
The NIPP assigns each sector one or more federal agencies (referred to as Sector-Specific Agencies, or SSAs) that lead the federal government's efforts to protect that sector's CI assets. The federal government also organizes Government Coordinating Councils (GCCs) to facilitate interagency support to each sector. Like the federal government, the private and non-profit sectors – which own and operate most of the nation's CI assets – are also organized according to CI sector. Each CI sector has an industry counterpart to the GCCs: Sector Coordinating Councils (SCCs) are comprised of industry leaders, enabling alignment of strategies, policies, and planning, among other functions. CI sectors also have one or more Information Sharing and Analysis Centers (ISACs) that enable members to share information about threats and responses in a secure fashion. Several other mechanisms exist to create alignment within sectors and across them.

The 2017 *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* provides further executive direction on cybersecurity and critical infrastructure. The executive order directs relevant executive agencies to engage critical infrastructure stakeholders and

support cybersecurity risk management efforts. The order also requires that agencies use the NIST Framework for Improving Critical Infrastructure Cybersecurity to manage cybersecurity risk and submit a report on their cybersecurity to the President by early November 2017.^{lxxxvii}

Everything we’ve discussed so far could be considered to be the broad upper level of the CI universe (which we’ve represented in Figure 1). The upper level corresponds to national-level stakeholders, and it represents national-level interests. It has also received the lion’s share of attention and resources, focusing on broad, enterprise risk management among the CI sectors. At the narrowest level, too, there have been significant efforts – to protect citizens’ rights, security, and financial well-being.

Figure 1 // Levels of Critical Infrastructure Stakeholders



The states, including the Commonwealth of Kentucky, have been stalwart supporting partners to these efforts. However, parallel programs to organize and mature critical infrastructure governance frameworks from the perspective of states and individual organizations are less evolved. The time has come for increased focus on the “middle level,” with state, local, tribal, and territorial governments taking the lead in establishing durable security and risk management governance structures for CI assets of importance to their jurisdictions.

Kentucky’s role in protecting critical infrastructure

The discussion about who is responsible for protecting CI assets can become very complicated very quickly. Ownership and operation of a CI asset can be the responsibility of a federal agency, the military, a State agency, a local agency, a tribal agency, a territorial agency, a public-private partnership, a for-profit business, or a non-profit organization – and all are matters of interest to the general public. Complicating matters further, a single CI asset may be owned by a government entity and operated by a private business, each with different capabilities and interests.

















What is Kentucky’s role in protecting CI assets in the Commonwealth? Some of those assets are high priorities for the federal government, and they will command federal resources accordingly. But which assets are most deserving of the Commonwealth’s resources? It is imperative for state-level planners to differentiate between the various types of critical infrastructure within their state’s boundaries. Figure 1 depicts four “classes” of CI assets that are geographically located within Kentucky: national CI, defense CI, defense industry CI, and Kentucky CI. It also shows that – while the Commonwealth has the lead responsibility for Kentucky CI – it also has a supporting role to play for other assets.

Figure 2 // Categories of critical infrastructure located in Kentucky

CI CATEGORY	National	Defense	Defense Industry	Kentucky
LEAD AGENCIES	DHS	DoD	DoD + Commerce	KOHS + other KY agencies
GOVERNANCE FRAMEWORK	NIPP	Defense CI Program + DoD Mission-Based Critical Asset Identification Process	NIPP	Kentucky-specific governance framework
KENTUCKY'S ROLE	KOHS should proactively participate in and support NIPP initiatives	Kentucky should engage if requested by DoD, but the state is not a stakeholder	Kentucky has limited direct interest in the security of defense industry assets	Kentucky should actively assess and manage risk

This chapter primarily concerns itself with the rightmost column: critical infrastructure located in Kentucky for which the Commonwealth has the lead responsibility. Kentucky does (and should continue) to integrate directly with the federal structure, and KOHS (supported by the KIFC) has appropriately led the Commonwealth’s critical infrastructure coordination efforts. We suggest that the Commonwealth take this integration a step further. As the federal government has done, we recommend that Kentucky also establish a sector-specific state agency for each of the 16 CI sectors. While KOHS maintains primary responsibility for the protection of critical infrastructure throughout the Commonwealth, this action would facilitate the management of cyber risk, which we will discuss next. Table 1 lists the 16 CI sectors, the corresponding federal Sector-Specific Agency, the recommended Kentucky agency that should be made responsible for state-level CI, and an example of a corresponding digital state-level CI asset.

Table 1 // The 16 critical infrastructure sectors and corresponding Kentucky agencies

Sector	Federal Agency	Kentucky Agency	Digital Asset Example
 Chemical	Homeland Security	KOHS	Industrial control system at a chemical plant
 Commercial Facilities	Homeland Security	KOHS	Public announcement system at a mall
 Communications	Homeland Security	KOHS	Public notification system for emergencies
 Critical Manufacturing	Homeland Security	KOHS	Assembly system at an automobile plant
 Dams	Homeland Security	Division of Water	Dam monitoring and control system
 Defense Industrial Base	DoD	Department of Military Affairs	IT provider for a military network
 Emergency Services	Homeland Security	Division of Emergency Management	9-1-1 system
 Energy	Energy	Division of Energy	Industrial control system at a power station
 Financial Services	Treasury	Public Protection Cabinet, Dept. Financial Institutions	Revenue collection systems
 Food and Agriculture	Agriculture; Health + Human Svcs.	Department of Agriculture	Food inspection database
 Government Facilities	Homeland Sec.; General Svcs. Administration	Department for Facilities Management	Building access control system
 Healthcare and Public Health	Health + Human Services	Health Services Cabinet	Electronic medical records
 Information Technology	Homeland Security	KOHS	Data center for a major public university
 Nuclear Reactors, Materials, Waste	Homeland Security	Division of Public Health Protection and Safety	Reactor control system
 Transportation Systems	Homeland Security; Transportation	Transportation Cabinet	Air traffic control system
 Water + Wastewater Systems	Environmental Protection Agency	Division of Water	Public water contaminant monitoring

Adding the cyber dimension to critical infrastructure protection

Cyber risk adds another dimension to the critical infrastructure protection landscape at the state level. Managing cyber risk is vital to enhancing the security of critical state and local services, assisting organizations and the public to protect their intellectual property and personal information, and stimulating economic growth in high-wage knowledge industries. Several of the larger states have been proactive in this regard and have launched multi-stakeholder initiatives designed to reduce cyber risk by identifying threats, vulnerabilities, and mitigation strategies to protect state assets and industries. (Please see Chapter 9 for more details on these initiatives.)

The National Governors Association (NGA) strongly supports these individual efforts and has endorsed the proposition that the states collectively are essential players in the national cybersecurity effort. The NGA has invested significant resources to assist. In 2015, NGA launched a Resource Center for State Cybersecurity and Best Practices. The Center's goal is to help governors address growing cybersecurity responsibilities from their unique position as the public sector executive decision-makers nearest to commerce, manufacturing, transportation, education and training, workforce development, and public service delivery. The Center provides guidance and tools to assist in establishing governance strategies and offer best practices in working with both industry and the public in addressing technological threats. The NGA Resource Center draws heavily on generic "best practice" governance principles that are easily adaptable and are based on the principles of unity of effort, clarity of planning, and ease of implementation. This approach has the added benefit of creating transparency for business stakeholders and to ensure full access to federal resources with state assistance.

An analysis of successful cybersecurity programs in other states, coupled with best practices developed by the NGA, reveals a consistent, common element for success: the establishment of a proactive governance model. Under this "planning umbrella," all cybersecurity issues are addressed among state agencies and between the state and private sector partners. Issues are identified and addressed at the appropriate level, whether strategic or operational.

Like several other states, the Commonwealth of Kentucky has aggressively worked to improve the security of state systems and has been "forward-looking" relative to cybersecurity planning, information sharing, education, research, and workforce development. Several prominent examples include:

- establishment of a Chief Information Security Officer;
- centralization of cybersecurity strategy and planning for state agencies through the Commonwealth Office of Technology;
- creation of a Financial Cybercrime Task Force;
- recognition of the cyber threat in homeland security, law enforcement, and emergency strategic and operational planning;
- forming fundamental homeland security and information sharing partnerships;
- a nationally competitive Kentucky National Guard cybersecurity unit;
- an operational Kentucky Intelligence Fusion Center;
- a track record of cybersecurity exercises; and
- cybersecurity opportunities in higher education.

Leveraging this commitment to addressing the growing threat, the Commonwealth is poised to establish itself as a leading actor in the nation's cyber defense. The adoption of a robust governance model will jumpstart this effort, and we'll recommend one for Kentucky later in this chapter. But first, we must define the space: what is cyber critical infrastructure?

Establishing a definition for cyber critical infrastructure

While the definition of critical infrastructure (provided earlier in this chapter) is widely accepted, there is no uniform definition of *cyber* critical infrastructure (which we'll refer to as CCI). This is problematic, as CCI represents a distinct class of critical infrastructure assets that risk managers are charged with protecting every day.

It is important to point out that CCI overlaps significantly with the well-defined communications and information technology critical infrastructure sectors. The **communications sector** is often referred to as the “critical infrastructure of the critical infrastructures” as it is the “enabling function” across all the other sectors^{lxxxviii}. The **information technology (IT) sector**, which is dominated by large corporations, is comprised of the global Internet “backbone” or “the principal data routes between large, strategically interconnected computer networks and core routers on the Internet,” as well as a wide array of voice services, networks, systems and other interconnected commercial terrestrial, space, and wireless transmission systems that ride on it.

Nevertheless, CCI requires its own definition because it necessitates its own risk management approaches. To allow Kentucky's risk planners to clearly focus on the identification, prioritization, and implementation of protective measures for Kentucky's CCI, we propose the following definition:

What is Cyber Critical Infrastructure?

Digital and physical assets located in Kentucky
the **compromise** or **failure** of which
would **cause harm to critical functions** across the public and private sectors.

The definition divides CCI assets into two categories. The term **digital assets** refers to electronic information and the applications, systems, and networks used to generate, access, transfer, or store electronic information. Examples include citizens' health records and industrial control systems. The term **physical assets** refers to hardware, people, facilities, and other tangible infrastructure upon which the virtual assets depend to function. Examples include data centers, emergency operations centers, and essential operational and support personnel and equipment.

A **compromise**, often termed a security breach, is the digital equivalent of a physical intrusion. It occurs when a user or application gains access to data, an application, a system, a service, or a network without authorization to do so. A compromise can result in a degradation of the asset's operability, and/or the loss or corruption of data. A **failure** refers to the inoperability of the asset, and it may occur as the result of a compromise, an accident, or a natural disaster. Compromises and failures can be inconvenient, and they can go unnoticed in many cases. But if a compromise or failure causes **harm**, it would be categorized as a **cyber disruption event**.

Broadly speaking, harm is defined in two ways:

- a) impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks that provide direct information technology services or enabling and support capabilities for other services; and/or
- b) threatening public safety, undermining public confidence, having a negative effect on the state economy, or diminishing the security posture of the state.

Examples of cyber disruption events and attendant consequences include:

- a compromise of the power grid, leading to loss of power to a significant population;
- a compromise of a water treatment and delivery system, leading to a loss of potable water supply to a significant population;
- a compromise of financial management, healthcare, transportation, or education systems, leading to the disruption of essential services or loss of personally identifiable information;
- a compromise of government communications systems, which then hampers, interrupts, or prevents the operation of the government and requires implementation of a Continuity of Operations Plan;
- a compromise caused by malicious actors during a natural disaster, further complicating response and relief efforts; and
- a failure caused by a hurricane, flood, tornado, earthquake, or other natural disaster that impairs or destroys a data center, which then precipitates loss of connectivity or loss of data access and requires implementation of a Continuity of Operations Plan.

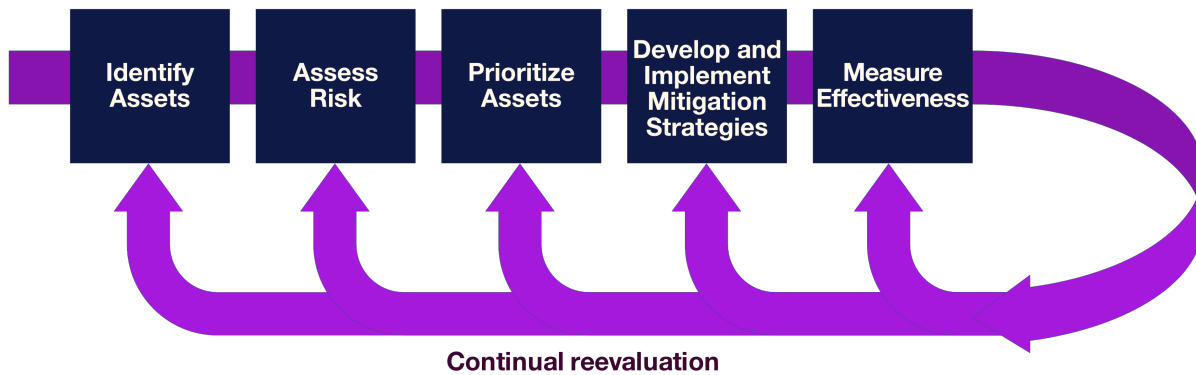
Cyber disruption events may have widespread, significant consequences, but they can have much smaller, insignificant beginnings. Among the most overlooked and easiest cybersecurity measures are locking doors, using shredders, and restricting access to hardware. Simple measures like these can plug many holes in an organization's cybersecurity posture.

A framework for CCI risk assessment

For state-level planners, the challenge is how to minimize the incidence and mitigate the impact of cyber disruption events. Successful planners view cybersecurity through the lens of risk management: how do we identify risks and prioritize application of our limited resources? Effective critical infrastructure risk management should prioritize the higher end of the risk spectrum where disruption of a network or system can cause large-scale loss of life, social disruption, economic harm, and loss of public confidence. Compromise of an industrial control system at a chemical plant, alteration of online health records, disruption of state revenue collection systems, and inability for police and emergency responders to field 9-1-1 calls are relevant examples for state level-risk managers. But to understand which specific CCI assets exist on the higher end of the risk spectrum, planners must implement a comprehensive risk management framework.

We propose that the KOHS Intelligence Fusion Center (KIFC) – which is taking the lead on identifying and prioritizing CCI within the Commonwealth – adopt the process represented in Figure 3. The framework will allow KIFC to determine whether an asset in question (AIQ) is, in fact, a CCI asset. It will enable a clear, understandable, and repeatable process. And it will facilitate the integration of methodologies already being used to protect critical infrastructure in Kentucky, which is particularly important in the case of the four lifeline sectors: water, transportation, energy, and communications.

Figure 3 // Proposed Kentucky CCI Risk Management Process^{lxxxix}



The proposed CCI risk management process has five phases: identify assets, assess risk, prioritize assets, develop and implement mitigation strategies, and measure effectiveness. Each phase is discussed in more detail below.

Step 1: Identify Assets

To identify assets, KIFC must first assemble a list of assets in question (AIQs). Assembling the AIQ list should be a thorough and deliberate process that considers every local jurisdiction in the Commonwealth. KIFC should review lists of previously considered physical CI assets, conduct open-source research, and solicit nominations from key stakeholders in each of the 16 CI sectors.

Next, KIFC must determine whether an AIQ is sufficiently critical to merit designation as a CCI asset. We propose two methods of doing this, and both methods should be applied for each AIQ. The first method addresses **criticality**, and considers five categories of criteria; in Table 2, we show these categories and include a question for KIFC risk planners to ask about the AIQ when conducting their assessment.

Table 2 // Criticality criteria

Category	Question to Ask
Legal	Is there a constitutional, legal, or policy requirement for the state government to protect the AIQ?
Provision of services	Is the AIQ vital to state government functions or to the provision of vital services to the public?
Critical capability	Does the AIQ enable a critical capability (e.g., emergency communications)?
Leadership-designated	Is the AIQ designated as “critical” by senior leadership based on priorities not listed above?
Federal status	Is the AIQ already categorized as a federal CI asset? ¹

¹ KIFC should hold discussions with owners of federal CI and establish agreed-upon protection MOUs to better plan for adequate incident response and asset protection.

The second method considers each AIQ within the context of **interdependency** of important state functions and systems. Table 3 details the different types of interdependency that can inform CCI asset identification.

Table 3 // Interdependencies

Type	Description	Example
Physical	Physical linkages between two systems; when one is impeded, the other is impacted.	The river barge system is closed due to inclement weather, halting grain shipments.
Cyber	Data transmission through the information infrastructure.	A targeted cyber attack against a government system prevents state employees from accessing databases.
Geographic	The local environment can impact the state of another infrastructure.	A dam breach causes a chemical spill at a downstream plant.
Logical	Interdependency based on a connection other than physical, cyber, or geographic, such as a regulatory interdependency.	Electrical sector regulations destabilize a financial market or undermine public confidence in the reliability of a given CI asset.

Once an AIQ has met any one of the criteria, or it is tied to a CI interdependency, KIFC should deem it critical. It is then considered a cyber critical infrastructure asset (CCIA).

The process here endeavors to provide some structure to CCIA identification, allowing for objectivity and comprehensiveness. But in practice, CCIA identification will sometimes be more art than science. To be effective, we encourage KIFC to focus on fundamentals, and not to be overwhelmed by complexity. Most state-level CCI is self-evident and has been directly or indirectly defined in other plans, such as Kentucky’s Continuity of Government (COG) Plan and the Emergency Operations Plan. The initial effort should ensure that these assets are correctly added to the CCI list.

Step 2: Assess Risk

The second step of the risk management process is risk assessment of CCIAAs. As detailed in Table 4, risk assessment considers three factors: threat evaluation, asset vulnerability, and the consequences of a successful attack on the CCIA.^{xc}

Table 4 // Risk factors

Factor		Explanation	Score range
T	Identification and assessment of threat level for the CCIA	Primarily external, threat refers to the capability and intent of malicious actors to disrupt the CCIA	1 to 5
V	Identification of the CCIA’s vulnerability level	Primarily internal, vulnerability refers to the exposure of the CCIA to cyber disruption event	1 to 5
C	Evaluation of an attack’s consequence on the CCIA	Primarily external, consequence refers to the adverse impact of a cyber disruption event	1 to 5

Risk (R) can be scored by averaging threat, vulnerability, and consequence

The factors above can be represented in an equation that will provide a quantitative “score” of the risk (R) associated with a CCIA, where $R = (C + V + T)/3$. The resulting numerical value is an approximate representation of a CCIA’s risk, where a higher number represents high risk and a lower number represents low risk. The following paragraphs explain how to assign values for each of threat, vulnerability, and consequence, in order to ultimately identify the risk level for each CCIA.

Threat should be assigned a value between 1 and 5. Table 5 provides KIFC with benchmarks that it should consider for assigning a particular score for a particular asset. It is important to keep in mind that these are only benchmarks to enable consistency. However, this is not a prescription for scoring; analysts will need to apply their judgment and expertise to each scenario. Threat benchmarks should be informed by intelligence assessments from Federal, state, and local government sources (including after-action reports from previous incidents); private and non-profit sector reports; and academic research. Attention should be paid to sectoral-level threat assessments, as increased malicious activity towards an asset (like a healthcare facility) may indicate an elevated threat level against other assets in that sector.

Table 5 // Threat scoring

Score	Threat benchmarks to consider
5	It is extremely likely that malicious actors will attempt a cyber disruption event. Threat actors are extremely motivated and highly capable. Multiple assets in this sector have been recently targeted.
4	It is likely that malicious actors will attempt a cyber disruption event. Threat actors are motivated and capable. Another asset in this sector may have been recently targeted.
3	It is possible that malicious actors will attempt a cyber disruption event. Threat actors have some motivation and some capability. Another asset in this sector may have been recently targeted.
2	It is unlikely that malicious actors will attempt a cyber disruption event. Threat actors may have motivation or capability, but not both. Another asset in this sector has been targeted recently, but not successfully.
1	It is extremely unlikely that malicious actors will attempt a cyber disruption event. Threat actors lack motivation and capability. Assets in this sector have not been targeted recently.

Vulnerability should be also assigned a value between 1 and 5. Table 6 provides KIFC with vulnerability benchmarks that it should consider. As with threat scoring, this is not meant to be prescriptive; analytic judgment should be applied for each scenario. Vulnerability benchmarks rely in large part on information provided by the CCIA owner or operator itself, meaning that developing an accurate vulnerability score can be challenging. Where available, KIFC should maximize use of reports developed following a vulnerability assessment of CI assets, taking care to focus on cyber-specific information when determining a vulnerability score. At the Federal level, the DHS Cyber Security Advisor for Region IV may prove a helpful resource for determining CCI asset vulnerability.

KIFC may also consider designing a secure survey that solicits information from CCIA owners. CCIA owners and operators may generally be reluctant to answer any questions about their cybersecurity posture, but avoiding length and specificity may encourage responses. Example questions may be:

- Do you use a cybersecurity risk management framework?
- Do you implement security protocols appropriate for your needs?
- Do you use the latest technologies appropriate for your needs?
- Do you have in-house or contracted cybersecurity expertise appropriate for your needs?
- Do you have a cybersecurity awareness program for your employees?

Table 6 // Vulnerability scoring

Score	Vulnerability benchmarks to consider
5	The CCIA is extremely exposed to a cyber disruption event. It lacks a risk management framework; implemented security protocols, current technologies, and cybersecurity expertise appropriate for its needs; and an employee awareness program.
4	The CCIA is very exposed to a cyber disruption event. It lacks four of the following: a risk management framework; implemented security protocols, current technologies, and cybersecurity expertise appropriate for its needs; and an employee awareness program.
3	The CCIA is exposed to a cyber disruption event. It lacks three of the following: a risk management framework; implemented security protocols, current technologies, and cybersecurity expertise appropriate for its needs; and an employee awareness program.
2	The CCIA is somewhat exposed to a cyber disruption event. It lacks one or two of the following: a risk management framework; implemented security protocols, current technologies, and cybersecurity expertise appropriate for its needs; and an employee awareness program.
1	The CCIA is minimally exposed to a cyber disruption event. It lacks none of the following: a risk management framework; implemented security protocols, current technologies, and cybersecurity expertise appropriate for its needs; and an employee awareness program.

Last but not least, **consequence** should be also assigned a value between 1 and 5. Table 7 provides consequence benchmarks for consideration. As with threat and vulnerability scoring, these benchmarks are meant only to guide scoring in a consistent way. The DHS Office of Cyber and Infrastructure Analysis (OCIA) is the lead Federal agency for conducting consequence analysis of critical infrastructure. Consequence analysis is still an emerging discipline, and KIFC should ensure its process for forecasting consequence is aligned with OCIA's.

Table 7 // Consequence scoring

Score	Consequence benchmarks to consider
5	A successful cyber disruption event would have an extremely significant impact. It would stop critical services for a long period of time; kill or injure large numbers of people; and/or lead to extremely high recovery costs.
4	A successful cyber disruption event would have a significant impact. It would temporarily stop critical services; kill or injure some people; and/or lead to high recovery costs.
3	A successful cyber disruption event would have a moderate impact. It would temporarily degrade critical services; injure some people; and/or lead to some recovery costs.
2	A successful cyber disruption event would have a minor impact. It would briefly degrade critical services; be unlikely to cause any injuries; and lead to minor recovery costs.
1	A successful cyber disruption event would have virtually no impact. It would not stop or degrade critical services; it would not kill or injure any people; and it would lead to negligible recovery costs.

Step 3: Prioritize Assets

Following the establishment of T, V, and C scoring for each CCIA, KIFC can calculate risk for each asset. We propose that KIFC organize assets into four tiers, as shown in Figure 4.

Figure 4 // CCI risk tiers



Asset prioritization will inform the discussion of resource allocation that accompanies mitigation strategy development, as discussed below.

Step 4: Develop and Implement Mitigation Strategies

Now that assets have been identified, given a risk score, and prioritized, strategies to mitigate the identified vulnerabilities and risks should be developed and implemented. This is a responsibility of the proposed Kentucky Cyber Council and Kentucky Cyber Steering Group, detailed below in the section titled, “*A cyber governance model for Kentucky.*” The Kentucky Cyber Council and Kentucky Cyber Steering Group should work with CCI owners and operators to improve their cybersecurity posture by implementing the National Institute for Standards and Technology’s Cybersecurity Framework (NIST CSF). For more on the NIST CSF, see Chapter 8: Risk Management.

Step 5: Measure Effectiveness

Effectiveness measurement is not a final stage; rather, it is a continual process. Identification of new assets, risk assessment of both new assets and re-assessment of older assets, and prioritization and mitigation are all steps that must be carried out on a rolling basis to ensure that Kentucky’s CCI is secure and protected. In addition to such ad hoc updating of risk identification and prioritization, KIFC should conduct a comprehensive review of all CCI assets every two years to ensure that the list accurately reflects current realities, and that resources are allocated in accordance with the latest understanding of cyber risk in the Commonwealth.

Information sharing

In the preceding section, we discussed the process for identification and prioritization of CCI and management of attendant cyber risks. Critical to that process is the healthy functioning of a streamlined and vibrant cybersecurity information sharing ecosystem, which empowers both enterprise-focused organizations (like a fusion center) and asset operators (like a power plant) to identify and resolve risks in a timely fashion. At all levels of government and within industry, information sharing organizations have been established to create this ecosystem.

At the Federal level of government, the Department of Homeland Security has established the Cyber Information Sharing and Collaboration Program (CISCP) at the National Cybersecurity and Communications Integration Center (NCCIC).^{xci} The CISCP is intended to foster a community of trust, and it enables participants to secure their networks. The program was established to facilitate information sharing and collaboration between CI owners and operators. The information sharing component provides participants with information on cyber threats, incidents, and vulnerabilities.

The program encompasses both government and industry partners that contribute threat data, thereby bolstering the strength and accuracy of the CISCP's analyses. Multiple steps are taken to ensure that sensitive data from industry partners is protected; any industry-provided Protected Critical Infrastructure Information (PCII) is exempted from release via Freedom of Information and State Sunshine laws and from regulatory use.^{xcii}

At the State, local, tribal, and territorial (SLTT) levels of government, the Multi-State Information Sharing and Analysis Center (MS-ISAC) is the preeminent resource for sharing cybersecurity information. The MS-ISAC serves as a focal point for identifying, protecting, detecting, responding, and recovering from cyber threats to SLTT governments. Membership is restricted to SLTT entities. Members have access to the following services and products:

- 24/7 security operations center
- Incident response services
- Advisories and notifications
- Access to secure portals for communications and document sharing
- Cyber alert map
- Malicious Code Analysis Platform (MCAP)
- Weekly top malicious domains/IP reports
- Monthly members-only webcasts
- Access to cybersecurity tabletop exercises
- Vulnerability Management Program (VMP)
- Nationwide Cybersecurity Review (NCSR)
- Awareness and educational materials

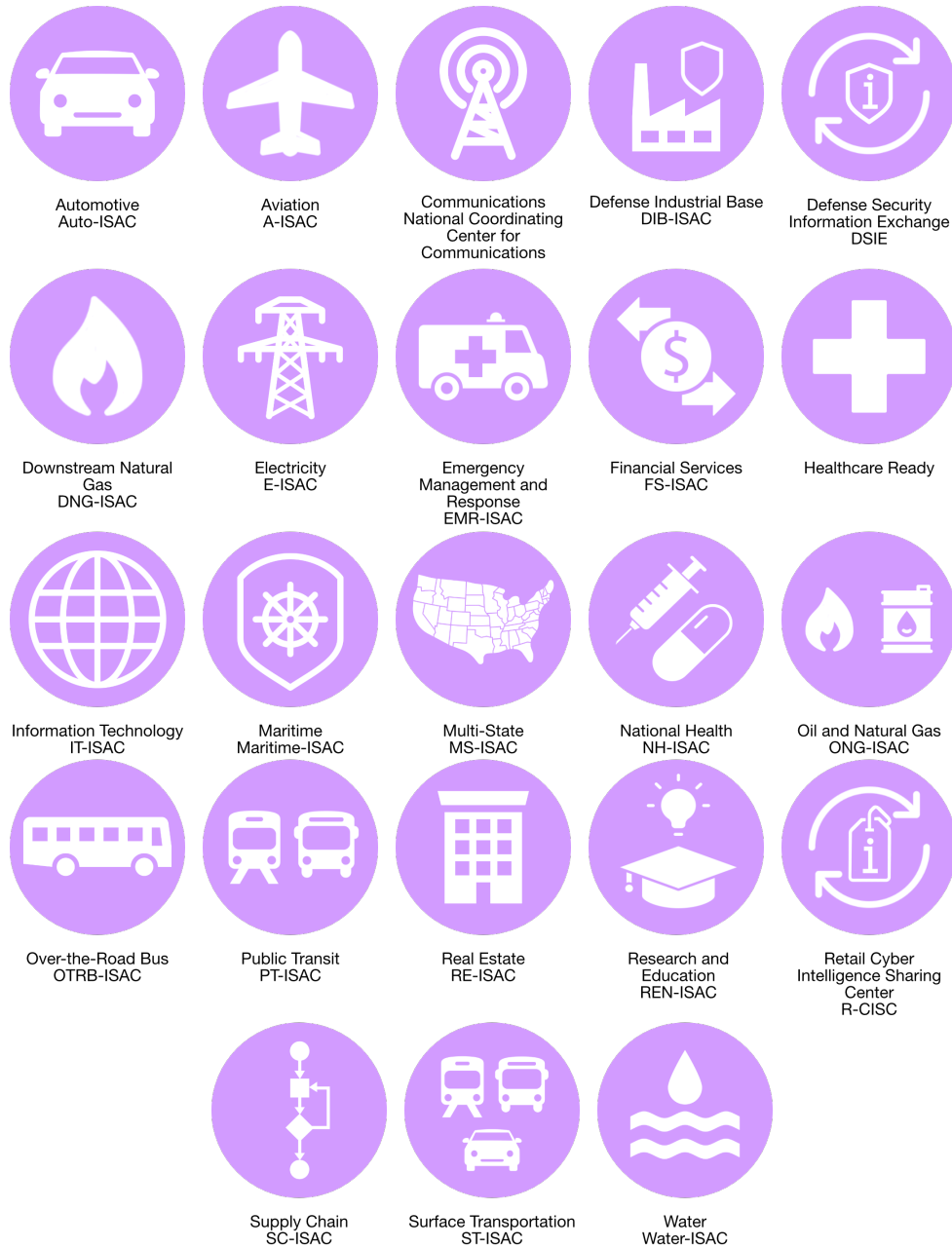
The MS-ISAC is managed by a non-profit organization, the Center for Internet Security, enabling its leadership structure to remain impartial and fostering the trust that is critical to effective information sharing. Every state government participates, and, in almost every case, is represented on both cybersecurity and homeland security issues. For Kentucky, COT participates as the principal office for cybersecurity issues, and KOHS participates for homeland security information. Notably, only three local governments in Kentucky participate: Frankfort, Louisville and Jefferson County, and Lexington. By contrast, neighboring Ohio has 26 participating local entities, including city and county governments and community colleges.

