STATE OF CONNECTICUT

Cybersecurity Study
Pursuant to Special Act 15-13

Melody A. Currey, Commissioner
Mark Raymond, Chief Information Officer
Department of Administrative Services
January 1, 2017

Contents

Transmittal

Governor Dannel P. Malloy
State of Connecticut
210 Capitol Avenue
Hartford, CT 06106

Public Safety & Security Committee
Legislative Office Building Room 3600
300 Capitol Avenue
Hartford, CT 06106

Dear Governor & Distinguished Chairs;

Special Act 15-13 "An Act Concerning Cybersecurity" directed the Department of Administrative (DAS) in consultation with the Department of Emergency Services and Public Protection (DESPP) to conduct a study to identify cybersecurity issues facing the state including recommendations and coordination efforts amongst impacted stakeholders—government, law enforcement, etc. to improve cybersecurity preparedness in the State of Connecticut.

I would like to extend special thanks to CIO, Mark Raymond, (DAS/BEST), Deputy William Shea (DESPP), David Geick, (DAS/BEST), John Vittner (OPM), Dr. Michael Mundrane (CIO / University of Connecticut), Chief Cybersecurity Risk Officer, Arthur House (DAS) and the entire Cybersecurity Strategy Team for their tireless efforts in developing this report for you and the Legislature. The coordinated effort of this group has led to the preparation of a substantive and comprehensive report. I am hopeful that in the months ahead the content of this document will be useful to the Administration and policymakers as they explore the issues surrounding cybersecurity preparedness.

Sincerely,

Melody A. Currey

Executive Summary

In response to the Connecticut General Assembly's direction in Special Act 15-13, the Department of Administrative Services studied the complex and evolving subject of cybersecurity. The study assesses the topic, and offers a set of recommendations to improve Connecticut's ability to manage our increasing cybersecurity threats.

Technology advances have improved our daily life. All sectors of our economy rely on technology for efficiency and operation. Our citizens utilize technology for communications and to manage their financial and personal lives. While technology has become critical to everyday living, our reliance on technology is endangered by cybersecurity threats. These growing threats make us vulnerable in unprecedented ways and endanger the very benefits we gain through technology use.

Cybersecurity is becoming part of our general consciousness. Computer viruses, malware, and ransomware are common terms. The potential impacts of cybersecurity on our national security and even our elections cover the front pages of our newspapers. Millions of citizens have had personal information stolen through data breaches.

Governments and private industry have applied a range of techniques to combat growing cybersecurity risks. These efforts have been somewhat successful and much progress has been made. However, rapidly increasing technology change and a corresponding growth in threats have made it difficult for businesses, citizens, organizations and governments to react in a timely manner to the evolving landscape. There are not enough qualified workers to fill open cybersecurity positions.

Alone and using current defenses, no entity can withstand the onslaught of cybersecurity threats in the future. Fortunately, federal, state, and local governments, along with private industry and the general public, recognize the benefits to new approaches and a coordinated response. Federal government agencies and private cybersecurity firms continue to generate information and tools useful in combating cyber threats. Sharing these capabilities with a greater audience will help raise awareness and reduce risk.

Recent research has shown that a statewide cybersecurity strategy, developed in collaboration between federal, state, and local government, education, and private industry, may provide the best opportunity to reduce cybersecurity risks. The State of Connecticut will complete its first cybersecurity strategy in the spring of 2017.

Connecticut state government has made significant efforts over many years to plan for and manage a variety of public service disruptions and public safety emergencies. Our response to this growing cybersecurity threat will enhance Connecticut's security and ability to compete in the future.

As we develop the strategy and execute our cybersecurity plan, Connecticut must:

- Be as prepared as possible and practice our responses to cybersecurity incidents;
- Share information on threats and best practices;

- Build skills required to be a center of cybersecurity strength;
- Coordinate regularly to improve our defenses and share limited resources; and
- Recognize that the success of our state and the safety of our citizens require special commitment and mutual responsibility as we respond to and mange tomorrow's cybersecurity threats.

Statutory Authority

Special Act No. 15-13

AN ACT CONCERNING A STUDY OF CYBERSECURITY.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (*Effective from passage*) (a) The Department of Administrative Services, in consultation with the Department of Emergency Services and Public Protection, shall, within available appropriations, conduct a study to identify cybersecurity issues facing the state and to make recommendations regarding specific actions that the state can implement to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness.