In the private sector, independent, industry-managed Information Sharing and Analysis Centers (ISACs) enable the secure sharing of cybersecurity information within critical infrastructure sectors and other communities of interest. The ISACs provide sector- and asset-specific threat information to assist members with security planning and response for both steady-state and heightened threat levels.

Because these ISACs are managed by industry for industry members, they lack the complicating factors (e.g., procedural or protocol-based) that government organizations introduce. Trust – which is the essential ingredient for effective information sharing – is therefore easier to establish and maintain, since a member company is not concerned that it may be exposed to liability risks that may present themselves when they share information with the government.

The National Council of ISACs is a coordination body for ISACs that provides for cross-sector partnerships and centralized representation to governmental entities. The National Council of ISACs members are represented below in Figure 5.

Figure 5 // National Council of ISAC members



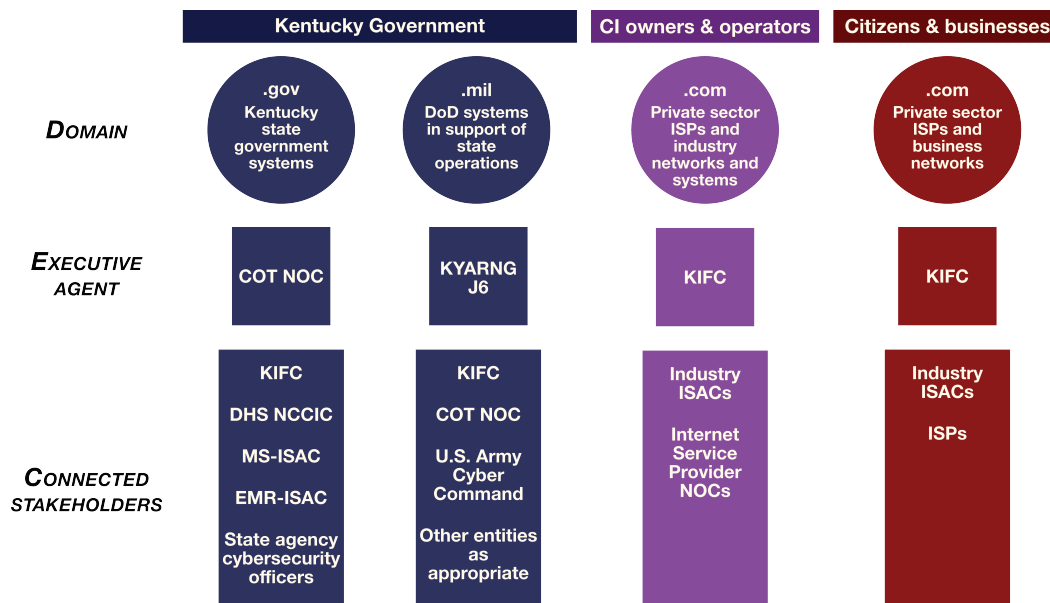
Through the NCCIC, DHS maintains open and regular communications with the ISACs by analyzing incident reports, facilitating the sharing of security best practices, and disseminating threat information in real-time. In this capacity, DHS also acts as an integrator of "sanitized" classified findings on specific threats collected and analyzed by the intelligence and law enforcement communities.

The CISC and the ISACs are only a representative sample of the intelligence analysis and information sharing organizations available to public and private sector CCI risk managers. On the one hand, the proliferation of these organizations is a positive development, validating the notion that information sharing partnerships are vital risk management resources for cyber planners. On the other hand, the proliferation of such organizations causes confusion, particularly for small to medium-sized businesses (SMBs), as to how and with which groups to participate in the larger cybersecurity and CCI discussions.

Our analysis of successful state-level information sharing structures shows that the proper organization and resourcing of an intelligence fusion center can be of enormous benefit to CCI owners and operators, businesses, and the public in managing risk. The KIFC is well positioned to serve as the principal conduit of cybersecurity information between the Commonwealth government, the owners and operators of Kentucky's critical infrastructure, Kentucky's businesses (especially SMBs), and Kentucky's citizens. The KIFC can be developed to provide a "one-stop shop" for cyber threat and information analysis, particularly for SMBs and individual citizens with limited resources.

COT (which will ultimately be home to a more formal network operations center, or NOC) and the Kentucky Army National Guard J6 each play principal roles in their respective "lanes": state government for the former, and military networks in support of the state for the latter. With the KIFC oriented towards industry and the public, the Commonwealth's cybersecurity information sharing ecosystem becomes complete. This ecosystem is represented in Figure 6.

Figure 6 // Proposed Kentucky information sharing ecosystem



In Chapter 10, we recommend the establishment of the Kentucky Cybersecurity Council (KCC), envisioned as the umbrella framework for Kentucky's statewide cybersecurity efforts. The KCC operates on a committee structure, and KOHS (and, by extension, KIFC) is recommended as the lead agency for two committees: critical infrastructure and public awareness. These committees are effectively the working groups for the purple and red columns in Figure 6, respectively.

Laws

Current laws in Kentucky

In 2014, Kentucky became the 47th state in the nation to adopt a law concerning notification of a data breach.^{xciii} Kentucky actually has two cybersecurity laws, House Bill 5 (HB5) and House Bill 232 (HB232), both of which deal with the protection of personally identifiable information (PII).

House Bill 5

Introduced by the Kentucky House of Representatives in January 2014 and signed into law by the Governor three months later, Kentucky HB5 addresses the PII held by Kentucky's state and local government agencies, including school districts and higher education institutions.^{xciv} The law directed COT to develop a coordinated framework for protecting PII, which would designate vital infrastructure, define methods for protecting that infrastructure, and establish a cybersecurity incident response plan. HB5 also includes a training and communication component designed to increase awareness of PII protection protocols and cybersecurity generally. Before October 1 of every year, COT must submit a report detailing security breaches within the executive branch, actions taken to resolve said breaches, and the security status of PII.

Agencies are required to notify the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General in the event of a security breach related to PII that they hold. If the subsequent investigation reveals that a breach did in fact occur, the agency is required to notify the individuals whose PII was compromised. However, if the agency determines that "the misuse of personal information has not occurred and is not likely to occur," even in the case of a security breach, then the agency is not required to notify individuals.

House Bill 232

Kentucky HB232 was similarly introduced in early 2014 and was signed into law by the Governor in the same year.^{xcv} Whereas HB5 explains notification requirements for state agencies that lose PII, HB232 focuses on PII loss by non-government information holders (defined as "any person or business entity that conducts business in this state"). In the event of a breach that results in the loss of a Kentucky resident's PII, businesses and individuals are required to notify the affected individual. Notification must be made as soon as possible, unless a criminal investigation requires delaying the notification protocols. Additionally, if an information holder must notify more than 1,000 individuals, the information holder must also notify consumer reporting agencies and credit bureaus that "that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices." This definition does not include the Kentucky Attorney General's Office of Consumer Protection, which, as a state office, presumably does not maintain files of consumer notices on a national scale.

How other states address key cybersecurity issues in the law

State laws typically address three categories of issues related to cybersecurity: breach notification and privacy, risk management, and cyber crimes. Here, we highlight a few notable examples of laws that have been passed in other states.

Breach notification and privacy

Almost every state in the nation (New Mexico will be the 48th state, as of June 2017) has a law requiring at least some information holders to issue notifications if PII has been lost or stolen.^{xvii} But who is required to notify, whom is required to be notified, and under what circumstances notification occurs varies by state. In three states we reviewed closely (Maryland, Washington, and Michigan), there is no indication that the state government has an explicit “right to know” if an individual’s PII is involved in a security breach.

Since 2008, Maryland has required that businesses notify citizens in the event of a security breach that affects the security of their PII. In these cases, businesses must also notify the Maryland Attorney General of the breach.

In Washington, any person or business that holds PII and experiences a security breach must notify citizens of the breach. The additional requirement of notifying the Washington Attorney General is placed on health insurers, financial institutions, and any company that has to notify more than 500 Washington residents.

Michigan does not require businesses to notify the state government or Attorney General in the event of a security breach. However, health insurers, financial institutions, and public utilities have special notification requirements.

Risk management

State laws do not typically impose cybersecurity risk management requirements on businesses, with the exception of highly regulated industries.

The Maryland Cybersecurity Council, created by legislation in 2015, reviews and conducts risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks. In service of this mission, the council is compiling a list of CCI. Beginning in July 2017, the council is required by law to submit a biannual report on CCI to the Maryland legislature.

In Virginia, the state’s Chief Information Officer manages the complete risk management program for the state. This responsibility, among others, is codified in the Code of Virginia Chapter 20.1 §2.2-2009. However, there is no explicit mention of cybersecurity in Virginia’s risk management program.

In 2011, Washington Senate Bill 5931 directed the Department of Enterprise Services to create an Office of Risk Management for the purpose of implementing a risk management policy delineated in Revised Code of Washington 43.41.280. However, that framework makes no mention of CCI.

The Michigan Department of Technology, Management and Budget handles the risk management plans for state government, but there is no mention of cybersecurity and critical infrastructure as they are related to statewide risk management. Section 18.1204 of Michigan Compiled Laws details the department’s specific risk management responsibilities.

Cyber crimes

The definition of a cyber crime varies from state to state, although the differences often pertain to the degree of specificity articulated by the law (rather than more substantive distinctions).

While Maryland defines cyber crime as the unlawful access of a computer, Virginia is very descriptive in its list of computer-related crimes and penalties. Virginia includes computer fraud, spam, computer trespass, computer invasion of privacy, computer use to gather PII, theft of computer services, personal trespass by computer, harassment by computer, computer as an instrument of forgery, and encryption used in a criminal activity. This list of cyber crimes has been amended and augmented multiple times between 1984 and 2015.

Like Virginia, Washington has passed cybercrime legislation. The 2016 legislation focuses on computer trespass, or unauthorized computer access, spoofing (communication under false pretenses with a victim in order to gain unauthorized access to the victim's electronic data), electronic data tampering and theft, and the use of computers in the commission of other crimes. The laws are based on STRIDE, a computer security threat modeling system developed by Microsoft. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Michigan's law concerning fraudulent access to computers took effect in 1980 and was most recently amended in 2004. The laws broadly concern unauthorized access to computers and the usage of computers in the commission of other crimes.

How Kentucky has addressed key cybersecurity issues in the law

Our review of Kentucky's laws – the Kentucky Revised Statutes (KRS) – considered the same three categories as discussed above.

Breach notification and privacy

In the event PII held by Kentucky government agencies is lost or stolen, the data-holding agency is required to notify the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General. There are no statutes in the KRS that direct non-government information holders to notify the state in the event of a data breach. KRS 365.732 and 365.734 require non-government information holders to notify Kentucky residents of PII loss or theft. *This means that, unless law enforcement opens an investigation into a security breach of data held by a private business or individual, state government is not notified and does not have a record of such security breaches.* There is also no indication that organizations or individuals that share information with the government regarding a breach of their own networks enjoy protection from liability.

While information holders are required to notify individuals of a security breach involving PII, there does not appear to be a statutory requirement for information holders to protect PII. Minors are not given any special designation with regard to their personal data, and there is no indication of an individual's right to know if his or her data is stolen. However, citizens can bring a civil suit against businesses that fail to comply with Kentucky law regarding PII.

Risk management

Kentucky law does not require critical infrastructure owners to implement cyber risk management protocols. *The term "critical infrastructure" is mentioned once – in KRS 257.495. One other instance, KRS 61.878 1.(m)1.f., can be considered as referring to critical infrastructure, although it does not use that specific term.* Critical infrastructure, as defined by 42 U.S. Code, section 5195c(e), refers to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such

systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” This definition is referenced in KRS 257.495, which describes the confidentiality of information and makes exceptions for its disclosure as it relates to critical infrastructure.

Cyber crimes

KRS 434.840 to 434.860 concern crimes relating to the unlawful access of computers. The statutes were last updated in 2002. Gaining or attempting to gain unlawful access to a computer without consent is a crime in Kentucky, with specific classifications (from misdemeanor to felony) depending on the monetary loss or damage caused by the unlawful access. For example, unlawful access to a computer that results in less than \$300 of loss or damage will result in a Class A misdemeanor, while loss or damage greater than or equal to \$300 is a Class D felony.

KRS 434.855 describes the misuse of computer information, which includes receiving or concealing information gained through unlawful computer access or aiding in the unlawful act.

Gaps in the law

Our review identified two gaps in Kentucky’s cybersecurity laws that some other states have chosen to address through their own legal frameworks:

- Kentucky does not require businesses and individuals to disclose to the government a security breach that resulted in loss of PII. As a result, there is no mechanism for the state to track these breaches. Some other states require businesses and individuals to notify the Attorney General.
- Kentucky does not require critical infrastructure owners and operators to adopt a specific risk management framework. As we discuss in this chapter and in Chapter 8, it is vital that such organizations do so, and states like Maryland are proactive in explicitly urging or requiring the analysis of state critical infrastructure through the lens of cybersecurity. However, most states do not appear to require a risk management framework for cyber critical infrastructure.

That said, we recognize that not every gap needs to be addressed by the law; the Commonwealth may pursue other avenues, or it may choose to leave these gaps untouched. Each state is different, and culture, economics, and politics all play a role in shaping the legal system. Nevertheless, it worth highlighting these gaps for the Commonwealth’s consideration.

The Commonwealth Cybersecurity Committee

"[S]tates should contemplate creating a governance body, or increasing a relevant state agency's authority, that is responsible for implementing a response plan, and eventually expanding their scope to implement the statewide cybersecurity strategy."

**National Governors Association
Statement to Governors on Confronting Cyber Challenges 2016-2017**

Purpose

In light of our review and guidance from leading organizations like the National Governors Association, we propose that Kentucky's state government establish the Commonwealth Cybersecurity Committee (C3). The C3 should be considered a formalization of the internal cybersecurity working group already led by COT. It will accomplish the following goals:

- provide accountability, structured decision-making, and enterprise direction for cybersecurity;
- ensure risk assessments are conducted and resources allocated accordingly;
- implement continuous vulnerability threat monitoring practices;
- ensure compliance with current security methodologies and business disciplines; and
- create a culture of risk awareness.

The C3 is derived from benchmarking against other similar statewide models, adopting best practices offered by the NGA, and leveraging existing organizational bodies already established by the Commonwealth. It also aligns with established federal planning and response structures. And most importantly, it builds on the excellent work already being done by COT and IT professionals throughout the Commonwealth government. The C3 therefore does not represent a major overhaul; instead, it is an evolutionary step to hone the government's existing internal cybersecurity governance.

The establishment of the C3 should be directed by the Governor through an Executive Order. Although the Governor will not be involved in day-to-day execution, the C3 should be stamped with this executive-level authority and, accordingly, it should be accountable to the Governor.

Organization

The C3 should be chaired by the COT Chief Information Security Officer (CISO), who reports to the Chief Information Officer (CIO). Core membership should include COT leaders and senior IT professionals from other state government agencies. The C3 should also involve a wider group that includes a cyber risk manager from KOHS, an emergency response planner from KYEM, a cybersecurity representative from the Kentucky National Guard, and training, workforce, and budget personnel as necessary. The C3 should meet every two months, and the wider group should attend every other meeting.

Responsibilities

The C3 will be responsible for strategic guidance of the Commonwealth's IT security enterprise and for developing and advancing policies to support agency missions and special requirements. It addresses enterprise issues security such as risk management; shared-service agreements; capital improvement

projects; large resource investments and budgeting; workforce acquisition, training and development; outsourcing decisions; and adoption of transformative policies and technologies.

The C3 will also facilitate coordination, direction, change management, and planning for day-to-day cybersecurity issues. To do this, the Commonwealth should fully resource an advanced network operations center (NOC) within COT. During elevated threat conditions, the C3 (via the COT NOC) would serve as an operational conduit into all agencies and programs to facilitate response efforts. The C3 would be responsible for:

- conducting (for state government assets) risk assessments, identifying system vulnerabilities, and developing mitigation strategies;
- overseeing compliance with technical control programs (e.g., password protection and physical security);
- conducting joint planning for shared services;
- maintaining and exercising all cybersecurity prevention, response, and recovery plans, as well as approving state government assets for inclusion on the Cyber Critical Infrastructure Asset list; and
- executing a training and awareness program for state government employees.

Recommendations

Our governance recommendations can be divided into two levels: strategic and operational. Strategic recommendations are higher-level and involve leadership roles, responsibilities, and actions. Operational recommendations are more specific and speak to particular steps that agencies can take to begin to improve cybersecurity resiliency.

Strategic

- **Establish the C3, following a validation process.** The proposed model is intended to build on existing efforts and the gains made to date. Therefore, it should be submitted to COT and key stakeholders for review and revision. Following this validation process, we recommend that the proposed construct be codified through executive order.
- **Establish executive support.** Per our review of other states (fully documented in Chapter 10), the public backing of the Governor has proved vital to the success of cybersecurity initiatives promulgated throughout state government. In addition to the suggested executive order, we recommend including language in the Governor's strategic plan making cybersecurity a priority across the state government.
- **Designate state-level sector-specific agencies.** While the responsibility for coordinating critical infrastructure protection efforts in Kentucky falls to KOHS, we recommend that Kentucky mirror the Federal framework of assigning a sector-specific agency for each of the 16 critical infrastructure sectors.
- **Expand the data breach notification law.** As mentioned earlier, the law may not be the appropriate avenue for addressing certain cybersecurity issues. Kentucky's laws and policies regarding cybersecurity are in good standing when compared to those of other states. However, there is one instance in which the KRS is deficient: When a business or individual experiences a security breach that results in the loss of PII, they are required to notify the citizens whose PII was affected, but the government is not made aware. The Kentucky legislature should require those individuals and businesses to also notify the Office of Attorney General of the breach and PII loss.

Operational

- **Formalize a concept of operations for the KIFC's cybersecurity mission.** As discussed in the section on information sharing, KIFC is well-positioned to be the "one-stop shop" for the sharing of cybersecurity information between government and industry. This expansion of KIFC's role should be met with sufficient resourcing to ensure it can fulfill this vital function.
- **Adopt the proposed Kentucky CCI Risk Management Process.** Following a validation process by KIFC and key stakeholders, we recommend that the process (as shown in Figure 3 and elaborated upon in the accompanying narrative) become KIFC's approach to identifying and managing risk across the Commonwealth's CCI.
- **Host a workshop for the first iteration of the CCI Risk Management Process.** KIFC should host a full-day workshop for key stakeholders from KOHS and Kentucky's sector-specific agencies. The purpose will be to educate stakeholders on the CCI Risk Management process and to generate a comprehensive list of assets in question (AIQs). Stakeholders should nominate AIQs on an annual basis, although a refresher workshop may be necessary on a biennial basis.

CHAPTER

6

Defense
Partnerships +
Emergency
Management



Chapter 6 | Defense Partnerships + Emergency Management

One key to a successful critical infrastructure program is the strength of partnerships between the Department of Defense and state governments. State governments are right to cultivate those partnerships by investing time and resources in defining roles and responsibilities, “stress-testing” them through exercises, and formalizing them through memoranda of understanding. In an emergency, those partnerships will be put to the test. In this section, we’ll discuss emergency management in the cyber context, and we’ll provide a high-level overview of key Kentucky emergency management resources, as well as military entities based in Kentucky. We’ll also provide recommendations for how the Commonwealth can strengthen partnerships between its emergency management resources and military installations in Kentucky to improve Kentucky’s resilience in the case of an emergency.

Emergency management in the cyber context

For state government systems, Kentucky has made enormous strides in moving cyber preparedness from for the server room to the boardroom. As documented in Chapter 5, the Commonwealth Office of Technology has institutionalized sound cyber prevention, mitigation, response and recovery processes for both steady-state operational and for non-cyber state-wide emergencies. Kentucky also has established a top-flight emergency response structure and delivery system.

However, it is conceivable that emergency management and cybersecurity functions are tracking and mapping the same event with little or no interaction or awareness. This orchestration of efforts – particularly when it involves the competing authorities of military, other government, and industry assets – is essential to effective CCI threat response. The challenge ahead is to expand Kentucky’s emergency planning efforts to account for the full spectrum of cyber threats – scaling from “steady-state” network threats, to local disruptions, to regional disasters, to national catastrophes.

Such cyber threats may initially manifest themselves with the incapacitation or derogation of state-managed or -coordinated activities such as local power, water, transportation or emergency services, registering first with the emergency management and local law enforcement communities. Though the initial indicators may be localized, the consequence may not be. The potential scope of a cyber disruption event adds a new dimension to traditional emergency management planning and response.

The August 2014 promulgation of the Kentucky Emergency Operations Plan (EOP) goes a long way in positioning the Commonwealth to be more resilient to cyber risk. The 2014 revisions to the EOP were forward-looking and will aid significantly in the easy synchronization with the cyber governance model proposed in Chapter 5. Highlights include:

- Adoption of the Homeland Security Act and Presidential Homeland Security Directives 1 through 12 as guiding directives;
- Listing of cyber-terrorism as a “high probability” threat;
- Emphasis on an “all-hazards” planning approach;
- Acknowledgement that “the most likely (man-made) threat is a coordinated and prolonged cyber-attack on the U.S. electrical grid that could result in a power outage across the Commonwealth for a prolonged period during the summer months.”

- Clarification and updates to the roles and responsibilities of the Commonwealth’s Systems and Communications Group (CSCG)/ESF 2; and Energy and Utility Services /ESF 12 (Energy Management Response Board included). Basic recognition of major cyber response components including the State Fusion Center, KYARNG J6 and DHS National Cyber Security Division.
- Designation of the Kentucky Office of Homeland Security (KOHS) as the coordinating agency between the Commonwealth and DHS for management of critical infrastructure issues and liaison to FBI for terrorist (including cyber) incidents.

At the national level, considerable progress has been made to address public/private sector response to large scale attacks on critical cyber and physical infrastructure. *Presidential Policy Directive – 41: United States Cyber Incident Coordination* (PPD–41) outlines processes, guided by the National Response Framework (NRF), to monitor, respond and recover from “significant cyber events” (read: regional level and above disruptive events). PPD–41 mandates the use of the National Incident Management System (NIMS) for coordination between cyber and physical response processes and integration of threat and reconstitution efforts. NIMS is the recommended protocol for managing cyber incidents, and major disruption or a “blended” physical and technological attack.^{xcvii}

Also relevant to this discussion, the PPD directs several follow-on tasks to ensure its full implementation. It requires that DHS to “develop and finalize the National Cyber Incident Response Plan – in coordination with State, Local, Territorial, and Tribal governments, the private sector, and the public – to further detail how the government will manage cyber incidents affecting critical infrastructure.” In the near future, federal and state cyber response planning efforts will need to align as the physical preparedness and response processes do under the NRF. Kentucky will be well positioned to easily assimilate the changes.

Many of the states that have placed a premium on cybersecurity and economic development as a strategic initiative have formalized the operational components into a comprehensive response plan that is harmonized with other incident specific emergency management plans. Michigan’s efforts in this area have been particularly noteworthy and its cyber plan is considered a benchmark document for other states. For example, the Federal Emergency Management Agency lists the Michigan Cyber Disruption Response Strategy as an innovative, best practice on its Lessons Learned Information Sharing webpage - [LLIS.gov](https://llis.gov).^{xcviii} Michigan’s approach is also cited by the National Association of State Chief Information Officers (NASCIO) as comprehensive and far-reaching blue-print for building a stand-alone cybersecurity strategy and associated operational structure (see Chapter 5). NASCIO has developed a comprehensive Cyber Disruption Response Planning Guide^{xcix} and offers it as:

“A call to action for states to develop state cyber disruption response plans that include: a governance structure that clearly designates who is in charge in a given event or phase of an event; development of a risk profile for state assets; collaboration among the various agencies that have cyber responsibility; and a communication plan to ensure the right people have the right information as early as possible so they can respond effectively.”

This NASCIO guidance, adapted from Michigan’s approach, also leverages the strengths of key longstanding emergency management principals including: unity-of-effort, common operating picture, pre-event planning, partnership and information sharing.

For the sake of clarity, the discussion above is not an argument for Kentucky’s emergency management structure to be placed “in charge” of CCI assessment and mitigation, preparedness, response and recovery processes. Rather, it is an endorsement of existing emergency management constructs in Kentucky – and that the Commonwealth need not reinvent the wheel to manage a cyber emergency. Instead, CCI should be addressed and resourced as a stand-alone concept in the EOP.^c

Key emergency management resources

The EOP is comprehensive; we do not intend to revisit the roles and responsibilities of key actors that are well established in both. But to frame the discussion about partnerships, it is important to highlight a few non-military resources that play an important role in emergency management in the Commonwealth – particularly when it comes to managing a cybersecurity emergency. Those resources are listed in Table 1.

Table 1 // Kentucky Emergency Management Resources

Resource	Description
Kentucky Emergency Management (KYEM) Emergency Operations Center (EOC)	KYEM is responsible for managing the Commonwealth’s response to an emergency. From its base at the EOC, it coordinates state resources and information sharing with relevant stakeholders. Its roles and responsibilities are detailed in the Kentucky EOP. ^{ci}
Kentucky Office of Homeland Security Intelligence Fusion Center (KIFC)	KIFC coordinates the sharing of threat information between all levels of government and critical infrastructure owners and operators. KIFC is establishing itself as the Commonwealth’s hub for cybersecurity information sharing with industry.
Commonwealth of Technology (COT) Network Operations Center (NOC)	COT’s NOC maintains the security and integrity of state government networks. In the event of a compromise or failure of a state government CCI asset, COT’s NOC would play a key role in response and recovery.
Kentucky Public Service Commission (KPSC)	The KPSC has quasi-judicial and quasi-legislative power with regard to over 1,500 utilities in Kentucky. It is a useful source of expertise and authority concerning utilities in the event of an emergency.

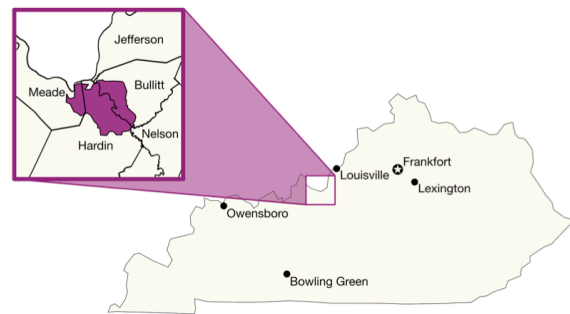
Department of Defense installations in Kentucky

The Department of Defense (DoD) plays a significant role in Kentucky's economy, workforce, and culture. In fiscal year 2015, DoD spending accounted for 4.7% of Kentucky's Gross Domestic Product – the ninth-highest percentage of any state in the nation.^{cii} The DoD is also the largest employer in the Commonwealth by far: its 38,700 active duty and civilian employees constitute a workforce nearly twice the size of the nearest employer – and that's before another 15,421 Reserve and National Guard personnel are included in the count.^{ciii}

Aside from a concentration of smaller DoD facilities in the Louisville area, the DoD's presence is primarily spread across three military installations: Fort Knox, Fort Campbell, and Blue Grass Army Depot. In addition to being the bedrocks of their local communities, these installations are strong partners for the state government. The Commonwealth can continue to cultivate these partnerships, particularly in the context of managing cyber emergencies. In this section, we profile these installations.

==== FORT KNOX ====

Size	109,000 acres
Active Duty, Guard, Reserve	6,500 employees (2014)
Civilians	4,800 employees (2015)



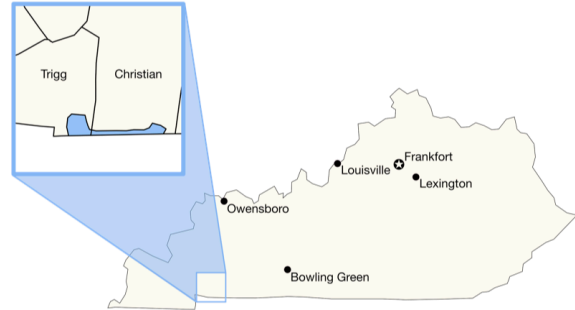
Just south of Kentucky's largest city, Louisville, and across the Ohio River from Indiana, Fort Knox is the largest DoD installation located entirely in Kentucky. Home to the United States Bullion Depository – where the United States Treasury stores 60% of the country's gold reserves^{civ} – Fort Knox is recognized internationally as a symbol of both impenetrable strength and American prosperity.

Although it is most famous for protecting the nation's gold, much of the activity at Fort Knox focuses on career development for soldiers: it is the headquarters for U.S. Army Cadet Command, U.S. Army Recruiting Command, and U.S. Army Human Resources Command. Fort Knox also features significant training assets, including the 84th Training Command, Army Reserve Readiness Training Center, 100th Training Division, and 4th Cavalry Brigade. It is truly a multifunctional installation; home to more than 35 Army and Army Reserve elements, 4 Kentucky Army National Guard elements, a small group of Air Force and Marine Corps elements, and an array of other defense and federal functions.

From a cybersecurity perspective, the most relevant resource is the Fort Knox Network Enterprise Center (NEC) The NEC is responsible for the security and functionality of the installation's information technology systems and networks.^{cv} Fort Knox's network – the Fort Knox Installation Campus Area Network (FKICAN) – belongs to the Western Region of a much larger infrastructure called the Department of Defense Information Network, or DoDIN.^{cvi} Accordingly, the NEC is actually part of a much larger enterprise responsible for protecting DoD systems and networks.

==== FORT CAMPBELL ====

Size	112,000 acres (KY + TN)
Active Duty, Guard, Reserve	30,000 employees (2014)
Civilians	2,300 employees (2015)

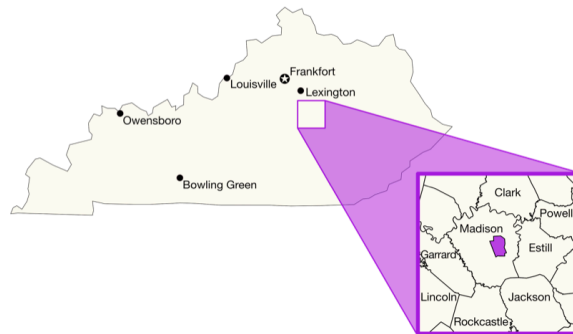


Fort Campbell is unusual in that it straddles the state border between Kentucky and Tennessee. Although more than 90% of Fort Campbell is geographically in Tennessee, its post office is in Kentucky – meaning that, from the perspective of the Army and the Federal Government, the installation is located in Kentucky. Home to the fifth largest military population in the Army, Fort Campbell employs nearly 60% of Kentucky’s entire uniformed military workforce.^{cxvii} In terms of local impact, that workforce constitutes almost half of the entire population of Christian County. The Christian County Chamber of Commerce has its own committee for military affairs, and it is being recognized by the Association of Defense Communities as part of its 2017 class of Great American Defense Communities.^{cxviii}^{cxix}

Fort Campbell is home to the only Air Assault Division in the Army: the 101st Airborne Division. The 101st is the installation’s anchor force, and major tenants include 5th Special Forces Group (Airborne), 160th Special Operations Aviation Regiment (Airborne), the 52nd Ordnance Group (EOD), and several healthcare (medical, dental, and veterinary) facilities.^{cx} From a cybersecurity perspective, the most relevant resource is Fort Campbell’s Regional Network Enterprise Center (RNEC) – Bluegrass. RNEC-Bluegrass is responsible for the integrity of the systems and networks used by Fort Campbell personnel.

== BLUE GRASS ARMY DEPOT ==

Size	14,500 acres
Active Duty, Guard, Reserve	N/A
Civilians	900 (2015)



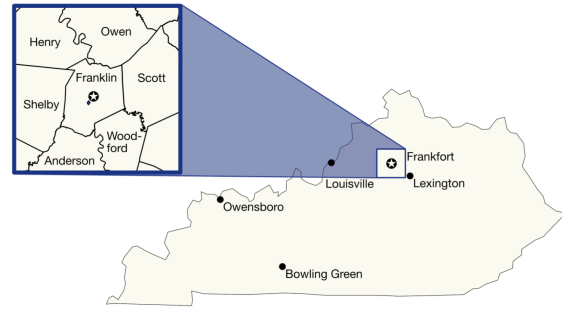
A much smaller facility than either Fort Knox or Fort Campbell, the Blue Grass Army Depot (BGAD) is staffed by a relatively small civilian workforce under the command of an Army colonel. BGAD is used for the storage, distribution, and destruction of munitions – both conventional and chemical.^{cx} It services Army units throughout the Southeastern U.S. and also those supporting missions overseas.^{cxii}

BGAD also houses the Blue Grass Chemical Activity (BGCA) and its stockpile of 523 tons of chemical weapons. In 1997, the United States ratified the Chemical Weapons Convention (CWC), which banned such weapons.^{cxiii} To comply with the CWC, the Program Executive Office, Assembled Chemical Weapons Alternatives (PEO-ACWA) has contracted with Bechtel Parsons Blue Grass to design and build the Blue Grass Chemical Agent-destruction Pilot Plant (BGCAPP), where the stockpile will be safely destroyed.^{cxiv} BGAD employs a highly skilled workforce of engineers and chemical experts, and it fills an important role in Kentucky’s emergency management landscape. Through the Chemical Stockpile Emergency Preparedness Program, BGAD is already well integrated with state and local emergency management professionals and response structures.^{cxv}

**BOONE NATIONAL
GUARD CENTER**

Size 655 acres

Army National Guard 6,600 employees (2016)*



**This figure includes all Kentucky Army National Guard service members in the Commonwealth, including those not stationed at the Boone National Guard Center*

Located just south of Kentucky’s capital, Frankfort, Boone National Guard Center houses Joint Forces Headquarters Kentucky and is the headquarters of the Kentucky Army National Guard (KYARNG).^{cxvi} BNGC also houses the 63rd Aviation Brigade^{cxvii} and the main office of Kentucky Emergency Management, which is a division of the Kentucky Department of Military Affairs.^{cxviii}

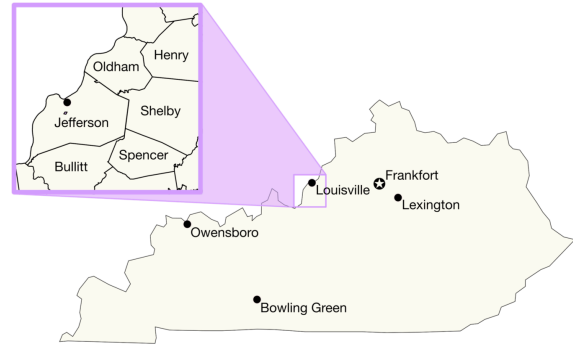
In addition to its military obligations as a component of the U.S. Army, the Kentucky Army National Guard is an important component of Kentucky’s emergency response apparatus. KYARNG can be called upon to provide support and assistance to state response and recovery efforts, and its emergency response capabilities extend beyond traditional logistics and transportation capacities.^{cxix}

The Kentucky Army National Guard J6 Command, Control, Communications & Computer Unit is located at Boone National Guard Center. A critical component of KYARNG and an asset for the commonwealth at large, J6 manages the federal DoD network that the Kentucky Army National Guard and KYEM rely on for operations. (However, some KYEM networks are not under the control of the J6.) In the event of an emergency, J6 manages the network that makes Kentucky’s response and recovery efforts possible.

As J6 is well versed in cutting-edge technologies, tactics, and techniques, it represents an important asset to the Commonwealth. The KYARNG has been recognized as an important player in the cyber landscape on a national level; the National Guard has announced plans to establish an Army National Guard Cyber Protection Team in the Commonwealth by FY19.^{cxx} Working in conjunction with J6, this new unit has the potential to add immense value in defining and maturing cybersecurity assessment, protection, response, and recovery processes.

KENTUCKY AIR NATIONAL GUARD BASE

Size	N/A
Army National Guard	1,210 employees (KY, 2016)



**This figure includes all Kentucky Air National Guard service members in the Commonwealth, including those not stationed at the Kentucky Air National Guard Base*

The Kentucky Air National Guard Base is located at Louisville International Airport, and it is the headquarters for the Kentucky Air National Guard (KANG). KANG fulfills a number of missions, including Air Mobility, Special Operations, Explosive Ordnance Disposal, Homeland Defense, and Intelligence, Surveillance, and Reconnaissance. Special Operations Missions include Special Operations Aircraft, Combat Control, Combat Weather, and Pararescue.^{cxxi}

The base is home to the 123rd Airlift Wing, which, in addition to the tasks listed above, provides airlift capabilities, contingency response, special operations, civil engineering, medical support and operations, and explosive ordnance disposal. The 123rd's units include the Mission Support Group, Maintenance Group, Operations Group, Medical Group, and Contingency Response.^{cxxii} From an emergency management and critical infrastructure perspective, the 123rd represents a valuable logistics and disaster response resource.

Recommendations

DoD installations play an important role in the Commonwealth. But in an emergency management context, it is important to emphasize that the assets at those installations are under Federal control. In other words, the President would need to authorize the use of those assets to fulfill a civil support function in the case of an emergency. (A key exception to this is the U.S. Army Corps of Engineers (USACE), which serves both military and civil missions.) The roles of the DoD, USACE, and other Federal agencies like the United States Coast Guard are well documented in the Kentucky EOP.

At the command of the Governor of Kentucky through the Adjutant General, the military assets of the Kentucky National Guard will fulfill a frontline function in the case of an emergency, and they are well equipped to do so. Likewise, the roles and responsibilities of the Kentucky Army National Guard and Kentucky Air National Guard are well documented in the EOP.

But for the EOP to function well in practice, the DoD, the Kentucky National Guard, and Commonwealth agencies must pursue and maintain strong partnerships. The increasing prominence of cybersecurity on the Commonwealth's agenda presents an excellent opportunity to enhance those partnerships. Pursuant to our recommendations in Chapter 5, we offer the following recommendations:

- **Integrate cybersecurity into the EOP.** The EOP does address the threat of cyber terrorism, and it has a well-documented concept of operations for Emergency Support Function (ESF) 2: Communications. Moreover, COT has a cyber incident response plan for state government functions. However, the EOP should document the Commonwealth's processes for managing a cyber disruption event that affects CCI outside of the public sector.
- **Capitalize on the cybersecurity capability of the KYARNG.** The KYARNG is rapidly establishing itself as a cybersecurity leader among its peers in other states. Currently a primary agency for ESF 2, the J6 is already one of the state's foremost cybersecurity centers of excellence. The Commonwealth should consider expanding its cybersecurity roles and authorities in the case of an emergency, provided it is allocated appropriate resources and staff to fulfill additional obligations. As an example, the cyber annex to Washington State's Emergency Management Plan specifically highlights the Governor's authority to activate the National Guard.
- **Formalize Kentucky's cybersecurity exercise program.** The cybersecurity exercises conducted in Kentucky are an excellent starting point for a formal exercise program under the leadership of KOHS. Exercises can be held two or three times per year, with one strategic-level exercise and one or two with an operational focus. To ensure that progress is made in the intervals, each exercise should build on the findings of the previous one, and they should all be deliberately designed to stress-test gaps in plans and capabilities. Exercises provide an excellent opportunity to understand and strengthen partnerships, so it is critical that Kentucky's military installations are included.
- **Organize a government and military CISO roundtable.** Because they are funded by taxpayer dollars and serve the public interest, government and military agencies at the federal and state levels share common concerns and constraints. We suggest that an informal roundtable of major government and military chief information security officers (CISOs) in Kentucky meet on a quarterly basis to discuss best practices and lessons learned. Although their authorities and scopes of responsibility vary significantly, CISOs from COT, the Kentucky National Guard, the Fort Knox NEC, the RNEC-Bluegrass, and major local jurisdictions (like Louisville and Lexington) could work together to address challenges shared by the enterprises they oversee.



CHAPTER

7

Capability +
Awareness

Chapter 7 | Capability + Awareness

Cybersecurity preparedness can be framed in the context of a three-legged stool: technology, people, and process. In this chapter, we discuss the first two legs of the stool: how organizations can adopt enhanced capabilities (technology) and how they can improve user awareness (people). In Chapter 8, we will discuss the third leg of the stool: risk management (process). Taken together, these two chapters provide best practices for any Kentucky-based organization, whether a government agency or a business, to develop a coherent cybersecurity plan. We pay particular attention to small and medium-sized Kentucky businesses, for which resources may be limited but the risk posed by a cyber disruption event is no less critical.

Capability adoption

The need for organizations to invest in cybersecurity capability

Technology is advancing at a breakneck pace. New technologies are empowering people and groups to do things that were never before possible – and to do them faster, better, and cheaper. This is the objective of innovators everywhere: to create new *functionality*. But with every step forward in functionality comes new *vulnerability*, especially when security is not baked into the technology's design.

Threat actors are constantly endeavoring to stay ahead of the latest technologies, so that the *malware* (“malicious software”) they create can be effective before security researchers find a way to beat it. Some threat actors will introduce malware that exploits *zero-day* vulnerabilities. Zero-day refers to vulnerabilities that have not yet been identified by the cybersecurity community; in other words, researchers have zero days to develop a solution when they're exploited. Once a solution is developed, threat actors are on to the next vulnerability to exploit.

Amidst this ongoing, epic battle between security researchers and threat actors are regular organizations – businesses, non-profits, and public sector entities – that are simply trying to operate. Nearly all organizations rely on information technology (IT) in some way, benefitting from its functionality but also becoming exposed to any attendant vulnerabilities. Most (especially small businesses) rely on a *managed services* model, meaning that the IT services they use – e-mail, data storage, and so on – are managed by a third-party provider. The managed services model shifts much of the responsibility for investing in cybersecurity technologies to the third party. The cost of that investment is then passed on to the organization via the fee for those services.

But as organizations become more sophisticated, their IT infrastructure becomes more complex. They may invest in their own private information networks, on-site servers, and custom applications. While many of their services might still be managed by a third-party provider, more of the responsibility for securing their own IT infrastructure now lies with them. Executives then need to make decisions about which security technologies are necessary, effective, and cost-efficient. They must also take care to avoid situations where they end up handcuffed to a technology that becomes obsolete; a vendor that is no longer providing appropriate value; or a system with snowballing enterprise costs.

In the following sections, we won't recommend specific technologies; the field is too dynamic, and we are not in a position to recommend particular vendors. We will, however, discuss ways organizations can think about investing wisely in key capabilities and the technologies that enable them.

The essentials

Until recently, discussions between business managers and IT staff regarding cybersecurity solutions often focused on the *who*. In other words, **who should provide the organization with solutions** to cybersecurity challenges? Is it anti-virus company X, firewall provider Y, and monitoring system Z? However, current expert thinking, gleaned from analysis of major widespread attacks and technology risk assessments, advises business leaders to focus on the *what*. That is, **what capability is needed** to ensure the organization is defended against active and emerging threats? In general, industry thought leaders agree on several high-level cybersecurity capabilities that businesses should adopt. The National Institute of Standards and Technology (NIST) has compiled a list of “absolutely necessary” cybersecurity actions that small businesses should take.^{cxxiii} These are represented in Table 1.

Table 1 // NIST’s essential actions to protect small business data, systems, and networks

Essential action	Example
Install and activate software firewalls on all your business systems	Software like Windows Defender and Symantec Endpoint Protection provide active firewalls to protect against malicious attacks.
Provide security for your Internet connection	A hardware firewall unit, made by such manufacturers as Cisco, SonicWALL, and Barracuda, provide an added layer of security to your Internet connection.
Protect information / systems / networks from damage by viruses, spyware, and other malicious code	Commercially available anti-virus and anti-malware software, such as McAfee Antivirus and AVG Internet Security, can protect systems against damage.
Ensure patches are up-to-date for systems, applications, and networks	Keeping device operating systems and applications and business network updates current helps to defend against device/network intrusion.
Securely back up vital business data and information	Backing-up data, through both physical- and cloud-storage and both on- and off-site, will ensure loss of devices or networks doesn’t cripple an organization.
Control physical access to your computers and network components	Instituting strong and vigilant computer and network login procedures will help to decrease user error and prevent unauthorized access.
Secure your wireless access point and networks	Both software and hardware solutions can provide an extra layer of security for access points and networks.
Require individual user accounts for each employee on business computers and for business applications	Requiring individual accounts for each employee may seem tedious, but it helps to ensure accountability.
Limit employee access to data information, and limit authority to install software	Enabling administrative controls and/or installing device management software on your company’s computers and networked devices will limit employee access to sensitive information.
Train your employees in basic security principles	A robust user awareness program can help to educate employees against common forms of malicious cyber attack and protect against security breach.

Security controls and enabling technologies

How an organization elects to adopt the capabilities described above depends on its exposure to cybersecurity risk. A deli and a power plant will have different degrees of risk – and therefore different technology needs. In Chapter 8, we discuss frameworks for how organizations can identify (and then manage) their cyber risk. We highlight the NIST Cybersecurity Framework (CSF), which guides organizations to adopt specific security controls based on their risk levels.

Security controls are the technical or administrative means used to detect, block, or mitigate the effects of malicious activity on a network or device. Examples of controls include encryption, authentication, passwords, audit logs, and backup storage. While some security controls are procedural or administrative in nature, many controls depend on an underlying security technology. In order to understand which technologies are worth the investment, an executive must understand which categories of controls his organization requires.

When we think about the timeline of a cybersecurity incident, we can categorize security controls according to three phases: preventative (before the incident); detective (during the incident); and corrective (after the incident). In Table 2, we describe each phase, and we give examples of security technologies that enable controls within each phase.

Table 2 // Categories of security controls and examples of enabling technologies

Category	Description	Technology examples
Preventative	Preventative controls are designed to block unauthorized access to the network or device.	Intrusion prevention systems automatically respond to potential malicious activity before it can access the network or device.
		Firewalls allow trusted traffic to access the network and block untrusted or suspicious traffic from accessing the network.
Detective	Detective controls enable an understanding of malicious activity occurring on the network or device.	Intrusion detection systems analyze network traffic to identify malicious activity.
		Security information and event management systems log and integrate events occurring across a network.
Corrective	Corrective controls allow an organization to restore the network or device to its pre-incident state, or to mitigate the effects of the incident.	Anti-virus software scans a network or device for suspicious or malicious applications.
		Data recovery systems create virtual copies of information so that it can be recovered in case it is lost or corrupted during a cyber incident.

The classification of security controls is important to business leaders for two reasons. First, it allows them to make sure they have adequate “coverage” across all three phases. Second, it provides a helpful lens through which to consider the long-term costs of technology investments. They should ask themselves several questions. Is this technology going to be obsolete in a few years? If I commit to this technology now, what costs will I incur if I decide to make a change later? If I ultimately move away

from a particular vendor, will I still have access to my data and infrastructure? If I invest in a particular technology, what other investments will I need to make in order to optimize use of that technology?

However an organization chooses to proceed, they should ensure that technology investments are made in accordance with their resource constraints, risk tolerance, and business strategy.^{cxxiv}

Resources

Organizations throughout the cybersecurity community publish – for public use – resources and tools to help organizations conduct self-assessments, baseline existing procedures, develop acquisition strategies, and generally determine what constitutes “adequate security.” Table 3 includes a list of useful resources for organizations to help them enhance their security controls.

Table 3 // Resources for cybersecurity assessments and security controls

Resource	Description
Carnegie Mellon University Software Engineering Institute OCTAVE^{cxxv}	The CERT Division of the Software Engineering Institute at Carnegie Mellon University developed OCTAVE, a workshop-based risk assessment approach that allows an organization to assess its cybersecurity requirements. Its current iteration, OCTAVE Allegro, is centered around identification and assessment of information assets.
DHS ICS-CERT Cyber Security Evaluation Tool (CSET®)^{cxxvi}	Developed by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at the Department of Homeland Security (DHS), CSET® is a software program that allows organizations with industrial control systems to assess their cybersecurity posture.
SANS Critical Security Controls^{cxxvii}	Developed by the SANS Institute, the Critical Security Controls are a set of guidelines that assist with cyber defense. The controls attempt to use threat data to inform security guidance. The best practice guidelines for computer security include methods, or critical security controls, that organizations can adopt to block known cyber attacks.
NIST Special Publication (SP) 800-53^{cxxviii}	NIST develops and updates a list of security controls for federal government information systems. At well over 400 pages, SP 800-53 should be viewed as a comprehensive catalog for information security professionals, rather than a how-to guide for small businesses. NIST publishes a separate document – <i>NIST Interagency Report 7621, Small Business Information Security: The Fundamentals</i> – designed to help small businesses with cybersecurity essentials. ^{cxxix}

User awareness

The need for organizations to adopt a cybersecurity awareness program

Human beings are the weakest link in any cybersecurity ecosystem. Although discussions about cybersecurity tend to focus on sophisticated hackers and game-changing technologies, the reality is that most cyber disruption events are still caused by human error. To break into a network or system, hackers depend on people's lack of basic cybersecurity awareness. For certain types of malware to infect a network, a human still needs to click on a link or download an e-mail attachment. Mundane actions like these can cause even the most well-intentioned of users to compromise their organization's data.

Virtually every organization today, in both the public and private sector, has its employees interact with technology in the course of doing business. It is imperative that organizations arm their employees with the information they need to safely navigate the perils of cyberspace. Every organization – no matter how small – should implement an awareness program to promote fundamental concepts, convey do's and don'ts, and enhance employees' "cyber hygiene."

There is an additional consideration for state government leaders. Promoting organizational cybersecurity awareness programs is not just smart for companies; it's good public policy. Millennials notwithstanding, many people interact primarily with information technology as a function of their jobs. Employers are therefore in the best position to directly reach and teach individuals. Imagine that every company in Kentucky implemented an effective cybersecurity awareness program for its staff. The net effect would be a much more informed citizenry, which is the foundation of the Commonwealth's cybersecurity ecosystem.





The challenge becomes how to devise a cybersecurity program that is cost-efficient, effective, and tailored for an organization's needs. In this section, we'll review best practices for any organization to meet those objectives.

Who will run the program?

The first question an organization must ask is: who is going to implement and manage our cybersecurity awareness program? Will we hire dedicated staff, outsource it, or simply designate current staff to be responsible for the program? The answer to this question depends largely on an organization’s financial resources. For example, many large companies and government agencies have staff dedicated to designing and managing a comprehensive user awareness and training program, which is fully integrated into the cybersecurity enterprise.

Other organizations completely outsource this aspect of cybersecurity to a commercial provider, and the internal IT department is responsible for integrating the program into the organization’s cybersecurity program. Outsourcing is often the desirable choice for industries subject to sector-specific security standards; retaining third-party impartial experts facilitates full documentation and compliance with requirements. Examples of these industries and standards are represented in Table 4.

Table 4 // Industry-specific standards for cybersecurity awareness

Industry	Relevant Standards
 Education	Family Educational Rights and Privacy Act
 Financial Services	Payment Card Industry Data Security Standard
	Financial Services Modernization Act of 1999
 Manufacturing	Common Industrial Protocol
 Healthcare	Health Insurance Portability and Accountability Act

What guiding principles should the program follow?

However, for most businesses that do not have significant resources (financial or personnel) to invest in security, they must designate current staff to design and manage the program. In effect, this becomes “collateral duty” for a senior manager, who must seek both commercial and no-cost resources to design and manage the program. Following a review of published best practices, we recommend – in Table 5 – guiding principles to help such a senior manager design an effective and cost-efficient user awareness program.

Table 5 // Principles for an effective cybersecurity awareness program

Principle	Description
Start at the top	A cyber-aware culture will never be actualized in an organization unless it is incorporated into the values of the company. This is the role that executives and senior managers have to play in creating a successful cyber awareness program. Make it a priority, make it a requirement to participate, ensure it is resourced, and energetically support it.
Designate a point person	Someone needs to lead and be accountable for the development and execution of the program. Depending on the size of the business, the person in charge may range from the business owner, to a collateral duty senior manager, to a trained full-time employee. In any case, the first task of the point person is to validate the support of senior management, as the initial focus of the program may require direction by company leadership before they can credibly approach employees.
Create a culture of security	Personal responsibility is a major component of any security program. Building a durable and pervasive security culture is about influencing user behavior to understand that responsibility and how to uphold it. Different people learn in different ways, so a variety of tactics should be used and constantly reinforced. A ‘constant learning’ program should include required formal training, periodic refresher training, simulations, posters, email tips, a newsletter, and guest speakers. It should rely heavily on no-cost materials from public, for-profit, and non-profit sources.
Develop and promote clear policies	Develop and widely disseminate easily understandable policies for new employees, contractors, and vendors. Employees should be specifically briefed on requirements and expectations the company has with regards to cybersecurity from their first day on the job. Also, employment agreements and vendor contracts should have sections that clearly define these security requirements.
Operate on shorter, more focused cycles	According to research performed by Ira Winkler and Samantha Manke of Secure Mentem, the most successful awareness programs operate on a 90-day cycle as opposed to a one-year cycle. They observed that the yearly cycle is too easily disruptive, is too rigid for users, does not reinforce learning, and does not allow ample time for feedback. On the other hand, creating clear focus areas that are reinforced throughout the course of a 90-day cycle improved results. At the end of each 90-day cycle, a formal review should take place, user feedback incorporated, and next steps planned. ^{cxxx}
Measure results	For an executive who is concerned about cyber risk, the best way to measure return on an investment in a cybersecurity program is to define, baseline, and monitor key metrics over time. An organization that has invested in network monitoring software will be able to observe technical metrics like the number of security incidents and online behaviors deemed risky (like visiting a suspicious website). A resource-constrained organization may need to rely on questionnaires that gauge their employees’ understanding of cybersecurity best practices.
Make it fun	Even the most technically sound cybersecurity awareness program will be meaningless if employees aren’t engaged. It’s no surprise the words “mandatory training” don’t inspire most people. But cybersecurity does not have to be boring. See the next section for best practices on making a cybersecurity awareness program resonate with employees.

How can an organization make a cybersecurity awareness program engaging?

Cybersecurity awareness programs have a reputation for being dry, boring experiences that do little to engage trainees. An inattentive trainee is more likely to skim through or ignore training, negating its purpose, doing little in practice to lower risk, and wasting the valuable resources invested to create and implement the program. To truly educate users, awareness programs should be regularly updated, inventive, and interesting.