(b) Not later than January 1, 2017, the Department of Administrative Services shall submit the results of such study and any recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to public safety and security, in accordance with the provisions of section 11-4a of the general statutes.

Introduction

Pursuant to Special Act 15-13, the Department of Administrative Services (DAS) has conducted a study of cybersecurity issues facing Connecticut and recommends certain actions "to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness." To complete this task, DAS collected information and requested perspectives from Connecticut's citizens, businesses and public and private institutions. We used several sources and methods to write this report, including the following:

- **Public Survey.** We conducted a public online survey to gather information from interested parties, including, but not limited to, private citizens and businesses. The survey sought to measure awareness of cybersecurity threats and identify cybersecurity concerns.

- **State Agency Survey.** We conducted a separate state agency survey to assess state systems' cybersecurity readiness. This survey assessed security using a set of controls defined by the Center for Internet Security (the CIS 20 Critical Controls). These controls assess secure practices similar to the audit controls used to ensure regulatory compliance for work in areas as diverse as the Health Insurance Portability and Accountability Act (HIPAA); Federal Tax Information (FTI) standards; and protection of Personally Identifiable Information (PII). The first five of these control are identified as "foundational" and should be implemented first.

- **Cybersecurity Workshop.** In September 2016, Connecticut's Chief Information Officer (CIO) and the Connecticut Cybersecurity Strategy Core Team held a full-day workshop focused on cybersecurity. Attendance included more than fifty representatives from federal agencies, state and local government, the education field and the private sector. The workshop focused on identifying key cybersecurity challenges, coordination between the audiences, recognition of performance standards and workforce development.

- **Review of Assets and Capabilities.** We examined and assessed Connecticut's current cybersecurity assets and capabilities, including Connecticut agencies' planning and response plans and available training.

After gathering information and analyzing the research, we crafted the recommendations in this report to improve communications and cybersecurity preparedness in Connecticut.

Background

Cybersecurity Threats

Almost every aspect of our daily life is affected by information technology. While technical advances enrich our lives, our reliance on technology makes us vulnerable to attacks intended to steal resources, information and intellectual property, disrupt our lives and potentially subject us to the consequences of critical infrastructure compromise. This section offers a general summary of cybersecurity threats facing Connecticut, with some more detailed information included in the appendix.

The Internet: Why we are at risk

The Internet allows any electronic device to connect to almost any other device. It allows individuals to shop online and businesses to attract customers and offers powerful tools to search through massive amounts of information. The Internet allows global entities such as financial services companies, governments, manufacturing companies and media companies to provide services anywhere.

The ability to connect person-to-person and computer-to-computer-to-machine enables the global, digital economy. It also creates opportunity for malicious individuals and organizations to inflict damage.

Cellular Data and Wi-Fi: Expanding the risk

The introduction of wireless networking in the late 1990s and early 2000s greatly increased the number of devices able to connect to the Internet. No longer were physical, stationary wires required to connect a user or a device to the Internet. Mobile phones and cellular networks now allow connections from anywhere. Wi-Fi wireless networking allow computing devices to connect to networks almost anywhere.

The emergence of these two technologies combined with continuous reduction in the size of computing devices created the "Internet of Things" (IoT), interconnections that had previously not been linked for computing purposes. Examples are traffic monitoring cameras, heating and cooling control systems and alarm systems, digital video recorders (DVR), tablets and appliances.

Attack Surface and Opportunity

The Internet was not created to be inherently secure. Security has been added to many aspects of the Internet, however each new device added to our connected environment increases the opportunity for entry of malicious actors.

Devices that collect and hold information become potential targets for cybersecurity attack. They have been commandeered to inflict harm and disruption.

Malicious Actors

Individuals and organizations utilize the Internet for purposes other than those originally designed. Malicious actors fall into several broad categories with similarities to their physical world counterparts:

- Cyber Criminals use the Internet to steal information for financial gain. They may steal financial account information to withdraw funds, PII to establish lines of credit for financial gain, or medical information to effect billing or prescription fraud. Cyber criminals may make data unusable unless the victim pays ransom.

- **Cyber Spies**, sometimes referred to as nation state or advanced persistent threats, use the Internet to obtain information to further industrial or national interests. They access systems to steal intellectual property, look for weaknesses or gain negotiation advantages.