Organizations like PricewaterhouseCoopers have developed “games” to simulate data breaches and engage trainees.^{cxxxix} In the case of PwC’s “Game of Threats,” trainees are split into two groups: a defensive group and a threat actors group. The simulation requires trainees to think quickly and strategically, and to be decisive with minimal information. “Game of Threats” is structured in such a way as to reward good decisions and penalize bad ones, reinforcing the principles that must be followed in the event of a cyber attack. Trainees have said that, after the exercise, they have a better understanding of cybersecurity trends and terms and of what their company can and must do during an incident.

In 2011, Northrop Grumman, an aerospace and defense company, created its own Cyber Academy. The academy provides training courses and helps employees improve their understanding of cybersecurity and its associated challenges.^{cxxxix} The academy’s training includes games, and Northrop Grumman has worked to make similar games available for school-age children to learn about cybersecurity. The company has used a game that places users in the role of an executive in charge of new employees. Users give the employees laptops, set up their network connections and physical zone security, and defend against cyber attacks. The training tool responds and reacts to users’ inputs; for example, if the user did not purchase anti-virus software for the employees’ computers, a successful malware attack will occur and compel the company to incur recovery costs.^{cxxxix}

These vignettes are two examples of the new and innovative kinds of cybersecurity awareness programs that have a real impact on users. However, developing games or simulations is expensive and likely beyond the resources of small- and medium-businesses. The programs described above are not meant to be strictly prescriptive or limiting; rather, they should highlight the fact that awareness programs can and should be novel and stimulating. Based on these programs and additional research into training methodologies, we are highlighting the following best practices:

- Use games and exercises to understand how employees will respond to a cyber attack.
- Use scenarios to tell a story, making the experience more engaging.
- Rely on the game or the scenario, not the reference materials; many users will simply skip or skim them.
- Integrate quizzes periodically to ensure users are thinking critically.
- Allow users to complete scenarios at their own pace in order to improve receptivity to new concepts.

What topics should the program cover?

Finally, it is important to consider the content of a cybersecurity awareness program. While each organization is different, every awareness program should address the topics in Table 6, at a minimum.

Table 6 // Key topic areas for a cybersecurity awareness program

Topic	Rationale
Company policies	Every employee must understand their role and responsibility in maintaining and promoting a cybersecurity culture. Accordingly, he must be made aware of the company’s expectations of him during his tenure there.
Malware	Employees should understand the basic categories of malware and how they work in practice. For example, some malware will destroy information, some will lock it, and some will copy it. There are numerous varieties of malware, but the key to understanding how to protect information is understanding what it is being protected from.
Threat actors	Likewise, employees should understand the basic categories of malicious actors and their various degrees of sophistication – from amateur hackers to more advanced enterprises.
Passwords	Although it may one day be replaced by biometric tools like fingerprint, iris, or facial recognition scanners, the password is still the private key most people use to unlock their data. The simpler a password is, the simpler it is to break it. Many people still use passwords that are too basic, making it easy for malicious actors to guess or crack them. Moreover, they often use the same password across multiple accounts (meaning that if one account is hacked, the user’s other accounts are vulnerable). A discussion of passwords should include an organization’s two-factor authentication policy, if it has one. A two-factor authentication policy, usually requiring both a written password and a code that can be texted to a user’s phone, is an important and essential step in securing critical accounts.
Social engineering	Social engineering refers to a category of tactics that exploit normal human behavior in order to trick users into breaking security policies. A common tactic is phishing, which refers to the practice of e-mailing individuals to get them to divulge personal information or perform some other action. E-mail service providers have become better at blocking phishing attempts, but many phishing e-mails get through spam filters, and it is still a common way for systems to become infected with malware. Recognizing the signs of a phishing attempt are therefore critical to any awareness program.
Mobile	It is becoming cliché to say that people are tethered to their smartphones. But it is the reality, and – as mobile devices become more powerful and sophisticated – more personal data will reside on them. An awareness program should cover best practices for personal and company mobile devices, paying attention to the differences between major smartphone operating systems.
Social media	We live in the social age. Vast amounts of personal information are being shared – by design – on the Internet every day. It is important for employees to understand best practices for protecting private data and maintaining cyber hygiene when using social media platforms.

Resources

Many commercial and free resources are available for developing and implementing a tailored cyber awareness and technical training program for businesses of all sizes – from a small local business to a large global enterprise. Table 7 provides a sampling of those resources.

Table 7 // Cyber awareness and technical training program resources

Resource	Description
<p>National Cyber Security Alliance^{cxxxiv}</p>	<p>The National Cyber Security Alliance (NCSA) manages StaySafeOnline.org, home to an excellent suite of free resources for individuals and organizations to learn about ways they can improve their cyber hygiene. They promote the “STOP. THINK. CONNECT.” online safety campaign; National Cyber Security Awareness Month; Data Privacy Day; and the RE: Cyber initiative (designed specifically for boards and executives).</p>
<p>Payment Card Industry Security Standards Council^{cxxxv}</p>	<p>The Payment Card Industry Security Standards Council publishes security awareness program best practices for organizations that rely on credit and debit card transactions. For many small merchants (consider an ice cream shop or a mechanic), payment cards are both vital to their businesses and one of their only touch points with information technology.</p>
<p>NIST SP 800-50^{cxxxvi}</p>	<p><i>NIST SP 800-50, Building an Information Technology Security Awareness and Training Program</i> includes guidance on how IT security professionals can identify awareness and training needs, develop a training plan, and get organizational buy-in for the funding of awareness and training program efforts. This document also describes how to select topics; find sources of material; put that material into action; evaluate program effectiveness; and update the program as technology and organizational priorities evolve.</p>
<p>Michigan Cyber Range^{cxxxvii}</p>	<p>The Michigan Cyber Range (MCR) is an excellent example of a state-led initiative to advance cybersecurity education and training. While the MCR has capabilities that extend far beyond the realm of user awareness, it does allow organizations to educate their staff (through online classes and exercises) and test new concepts. The MCR is the result of collaboration between Merit Network, NIST, the Michigan State Police, the Department of Homeland Security, among other partners.</p>
<p>SANS Security Awareness Resources^{cxxxviii}</p>	<p>The SANS Institute provides an impressive collection of resources for business at all levels of cyber maturity, allowing them to plan and maintain an awareness program that is compliant, engaging for employees, and focuses on reducing risk by changing their behaviors. SANS’s program is structured around the elements of gaining internal support, planning, and measuring results. SANS materials have been developed for general use by the cybersecurity community, and many are available under a Creative Commons license.</p>

Recommendations

It can be daunting for an organization – especially a small or medium-sized business – to approach the topic of cybersecurity. The guidelines recommended in this chapter will help any organization make smarter technology investments and promote cybersecurity awareness among its employees. The Commonwealth of Kentucky can take several steps to ensure that these guidelines are promoted to organizations throughout the state. Because Chapter 8 also includes guidance to Kentucky-based organizations – and because the role of the Commonwealth is similar in both cases – the recommendations here will be largely similar in both chapters.

- **Create a resource database.** While not endorsing a specific methodology or product, the Kentucky Cybersecurity Council should establish a centralized database for cybersecurity resources for private sector cybersecurity practitioners. The database should include available government resources, non-commercial assessment tools, standards, information sharing organizations, and community best practices.
- **Emphasize SMB cybersecurity as a priority.** Use the Kentucky Cybersecurity Council’s public awareness committee (see Chapter 10) to advance this objective. The committee should spearhead efforts to disseminate resources to SMBs to improve awareness, best practices adoption, and information sharing. The Kentucky Office of Homeland Security (KOHS) and other appropriate agencies could partner with DHS and the U.S. Small Business Administration (SBA) Region IV to develop a “virtual” Small Business Cybersecurity Advisory National Pilot Program at all Kentucky SBA offices.
- **Codify guidelines.** The Kentucky Cybersecurity Council should validate and codify the capability adoption and user awareness guidelines presented in this chapter. Once endorsed by the Commonwealth, those guidelines should be featured prominently on the centralized resource database. A process should be established to review these guidelines on a periodic (annual or biennial) basis.
- **Promote the planning guidelines.** The guidelines should be distributed far and wide, through existing industry associations and industry-government interfaces, and through a cybersecurity promotion campaign. Part of the challenge with cybersecurity is that it seems complex, but it doesn’t need to be. If an organization’s needs are not complex, its plan does not need to be, either. This promotion should aim to demystify cybersecurity and make it accessible to SMBs, in particular. KOHS should consider publishing an article “Cybersecurity for Kentucky Small Business Owners” in the next publication of the SBA’s *Resource Guide for Small Business – Kentucky Edition*.



CHAPTER

8

**Risk
Management**

Chapter 8 | Risk Management

In this chapter, we provide a roadmap for any Kentucky organization – whether a business, a government agency, or a non-profit organization – to adopt a risk management strategy and a cybersecurity plan. This chapter is a companion to Chapter 7, which discusses the criticality of technology and people in designing a coherent internal cybersecurity program. Here, we discuss the third leg of the stool (process) and how it integrates with technology and people through a coherent risk management framework and cybersecurity plan.

Why every organization should have a risk management strategy

Managing cyber risks is one of the most significant challenges facing senior executives today. They recognize that cybersecurity is complex, rapidly evolving, and connected to all aspects of their organizations. How can they design and implement a strategy that accounts for all these realities?

A robust and flexible risk framework that incorporates a cybersecurity plan is essential to enabling cyber decision-makers to clearly “see” and manage all types of cyber risks. Adopting and supporting comprehensive risk frameworks and cybersecurity plans offers the following advantages:

- Establishes common assessment and prioritization of risks;
- Facilitates vertical/horizontal alignment of planning;
- Encourages shared intellectual resources, best practices, and mutual aid;
- Accelerates risk-related partnerships and information sharing;
- Provides a clear delineation of roles and responsibilities;
- Sets security goals, measures, and outcomes; and
- Maximizes the impact of protective programs.

Scarcity of personnel and financial resources is the single most limiting factor in addressing cyber risk among both public and private stakeholders. This complicates investment in protecting networks, systems, and critical assets. Therefore, it is essential that cyber risk be weighed and evaluated at all levels of an organization and properly prioritized during resource allocation.

The national cybersecurity, critical infrastructure, and emergency management planning processes are premised on the type of risk framework detailed above. The National Infrastructure Protection Plan (NIPP) calls for a robust “layered defense” for cybersecurity across all aspects of the information domain. At the national level, much has been accomplished in operationalizing partnerships and information sharing among public and private sector elements.

However, progress at the state level has been focused on supporting national goals and organizing industry sectors to achieve national objectives. The Commonwealth of Kentucky has been a strong partner to the federal government and private sector from this perspective, and it has also worked to manage cyber risk for the state government. But it can also help organizations within the Commonwealth manage their own cyber risks. Here, we focus on how it can do that.

Frameworks for risk management

There are a number of well-respected global risk standards to assist organizations in systematic and effective implementation of risk management at all levels – the process level, the enterprise level, or across a diverse community of stakeholders. At its core, the goal of risk management is to provide a common view and understanding of threats, vulnerabilities, and consequences, to provide for "the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, assessing, treating, monitoring and communicating" organizational risk.^{cxxxix}

Several commonly used industry risk standards are described in the Table 1.

Table 1 // Standards for Risk Management

Document	Description
<p>SANS Critical Security Controls^{cxl}</p>	<p>Developed by the SANS Institute, the Critical Security Controls are a set of guidelines that assist with cyber defense. The controls attempt to use threat data to inform security guidance. The best practice guidelines for computer security include methods, or critical security controls, that organizations can adopt to block known cyber attacks.</p>
<p>ISO 31000:2009 – Risk Management Principles and Guidelines^{cxli}</p>	<p>This International Organization for Standardization (ISO) document provides risk management principles for use by public, private, or community organizations and is not tailored to any particular industry. The standard’s guidelines outline design, implementation, and maintenance of risk management processes. The standard defines risk as the “effect of uncertainty on objectives” and is meant to be applied within existing management systems, as opposed to completely replacing said systems.</p>
<p>ISO 27001:2013 – Information Security Management System Principles and Guidelines^{cxlii}</p>	<p>This document details the establishment, implementation, maintenance, and continual improvement of an information security management system. The standard also includes guidance on information security risk assessment. As part of risk assessment and treatment, the standard includes over 100 risk controls to consider based on an organization’s particular information security system.</p>
<p>COSO 2004 – Enterprise Risk Management – Integrated Framework^{cxliii}</p>	<p>The Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004 document focuses on systems of internal control, which is a component of enhanced enterprise risk management. The framework comprises internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The framework is divided into four high-level categories: strategic, operations, reporting, and compliance.</p>
<p>NERC Critical Infrastructure Protection Reliability Standards^{cxliv}</p>	<p>The North American Electricity Reliability Corporation (NERC) is a non-profit organization that establishes reliability standards for the energy critical infrastructure sector. NERC has published CI protection standards that provide guidelines for general CI protection and include security management controls and system security management.</p>

Table 1 (continued) // Standards for Risk Management

Document	Description
<p>Payment Card Industry Data Security Standard^{cxlv}</p>	<p>This standard is developed by the Payment Card Industry Security Standards Council and is used by organizations that handle credit cards from companies such as Visa, MasterCard, and American Express. The standard increases controls to protect cardholder data and prevent fraud.</p>
<p>NIST Special Publication (SP) 800-37^{cxlvi}</p>	<p>Produced by the National Institute of Standards and Technology (NIST), SP 800-37, <i>Guide for Applying the Risk Management Framework to Federal Information Systems</i>, is also known as the NIST Risk Management Framework (RMF). The RMF details a six-step process that helps Federal agencies comply with their requirements under the Federal Information Security Management Act, or FISMA.</p>
<p>NIST HIPAA Risk Management Guidance^{cxlvii}</p>	<p>Produced by the National Institute of Standards and Technology (NIST), the Health Insurance Portability and Accountability Act (HIPAA) Risk Management Guidance addresses the HIPAA requirement that calls for risk analysis as a prerequisite for compliance. This guidance specifically addresses risk as it relates to electronic protected health information, an important component of HIPAA regulations.</p>

These risk standards are in use by government agencies and businesses across the United States – on a voluntarily or required basis, depending on the situation. A 2016 industry survey of over 300 leading IT security professionals found that “84% of organizations have at least one security framework in place.”^{cxlviii} Therefore, when industry leaders craft cybersecurity policies and practices, it is important to adopt risk practices that are flexible, adaptable, and can be harmonized with those already in place.

The NIST Cybersecurity Framework

For an organization that is new to cybersecurity planning, the web of risk management frameworks can be daunting – even for an executive who is eager to move down the pathway of improved cybersecurity. And when that executive manages a critical infrastructure asset, he shouldn’t select one framework when his peer is using another. Recognizing that these problems were deterring adoption of cybersecurity standards and complicating information sharing, President Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, in 2013. EO 13636 (and the *Cybersecurity Enhancement Act of 2014*) directed NIST to (among other actions) create a new cybersecurity framework that could unify or replace the others.

The result was what is now known as the NIST Cybersecurity Framework (CSF). The NIST CSF was developed through a collaborative public process, and NIST paid special attention to the needs of industry-specific Sector Coordinating Councils (SCCs) and Information Sharing and Analysis Centers (ISACs) to ensure the representation of highly specialized industries such as energy, financial services, healthcare, and those (like manufacturing) that rely on industrial control systems (ICS).^{cxlix} The NIST CSF empowers organizations to identify their own risk level in a structured and coherent way, and then implement security protocols that map to their specific needs. The NIST CSF was built for use by critical infrastructure operators, allowing them to read from the same sheet of music when preparing for, managing, or responding to a cybersecurity incident. The NIST CSF is also designed in such a way that allows organizations to map existing frameworks to it, eliminating the need to undo organizational processes that already work.

Relevant to critical infrastructure planning efforts, the NIST CSF has been identified by industry as a useful high-level assessment tool to identify systemic risk management “gaps.” Correspondingly, the NIST CSF is being used by critical infrastructure owners and operators to fill a particular “cybersecurity gap” in their current risk management frameworks. The NIST CSF has also been adopted by many public sector enterprises, including the Kentucky state government. The Commonwealth Office of Technology adopted NIST CSF best practices in its 2014–2018 Strategic Plan.^{cl}

In the same survey cited above, 70% of organizations viewed the NIST CSF as a “security best practice” and identified it as the “most popular choice of security frameworks to be implemented over the next year”^{cli}. The NIST CSF enables executives to operate within a standard cyber risk lexicon, identify specific security protocols that their organizations should adopt, and make investments that correspond specifically to their organization’s level of risk.

Cybersecurity planning

Planning resources for Kentucky-based organizations

No risk management framework – including the NIST CSF – is recommended as a comprehensive solution. A risk management framework should be part and parcel of a comprehensive cybersecurity plan that addresses all aspects of an organization’s needs. This section will focus on cybersecurity planning in the private sector.

Most large organizations, with operational IT departments, adequate resourcing, and clearly defined IT responsibilities across all levels of employment, can be expected to already have a cybersecurity plan in place – even if it goes by a different name (like an information security plan). The Commonwealth can and should provide resources to those large organizations – especially those that operate critical infrastructure – seeking to improve their cybersecurity plans or better integrate them into the governance structure proposed in Chapter 5.

But the Commonwealth can have a greater impact on statewide cybersecurity resiliency by providing planning guidance to small and medium-sized businesses (SMBs) without dedicated IT resources. More than 90% of Kentucky’s businesses employ fewer than 100 people, and those companies are responsible for employing about a third of Kentucky’s entire workforce.^{clii} While some SMBs will have made an investment in cybersecurity, most still lack an adequate cybersecurity plan. SMBs are often overlooked when it comes to cybersecurity, yet they are perhaps the most vulnerable. Consider a coffee shop that provides Wi-Fi to customers, an Internet-based e-commerce firm, or a restaurant that provides online ordering. Any small business that employs the Internet as a principal component of service or product delivery must have a fundamental cybersecurity plan, even if it is a basic one.

The Commonwealth should lead a proactive public awareness campaign to assist the small business community in addressing cyber vulnerabilities. Such a campaign should draw on recommendations from recognized cybersecurity planning resources, which include those described in Table 2.

Table 2 // Cybersecurity Planning Resources

Resource	Description
<p>Federal Communications Commission (FCC) Cybersecurity Planning Guide^{cliii}</p>	<p>This guide is a component of the FCC’s Small Biz Cyber Planner, which is a tool for SMBs to create cybersecurity plans commensurate with the organization’s size. The guide is designed for organizations that lack dedicated IT departments.</p>
<p>Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT) Tips^{cliv}</p>	<p>US-CERT offers tips and best practices to handle common cybersecurity issues. The best practices are categorized into Attacks and Threats, Email and Communication, General Information, General Security, Mobile Devices, Privacy, Safe Browsing, and Software and Applications. These tips can be applied both to IT-related operations in SMBs and in individuals’ interaction with computers, mobile devices, and the Internet.</p>
<p>National Rural Electric Cooperative Association (NRECA) Guide to Developing a Cybersecurity and Risk Mitigation Plan^{clv}</p>	<p>This guide is based on NIST-IR 7628, which concerns standards and security considerations for smart grids. The NRECA guide was designed to help power cooperatives develop their own cybersecurity plans. It is just one example of a planning guide that is tailored to meet the needs of a specific industry.</p>
<p>NIST-IR 7621^{clvi}</p>	<p>NIST recognizes that the NIST CSF may be too complex for the average SMB – especially those that don’t have sophisticated IT systems. So, they developed NIST-IR 7621, which draws on the CSF’s fundamental principles but is tailored to SMBs.</p>
<p>NIST Small Business Community Workshops^{clvii}</p>	<p>NIST, working with the Small Business Administration and the FBI, conducts workshops for SMBs focusing on information security threats and solutions. NIST suggests that SMB owners and employees attend these workshops.</p>
<p>National Cybersecurity Alliance (NCSA) Re:Cyber Initiative^{clviii}</p>	<p>Re:Cyber is an initiative focused on cybersecurity and risk management at the CEO and board-level. NCSA and Business Executives for National Security (BENS) are both non-profit organizations that created the initiative to help SMBs tailor cybersecurity plans and risk management frameworks to better protect themselves from cyber threats and attacks.</p>
<p>SANS Small Business 20 Security Control Implementation^{clix}</p>	<p>The SANS 20 Security Controls were developed to help businesses of any size adopt a plan that increases organizational cybersecurity. This report provides guidance for SMBs to adopt the 20 Security Controls with considerations for their small size and limited available resources.</p>

Planning Guidelines for Kentucky-based Organizations

“Addressing cybersecurity issues starts at the top with senior management and the board of directors. Good policies and practices need to be in place, and they need to be reviewed and tested often.”

Commissioner Charles Vice
Kentucky Department of Financial Institutions

The Executive Leadership on Cybersecurity Seminar
March 2016

Developing a sound cybersecurity plan is a must for every business, regardless of size. The scope and complexity of the plans will vary, but the approach to the problem and general issues for consideration are the same. Regardless of whether a company is global with 50,000 employees, regional with 5000 employees, local with 500 employees, small with 50 employees, or home-based with 5 employees – all should have some form of cybersecurity plan. It is the obligation of the business leader to ensure appropriate cyber planning is conducted, protections are in place and that all users implement them – be they presidents, chief executives, owners, proprietors or bosses.

At any level, approaching the cyber planning process can be challenging, particularly for medium to small business that lack chief information officers (CIOs) and chief information systems security officers (CISSOs), trained IT staff, and resources to invest in cybersecurity. The following information is intended to help business leaders approach cybersecurity in a direct, rational, and requirements-driven manner that is fully transparent at all levels of the business.

Framing the problem

Before directing or leading a planning effort, the business leader should be able to articulate high-level “shaping” guidance about the business, its organization, and its goals. The following strategic questions^{clx} should be determined or validated by the executive and her senior management group and provided as “input data” to the actual planning team.

- What are the business’s “crown jewels” or key business assets? Are they adequately protected?
- What is my corporate risk tolerance? How much risk will (must) I accept (legal obligations)?
- Does my company fully understand what information it manages, where the information is stored, how sensitive the information is, and who has access to it?
- How do we identify and manage all risk, including cyber?
- What do I, as an executive, need to know about those risks and in what timeframe?
- What broad mitigation strategies will I employ? Asset duplication, risk buy-down, risk-transference (insurance), outsourcing?

What needs to be done

“44% of small business reported being the victim of a cyber-attack at an average cost of approximately \$9000 per incident.”

National Small Business Association Survey

An analysis of industry best practices for implementing a comprehensive cyber program based on technical controls and cultural adjustment reveals several constructs that are hallmark to organizations with high levels of cyber preparedness.^{clxi} They are briefly discussed below.

Determine who will be involved

Strong collaboration among internal stakeholders is essential for effective planning, training, and response. While the coordination responsibility for managing these key cybersecurity processes resides with the CIO, CISSO, and IT department – the execution responsibility for all of the above lies with the enterprise, particularly with respect to recognizing attack warning signs and initiating response procedures. In addition to IT, a company’s cyber planning and response team should be comprised of senior representatives from the business units and the operational units (including human resources, security, finance, and legal). The plan should detail roles and responsibilities for each department and should directly address how everyone in the organization is to recognize the signs of an attack. It should also explain how to implement immediate defensive actions and rapid incident notification to trigger technical response procedures. A robust cyber awareness and employee training program is among the most cost-effective ways to stop or mitigate social engineering "tricks," introduction of malicious software on the network, or loss of corporate data.

Determine processes for receiving, sharing, and applying cybersecurity threat information

Information is power. The more information an organization has regarding the general threat and specific threat vectors, the better decisions business and technical managers can make during actual attacks. Threat intelligence is aimed at understanding cybersecurity trends and the tactics malicious actors are using to steal data from companies. It can be so detailed as to provide vulnerability information for technology assets (down to the level of model and manufacturer) used by various industries.

Specific threat data is readily available for financial, health care, manufacturing, and industrial control systems. Chapter 5 provides a detailed discussion of information sharing and analysis resources publicly available to Kentucky critical infrastructure owners and operators, as well as other businesses – large and small. Kentucky’s businesses should participate in information sharing organizations, to include the Kentucky Intelligence Fusion Center, the Financial Cybercrime Task Force of Kentucky, industry-specific Information Sharing and Analysis Centers (ISACs), the FBI’s InfraGard program, or a commercial cybersecurity analysis service.

Ensure compliance with laws and regulations

Cyber regulations for specific industry sectors and general liability for businesses is on the rise. Companies in industries that are already highly regulated – like energy, health care, and financial services – are required to meet certain thresholds of cybersecurity, particularly when it comes to notification of a breach. Additionally, any business that owns or processes personally identifiable

information (PII) must be aware of the legal risks associated with a compromise of such data. From a technical standpoint, it is essential that IT managers maintain proper network audit logs in accordance with current best practices. From a liability standpoint, it is critical that the legal department is involved in cyber planning, response, and recovery efforts, and that there is an independent and empowered compliance program.

Establish a baseline

The next step is to baseline existing processes and ensure that the security systems and practices that are in-place are running and are being implemented correctly by users. This simple step of "due diligence" offers one of the best returns on investment for enhancing security. A baseline review should include access control (consider: passwords, two-factor authentication, identity and access management); firewalls and intrusion detection and prevention systems; security incident and event management (SIEM) systems; e-mail and malware scanning systems; mobile security systems; and encryption protocols. A final essential baseline check is to ensure all critical information is backed up to prevent loss in the event of a cyber attack or natural disaster. All backup data should be stored in remote locations away from the office, and sensitive data about the organization and its customers should be encrypted.

Assess risks

This report delves deep into the importance of risk assessment, both in this chapter and in Chapter 5. Risk assessment is a process that prioritizes threats based on their likelihood of occurring and what damage they could do. Risk owners should be identified for each major system, threats should be prioritized, and potential solutions should be evaluated. As with any risk management strategy, those solutions would include risk elimination, mitigation, transference (i.e., insurance), or acceptance.

Risk assessment not only facilitates and informs cybersecurity response, but it also helps prevent attacks in the first place. Risk-based planning is designed to disrupt the attacker's avenues of entry into the network. It also helps determine what data is most critical to the business, and it helps "harden the target" while generally making it difficult for a malicious actor to operate undetected in the network. Making risk-based cyber decisions helps business owners focus limited resources on protecting the most valuable information.

Plan to respond

If an attack occurs, a business must be prepared to respond. Every organization's cybersecurity plan should include a response annex, which must be up-to-date, widely disseminated, and regularly tested with employees. All personnel required to act under the plan should be formally made aware of their roles and any changes in procedures. The war planner's axiom - "no plan survives contact with the enemy" - applies to cyber as well. Despite all best efforts - people, process, and technology - a security breach will occur. This is why being vigilant and proactive in cybersecurity risk management, assessment, counter-measures, training and awareness training is essential.

Developing a plan

“Nearly 59% of U.S. small and medium-sized business do not have a contingency plan that outlines procedures for responding to and reporting data breach losses.”

National Cyber Security Alliance

Risk management planning is about making the best decisions with the resources you have. While large businesses can dedicate trained professionals to manage cybersecurity planning and response, small businesses face the same cybersecurity challenges and threats with limited resources, capacity, and personnel. There are literally thousands of public, non-profit and commercial organizations offering comprehensive planning guidance and automated tools for developing tailored cybersecurity plans for the full spectrum of business sizes. Choices are often overwhelming.

Two exceptional government programs offer comprehensive “touchstone” resources to businesses for building and maintaining cyber programs and tailored organizational plans. These resources are offered by the Department of Homeland Security (DHS) and the Kentucky Public Protection Cabinet – Department of Financial Institutions (DFI).

The DHS program is a broadly focused national cyber awareness campaign titled “Stop. Think. Connect.” It includes an exceptionally well organized website that houses resources and materials to help businesses and the public become cyber secure. The campaign offers a publications library, planning templates, ready-made presentations, and tip sheets on all facets of cybersecurity. Representative topics include cybercrime, threats, employee and customer records, financial and banking security, access to large networks, protecting the workplace, and social media guidance. The site also centralizes automated planning tools and resources offered by key federal agencies, including:

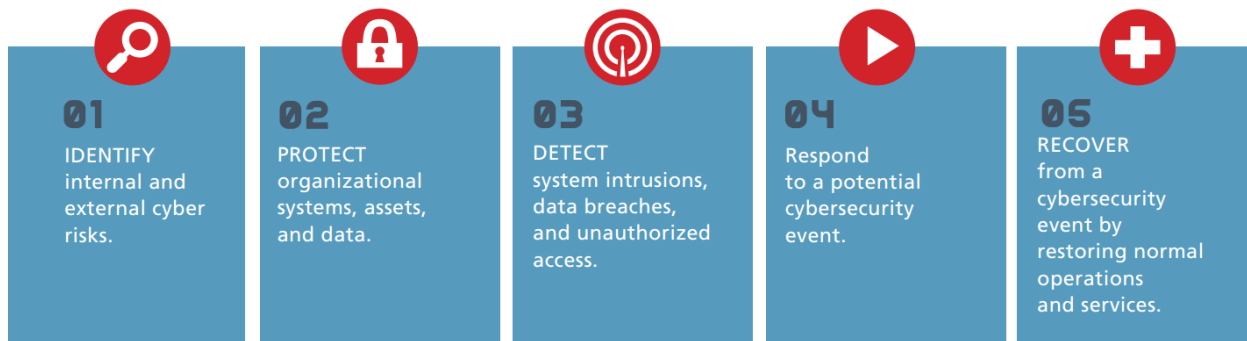
- the Small Biz Cyber Planner 2.0, developed by the Federal Communication Commission;
- detailed planning guidance from the U.S. Computer Emergency Readiness Team;
- legally vetted strategies from the Federal Trade Commission on collecting sensitive employee and customer data; and
- business safeguards and best practices from the National Cyber Security Alliance.

The Kentucky Department of Financial Institutions (DFI) – along with its sub-unit, the Financial Cybercrime Task Force of Kentucky – offers one of the highest quality and robust cybersecurity reference sites compiled by a state. While focused on the financial services industry and cybercrime, its resource library, information sharing links, best practices and threat alert notifications are useful across all industry sectors. The DFI has also established a highly effective cyber partnership with the Conference of State Bank Supervisors (CSBS), as evidenced by the Executive Leadership of Cybersecurity (ELOC) Seminar. The seminar provided a non-technical overview of cyber threats and sector best practices. Most relevant to Kentucky business leaders, the DFI has actively promoted and distributed the CSBS’s superior planning guide, “Cybersecurity 101: A Resource Guide for Bank Executives.” Again, while focused on the financial services sector, the guide is a complete and succinct planning reference for any CEO or small business owner in Kentucky.

“Cybersecurity 101” is offered as a “non-technical, easy-to-read resource on cybersecurity” and provides a wide-ranging and step-by-step discussion of how to develop a plan to mitigate cybersecurity risks.

The guide is a template for planners to create a fully developed plan.^{clxiii} Elements can be customized based on the scale and complexity of the business. Notably, CSBS's Cybersecurity 101 is organized around the five core cybersecurity functions of the NIST CSF. Alignment with the NIST CSF allows for a straightforward breakdown of plan components, and it enables compatibility with other more detailed technical standards that may be in use within the organization – in this case a financial institution. Those five core functions are shown in the figure below:

Figure 1 // Cybersecurity 101 model provided by CSBS



Recommendations

In the cybersecurity world, the old rule-of-thumb applies: 80% of the problems can be resolved with 20% of the effort. Developing a fundamental cybersecurity plan that is synchronized with a recognized risk management framework represents that 20% of the effort. Organizations throughout Kentucky should be encouraged and empowered to develop one that suits their needs.

The Commonwealth of Kentucky can take the following steps to improve risk management framework and cybersecurity plan adoption and awareness across the state:

- **Emphasize SMB cybersecurity as a priority.** Use the Kentucky Cybersecurity Council’s public awareness committee (see Chapter 10) to advance this objective. The committee should spearhead efforts to disseminate resources to SMBs to improve awareness, best practices adoption, and information sharing. The Kentucky Office of Homeland Security (KOHS) and other appropriate agencies could partner with DHS and the U.S. Small Business Administration (SBA) Region IV to develop a “virtual” Small Business Cybersecurity Advisory National Pilot Program at all Kentucky SBA offices.
- **Create a resource database.** While not endorsing a specific methodology or product, the Kentucky Cybersecurity Council should establish a centralized database for cybersecurity resources for private sector cybersecurity practitioners. The database should include available government resources, non-commercial assessment tools, standards, information sharing organizations, and community best practices.
- **Codify planning guidelines.** KOHS can leverage the exceptional work of the Kentucky Public Protection Cabinet – Department of Financial Institutions (DFI) in developing a similar planning guidebook that can be provided to organizations throughout the state. They should be reviewed by the Kentucky Cybersecurity Council. Once endorsed by the Commonwealth, those guidelines should be featured prominently on the centralized resource database.
- **Promote the planning guidelines.** The guidelines should be distributed far and wide, through existing industry associations and industry-government interfaces, and through a cybersecurity promotion campaign. Part of the challenge with cybersecurity is that it seems complex, but it doesn’t need to be. If an organization’s needs are not complex, its plan does not need to be, either. This promotion should aim to demystify cybersecurity and make it accessible to SMBs, in particular. KOHS should consider publishing an article “Cybersecurity for Kentucky Small Business Owners” in the next publication of the SBA’s *Resource Guide for Small Business – Kentucky Edition*.

CHAPTER 9

Privacy



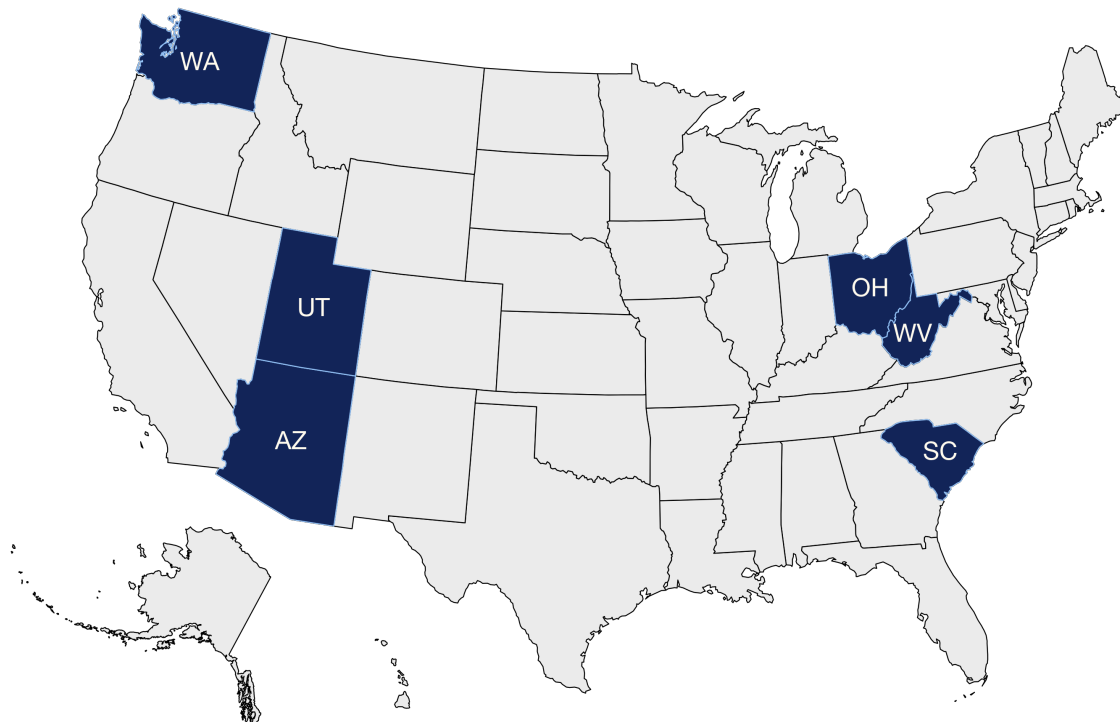
Chapter 9 | Privacy

Cybersecurity and privacy are inextricably linked. In the absence of effective cybersecurity, neither an organization nor an individual can be assured that their private data is reasonably safe from theft or loss. The Commonwealth of Kentucky is interested in enhancing protections for citizens' privacy, and so it is considering whether a statewide Chief Privacy Officer (CPO) is necessary and appropriate for the state. We conducted comprehensive research and analysis on statewide CPO programs, and we interviewed half of the statewide CPOs currently holding office in the United States. This chapter explains the function of a statewide CPO, explores three case studies, and then concludes with our recommendation that Kentucky install a CPO (along with our explanation for why).

What is a Chief Privacy Officer?

The concept of a Chief Privacy Officer, in government and in the private sector, is still relatively new. Although roles and responsibilities vary among them, CPOs are generally responsible for strengthening privacy protections and assessing how privacy considerations impact processes and decisions within their organization. While more companies are realizing the benefits of creating a new C-suite role dedicated to privacy, only six states have a statewide CPO: West Virginia, South Carolina, Washington, Ohio, Arizona, and Utah (See Figure 1).

Figure 1 // States with a statewide Chief Privacy Officer



Why is privacy so important?

The rise of the CPO mirrors a rapidly growing public interest in privacy. The International Association of Privacy Professionals (IAPP), the preeminent independent privacy organization, didn't exist twenty years ago.^{clxiii} Today, it has over 20,000 members, more than half of whom joined in the last five years.^{clxiv} In many board rooms – especially in information-intensive industries like healthcare – privacy has become a fundamental business consideration.

This focus on privacy has been the natural reaction to a dizzyingly complex and evolving information landscape. In advanced economies like the United States, virtually every aspect of a citizen's life now has a digital footprint. From essential services like banking and healthcare to leisure activities like photo sharing and text messaging, information about individuals is being transmitted and stored in cyberspace in massive quantities. Laws to protect that information typically lag behind technological development and adoption, creating gaps in the public's expectations when it comes to the privacy of their data. And although attitudes toward privacy vary by country and culture, most people would consider much of the information they generate and share online to be private; i.e., only for their own use or the use of certain other people.

This information is the lifeblood of the digital economy. This is especially true for information that can identify a particular person, which allows businesses and government agencies to provide more sophisticated and hyper-personalized services, like alerting owners of a particular product to a recall or ordering a driver's license. But if personally identifiable information (PII) is lost or stolen, it can endanger an individual's financial or physical security. It can be used to gain unlawful access to his accounts (e.g., e-mail, social media, or banking), to aid in targeting phishing attacks (also known as spear phishing), or even to steal his identity.

Accordingly, PII protection is associated with growing legal and reputational risks. When PII is stolen, the data-holding organization is typically held responsible. Law enforcement authorities often conduct an investigation to find the individual or organization that is responsible for the data theft, and this can be costly for data-holding organizations – especially if they are found to be culpable.

Enter the CPO

Privacy cuts across all aspects of a business or government enterprise. Any time an employee, user, or citizen shares PII with any department within that enterprise, a privacy risk is introduced. Not every department is well-equipped to manage that risk appropriately. With different mandates, data, and goals, each department must establish its own policies and controls – if they develop them at all. This approach can be inadequate, incoherent, and inefficient. A CPO centralizes or coordinates privacy policies and authorities across the enterprise.

For state governments, establishing a CPO requires a considerable amount of planning and stakeholder input. In some states, the CPO fulfills an **inward role**; in other words, the CPO is only concerned with privacy as it relates to government agencies. In such a scenario, there is little to no public engagement. In other states, the CPO has an **outward role** in educating the public on privacy issues and best practices to avoid personal data loss.

The considerations of the office of the CPO's structure, budget, and location in government are informed by the office's roles and responsibilities. For example, if the office focuses on training state employees in best practices, its budget needs to be larger than if the office serves only in a policy advisory role. Very generally, the universe of possible roles for a CPO are described in Table 1.

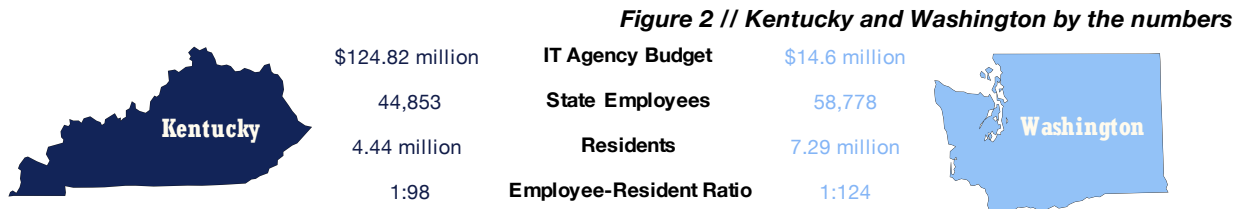
Table 1 // Potential Roles for a CPO

Role	Description
Training and education	Ensuring government employees are aware of privacy issues and trained in best practices when handling sensitive data
Public awareness	Conducting outreach or campaigns to educate the public on privacy issues and to share techniques to avoid data theft
Standards	Advocating for the development of privacy standards, or enforcing compliance with those standards
Best practices	Advocating for the development of privacy best practices, or promoting their adoption
Policy recommendations	Advising the executive and legislative branches on policies that can strengthen privacy, or the privacy impacts of policies under consideration
Technology regulations	Advising on the privacy implications of new technologies, especially in the context of policies that may regulate adoption or use of those technologies
Stakeholder engagement	Engaging with stakeholders in government and industry to improve the function and utility of the CPO

Case Study: Washington Office of Privacy and Data Protection

Washington’s government is federated, which means that each of the 15 executive branch agencies has a great deal of autonomy over its information technology (IT) systems and the data they contain. In 2014, Washington’s Department of Enterprise Services (which managed state government IT systems) and the office of the CIO merged to become Washington Technology Solutions (WaTech). WaTech is the state’s central IT organization and it controls Washington’s IT infrastructure under the direction of the CIO. In 2015, Governor Jay Inslee created the Office of Privacy and Data Protection (OPDP), headed by the newly created position of Chief Privacy Officer. This office is located within WaTech and includes the CPO and one additional full-time staffer.

Key Takeaways
Office created in 2015
Located in the state government’s information technology department
Privacy expertise resource for state government agencies
Significant public awareness and education function



The graphic above is provided for comparative purposes. IT Agency Budget refers to the estimated 2016-17 budget for the Commonwealth Office of Technology in Kentucky and for WaTech in Washington. State Employees refers to the number of people employed by the state in 2015, excluding education employees. Employee-Resident Ratio refers to the ratio of state employees to the number of residents.

In Washington, the CPO helps align the disparate privacy policies and activities of the state’s government agencies. OPDP centralizes privacy expertise so that state agencies have a single resource for advice on privacy issues. OPDP also analyzes the privacy implications of nascent technologies – like smart appliances and unmanned aerial systems – to provide informed policy guidance to state regulators. Unlike many of its counterparts in other states, OPDP views itself as a citizen-oriented resource, conducting consumer and citizen outreach to further public education on privacy issues.

Washington’s state government agencies have welcomed the creation of OPDP. This can be attributed to the office’s lack of enforcement authority (which creates buy-in among stakeholders), and its position as what is effectively an in-house privacy consultancy. Government agencies recognize that they have PII-related risks, and that OPDP’s expertise can help them manage those risks. OPDP has been able to cultivate a level of approachability that would be difficult to match if it had more authority; its authority would likely have scared potential collaborators and other state agencies away.

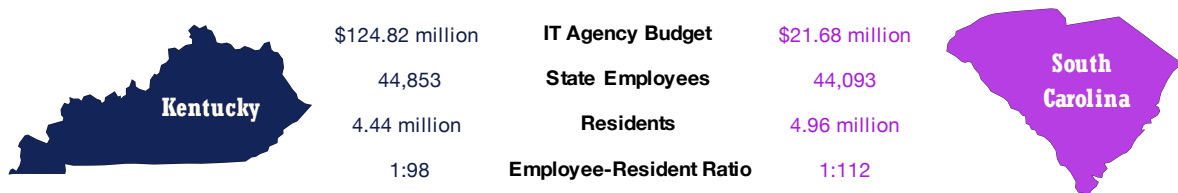
OPDP’s position in WaTech enables close cooperation and collaboration with the CIO, which is fundamental to the CPO’s success. The federated nature of Washington state government fostered a collaborative approach to privacy as opposed to a centralized one. Collaboration – and the coordination that goes along with it – would not be possible if it weren’t for OPDP’s approachability.

Case Study: South Carolina Enterprise Privacy Office

In 2013, South Carolina commissioned the consulting firm Deloitte & Touche LLP (Deloitte) to assess South Carolina’s information security and privacy risks and vulnerabilities. Among other findings, Deloitte recommended that South Carolina create a Chief Privacy Officer to lead a newly created Enterprise Privacy Office (EPO). Having previously lacked a dedicated interagency framework to address privacy issues within state government, the state moved swiftly to implement the report’s recommendation.

Key Takeaways
Office created in 2015
Located in the state government’s information technology department
Provides privacy guidance to privacy liaisons at 80 state agencies
No public role, but reviews consumer division materials from privacy angle

Figure 3 // Kentucky and South Carolina by the numbers



The graphic above is provided for comparative purposes. IT Agency Budget refers to the estimated 2016-17 budget for the Commonwealth Office of Technology in Kentucky and for the Division of Technology and Budget in South Carolina. State Employees refers to the number of people employed by the state in 2015, excluding education employees. Employee-Resident Ratio refers to the ratio of state employees to the number of residents.

The EPO is located in the Department of Administration’s Division of Technology, and it advises state agencies on the handling of PII. It also establishes, assesses, and enhances privacy protection policy, training, and compliance measures. The CPO leads the EPO and reports to the director of the Department of Administration. Currently, the office has three employees and four contractors. In addition to the EPO, the Division of Technology also houses the Division of Information Security and the Division of Technology Operations.

South Carolina, like Washington, has a federated system, with 80 independent state agencies. Each agency has a privacy liaison that serves as the agency’s lead on privacy issues and is the point of contact for interfacing between the agency and the EPO and CPO. The state’s Division of Information Security maintains and updates standards for all agencies, and it requires that each agency appoint a privacy liaison. Some agencies have faced difficulties in staffing and funding the privacy liaison role. This federated system has resulted in a range of differing privacy regulations that apply to South Carolina’s state government. Agencies look to the EPO to be the expert on privacy law in general (i.e., across the state), and specifically as it pertains to particular agencies.

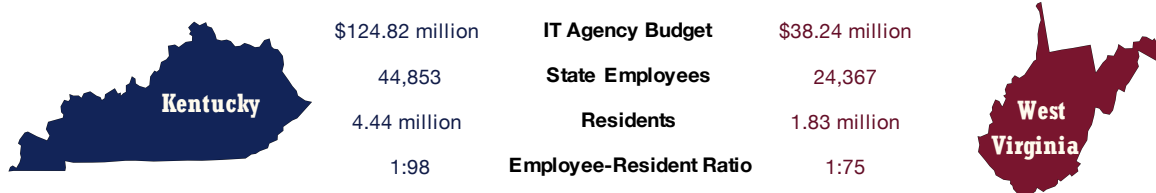
South Carolina’s CPO works closely with the state’s CIO and CISO – a key ingredient in the CPO’s success. In addition to leading the EPO, the CPO serves as the privacy liaison for the entire Department of Administration. It is an inward role, primarily serving the privacy needs of the state government. However, the EPO does work with the state’s Consumer Affairs Division and reviews materials to ensure accuracy of information. The Consumer Affairs Division and each agency’s privacy liaisons participate in citizen outreach, informing the public of best practices. Privacy training is a challenge facing the EPO; training must be customized to remain relevant and applicable across different missions and agency structures.

Case Study: West Virginia State Privacy Office

West Virginia’s state-wide CPO position was created in 2013 by then-Governor Earl Ray Tomblin. The role was filled by the state Health Care Authority’s CPO, and the position has remained in that agency ever since. Despite being situated in an issue-focused agency, the three-person State Privacy Office (SPO) – consisting of the CPO, a deputy CPO, and an assistant – is responsible for privacy issues across the state government. West Virginia’s CPO is, like that of South Carolina, is an inward role. While the Attorney General’s Consumer Division could fill a public awareness function for privacy issues, this remains a gap for the state.

Key Takeaways
Office created in 2015
Located in the state government’s health care authority
Serves as both a privacy expert resource and ombudsman for privacy officers throughout state government
No public role

Figure 4 // Kentucky and West Virginia by the numbers



*The graphic above is provided for comparative purposes.
IT Agency Budget refers to the estimated 2016-17 budget for the Commonwealth Office of Technology in Kentucky and for the Division of Information Services in West Virginia.
State Employees refers to the number of people employed by the state in 2015, excluding education employees.
Employee-Resident Ratio refers to the ratio of state employees to the number of residents.*

Each West Virginia state government agency has a privacy officer who coordinates and collaborates with the SPO. It is the privacy officer’s responsibility to set privacy policies for the agency and communicate those policies to agency employees. Privacy officers are trained by the SPO; this training uses a significant amount of the office’s resources. Turnover of privacy officers is another challenge, as some of the agency’s appointed individuals are not particularly knowledgeable of or interested in privacy. Most privacy officers have another job or role in the agency they represent.

The SPO holds Privacy Management Team meetings to engage privacy officers and provide a platform where breaches and incidents can be discussed without hesitation. All participants sign confidentiality agreements, and privacy officers from other organizations (such as higher education institutions or regulatory agencies) have asked to participate. Subject-matter experts also work with the team to develop privacy policies and procedures for state agencies. Additionally, the SPO regularly pushes Privacy Tips to the state employees to ensure continuing education on privacy of the workforce.

If received, additional funding for the SPO would be put toward hiring more employees to better resource the office; with only three full-time employees, the office is under-staffed. The SPO has found that its small size makes keeping up with the flow of data across state government very challenging. When a West Virginia agency adopts new technology and updates its systems and processes, the “new” data is integrated into the SPO’s data stream.

Recommendations

As Kentucky considers whether to create its own CPO position, our research highlights several key takeaways that should factor into that decision, namely:

- States with successful CPOs all have governors who understood the importance of privacy and cybersecurity and supported their CPO through engagement and funding.
- An enterprise-oriented CPO should be situated in the state's information technology department, while a policy-oriented CPO should be closer to the governor or in the cabinet.
- A CPO with enforcement authority can dissuade cooperation, isolate the CPO, and weaken privacy initiatives.
- Privacy can be a thorny issue among the public; the term means different things to different people. An external-facing CPO can educate the public on privacy best practices and communicate policies clearly and coherently to the business community.

Informed by interviews with other state government CPOs and research into the role itself, **we assess that Kentucky's government, businesses, and citizens would benefit from the creation of a statewide CPO.** Setting up a CPO would be an important step in improving Kentucky's cybersecurity posture and in assuring Kentucky's residents that their private data will be protected by state government and by the private sector.

But creating a new position will come at a cost. Based on our analysis of Kentucky state government compensation rates, we estimate that an appropriate salary for a CPO would be between \$80,000 and \$110,000, which would broadly translate to a range of \$100,000 to \$137,500 once benefits are included. CPOs – especially those with key qualifications like privacy experience in a large government enterprise or legal experience in the private sector – could command an even higher salary. In one state, the CPO earns more (\$123,000) than the governor (\$106,000). Once cost-of-living adjustments are factored in, that state CPO would earn about \$117,000 in Kentucky, close to the higher end of our proposed range.

Fortunately, CPOs in other states usually have a small staff, and they leverage the existing state government infrastructure to function. In Kentucky's case, current staff could be used to support the CPO's mission, but the Commonwealth may want to consider hiring a deputy or an assistant to help the CPO be more effective.

Before deciding whether to create a CPO position, **we recommend that Kentucky conduct an enterprise survey of IT managers throughout state government to answer fundamental questions about their privacy needs.** For example, the survey would determine whether cyber risk owners believe they have the resources necessary to identify and meet their privacy obligations and the best practices they can adopt to meet those obligations. The survey would (presumably) validate the need for a CPO, clarify its ideal function, and give policymakers the data they need to make decisions about budgeting and authorities.

If Kentucky chooses to install a CPO, we would make the following recommendations:

- **Install the CPO in COT.** The Commonwealth Office of Technology (COT) manages cybersecurity for the state government's IT networks, so a privacy function is a natural (and relatively small) expansion of the office's responsibilities. Moreover, COT already houses the state's Chief Information Security Officer, and successful CPOs have a strong working relationship with state CISOs.

- **Mirror the cybersecurity model.** The cybersecurity model for Kentucky’s state government is partially federated and partially centralized. It is federated in that each state agency is responsible for the security of its own data, and it is centralized in that COT is responsible for managing the security of the networks that transmit the data. COT also functions as a cybersecurity knowledge center – advocating for best practices and creating uniform policies throughout state government. The state’s privacy construct would function in a similar way. Agency data owners would still be responsible for managing privacy risks, but COT would set privacy standards, promote best practices, and serve as a source of expertise on the subject. If the cybersecurity model becomes more centralized over time, the privacy model should, too.
- **Ensure executive buy-in.** It will be challenging to create a culture of privacy throughout state government. For each individual agency’s privacy officer, privacy will usually be a responsibility that comes second to his day job. The demonstrated commitment of the governor or lieutenant governor to privacy is vital to empowering the CPO to be effective in building and maintaining that privacy culture.
- **Commit adequate resources.** Most CPOs operate (valiantly) with a skeleton staff. CPOs ensure that state agencies designate (if they haven’t already) privacy officers from among current staff to minimize additional budget pressures. But CPOs still need sufficient resources to be effective. Once the function and scope of the role is determined, the legislature must fund a CPO in addition to supporting staff (we would recommend one deputy and one junior staff member). It is possible that these positions could be repurposed from existing billets.
- **Develop a resource center.** To empower citizens and address misconceptions about privacy, the CPO should develop a privacy resources webpage for public consumption. Most CPOs who are tasked with developing a resource center have a website (or a portal requiring login) where regular citizens, state employees, and private business owners can learn tips and best practices for protecting their personal data. Some CPOs also publish white papers and reports on the status of privacy in their state.
- **Weave privacy into the cybersecurity narrative.** Ensure that privacy is rolled into any public awareness campaign about cybersecurity. Even if a CPO is not externally facing, they should work with the appropriate state agencies to ensure that efforts to educate the public about cybersecurity include information about privacy. The state government and the general public will benefit from increased discussion of privacy in a cybersecurity context.



CHAPTER
10

**Cybersecurity
Initiative**

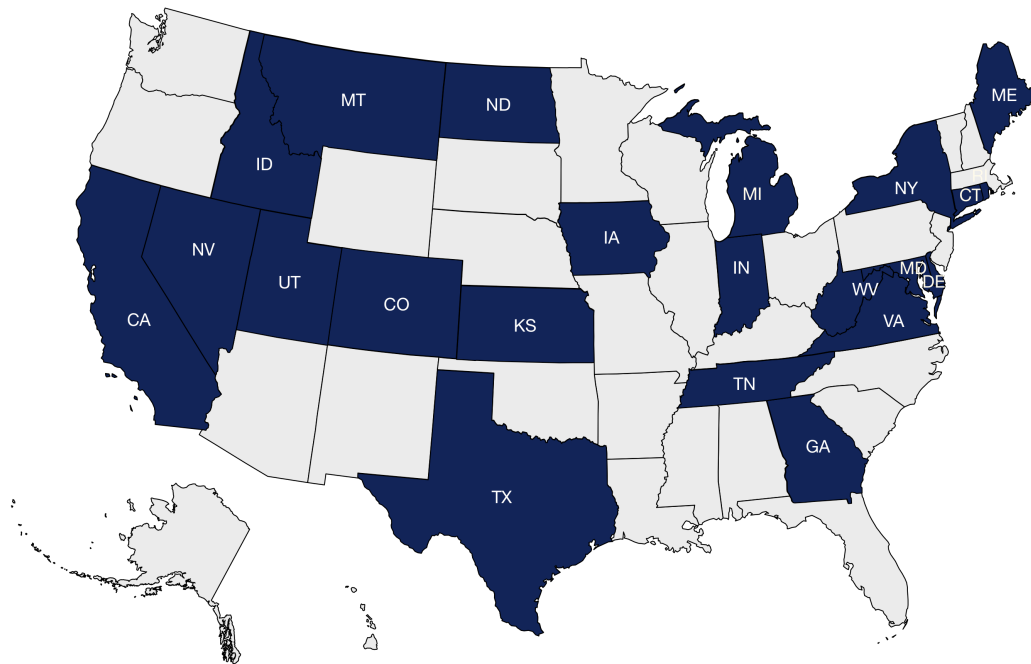
Chapter 10 | Cybersecurity Initiative

Cybersecurity is not a single issue. It represents a set of interconnected topic areas that are the province of government agencies, the private- and non-profit sectors, and individuals. Recognizing the complexity and broad reach of cybersecurity, many state governments have launched multi-stakeholder initiatives to bring relevant parties to the table. Initiatives allow states to address cybersecurity holistically and to focus limited resources towards pressing aspects of the cybersecurity challenge. This section reviews cybersecurity initiatives across the nation, discusses two case studies, and presents a structure for the Kentucky Cybersecurity Council. It then concludes with recommendations on best practices for structuring a multi-stakeholder initiative.