- **Cyber Hacktivists** tend to be ideologically motivated and use the Internet to influence behavior, draw attention to a cause, or voice opinions. Sometimes they disable or deface systems to advance their messages.

- **Cyber Terrorists** utilize the Internet to inflict harm often for ideological reasons. They seek to damage, disable or disrupt critical infrastructure or facilities. Examples include the shutdown of an electric grid, destruction of power facilities through manipulation of control systems and flooding by manipulation of dams and water control systems.

Prosecution Difficulty

Most cyber attacks against citizens, businesses and governments within Connecticut are perpetrated from outside the physical boundaries of the state, often from jurisdictions that make prosecution difficult or almost impossible. Perpetrators are sometimes shielded by jurisdictions sympathetic to the mission.

Changing Landscape

Cybersecurity risks and attacks are increasing in numbers and sophistication. Mandiant Consulting published in February 2016[1] research findings of an increase in reported data breaches and greater diversity and origin of attackers. Its report identified three trends from 2015 cyber incident responses. The first was the rise of attacks aimed at disrupting

[1] (Mandiant Consulting, 2016)

business systems, for financial, political or reputation purposes. The second was the targeted theft of large volumes of Personally Identifiable Information by threat actors linked to China. Thirdly, Mandiant observed more advanced attacks on network infrastructure.

The National Association of State Chief Information Officers (NASCIO) and Deloitte conduct a biennial survey of the states related to cybersecurity. The 2016 Deloitte-NASCIO Cybersecurity Study[2] profiled several areas identified by state Chief Information Security Officers (CISOs) as prevalent threats across state governments. Such threats include malicious software exploiting weak security awareness by users, increasingly sophisticated attacks and threats originating from emerging technologies such as cloud computing and the Internet of Things.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) briefed the Connecticut Strategy Home Team (see Appendix for participating organizations) at a September 2016 workshop. MS-ISAC listed Personally Identifiable Information, Personal Health Information (PHI), point of sale systems, industrial control systems, and medical control systems as principal targets. Criminal extortion, through use of Distributed Denial of Service (DDoS) attacks or ransomware, which encrypts files until the attacker provides a "key" to unlock them, were cited as increasing in frequency. Additionally, critical infrastructure is at risk from malicious attacks by terrorists, "hacktivists" and nation-state actors with the potential to cause significant harm to the safety and security of Connecticut citizens and businesses.

Verizon provided analysis of 64,199 security incidents from 2015 that resulted in 2,260 confirmed data breaches in its 2016 Data Breach Investigations Report[3]. It noted that financial motives remained the major reason for attempted breaches, with espionage a distant second. Together, those two motives accounted for 89% of breaches. Verizon confirmed that system vulnerabilities that had been identified months or even years earlier continued to be exploited by attackers. Although new threats and vulnerabilities continue to be identified each year, the need continues for regular assessment and remediation of IT systems to stay current regarding security patches and updates.

Workforce in Demand

Businesses and governments across the country have attempted to meet changing demands by hiring individuals with cybersecurity skills. The National Initiative for Cybersecurity Education, a program within NIST, sponsored a website to report supply and demand data in the cybersecurity job market. This tool can be found at CyberSeek.org. CyberSeek[4] reports there are almost 350,000 job openings in the United States in cybersecurity. Connecticut alone tallied 4,153 openings for individuals with cybersecurity skills.

---

[2] (Robinson & Subramanian, 2016)

[3] (Verizon, 2016)

[4] (CyberSeek, 2016)

Key Industries

Cybersecurity risks are not limited to individuals or to the public sector. Cybersecurity is also a rising risk for private industry. Connecticut's private sector has several key industry concentrations, including:

- Health care and Biosciences
- Defense
- Financial Services and Insurance
- Public Utilities

Cybersecurity threats to these industries carry risks of financial loss due to system downtime, loss of intellectual property and large costs due to mitigation of a data breach. Connecticut suffers not only from the loss of business to the companies involved but obviously also to the lack of tax revenue generated for the state.