What is a cybersecurity initiative?

22 states have established government-sponsored or -supported bodies or efforts that are tasked with addressing cybersecurity issues (see Figure 1). While all these states have undertaken cybersecurity initiatives, no two initiatives are alike. Variable factors include structure, purpose, type, authority, method of establishment, and number and responsibilities of participants. Some states, like Michigan and Texas, have prioritized private sector involvement, while other states have focused on internal measures and improving the state government's cybersecurity posture. The number of initiative members or participants varies from two to over 15, and some initiatives are permanent bodies, while others have a fixed timeline and end date.

Figure 1 // States with a cybersecurity initiative



State-by-state comparison

The following tables describe the method of establishment, type, participants, and roles and responsibilities across statewide cybersecurity initiatives in 22 states.

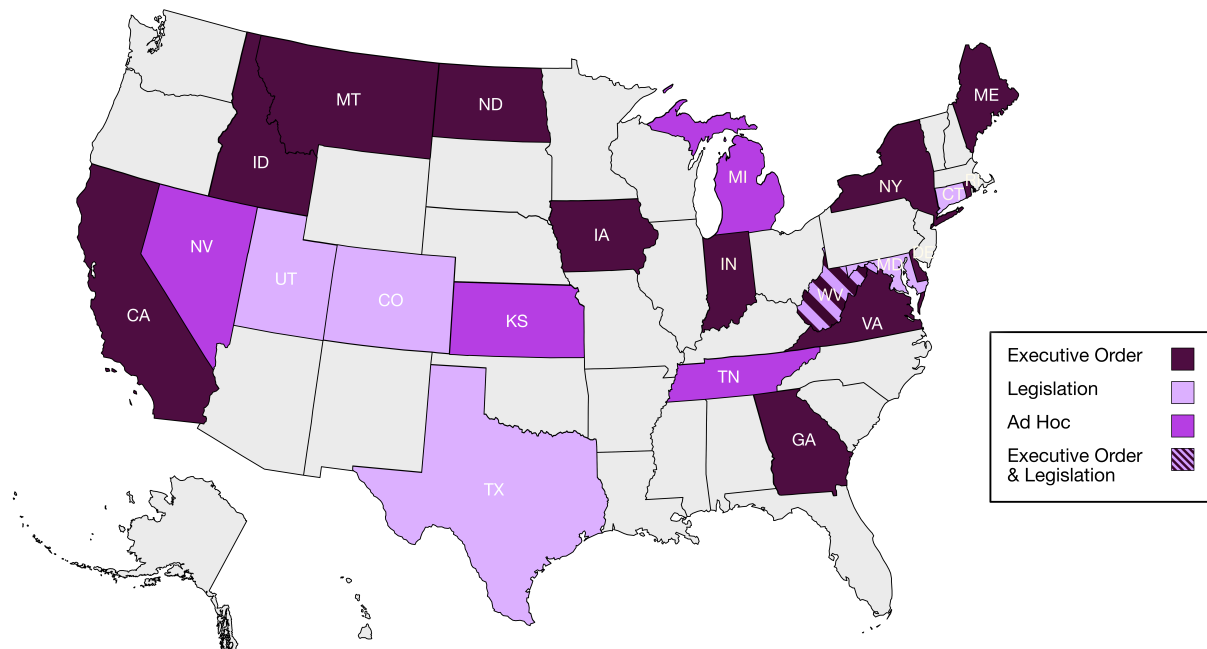
By method of establishment

As of late 2016, 22 states have created some sort of cybersecurity initiative and, while they tackle different issues in diverse ways, all were created through one of four methods: by executive order; legislation; a combination of executive order and legislation; and ad hoc^{clxv}. Executive order was the most common method of establishment, with 12 states; legislation was the second most common, with five states; four states created initiatives on an ad hoc basis; and only one state established a cybersecurity initiative through a combination of executive order and legislation (see Figure 2).

In the case of West Virginia, the only state to create its cybersecurity initiative through executive and legislative action, Governor Joe Manchin III issued an executive order establishing a statewide Chief Privacy Officer (CPO) role and creating a cyber initiative. The CPO role, initiative, and other directives were then incorporated into legislation.

Ad hoc initiatives in Kansas, Michigan, Nevada, and Tennessee were initiated by the governor but not codified by an executive order or legislation. For example, because of Michigan Governor Rick Snyder's decision to make cybersecurity a priority for his office and for the state, the state formed a Cyber Advisory Board to provide private industry and the governor a means to collaborate on cybersecurity.

Figure 2 // Method of initiative establishment

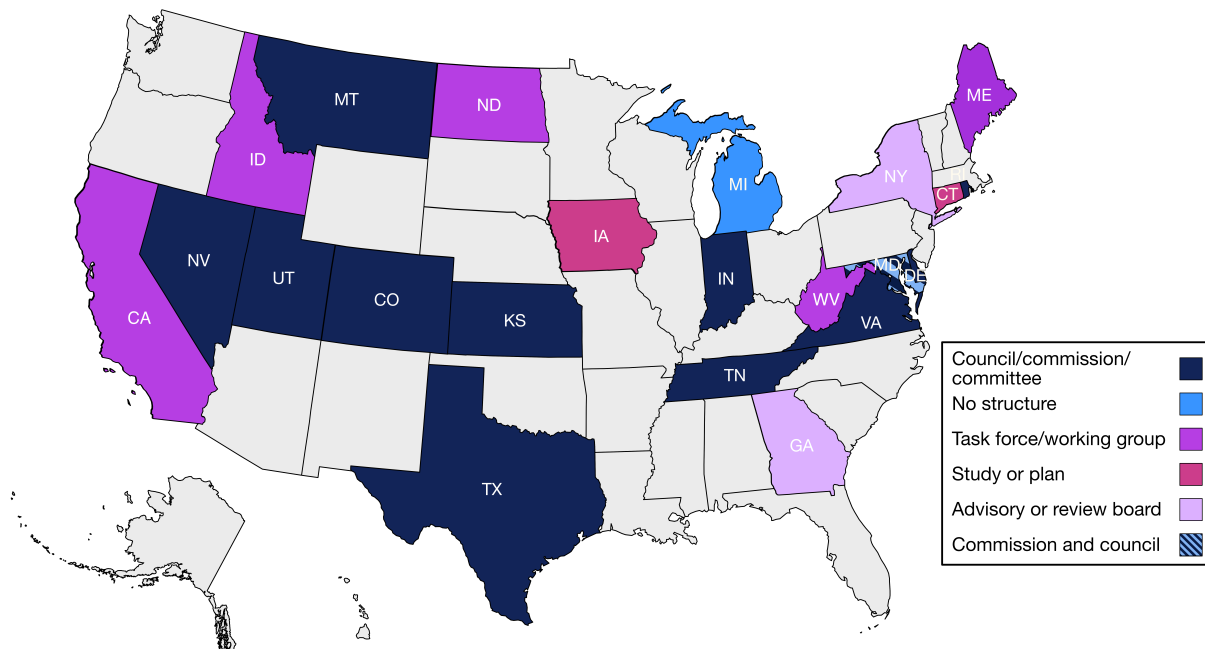


By type

Statewide initiatives have taken different forms in different contexts; by our categorization, there are five types (see Figure 3). A **council, commission, or committee** is the most common type of initiative, with twelve states; a **task force or working group** was created in five states; a **study or plan** and **advisory or review board** were assembled in two states each, and an initiative in one state has **no formal structure**. (Michigan, whose initiative has no structure, is discussed further in a case study on page 154.)

Maryland is the only state with two types of initiatives, as it has both the Maryland Cybersecurity Council and the Commission on Maryland Cybersecurity Innovation and Excellence. The Council conducts risk assessments of critical infrastructures, assists private businesses in implementing the NIST framework, and develops a strategic cyber response plan. The three-year Commission is tasked with reviewing state and federal cybersecurity laws, evaluating Maryland's role in promoting cyber innovation, recommending methods to attract cyber investment, and developing a strategic plan for cybersecurity innovation and excellence.

Figure 3 // Type of Initiative



By participants

Like the establishment and type of initiative, the participants vary greatly between state to state (see Table 1). Generally, there are 14 different types of organizations that participate in cybersecurity initiatives in various configurations, although all 22 initiatives have at least one representative from the state government's **IT department**, which may be centralized or federated depending on the state. While it is not surprising that every cybersecurity initiative involved the state government's IT function, it is notable that this was the only element common to all initiatives.

Higher education (specifically, public universities) are involved in 13 initiatives in some capacity. This is related to higher education's role in promoting cybersecurity education and the education of cybersecurity professionals, or – in some cases – it concerns the security and protection of sensitive data held by the universities themselves.

Private sector representatives are present on ten initiatives and often provide industry insight and input on policy and standards discussions. Initiatives with private sector representatives have an external component and are not focused solely on the state government's internal cybersecurity posture.

State homeland security agencies are involved in 14 initiatives and are usually involved with cyber attack mitigation, prevention, and response management. For similar reasons, **state emergency management** is represented in ten initiatives and the **state National Guard** component is represented in seven.

Other types of state government agencies are included in a number of initiatives. **Commerce and revenue** departments participate in six initiatives, as do **public safety** and **health** departments. **State administrative services** agencies are included in five initiatives. To represent the law enforcement perspective, **state attorney general's offices** participate in seven initiatives and **state police** in five initiatives. **State legislatures** and **economic development** agencies are the least represented elements, participating in three initiatives each.

Table 1 // Initiative participants

	IT Department	Higher Education	Homeland Security	Emergency Management	Commerce or Revenue	National Guard	Administrative Services	Attorney General	Public Safety	State Police	Health	Legislature	Economic Development	Private Sector
California														
Colorado														
Connecticut														
Delaware														
Georgia														
Idaho														
Indiana														
Iowa														
Kansas														
Maine														
Maryland														
Michigan														
Montana														
Nevada														
New York														
North Dakota														
Rhode Island														
Tennessee														
Texas														
Utah														
Virginia														
West Virginia														

By roles and responsibilities

The last – but perhaps most important – feature of an initiative is its roles and responsibilities. This element is greatly influenced by the initiative’s establishment, which usually dictates its authority and power; by its type, which is informed by the method of establishment and the roles and responsibilities; and by its membership, which is also determined by the initiative’s roles and responsibilities. The 22 initiatives spanned 16 different roles and responsibilities, with some initiatives having multiple goals and others having just one (see Table 2).

17 initiatives were tasked to **recommend policy to improve the state’s cybersecurity posture**. This was the most common goal and was often paired with one or more other goals to better focus the initiative’s efforts. In a similar vein, five initiatives worked to **facilitate collaboration and/or advise the government**. This collaboration could be intra-governmental or public-private, depending on the initiative. The advisory role includes advocating for cybersecurity best practices and standards across state government and providing expertise on cybersecurity issues. Five initiatives are likewise tasked with **identification, recommendation, and/or implementation of cybersecurity best practices**. Initiatives may have all three, or some combination, of the above tasks related to cybersecurity best practices.

Some responsibilities are focused on cyber attacks; for example, five initiatives are tasked with **identification and detection of cyber threats**. The initiatives with this role often include members from state homeland security and emergency management. This is true of **cyber incident response/cyber emergency preparedness**, which three initiatives are tasked to address.

Two initiatives must **create a strategic cybersecurity framework/strategy**, which often requires diverse stakeholder participation and focuses largely on state government. **Cyber awareness training for state employees**, a priority for three initiatives, is closely tied to a comprehensive cybersecurity framework, as is **recommendation of training and exercise best practices**, which is a responsibility of two initiatives. **Recommendations for improving critical infrastructure resiliency** is another aspect of a general cybersecurity framework that just one initiative focuses on. **Improving information sharing** is a wide-ranging directive that three initiatives are tasked with handling. The task often requires the involvement of many cyber stakeholders in state government and the private sector to establish a culture of information sharing and to ensure an awareness and understanding of the benefits of information sharing. **Establishment of data breach reporting and notification requirements** is a goal of one initiative (note that Kentucky has already met this goal with the passage of House Bills 5 and 232).

There are economic and workforce-related aspects of cybersecurity initiatives as well, including the **facilitation of cybersecurity-related economic development** (four initiatives) and **ensuring a robust cyber workforce and talent pipeline** (two initiatives). Cybersecurity-related economic development not only involves state economic development bodies but sometimes also relies on private sector stakeholder feedback for the state to better understand what measures would promote economic growth. A cyber workforce requires that higher education be committed and engaged in the cybersecurity initiative.

There are several tasks that are wide-ranging, including **identification sources and methods for accomplishing recommendations** (two initiatives), and **recommendation of a governance structure** (one initiative), which seeks to create an overarching state government body that is responsible for cybersecurity. Finally, three initiatives are explicitly tasked with **educating the public** on cybersecurity, a task that encompasses citizen outreach and holding public informational and stakeholder meetings.

Table 2 // Initiative roles and responsibilities

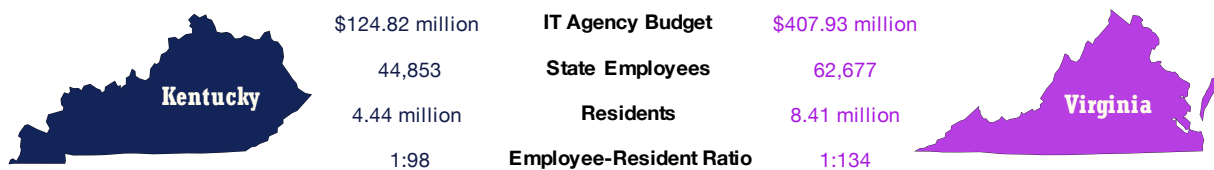
	Make policy recommendations	Facilitate collaboration/advise government	Identify, recommend, implement best practices	Identify and detect threats	Identify methods to fulfill recommendations	Create a strategy or framework	Improve critical infrastructure resiliency	Ensure robust workforce and talent pipeline	Improve cyber awareness training	Cyber incident response or cyber emergency	Facilitate economic development	Establish data breach reporting and notification	Training and exercise best practices	Improve information sharing	Educate the public	Recommend a governance structure
California																
Colorado																
Connecticut																
Delaware																
Georgia																
Idaho																
Indiana																
Iowa																
Kansas																
Maine																
Maryland																
Michigan																
Montana																
Nevada																
New York																
North Dakota																
Rhode Island																
Tennessee																
Texas																
Utah																
Virginia																
West Virginia																

Case Study: Virginia Cyber Security Commission

Cybersecurity is a priority for the Commonwealth of Virginia for good reasons. Because of its proximity to Washington, DC, Virginia is home to many Federal Government agencies and contractors that demand (and can pay for) a skilled cybersecurity workforce. It is also where vital digital infrastructure is located; approximately one-third of the world’s Internet-based activity runs through Amazon Web Services, which has multiple data centers in northern Virginia.

Key Takeaways
Fixed timeline
Independent body
Public and private sector participation
Active stakeholder engagement

Figure 4 // Kentucky and Virginia by the numbers



*The graphic above is provided for comparative purposes.
IT Agency Budget refers to the estimated 2016-17 budget for the Commonwealth Office of Technology in Kentucky and for the Information Technology Agency in Virginia.
State Employees refers to the number of people employed by the state in 2015, excluding education employees.
Employee-resident Ratio refers to the ratio of state employees to the number of residents.*

Governor McAuliffe established the Virginia Cyber Security Commission by executive order in 2014. The governor considered cybersecurity a priority upon entering office, and the structure of the commission took shape around this priority. The Commission was established for a fixed period because Virginia governors are prohibited from seeking immediate re-election after their four-year term is complete. (Note that the Commission completed its work in March 2016, before the completion of Governor McAuliffe’s term, allowing for implementation of recommendations.) While an end date could be a constraint for tackling an issue as broad as cybersecurity, it also presented a clear, time-delimited opportunity for realizing meaningful accomplishments.

While the Commission had a substantial government presence, it was designed to involve private sector leadership. When the Commonwealth invited industry experts to submit resumes, many people applied, signaling high interest from the cybersecurity community. Ultimately, the Governor appointed 11 citizen members in addition to five government cabinet secretaries, organized under a citizen co-chair and a government co-chair (see Figure 5 for a complete organization chart).

The Commission also appointed a citizen member to be its executive director, who managed daily operations. The executive director was the only paid position, meaning that the Commission did not need to secure significant funds for staffing. In fact, budget had already been allocated for cybersecurity-related activities, and the Commission was able to apply those funds to its work.

Figure 5 // Virginia Cyber Security Commission organizational chart



The commission was tasked with studying the state of cybersecurity in Virginia as it relates to five issue areas, as shown in Figure 6. The Commission selected these areas early in the process, in order to make efficient use of its limited time.

Figure 6 // Virginia Cyber Commission Issue Areas



The Commission held town hall meetings to solicit public input, and it also organized focused working groups with subject-matter experts for each issue area. The Commission ultimately produced a series of reports that described the current state of each issue area, along with specific stakeholder recommendations. Notably, the Commission didn't include any individual who could set policy; instead, its outputs served an advisory function. The Commission also produced a website with cybersecurity resources and minutes from its meetings.

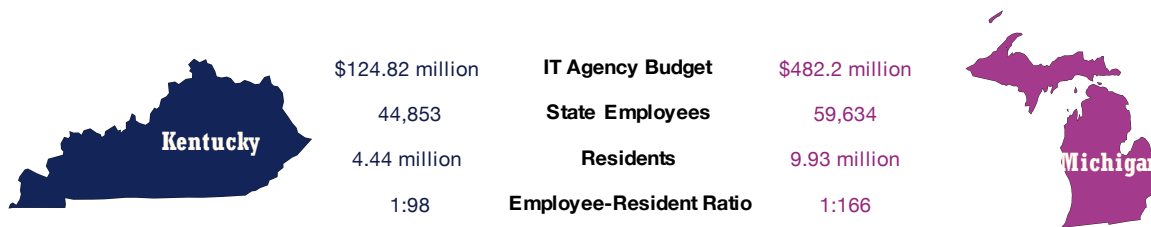
The experience of the Commission offers helpful lessons. First, the built-in end-date was beneficial in preventing repetitive discussions and a loss of momentum. It also spurred the Commonwealth to respond swiftly to recommendations, which were often addressed through legislative and executive actions while the Commission was still active. However, the Commission did lack dedicated staff; this presented some hurdles to implementation and underscores the need for adequate resourcing.

Case Study: Michigan Cyber Initiative

Governor Rick Snyder was elected to office in 2011, following a career in IT and finance that gave him both an understanding of cybersecurity and the desire to make it a top priority for Michigan. The Michigan Cyber Initiative began in late 2011 with an action plan from the governor, which detailed the initiative’s wide-ranging goals. The initiative is an interagency, public-private collaborative effort designed to raise awareness, provide robust solutions to complex cybersecurity problems in the state, and improve the state’s cybersecurity posture.

Key Takeaways
Indefinite timeline (continuing function)
Executive support
Comprehensive scope
Private sector participation
No independent structure or body

Figure 7 // Kentucky and Michigan by the numbers



*The graphic above is provided for comparative purposes.
IT Agency Budget refers to the estimated 2016-17 budget for the Commonwealth Office of Technology in Kentucky and for the Department of Technology, Management, and Budget in Michigan.
State Employees refers to the number of people employed by the state in 2015, excluding education employees.
Employee-Resident Ratio refers to the ratio of state employees to the number of residents.*

The Michigan Cyber Initiative spans various parts of the state government. On one end of the spectrum, it covers security through the Michigan State Police’s Michigan Cyber Command Center, which aims to coordinate the efforts of cyber emergency responders. On the other end, it addresses education through the Cyber Range, a public-private partnership that provides certifications and training (among other functions). The Cyber Advisory Board – which meets quarterly with the Governor – has executive-level representation from the finance and healthcare industries, the critical infrastructure community, and startup companies. The Board has seen a high level of engagement, and industry sectors have broken off to form their own sector-specific cybersecurity committees.

Unlike other multi-stakeholder initiatives, the Michigan Cyber Initiative lacks a formal structure, staff, or budget. However, several aspects of the initiative are spearheaded by David B. Behen, who is Michigan’s Chief Information Officer and the Director of the Division of Technology, Management, and Budget (DTMB). DTMB manages the state government’s IT systems, which are centralized under DTMB’s control – a notable step towards an enhanced cybersecurity posture. (It should be noted that Michigan is a leader in implementing best practices like these. In 2012, it merged its physical security and cybersecurity functions by creating a single Chief Security Officer position, centralizing decision-making across two domains that are becoming more integrated as time goes on.)

Initiative 1.0, the program’s first phase, ran from its inception in 2011 to 2015. Initiative 1.0 yielded a summary report that detailed the initiative’s numerous accomplishments, including:

- Multiple cyber exercises
- An overhaul of government employee cybersecurity training
- The creation of the Michigan State Police’s Cyber Command Center

- The creation of the Cyber Range
- The creation of the Michigan Cyber Civilian Corps, an effort to create cyber incident rapid response teams
- The publication of the Michigan Cyber Disruption Response Strategy

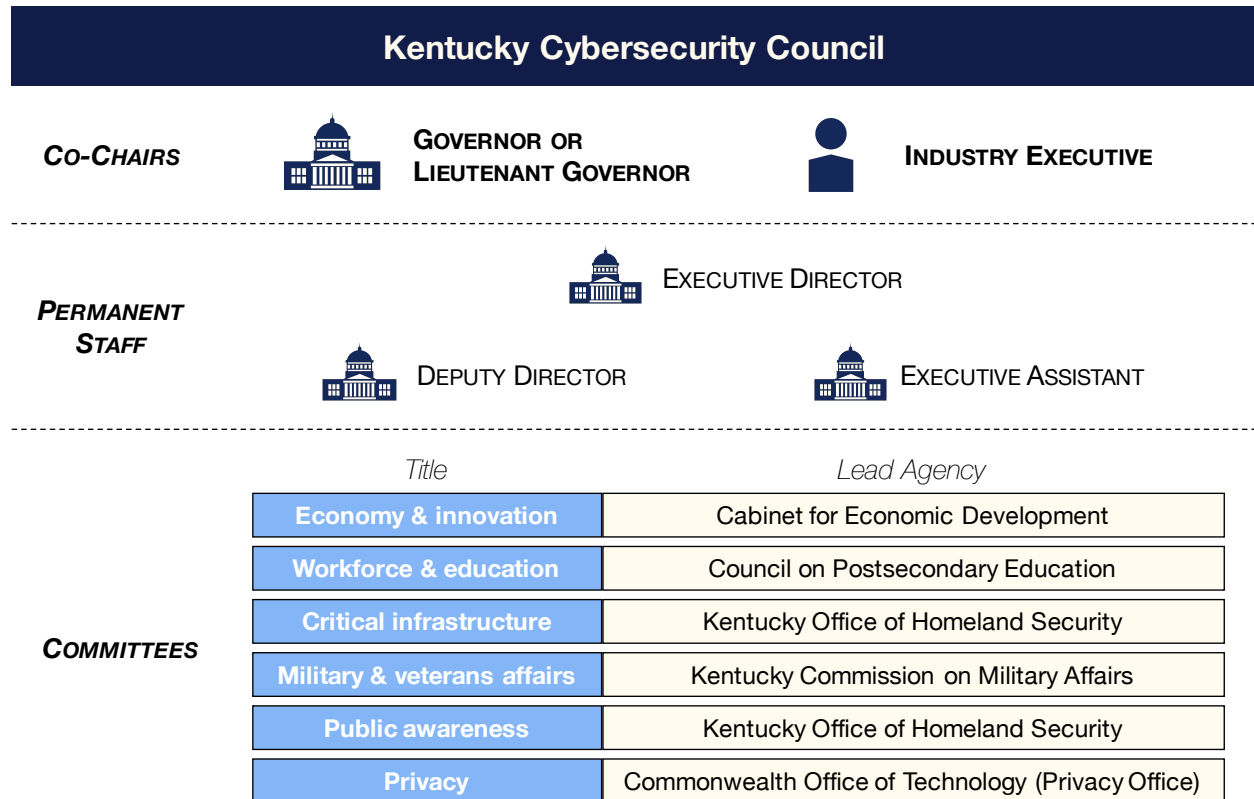
The second phase, Initiative 2.0, is underway and is scheduled to run until 2018.

Michigan's experience offers valuable guidance to decision-makers in other states. First, the state's success can be attributed to strong support from the governor and from the public-private partnerships that characterize many of the initiative's accomplishments. The governor's commitment, in the form of active involvement in initiative projects and increasing cybersecurity-related funding for the DTMB, proved critical in raising the profile of the initiative and ensuring success. Michigan's leaders promote a highly integrated and collaborative governance environment across all aspects of cybersecurity, streamlining decision-making and resourcing processes. It is important to remember that the initiative's lack of a formal structure is viable in large part because control of the state government's information technology is centralized within DTMB – meaning that DTMB's existing staff are empowered to advance the initiative's objectives.

The Kentucky Cybersecurity Council

Based on our analysis of Kentucky’s cybersecurity landscape, we recommend that the Commonwealth establish the Kentucky Cybersecurity Council (KCC, or the Council) in accordance with the structure depicted in Figure 8. The Council would be a comprehensive cybersecurity initiative that cuts across disciplines and draws on the best practices and lessons learned from the experiences of other states. It should be forward-leaning, action-oriented, and collaborative. The KCC should be a permanent organizational unit attached to the Office of the Governor.

Figure 8 // A structure for Kentucky’s cybersecurity initiative



At the helm of the KCC would be two co-chairs: the Governor (or the Lieutenant Governor) and a Governor-appointed industry executive. The co-chair structure ensures that both public and private sector concerns are appropriately considered. The co-chairs would set the agenda for the Council, serving strategic direction, guidance, and decision-making functions. The co-chairs would also preside over full Council meetings, which would occur on a biannual basis.

The KCC should be staffed by three permanent state government employees, who would represent the only salaried positions. The **executive director** would function like a chief operations officer, responsible for putting the Council’s strategic direction into practice. He or she would set tactical objectives and milestones for each of the committees, vet and validate findings, and ensure the Council’s recommendations are implemented. The executive director should bring considerable executive-level cybersecurity experience gained from both public and private sector roles. The **deputy director** would function in a senior policy role, providing research, analytic, and stakeholder engagement support to both the executive director and the committees. The **executive assistant** would handle administrative and coordination functions for the Council.

The Council would have six committees, each of which would comprise both public and private sector members. Each of the committees would meet independently on a quarterly basis, and each meeting would build on specific actions taken since the previous quarter. Each committee would be led by a representative of a Kentucky government agency. The committees are designed to be permanent, but biannual Council meetings would review the committee structure to determine whether changes are required. Committees may range in size, but they will probably average about a dozen members – whose inclusion depends on active and committed participation. In Table 3, we list responsibilities and members (lead agency in bold) for each committee, along with the chapters of this study whose recommendations each committee would be responsible for implementing.

Table 3 // KCC committees

Committee	Ch.	Responsibilities	Members
Economy & innovation	1, 2	<ul style="list-style-type: none"> • Attraction and retention of cybersecurity companies • Investments in research and development • Economic incentives • Kentucky’s cybersecurity brand • Economic analysis 	<ul style="list-style-type: none"> • Cabinet for Economic Development • KY Innovation Network • Universities • Industry associations • Chambers of commerce • Cybersecurity companies
Workforce & education	3, 4	<ul style="list-style-type: none"> • Postsecondary education • Primary and secondary education • Workforce training • Workforce framework adoption • Education and workforce analysis 	<ul style="list-style-type: none"> • Council on Postsecondary Education • Universities • KY Department of Education • School districts • Cybersecurity companies
Critical infrastructure	5	<ul style="list-style-type: none"> • Risk management • Emergency management • Training and exercises • Information sharing (intra-government + public-private) • Continual process improvement 	<ul style="list-style-type: none"> • KY Office of Homeland Security • KY Emergency Management • KY National Guard • Kentucky State Police • Commonwealth Office of Technology • CCI owners and operators
Military & veterans affairs	6	<ul style="list-style-type: none"> • Integration with DoD and National Guard • Veterans workforce development 	<ul style="list-style-type: none"> • KY Commission on Military Affairs • KY National Guard • KY Department of Veterans Affairs • DoD installations • Veterans associations • Defense contractors
Public awareness	7, 8	<ul style="list-style-type: none"> • Cybersecurity guidelines for organizations and individuals • Resource promotion • Fraud and scams • Small business outreach 	<ul style="list-style-type: none"> • KY Office of Homeland Security • Office of Attorney General • Cabinet for Economic Development • Kentucky State Police • Industry associations • Cybersecurity companies
Privacy	9	<ul style="list-style-type: none"> • Privacy 	<ul style="list-style-type: none"> • Commonwealth Office of Technology (Chief Privacy Officer) • Public interest ombudsman • Industry associations

Recommendations

Nearly half of all states have created some sort of cybersecurity initiative. In interviews, initiative principals stressed that their states benefitted in terms of enhanced coordination – not just within government, but also between the government and the private sector. Initiatives have also increased awareness of cybersecurity issues, and they have translated that awareness into actions that organizations can take to bolster their own cybersecurity. Initiatives provide a structured mechanism for stakeholders across the state to inform the government’s policy decisions on cybersecurity issues. An initiative with authority or – at the very least – stakeholder buy-in, could fill gaps identified in tabletop exercises and possibly serve as an advisory body to the governor and legislature on matters pertaining to cybersecurity.

It is not a matter of whether a cybersecurity initiative is necessary for Kentucky; it is. As Commonwealth decision-makers consider how to implement that governance structure, our review of multi-stakeholder initiatives highlights several best practices, namely:

- **Ensure executive buy-in.** The most successful initiatives are led by the Governor or the Governor’s executive-level designee. Inducing agencies and companies to prioritize cybersecurity is a challenge that the Governor’s public commitment can help overcome.
- **Ensure legislative involvement.** The legislature plays a vital role before (for budgeting and scoping), during (to provide advice), and after (to craft laws that achieve the initiative’s outcomes) initiative-driven activities. Ideally, the legislature would collaborate with the executive on the establishment and management of an initiative.
- **Set actionable goals and ambitious timelines.** Successful initiatives have clearly defined goals and the urgency that a serious issue like cybersecurity deserves. Most states still need to solve yesterday’s problems; they are in catch-up mode and need to act accordingly in order to prepare for the future’s problems.
- **Treat cybersecurity holistically.** Because cybersecurity is not a single challenge, its solutions should not be either. The purpose of a multi-stakeholder initiative is to allow policies on otherwise dissimilar issues (like education and critical infrastructure protection) to be developed and aligned in the context of cybersecurity. It is important for participants to collaborate and not retreat to familiar corners.
- **Commit adequate resources.** Although it is vital that an initiative involve many people who have “other” day jobs, an initiative that spans multiple domains should have staff dedicated to meeting the initiative’s objectives. This is especially true for Kentucky’s state government, which has not yet fully centralized its information technology. Resources should also be committed for coordination activities (to include workshops and focus groups) as necessary.
- **Include the public.** Cybersecurity is everyone’s responsibility, and the creation of an initiative presents an excellent opportunity to reach Kentucky’s citizens and convey fundamental messages about the importance of cybersecurity.
- **Develop a cybersecurity strategy.** Last but certainly not least, the Kentucky Cybersecurity Council should build on the findings of this study to develop a comprehensive statewide cybersecurity strategy. The strategy should be sweeping in scope but practical in design, and it should have achievable goals tied to measurable objectives that yield clearly defined outcomes.

Acknowledgments



Acknowledgments

In order to better understand Kentucky’s cybersecurity industry, we talked with many stakeholders, without whom this report would not have been possible. The table here does not include the more than 20 people who responded on behalf of their organizations to our industry survey, but we are equally grateful to them for their time and expertise.

Organization	Name
Office of the Lieutenant Governor of Kentucky	Lieutenant Governor Jenean Hampton
	Steve Knipper
Kentucky Commission on Military Affairs	MG (Ret.) Robert Silverthorn
	COL (Ret.) Blaine Hedges
	1st Lt (Ret.) Stewart Ditto
	Stacey Shane
Commonwealth Office of Technology	David Carter
Kentucky National Guard	LTC William Ewing
	Dean Kendrick
	CPT Dayna Sanders
	Jimmy Caudle
Department of Homeland Security	Gregory Howard
	Klint Walker
Kentucky Office of Homeland Security	John Holiday
	Jason Childers
	Kayla Matola
Kentucky Office of the Attorney General	John Moberly
Kentucky Emergency Management	Michael Dossett
	COL Wayne Burd
	Harry James
	Steven Brukwicki
	Sharon Goode

Organization	Name
Cabinet for Economic Development	Joe Lilly
	Caroline Baesler
	Karen Lefler
	Emmanuel Kyeremeh
	Josh Benton
Kentucky Center for Education and Workforce Statistics	Dr. Kate Akers
	Dr. Jessica Cunningham
	Barrett Ross
Kentucky State Police	Maj. Jeff Medley
	Cpt. Michael T. Kidd
	Lt. Jeremy Murrell
	Jerry Wright
	Angela Parker
Technology Association of Louisville Kentucky	Dawn Yankeelov
Kentucky Association of Manufacturers	Karen Ellis
Virginia Office of the Secretary of Technology	Secretary Karen Jackson
Michigan Department of Management, Technology, and Budget	David Behen
	Rajiv Das
	Ashley Gelisse
	Caleb Buhs
Washington Office of Privacy and Data Protection	Alex Alben
South Carolina Enterprise Privacy Office	Theodora Wills
	Alex White
	Michele Perrick
West Virginia Health Care Authority	Sallie Milam
Maryland Finance Programs	Mark Vulcan

Appendices



Appendix A: Key terms

In this section, we provide a list of key terms used throughout the report.

Term	Definition
Chief privacy officer	An individual who is responsible for strengthening privacy protections and assessing how privacy considerations impact process and decisions within his or her organization.
Compromise	The digital equivalent of a physical intrusion that occurs when a user or application gains access to data, an application, a system, a service, or a network without authorization to do so. A compromise can result in a degradation of the asset’s operability, and/or the loss or corruption of data.
Critical infrastructure	Defined by PCCIP as “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”
Cybercrime	An illegal act that has compromise (see compromise) of digital assets as its end goal or as a means to an end.
Cyber critical infrastructure	Digital and physical assets located in Kentucky, the compromise or failure of which would cause harm to critical functions across the public and private sectors.
Cyber disruption event	A compromise or failure that results in harm (see harm).
Cybersecurity	The protection of electronic information and the devices, applications, and networks used to generate, access, transfer, or store electronic information.
Cybersecurity company	A for-profit Kentucky-based company that sells cybersecurity capabilities (products, services, or both).
Cybersecurity initiative	A government-sponsored or –supported body or effort that is tasked with addressed cybersecurity issues.
Cybersecurity sector	Encompasses a broad diversity of companies, including large software providers that sell event monitoring systems, consultancies that advise on cybersecurity strategy, and non-profits that produce cutting-edge encryption technologies. Some companies sell products, some companies sell services, and some companies sell both. The sector also includes cybersecurity workers at non-cybersecurity companies.
Digital assets	Electronic information and the applications, systems, and networks used to generate, access, transfer, or store electronic information. Examples include citizens’ health records and industrial control systems.

Term	Definition
Failure	The inoperability of an asset, possibly as the result of a compromise, accident, or natural disaster.
Harm	1) Impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks that provide direct information technology services or enabling and support capabilities for other services; and/or 2) Threatening public safety, undermining public confidence, having a negative effect on the state economy, or diminishing the security posture of the state.
Physical assets	Hardware, people, facilities, and other tangible infrastructure upon which virtual assets depend to function. Examples include data centers, emergency operations centers, and essential operational and support personnel and equipment.
Security breach	See compromise.

Appendix B: Acronyms

In this section, we provide a list of acronyms used throughout the report.

Acronym	Definition
AIG	American International Group
AIQ	asset in question
ASTeCC	Advanced Science & Technology Commercialization Center
BENS	Business Executives for National Security
BGAD	Blue Grass Army Depot
BGCA	Blue Grass Chemical Activity
BGCAPP	Blue Grass Chemical Agent-destruction Pilot Plant
BIITC	Maryland's biotechnology investment incentive tax credit
C	consequence
CAE	National Center for Academic Excellence
CAE-CD	National Center for Academic Excellence in Cyber Defense
CAE-CDE	National Center for Academic Excellence – four-year cyber defense education program
CAE-CO	National Center for Academic Excellence in Cyber Operations
CAE-R	National Center for Academic Excellence – cyber defense research program
CAE-2Y	National Center for Academic Excellence – two-year cyber defense education program
CASP	CompTIA Advanced Security Practitioner
CCENT	Cisco Certified Entry Network Technician
CCFP	ISC(2) Certified Cyber Forensics Professional
CCI	cyber critical infrastructure
CCIA	cyber critical infrastructure asset
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CD	cyber defense
CECS	department of Computer Engineering and Computer Science
CED	Kentucky Cabinet for Economic Development
CEH	EC-Council Certified Ethical Hacker

Acronym	Definition
CEO	Chief Executive Officer
CI	critical infrastructure
CIITC	Cybersecurity Investment Incentive Tax Credit
CIO	Chief Information Officer
CIS	Center for Information Security – University of Louisville
CIS	department of Computer Information Systems
CISA	ISACA Certified Information Systems Auditor
CISCP	Cyber Information Sharing and Collaboration Program
CISM	ISACA Certified Information Security Manager
CISO	Chief Information Security Officer
CISSO	Chief Information Systems Security Officer
CISSP	ISC(2) Certified Information Systems Security Professional
CO	cyber operations
COG	Continuity of Government Plan
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COT	Commonwealth Office of Technology
CPO	Chief Privacy Officer
CSBS	Conference of State Bank Supervisors
CSCG	Commonwealth’s Systems and Communications Group
CSET	Cyber Security Evaluation Tool
CSI	Cyber Security Initiative
CSF	cybersecurity framework
CSIS	Center for Strategic and International Studies
CWC	Chemical Weapons Convention
DHS	Department of Homeland Security
DFI	Kentucky Department of Financial Institutions
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DTMB	Michigan Deivision of Technology, Management, and Budget
ELOC	Executive Leadership of Cybersecurity Seminar

Acronym	Definition
EO	Executive Order
EOC	Emergency Operations Center
EOD	explosive ordnance disposal
EOP	Emergency Operation Plan
EPO	Enterprise Privacy Office
ESF	Emergency Support Function
E3	Ohio Environmental Protection Agency's Encouraging Environmental Excellence Program
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
FKICAN	Fort Knox Installation Campus Area Network
GCC	Government Coordinating Council
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
GICSP	GIAC Industrial Cyber Security Professional
GDP	gross domestic product
GPEN	GIAC Penetration Tester
GSE	GIAC Security Expert
GSEC	GIAC Security Essentials Certification
GSLC	GIAC Security Leadership Certification
HB5	Kentucky House Bill 5
HB232	Kentucky House Bill 232
HIPAA	Health Insurance Portability and Accountability Act
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISP	internet service provider
IT	information technology

Acronym	Definition
KANG	Kentucky Air National Guard
KBI	Kentucky Business Investment program
KCC	Kentucky Cybersecurity Council
KCEWS	Kentucky Center for Education and Workforce Statistics
KCMA	Kentucky Commission on Military Affairs
KCTCS	Kentucky Community and Technical College System
KEDFA	Kentucky Economic Development Finance Authority
KEF	Kentucky Enterprise Fund
KEIA	Kentucky Enterprise Initiative Act
KIFC	Kentucky Office of Homeland Security Intelligence Fusion Center
KPSC	Kentucky Public Service Commission
KRS	Kentucky Revised Statues
KYARNG	Kentucky Army Reserve National Guard
KYEM	Kentucky Emergency Management
KOHS	Kentucky Office of Homeland Security
LDA	Louisville Digital Association
MCAP	Malicious Code Analysis Platform
MCR	Michigan Cyber Range
MS-ISAC	Multi-State Information Sharing and Analysis Center
NAICS	North American Industrial Classification System
NASCIO	National Association of State Chief Information Officers
NCCIC	National Cybersecurity and Communications Integration Center
NCSA	National Cyber Security Alliance
NCSR	Nationwide Cybersecurity Review
NCWF	National Initiative for Cybersecurity Education Cybersecurity Workforce Framework
NEC	Network Enterprise Center
NERC	North American Electricity Reliability Corporation
NGA	National Governors Association
NICCS	National Initiative for Cybersecurity Careers and Studies
NICE	National Initiative for Cybersecurity Education

Acronym Definition	
NICERC	National Integrated Cyber Education Research Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NKU	Northern Kentucky University
NOC	network operations center
NRECA	National Rural Electric Cooperative Association
NRF	National Response Framework
OCIA	DHS Office of Cyber and Infrastructure Analysis
OPDP	Washington Office of Privacy and Data Protection
PCCIP	President’s Commission on Critical Infrastructure Protection
PCII	Protected Critical Infrastructure Information
PEO-ACWA	Program Executive Office, Assembled Chemical Weapons Alternatives
PII	personally identifiable information
PPD	Presidential Policy Directive
PTC	Production Tax Credit
QMCC	qualified Maryland cybersecurity company
R	risk
RAMPS	Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development
RMF	National Institute of Standards and Technology Risk Management Framework
RNEC	Regional Network Enterprise Center – Bluegrass
R&D	research and development
SBA	United States Small Business Administration
SLTT	state, local, tribal, and territorial
SMB	small- and medium-sized business
SOC	Standard Occupational Classification system
SPO	State Privacy Office
SSA	Sector-Specific Agencies

Acronym Definition	
STRIDE	spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege
T	threat
TALK	Technology Association of Louisville Kentucky
TFP	total factor productivity
USACE	United States Army Corps of Engineers
US-CERT	United States Computer Emergency Readiness Team
UTSA	University of Texas at San Antonio
V	vulnerability
VMP	Vulnerability Management Program
WaTech	Washington Technology Solutions
WKU	Western Kentucky University

Appendix C: Educational institutions and degrees

In this appendix, we show all of the degrees, diplomas, and certificates that a) were issued to Kentucky residents between 2006 and 2016 (including those that are no longer available), and b) we considered to be relevant to cybersecurity for the purposes of our analysis. The degree, diploma, or certificate title is not typically a direct match for the actual name of the program. U refers to undergraduate degrees, diplomas, and certificates; G refers to graduate and post-graduate degrees.

University or College	Level	Degree, Diploma, or Certificate
Ashland Community & Technical College	U	Computer and Information Sciences, General
Bellarmino University	G	Computer and Information Sciences, General
		Data Modeling/Warehousing and Database Administration
	U	Computer and Information Sciences, General
		Computer Engineering, General
		Computer Systems Analysis/Analyst
Berea College	U	Computer and Information Sciences, General
Big Sandy Community & Technical College	U	Computer and Information Sciences, General
Bluegrass Community & Technical College	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
		Homeland Security
		Web Page, Digital/Multimedia and Information Resources Design
Brescia University	U	Computer and Information Sciences, General
Campbellsville University	U	Computer and Information Sciences, General
Centre College	U	Computer Science

University or College	Level	Degree, Diploma, or Certificate
Eastern Kentucky University	G	Computer Science
		Homeland Security
	U	Computer and Information Sciences, General
		Homeland Security
		Computer Technology/Computer Systems Technology Computer Engineering Technologies/Technicians, Other
Elizabethtown Community & Technical College	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
Gateway Community & Technical College	U	Computer and Information Sciences, General
Georgetown College	U	Computer and Information Sciences, General
		Computer Science
Hazard Community & Technical College	U	Computer and Information Sciences, General
Henderson Community College	U	Computer and Information Sciences, General
Hopkinsville Community College	U	Computer and Information Sciences, General
Jefferson Community & Technical College	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
Kentucky State University	G	Computer and Information Sciences, General
	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
		Information Technology
Kentucky State University	U	Web/Multimedia Management and Webmaster
Kentucky Wesleyan College	U	Computer and Information Sciences, General
	U	Computer Science
Lindsey Wilson College	U	Computer and Information Sciences, General
Madisonville Community College	U	Computer and Information Sciences, General

University or College	Level	Degree, Diploma, or Certificate
Maysville Community & Technical College	U	Computer and Information Sciences, General
Midway University	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
		Homeland Security
Morehead State University	U	Computer and Information Sciences, General
Murray State University	G	Information Technology
		Media Informatics
		Information Science/Studies
	U	Computer and Information Sciences, General
		Computer Science
		Information Technology
		Media Informatics
		Information Science/Studies
Northern Kentucky University	G	Computer and Information Systems Security/Information Assurance
		Computer Science
		Computer/information Technology Services Administration and Management, Other
		System, Networking, and LAN/WAN Management/Manager
	U	Computer and Information Sciences and Support Services, Other
		Computer and Information Sciences, General
		Computer Software and Media Applications, Other
		Computer/information Technology Services Administration and Management, Other
		Information Technology
		Media Informatics
		Information Science/Studies
		Computer Programming/Programmer, General
		Computer Programming, Specific Applications
Owensboro Community & Technical College	U	Computer and Information Sciences, General

University or College	Level	Degree, Diploma, or Certificate
Somerset Community College	U	Computer and Information Sciences, General
Southcentral Kentucky Community and Technical College	U	Computer and Information Sciences, General
		Computer Technology/Computer Systems Technology
Southeast Kentucky Community & Technical College	U	Computer and Information Sciences, General
Spalding University	U	Computer and Information Sciences, General
St. Catharine College	U	Computer and Information Sciences, General
Thomas More College	U	Computer and Information Sciences, General
		Data Processing and Data Processing Technology/Technician
		Information Technology
		Web Page, Digital/Multimedia and Information Resources Design
Transylvania University	U	Computer and Information Sciences, General
Union College	U	Computer and Information Sciences, General
		Information Technology
		Computer Programming/Programmer, General
University of Kentucky	G	Computer and Information Sciences, General
		Informatics
	U	Computer and Information Sciences, General
		Computer Engineering, General
		Informatics
	Media Informatics	
University of Louisville	U	Computer Engineering, General
		Computer and Information Systems Security/Information Assurance
		Computer Engineering, General
	Data Modeling/Warehousing and Database Administration	
University of Pikeville	U	Computer and Information Sciences, General

University or College	Level	Degree, Diploma, or Certificate
University of the Cumberlands	G	Computer and Information Systems Security/Information Assurance
	U	Computer and Information Sciences, General
Western Kentucky Community & Technical College	U	Computer and Information Sciences, General
		Homeland Security
West Kentucky University	G	Computer and Information Sciences, General
		Computer and Information Sciences and Support Services
		Computer and Information Sciences, General
	U	Computer and Information Systems Security/Information Assurance
		Computer Support Specialist
		Data Processing and Data Processing Technology/Technician
		Information Technology

Appendix D: Sources

- ⁱ Data is provided by JobsEQ®, a product of Chmura Economics and Analytics.
- ⁱⁱ “Cyber Innovation Center wants to weave cybersecurity into K-12 STEM instruction,” *National Integrated Cyber Education Research Center*, accessed May 30, 2017, <http://nicerc.org/2017/03/cyber-innovation-center-wants-to-weave-cybersecurity-into-k-12-stem-instruction>.
- ⁱⁱⁱ “Kentucky Becomes the Second State in the US to Adopt the Federal Cyber Engineering Pathway Curricula Designed by NICERC for 9-12th Graders For Use In Its School Districts,” *National Integrated Cyber Education Research Center*, accessed May 30, 2017, <http://nicerc.org/2017/03/kentucky-becomes-the-second-state-in-the-us-to-adopt-the-federal-cyber-engineering-pathway-curricula-designed-by-nicerc-for-9-12th-graders-for-use-in-its-school-districts>.
- ^{iv} Sgt. 1st Class Jon Soucy, “National Guard set to activate additional cyber units,” *United States Army*, December 9, 2015, accessed April 28, 2015, https://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units.
- ^v JobsEQ®, Chmura Economics and Analytics. Occupation Reports provided for the 13 cited SOC codes.
- ^{vi} At the time this analysis was produced, IMPLAN’s economic model was derived from economic and labor data for the year 2015. For more information about IMPLAN, visit implan.com.
- ^{vii} Note that the numbers we applied were rounded to the nearest tenth of a point, but they are represented as whole numbers in Table 5.
- ^{viii} Our outputs are measured in monetary year 2017, however most data are derived from 2015 and 2016.
- ^{ix} *San Diego’s Cybersecurity Industry – Executive Summary*, Cyber Center of Excellence, 2016, accessed May 26, 2017, <https://sdccoe.org/wp-content/uploads/2015/01/CCOE-EIS-2016-.pdf>.
- ^x “Cybersecurity 500,” Cybersecurity Ventures, accessed May 26, 2017, cybersecurityventures.com/cybersecurity-500-list/#home/?view_1_per_page=500&view_1_page=1.
- ^{xi} Blanco, Luisa, James Prieger, and Ji Gu, *The Impact of Research and Development on Economic Growth and Productivity in the US States*, Pepperdine University School of Public Policy Working Papers, November 2013, accessed May 26, 2017, <http://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1047&context=sppworkingpapers>.
- ^{xii} “What is Informatics?” *Information School, University of Washington*, accessed May 26, 2017, <https://ischool.uw.edu/academics/informatics/what-is-informatics>.
- ^{xiii} “Informatics Defined,” *Indiana University-Purdue University Indianapolis School of Informatics and Computing*, accessed May 26, 2017, <https://soic.iupui.edu/about/what-is-informatics/>.
- ^{xiv} Center for Applied Informatics,” *Northern Kentucky University*, accessed May 26, 2017, <http://inside.nku.edu/informatics/centers/cai.html>.
- ^{xv} “Center for Applied Informatics,” *Northern Kentucky University*, accessed May 26, 2017, <https://www.ccs.uky.edu/About/Mission/>.
- ^{xvi} “CCS Mission & Goals,” *University of Kentucky*, accessed May 26, 2017, <https://www.wku.edu/crd/>.
- ^{xvii} Lesk, Arthur M., “Bioinformatics,” *Encyclopaedia Britannica*, accessed May 26, 2017, <https://www.britannica.com/science/bioinformatics>.
- ^{xviii} “Research Computing,” *University of Louisville Information Technology*, accessed May 26, 2017, <http://louisville.edu/it/departments/research>.
- ^{xix} “Cardinal Research cluster takes flight at University of Louisville,” *IBM Systems and Technology – Case Study*, accessed May 26, 2017, <https://www.scribd.com/document/95857949/Cardinal-Research-Cluster-takes-flight-at-University-of-Louisville>.
- ^{xx} “About,” *Louisville CIO Series*, accessed May 26, 2017, <http://www2.cecsresearch.org/cio/about.html>.
- ^{xxi} *Code Louisville*, accessed May 26, 2017, <https://www.codelouisville.org/>.
- ^{xxii} “About,” *Louisville Digital Association*, accessed May 26, 2017, <https://www.louisvilledigital.org/about/>.
- ^{xxiii} “About Us,” *Technology Association of Louisville Kentucky*, accessed May 26, 2017, http://wp.talklou.com/?page_id=4.
- ^{xxiv} “Lexington Tech Forum,” *Meetup*, accessed May 26, 2017, <https://www.meetup.com/LexingtonTechForum/>.
- ^{xxv} “About,” *Nucleus*, accessed May 26, 2017, <http://nucleusky.com/about>.
- ^{xxvi} “About,” *Awesome Inc*, accessed May 26, 2017, <https://www.awesomeinc.org/about/>.
- ^{xxvii} “Advanced Science & Technology Commercialization Center (ASTeCC),” *University of Kentucky Research*, accessed May 26, 2017, <http://www.research.uky.edu/astecc/>.
- ^{xxviii} *Eastern Kentucky University Biz-Accelerator*, accessed May 26, 2017, <http://bizaccelerator.eku.edu/>.
- ^{xxix} *UpTech*, accessed May 26, 2017, <https://www.uptechideas.org/contact/uptech/>.
- ^{xxx} “Small Business Accelerator,” *Western Kentucky University*, accessed May 26, 2017, <https://www.wku.edu/accelerator/>.
- ^{xxxi} “Startup Weekend Louisville,” *Startup Weekend*, accessed May 26, 2017, <http://communities.techstars.com/usa/louisville/startup-weekend/10720>.
- ^{xxxii} *DerbyCon*, accessed May 26, 2017, <https://www.derbycon.com/>.
- ^{xxxiii} *TechFest Lou*, accessed May 26, 2017, <http://www.techfestlou.com/techfest/>.

- xxxiv "9th Annual NKU Cybersecurity Symposium," *Northern Kentucky University*, accessed May 26, 2017, <http://chaselaw.nku.edu/centers/lawinformatics/2015cybersecuritysymposium.html>.
- xxxv "Cyberstates 2017," *CompTIA*, accessed May 26, 2017, <http://www.cyberstates.org/pdf/CompTIA%20Cyberstates%202017.pdf>.
- xxxvi Ibid.
- xxxvii "Gross domestic product 2015 - World Bank data," World Bank DataBank, April 17, 2017, accessed April 26, 2017, <http://www.bing.com/cr?IG=4A3EDBF9011240EA9BE3468188F4A539&CID=3AB993341A7C6EBB3D2599441BEC6F93&rd=1&h=QAMAD88xH6qj6NtvBAqEaW0kRYrWTPg8AeZPFIf7o&v=1&r=http%3a%2f%2fdatabank.worldbank.org%2fdata%2fdownload%2fGDP.pdf&p=DevEx,5061.1>.
- xxxviii *Net Losses: Estimating the Global Cost of Cybercrime*, McAfee, June 2014, accessed April 26, 2017, <https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>.
- xxxix "Number of firms, establishments, employment, and payroll by firm size, state, and industry," United States Small Business Administration Office of Advocacy and United States Census Bureau, accessed April 17, 2017, <https://www.sba.gov/advocacy/firm-size-data>.
- xl "Data Breach Costs Rising, Now \$4 million per Incident," IBM News Room, June 15, 2016, accessed April 26, 2017, <https://www-03.ibm.com/press/us/en/pressrelease/49926.wss>.
- xli Shelton, Bill R, "Development Incentives: Pros and Cons," *Buxton Customer Analytics & Predictive Analytics Tools for Business*, accessed April 26, 2017, <https://www.buxtonco.com/pages/development-incentives-pro-and-con/>.
- Stinson, Preston C, *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Roberts, Michael, "Why Do Cities Offer Tax Incentives to Businesses?" *The Balance*, March 01, 2017, accessed April 26, 2017, <https://www.thebalance.com/why-do-cities-offer-tax-incentives-to-businesses-1669514>.
- xlii "Program Info," Renewable Electricity Production Tax Credit (PTC), Department of Energy, accessed April 26, 2017, <https://energy.gov/savings/renewable-electricity-production-tax-credit-ptc>.
- xliiii Kosseff, Jeff, "Cybersecurity Is Expensive--That's Why We Should Offer Tax Incentives," *Forbes*, September 23, 2015, accessed April 26, 2017, <https://www.forbes.com/sites/realspin/2015/09/23/cybersecurity-is-expensive-thats-why-we-should-offer-tax-incentives/#74f9aff95483>.
- xliv Basani, Vijay, "Cybersecurity insurance – weighing the costs and the risks," *MarketWatch*, March 25, 2015, accessed April 26, 2017, <http://www.marketwatch.com/story/cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25>.
- "Cybersecurity Insurance," *Cybersecurity Insurance*, accessed April 26, 2017, <https://www.dhs.gov/cybersecurity-insurance>.
- Cunningham, Kevin, "Cyber Security Insurance: A Good Thing or a Bad Thing?" *SailPoint*, March 10, 2016, accessed April 26, 2017, <https://www.sailpoint.com/cyber-security-insurance-pros-and-cons/>.
- Discussion of Recommendations to the President of Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program*, United States Department of Commerce, accessed April 26, 2017, <https://www.ntia.doc.gov>.
- End-to-End Cyber Risk Management Solutions*, AIG, April 2015, accessed April 26, 2017, <http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyberedge0418finalsingle-brochure.pdf>.
- Silobreaker, "The Pros & Cons of Cyber Insurance," *Silobreaker*, April 29, 2016, accessed April 26, 2017, <http://www.silobreaker.com/the-pros-and-cons-of-cyber-insurance/>.
- Stinson, Preston C, *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Toregas, Costis, and Nicolas Zahn. *Insurance for Cyber Attacks: The Issue of Setting Premiums in Context*. Report. Cyber Security Policy and Research Institute, The George Washington University. January 7, 2014, accessed April 26, 2017, <http://static1.squarespace.com>.
- "What is Cyber Liability insurance?" *Cyber Security Liability*, accessed April 26, 2017, <https://www.phly.com/campaign/cybersecurity.aspx>.
- xlv Garcia, Greg, "Time for a cybersecurity grant program for the states," *The Hill*, March 01, 2017, accessed April 26, 2017, <http://thehill.com/blogs/congress-blog/technology/321871-time-for-a-cybersecurity-grant-program-for-the-states>.
- "Gov't Cybersecurity Standards Could Impact Many Companies - Law360," *Law360*, August 16, 2013, accessed April 26, 2017, <https://www.law360.com/energy/articles/463650/gov-t-cybersecurity-standards-could-impact-many-companies>.
- Stinson, Preston C, *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Uchill, Joe, "Bipartisan bill would give cybersecurity grants to state and local governments," *The Hill*, March 02, 2017, accessed April 26, 2017, <http://thehill.com/policy/cybersecurity/322050-bipartisan-bill-would-give-cybersecurity-grants-to-state-and-local>.
- xlvi Homeland Security, *United States Department of Homeland Security Integrated Task Force*, June 12, 2013, accessed April 26, 2017, <https://www.dhs.gov>.
- "Gov't Cybersecurity Standards Could Impact Many Companies - Law360," *Law360*, August 16, 2013, accessed April 26, 2017, <https://www.law360.com/energy/articles/463650/gov-t-cybersecurity-standards-could-impact-many-companies>.

- ^{xlvii} Stinson, Preston C, *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Stuntz, Joe. *An Analysis of US Government Proposed Cyber Incentives*. Report. Security and Software Engineering Research Center, Georgetown University. February 7, 2014, accessed April 26, 2017, <http://s2erc.georgetown.edu>.
- ^{xlviii} Stinson, Preston C. Incentives to Encourage Adoption of the NIST Cybersecurity Framework. Washington Internships for Students of Engineering. Journal of Engineering & Public Policy. July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Stuntz, Joe. *An Analysis of US Government Proposed Cyber Incentives*. Report. Security and Software Engineering Research Center, Georgetown University. February 7, 2014, accessed April 26, 2017, <http://s2erc.georgetown.edu>.
- "The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)," *ICS-CERT*, accessed April 26, 2017, <https://ics-cert.us-cert.gov/>.
- ^{xlix} *Cybersecurity Incentives Pursuant to Executive Order 13636*, United States Department of the Treasury, accessed April 26, 2017, <https://www.treasury.gov>.
- Wood, Theodore A., and Sean Pool, "Tapping the Patent System for Innovation in Cyber Security," *Science Progress*, August 06, 2012, accessed April 26, 2017, <https://scienceprogress.org/2012/08/tapping-the-patent-system-for-innovation-in-cyber-security/>.
- ¹ *Cybersecurity Incentives Pursuant to Executive Order 13636*, United States Department of the Treasury, accessed April 26, 2017, <https://www.treasury.gov>.
- Homeland Security, *United States Department of Homeland Security Integrated Task Force*, June 12, 2013, accessed April 26, 2017, <https://www.dhs.gov>.
- Stinson, Preston C., *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- Stuntz, Joe, *An Analysis of US Government Proposed Cyber Incentives*, Security and Software Engineering Research Center, Georgetown University, February 7, 2014, accessed April 26, 2017, <http://s2erc.georgetown.edu>.
- ⁱⁱ Discussion of Recommendations to the President of Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program, *United States Department of Commerce*, accessed April 26, 2017, <https://www.ntia.doc.gov>.
- "Encouraging Environmental Excellence (E3) Program," *Ohio Environmental Protection Agency*, accessed April 26, 2017, <http://www.epa.state.oh.us/ocapp/ohioe3.aspx>.
- Stinson, Preston C., *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- ⁱⁱⁱ Discussion of Recommendations to the President of Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program, *United States Department of Commerce*, accessed April 26, 2017, <https://www.ntia.doc.gov>.
- Homeland Security, *United States Department of Homeland Security Integrated Task Force*, June 12, 2013, accessed April 26, 2017, <https://www.dhs.gov>.
- Stinson, Preston C., *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- ⁱⁱⁱⁱ "New cybersecurity requirements for government contractors," *Baker Tilly*, June 10, 2016, accessed April 26, 2017, <http://www.bakertilly.com/insights/new-cybersecurity-requirements-for-government-contractors>.
- ^{liv} *Cybersecurity Incentives Pursuant to Executive Order 13636*, United States Department of the Treasury, accessed April 26, 2017, <https://www.treasury.gov>.
- Stinson, Preston C., *Incentives to Encourage Adoption of the NIST Cybersecurity Framework*, Journal of Engineering & Public Policy, July 31, 2014, accessed April 26, 2017, <http://www.wise-intern.org>.
- ^{lv} "Just the Facts: Kentucky Business Incentives Overview," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Just the Facts: Kentucky Business Investment (KBI) Program," *Think Kentucky*, July 2016, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Locating and Expanding in Kentucky," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- ^{lvi} "Just the Facts: Kentucky Business Incentives Overview," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Just the Facts: Kentucky Economic Development Finance Authority (KEDFA) Direct Loan Program." *Think Kentucky*. June 2011, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Locating and Expanding in Kentucky," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- ^{lvii} "Just the Facts: Kentucky Business Incentives Overview," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Kentucky Enterprise Fund," *Kentucky Science and Technology Corporation*, accessed April 26, 2017, http://www.kstc.com/index.php?option=com_content&view=article&id=137%3Akentucky-enterprise-fund&catid=38%3Amain-menu-links.

- "Locating and Expanding in Kentucky," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Strategy," *Startups@KSTC*, accessed April 26, 2017, <http://startups.kstc.com/strategy/>.
- lviii "Governor O'Malley signs cybersecurity tax credit, InvestMaryland bills," *MDBIZNews*, May 03, 2013, accessed April 26, 2017, <https://mdbiznews.commerce.maryland.gov/2013/05/governor-omalley-signs-cybersecurity-tax-credit-investmaryland-bills/>.
- "Just the Facts: Kentucky Business Incentives Overview," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Just the Facts: Kentucky Enterprise Initiative Act (KEIA)," *Think Kentucky*, March 2017, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- "Locating and Expanding in Kentucky," *Think Kentucky*, accessed April 26, 2017, http://thinkkentucky.com/Locating_Expanding/kybizince.aspx.
- lix *Consolidated Incentives Performance Report*, Maryland Department of Commerce, January 2016, accessed April 26, 2017, <http://commerce.maryland.gov>.
- "Cybersecurity Investment Incentive Tax Credit (CIITC)," *Maryland Cyber Tax Credit, Maryland Department of Commerce*, accessed April 26, 2017, <http://commerce.maryland.gov/fund/programs-for-businesses/cyber-tax-credit>.
- "Maryland Cybersecurity Investment Incentive Tax Credit," *Hertzbach*, accessed April 26, 2017, <http://www.hertzbach.com/maryland-cybersecurity-investment-incentive-tax-credit/>.
- "MontgomeryCountyMD.GOV," *Montgomery County*, accessed April 26, 2017, <https://www.montgomerycountymd.gov/Biz-Resources/programs/financial-tax.html>.
- lx "Cybersecurity Workforce Framework," *National Initiative for Cybersecurity Careers and Studies*, accessed May 26, 2017, <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>
- lxi Shoemaker, Dan, Anne Kohnke, and Ken Sigler, *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*, 2016, CRC Press. Accessed May 26, 2017, <http://www.crcnetbase.com/doi/pdf/10.1201/b19962-1>
- lxii *State of California Report - Cybersecurity Task Force Workforce Development and Training*, Cybersecurity Task Force, June 2015, accessed May 26, 2017, <http://www.caloes.ca.gov/CybersecurityTaskForceSite/Documents/Workforce%20Objective%201%20Proposal%202015-06.pdf>.
- lxiii Ibid.
- lxiv Ibid.
- lxv JobsEQ®, Chmura Economics and Analytics. Occupation Reports provided for the 13 cited SOC codes.
- lxvi "Cyber Security Market worth 202.36 Billion USD by 2021." *Markets and Markets*, accessed May 30, 2017, <http://www.marketsandmarkets.com/PressReleases/cyber-security.asp>
- lxvii Spidalieri, Francesca, *State of the States on Cybersecurity*, Pell Center for International Relations and Public Policy, 2015, accessed May 26, 2017, <http://sentinelips.com/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf>.
- lxviii "Center for Information Security," *Northern Kentucky University*, accessed May 30, 2017, <http://inside.nku.edu/informatics/centers/cis.html>.
- lxix "CyberSecurity Lab – University of Louisville," *University of Louisville Speed School of Engineering*, accessed May 30, 2017, <http://cecs.louisville.edu/security/>.
- lxx "Cyber Security Initiative (CSI)," *University of Louisville*, accessed May 30, 2017, <http://www2.cecsresearch.org/csi/>.
- lxxi "Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)," *National Initiative for Cybersecurity Education*, accessed May 30, 2017, <http://csrc.nist.gov/nice/ffo/>.
- lxxii "NIST 'RAMPS' Up Cybersecurity Education and Workforce Development with New Grants," *National Institute of Standards and Technology*, accessed May 30, 2017, <https://www.nist.gov/news-events/news/2016/05/nist-ramps-cybersecurity-education-and-workforce-development-new-grants>.
- lxxiii "About NICCS," *National Initiative for Cybersecurity Careers and Studies*, accessed May 26, 2017, <https://niccs.us-cert.gov/about-niccs>.
- lxxiv "Cyber Innovation Center wants to weave cybersecurity into K-12 STEM instruction," *National Integrated Cyber Education Research Center*, accessed May 30, 2017, <http://nicerc.org/2017/03/cyber-innovation-center-wants-to-weave-cybersecurity-into-k-12-stem-instruction/>.
- lxxv "Kentucky Becomes the Second State in the US to Adopt the Federal Cyber Engineering Pathway Curricula Designed by NICERC for 9-12th Graders For Use In Its School Districts," *National Integrated Cyber Education Research Center*, accessed May 30, 2017, <http://nicerc.org/2017/03/kentucky-becomes-the-second-state-in-the-us-to-adopt-the-federal-cyber-engineering-pathway-curricula-designed-by-nicerc-for-9-12th-graders-for-use-in-its-school-districts/>.
- lxxvi "Governor Larry Hogan Announces 2017 Maryland Jobs Initiative," *Office of Governor Larry Hogan*, January 5, 2017, accessed May 30, 2017, <http://governor.maryland.gov/2017/01/05/governor-larry-hogan-announces-2017-maryland-jobs-initiative/>.

- lxxvii “The Grant,” *Cyber Pathways Across Maryland*, accessed May 30, 2017, <http://www.cyberpathwaysacrossmd.com/thegrant.html>.
- lxxviii *The National Higher Education and Workforce Initiative – Strategy in Action: Building the Cybersecurity Workforce in Maryland*, Business Higher Education Forum, 2014, accessed May 30, 2017, http://www.bhef.com/sites/default/files/BHEF_2014_maryland%281%29.pdf.
- lxxix “Cybersecurity Education at UMD,” *University of Maryland – Maryland Cybersecurity Center*, accessed May 30, 2017, <http://www.cyber.umd.edu/education>.
- lxxx “Michigan Cyber Range,” *Merit Network, Inc.*, accessed May 30, 2017, <https://www.merit.edu/cyberange/>.
- lxxxii Casura, Lily, “How San Antonio Can Compete for Cyberbusiness,” *The Rivard Report*, May 13, 2014, accessed May 30, 2017, <https://therivardreport.com/san-antonio-need-step-game-compete-cybersecurity-business/>.
- lxxxiii Vijayan, Jaikumar, “IT pros rank University of Texas San Antonio best school for cybersecurity,” *Computerworld*, February 24, 2014, accessed May 30, 2017, <http://www.computerworld.com/article/2487907/it-skills-training/it-pros-rank-university-of-texas-san-antonio-best-school-for-cybersecurity.html>.
- lxxxiii “ICS Vision,” *Institute for Cyber Security*, accessed May 30, 2017, <http://ics.utsa.edu/about.php>.
- lxxxiv “Building a 21st century workforce: The Alamo Academies,” *Port San Antonio*, accessed May 30, 2017, <http://www.portsanantonio.us/Webpages.asp?wpid=369>.
- lxxxv “Cybersecurity San Antonio,” *San Antonio Chamber of Commerce*, accessed May 30, 2017, <http://cybersecuritysa.com/>.
- lxxxvi “CyberTexas,” *Federal Business Council, Inc.*, accessed May 30, 2017, <https://www.fbcinc.com/e/CyberTexas/>.
- lxxxvii *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, The White House Office of the Press Secretary, May 11, 2017, accessed May 31, 2017, <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.
- lxxxviii “Communications Sector,” *United States Department of Homeland Security Office of Infrastructure Protection*, accessed May 4, 2017, <https://www.dhs.gov/communications-sector>.
- lxxxix Modified from the DHS National Infrastructure Plan in support of NIST directives. *National Infrastructure Protection Plan: Risk Management Framework*, United States Department of Homeland Security, accessed May 4, 2017, http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf.
- xc Based on the risk evaluation methodology found in: *Cyber Disruption Response Planning Guide*, National Association of State Chief Information Officers, 2016, accessed May 4, 2017, https://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf.
- xcii “Cyber Information Sharing and Collaboration Program (CISCP),” United States Department of Homeland Security, accessed May 4, 2017, <https://www.dhs.gov/ciscp>.
- xciii *Critical Infrastructure and Key Resources: Cyber Information Sharing and Collaboration Program*, United States Department of Homeland Security, accessed May 4, 2017, https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.
- xciv Dewson, Andrew, “Kentucky’s new cybersecurity statutes will change how you do business,” *Insider Louisville*, April 16, 2014, accessed May 4, 2017, <https://insiderlouisville.com/metro/accountability/kentuckys-new-cyber-security-statutes-will-change-business/>.
- xcv The text of HB5 can be found in Kentucky Revised Statutes (KRS) Chapter 61.931-61.934.
- xcvi The text of HB232 can be found in KRS Chapter 365.732 and 365.734.
- xcvii “Summary of U.S. State Data Breach Notification Statutes,” Davis Wright Tremaine, LLP, accessed May 4, 2017, <http://www.dwt.com/statedatabreachstatutes/>.
- xcviii *Presidential Policy Directive 41 Stakeholder Memo*, Industrial Control Systems Cyber Emergency Response Team, accessed April 28, 2017, <https://ics-cert.us-cert.gov/sites/default/files/documents/PPD%20Stakeholder%20Message.pdf>.
- xcviii “Lessons Learned Information Sharing,” Federal Emergency Management Agency, Accessed April 28, 2017, <https://www.fema.gov/media-library/resources-documents/collections/473>.
- xcix *Cyber Disruption Response Planning Guide*, National Association of State Chief Information Officers, April 2016, accessed April 28, 2017, https://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf.
- c *Kentucky Emergency Operations Plan*, Kentucky Emergency Management, August 2013, accessed April 28, 2017, <http://kyem.ky.gov/programs/Documents/KYEOP%20August%202013%20-%20Final.pdf>.
- ci Ibid.
- cii *Defense Spending by State, FY2015 – Kentucky*, Office of Economic Adjustment, accessed April 28, 2017, <http://oea.gov/sites/default/files/files-508/States/Kentucky.pdf>.
- ciiii Coomes, Paul, Ph.D. et al., “The Economic Importance of the Military in Kentucky,” 2016 Update. Sponsored by the Kentucky Commission on Military Affairs. Prepared by the Urban Studies Institute at the University of Louisville, June 2016, <http://kcm.a.ky.gov/Documents/Final%20Report.pdf>.
- civ “Status Report of U.S. Government Gold Reserve,” *United States Department of the Treasury Bureau of the Fiscal Service*, April 30, 2017, accessed April 30, 2017, https://www.fiscal.treasury.gov/fsreports/rpt/goldRpt/current_report.htm.
- cv “Fort Knox Network Enterprise Center – Mission & Vision,” *Fort Knox*, accessed April 28, 2017, <http://www.knox.army.mil/partners/nec/>.

- cvi Ibid.
- cvii Coomes, Paul, Ph.D. et al., "The Economic Importance of the Military in Kentucky," 2016 Update. Sponsored by the Kentucky Commission on Military Affairs. Prepared by the Urban Studies Institute at the University of Louisville, June 2016, <http://kcma.ky.gov/Documents/Final%20Report.pdf>.
- cviii "Military Affairs," *Christian County Chamber of Commerce*, accessed April 28, 2017, <http://www.christiancountychamber.com/pages/MilitaryAffairs>.
- cix "Great American Defense Communities," *Association of Defense Communities*, accessed April 28, 2017, <http://www.defensecommunities.org/great-american-defense-communities/>.
- cx "Fort Campbell, Kentucky Installation Overview," *Military Installations*, accessed April 28, 2017, [http://www.militaryinstallations.dod.mil/MOS/f?p=MI:CONTENT:0:::P4_INST_ID,P4_CONTENT_TITLE,P4_CONTENT_DIRECTORY,P4_TAB:2695,Installation%20Overview,30.90.30.30.0.0.0.0,1,IO](http://www.militaryinstallations.dod.mil/MOS/f?p=MI:CONTENT:0:::P4_INST_ID,P4_CONTENT_TITLE,P4_CONTENT_EKMT_ID,P4_CONTENT_DIRECTORY,P4_TAB:2695,Installation%20Overview,30.90.30.30.0.0.0.0,1,IO).
- cxii Coomes, Paul, Ph.D. et al., "The Economic Importance of the Military in Kentucky," 2016 Update. Sponsored by the Kentucky Commission on Military Affairs. Prepared by the Urban Studies Institute at the University of Louisville, June 2016, <http://kcma.ky.gov/Documents/Final%20Report.pdf>.
- cxiii Ibid.
- cxiiii "CWC Treaty," *United States Army Chemical Materials Activity*, accessed April 28, 2017, <https://www.cma.army.mil/CWCTreaty/Pages/default.aspx>.
- cxv "Blue Grass Chemical Agent-Destruction Pilot Plant," *Bechtel*, accessed April 28, 2017, <http://www.bechtel.com/projects/blue-grass/>. "Blue Grass Chemical Agent-Destruction Pilot Plant (BGCAPP)," *Program Executive Office, Assembled Chemical Weapons Alternatives*, accessed April 28, 2017, <https://www.peoacwa.army.mil/bgcapp/>.
- cxvi "Blue Grass Chemical Activity," *United States Army Chemical Materials Activity*, accessed April 28, 2017, <https://www.cma.army.mil/BGCA/Pages/default.aspx>.
- cxvii "Boone National Guard Center," *United States Department of Defense Office of Economic Adjustment*, accessed April 28, 2017, <http://www.oea.gov/project/boone-national-guard-center>.
- cxviii <http://kynghistory.ky.gov/Our-History/Major-Commands/Pages/63d-Theater-Aviation-Brigade.aspx>.
- cxix "63d Theater Aviation Brigade," *Kentucky National Guard eMuseum*, accessed April 28, 2017, <http://kyem.ky.gov/Who%20We%20Are/Pages/default.aspx>.
- cxix "About Us," *Kentucky National Guard*, accessed April 28, 2017, <http://kentuckyguard.dodlive.mil/about-us/>.
- cxix Sgt. 1st Class Jon Soucy, "National Guard set to activate additional cyber units," *United States Army*, December 9, 2015, accessed April 28, 2015, https://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units.
- cxxi "Louisville Air National Guard Base," *United States Air National Guard*, accessed April 28, 2017, <https://www.goang.com/locations/kentucky/Louisville-Air-National-Guard>.
- cxix "Units," *Air National Guard 123rd Airlift Wing*, accessed April 28, 2017, <http://www.123aw.ang.af.mil/Units>
- cxixiii Kissel, Richard, *Small Business Information Security: The Fundamentals*, NIST, October 2009, accessed May 16, 2017, <http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>.
- cxixiv The following are helpful articles outlining key considerations:
- Carter, Paulette, "The Pros and Cons of Custom Software vs. Off-the-Shelf Solutions," *PCD Group*, <http://pcdgroup.com/the-pros-and-cons-of-custom-software-vs-off-the-shelf-solutions/>.
 - O'Reilly, Jim, "Real Pros and Cons in the COTS Server Decision," *TechTarget*, <http://searchdatacenter.techtarget.com/opinion/Real-pros-and-cons-in-the-COTS-server-decision>.
- cxixv "OCTAVE," *Software Engineering Institute CERT Division*, accessed April 27, 2017, <http://www.cert.org/resilience/products-services/octave/index.cfm>.
- cxixvi *Cyber Security Evaluation Tool*, National Cybersecurity and Communications Integration Center, accessed May 16, 2017, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf
- cxixvii "CIS Critical Security Controls," *SANS Institute*, accessed April 27, 2017, <https://www.sans.org/critical-security-controls>.
- cxixviii *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST, April 2013, accessed April 27, 2017, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
- cxixix Paulsen, Cecilia and Patricia Toth, *Small Business Information Security: The Fundamentals*, NIST, accessed April 27, 2017, <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>.
- cxixx Manke, Samantha and Ira Winkler, "The 7 elements of a successful security awareness program," *CSO*, May 1, 2013, accessed April 27, 2017, <http://www.csoonline.com/article/2133408/network-security/network-security-the-7-elements-of-a-successful-security-awareness-program.html>.
- cxixxi "Game of Threats – A cyber threat simulation," *PricewaterhouseCoopers Financial Services Cybersecurity and Privacy Services*, accessed May 16, 2017, <https://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html>.
- cxixxii "Northrop Grumman Launches Advanced Cyber Technology Center, Dedicated to Solving Hard Problems in the Cyber Domain," *Northrop Grumman*, November 19, 2014, accessed April 27, 2017, http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=10109075.
- cxixxiii National Defense magazine, December 2010 issue. [Link broken].

- cxiiiiv "StaySafeOnline.org," *National Cyber Security Alliance*, accessed April 27, 2017, <https://staysafeonline.org/>.
- cxiiiiv "PCI Security Standards," *PCI Security Standards Council*, accessed April 27, 2017, <https://www.pcisecuritystandards.org/>.
- cxiiiiv Wilson, Mark and Joan Hash, *Building an Information Technology Security Awareness and Training Program*, NIST, October 2003, accessed April 27, 2017, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>.
- cxiiiiv "Michigan Cyber Range," *Merit Network, Inc.*, accessed April 27, 2017, <https://www.merit.edu/cyberrange/>.
- cxiiiiv "Security Awareness Resources," *SANS Institute*, accessed April 27, 2017, <https://securingthehuman.sans.org/resources>.
- cxiiiiv Australia/New Zealand, Joint Technical Committee OB-007, Risk Management, Council of Standards, August 31, 2004, accessed April 27, 2017, <https://www.standards.govt.nz/search-and-buy-standards/standards-information/risk-management/>.
- cxli "CIS Critical Security Controls," *SANS Institute*, accessed April 27, 2017, <https://www.sans.org/critical-security-controls>.
- cxlii "ISO 31000 - Risk management," *International Organization for Standardization*, accessed April 27, 2017, <https://www.iso.org/iso-31000-risk-management.html>.
- cxliii "ISO/IEC 27001:2013," *International Organization for Standardization*, accessed April 27, 2017, <https://www.iso.org/standard/54534.html>.
- cxliiii "Guidance on Enterprise Risk Management," *Committee of Sponsoring Organizations of the Treadway Commission*, accessed April 27, 2017, <https://www.coso.org/Pages/erm.aspx>.
- cxliiv "CIP Standards," *North American Electric Reliability Corporation*, accessed April 27, 2017, <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>.
- cxliv "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," *PCI Security Standards Council*, accessed April 27, 2017, <https://www.pcisecuritystandards.org/>.
- cxlv "Guide for Applying the Risk Management Framework to Federal Information Systems," United States Department of Commerce National Institute of Standards and Technology, February 2010, accessed April 27, 2017, <https://www.nist.gov/>.
- cxlvii "Guidance on Risk Analysis Requirements under the HIPAA Security Rule," United States Department of Health & Human Services Office for Civil Rights, July 14, 2010, accessed April 27, 2017, <https://www.hhs.gov>.
- cxlviii "NIST Cybersecurity Framework Adoption Hampered by Costs, Survey Finds," *Dark Reading*, March 30, 2016, accessed April 27, 2017, <http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901>.
- cxlix DHS has built upon NIST CSF to tailor the guidance for specific CI sectors, such as chemical, commercial, and critical manufacturing, among others. Tailored CSF implementation guides can be found at: "Cybersecurity Framework - Industry Resources," NIST, February 11, 2015, accessed April 27, 2017, <https://www.nist.gov/cyberframework/industry-resources>.
- cl One exception to this is Intel, which has implemented the NIST CSF as opposed to only using discrete parts: Casey, Tim, Kevin Fiftal, Kent Landfield, John Miller, Dennis Morgan, and Brian Willis, *The Cybersecurity Framework in Action: An Intel Use Case*, Intel, 2015, accessed April 27, 2017, <http://intel.ly/1e6mw5s>.
- cli "NIST Cybersecurity Framework Adoption Hampered by Costs, Survey Finds," *Dark Reading*, March 30, 2016, accessed April 27, 2017, <http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901>.
- clii "Number of firms, establishments, employment, and payroll by firm size, state, and industry," *United States Small Business Administration*, accessed April 27, 2017, <https://www.sba.gov/advocacy/firm-size-data>.
- cliii *Cyber Security Planning Guide*, United States Department of Homeland Security Federal Communications Commission, accessed April 27, 2017, <http://bit.ly/2oNQJeI>.
- cliv "Tips," *United States Computer Emergency Response Team*, accessed April 27, 2017, <https://www.us-cert.gov/ncas/tips>.
- clv Lebanidze, Evgeny, *Guide to Developing a Cyber Security and Risk Mitigation Plan*, NRECA Cooperative Research Network, accessed April 27, 2017, <https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf>.
- clvi Paulsen, Celia and Patricia Toth, *Small Business Information Security: The Fundamentals*, United States Department of Commerce NIST, November 2016, accessed April 27, 2017, <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>.
- clvii "SBC Computer Security Workshops," *Computer Security Division - Computer Security Resource Center*, March 6, 2017, accessed April 27, 2017, <http://csrc.nist.gov/groups/SMA/sbc/workshops.html>.
- clviii "RE: Cyber," *StaySafeOnline.org*, accessed April 27, 2017, <https://staysafeonline.org/re-cyber/>.
- clix Eubanks, Russell, *A Small Business No Budget Implementation of the SANS 20 Security Controls*, August 10, 2011, accessed April 27, 2017, <http://bit.ly/2pnObn>.
- clx Adapted from "Questions a Bank COE Should Ask," *Cyber Security 101: Cybersecurity: A Resource Guide for Bank Executives*, Conference of State Bank Supervisors, accessed April 27, 2017, <https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf>.

- clxi In addition to our independent technical opinion, this section drew on multiple resources. The cybersecurity firm WALLIX provided some of the fundamentals in "Elements of an Effective Cybersecurity Plan," *Wallix*, February 10, 2017, accessed April 27, 2017, <http://blog.wallix.com/elements-of-an-effective-cybersecurity-plan>.
- clxii The complete reference guide can be found at: *Cybersecurity: A Resource Guide for Bank Executives*, Conference of State Bank Supervisors, accessed April 27, 2017, <https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf>.
- clxiii "IAPP hits 20k Members – Meet One from Malaysia," *Daily Dashboard*, accessed April 27, 2017, <https://iapp.org/news/a/iapp-hits-20k-members-meet-one-from-malaysia/>.
- clxiv *Meet the Threat: States Confront the Cyber Challenge*, National Governor's Association, 2016, accessed April 27, 2017, <https://ci.nga.org/files/live/sites/ci/files/1617/docs/TaskForceMemoFinal.pdf>.
- clxv Ibid.