A recent report by the Center for Cyber and Homeland Security at the George Washington University states: *"The private sector is therefore on the front lines of cyber competition and conflict today. Businesses never anticipated the scale to which they would be responsible for defending their interests against the military and intelligence services of foreign countries."*[5]

[5] (Center for Cyber and Homeland Security, 2016)

Efforts and Capabilities

State Agency Efforts

Connecticut has actively addressed cybersecurity challenges for several years. Since the state started to connect computers through networks in the 1970's it has managed a centralized security unit to protect its resources. This section describes current capabilities to protect the state from cybersecurity risks.

Connecticut Cybersecurity Committee

The Connecticut Department of Emergency Services and Public Protection's Division of Emergency Management and Homeland Security (DESPP/DEMHS) and the Department of Administrative Services/Bureau of Enterprise Systems and Technology (DAS/BEST) formed a working group in 2012 to address potential cybersecurity disruptions of state systems, the Connecticut Cybersecurity Committee. This committee is now a voluntary group meeting monthly to discuss emerging threats and best practices and develop relationships required in the event of a large cybersecurity event. Attendees include federal and state agencies, local government, military, institutions of higher education, private industry and utilities.

Information Technology Security Officer Roundtable (ITSOR)

The ITSOR is a voluntary meeting of state agency security officers. It meets regularly to share best practices information and to develop and encourage in-house training for participating members. The ITSOR also helps provide agency perspective regarding proposed enterprise initiatives, assesses possible difficulties in executing initiatives and evaluates how new initiatives might affect existing technical controls.

National Governors Association (NGA) – Cybersecurity Policy Academy

In 2016, The State of Connecticut was selected as one of five participants to participate in the NGA Center for Best Practices Policy Academy on State Cybersecurity. A year-long effort started in June 2016 intended to improve the state's cybersecurity posture by producing:

- The state's first cybersecurity strategy;
- A cyber incident response plan;
- A cyber disruption response plan; and
- A communications plan for the public and private sectors.

This effort is expected to conclude in the spring of 2017. Many activities, including engagement with citizens and private businesses, were designed to inform this legislative report and to provide context for Connecticut's cybersecurity strategy.

Appointment of Chief Cybersecurity Risk Officer

In October 2016, during National Cybersecurity Awareness Month, Governor Malloy announced the appointment of Arthur House to be Connecticut's first Chief Cybersecurity Risk Officer. This position's charge is to enhance Connecticut's cybersecurity prevention, and protection efforts in a comprehensive, cross-agency and cross-sector manner and to execute the state's cybersecurity strategic plan. Building on Connecticut's public utility cybersecurity strategy and action plans, the Governor directed House to execute and coordinate work to "prepare for, prevent and respond to and to recover from threats to our cybersecurity infrastructure at the state, local and private sector levels."

National Level Exercise 2012 – (NLE)

The Federal Emergency Management Agency (FEMA) ran a national exercise focusing on cybersecurity incident management. Connecticut participated in the capstone exercise and received positive feedback from the evaluation team on its processes and procedures.

Cyberguard Prelude Exercise 2016-2017

In June 2016, Connecticut participated in the Cyber Guard Prelude exercise, a national-level training event conducted by the Department of Homeland Security testing DAS/BEST and DESPP/DEMHS incident response and analysis. The exercise emphasized information sharing between state agencies and federal partners. The Department of Homeland Security will conduct a nationwide cybersecurity exercise in the spring of 2017. Initial planning began in early December 2016; details and requirements for the exercise are forthcoming.

Cyber Yankee Annual Exercises 2015-2017

Since 2015, Connecticut National Guard members have participated in FEMA Region 1's annual New England regional cyber exercise. This event offers live training for cyber incident and network defense operations.

National Guard Cyber Shield Annual Exercises 2013-2017

Connecticut National Guard units have played key roles in this annual, national-level National Guard cyber exercise. This event also offers live training for cyber incident and network defense operations.

2016 Utilities Cybersecurity Action Plan

The Connecticut Public Utilities Regulatory Authority (PURA) released an action plan in 2016 to strengthen defenses against cybersecurity challenges in the state's public utilities. The

plan provides a process for PURA and DEMHS officers to review cybersecurity progress according to mutually agreed standards with electricity, natural gas and water companies. This plan was developed through a series of collaborative meetings with the state's public utility companies. The action plan has received national attention as an innovative, collaborative effort in the public utilities realm.

Alignment to State Response Framework

Should a large-scale cybersecurity incident be directed at Connecticut, the state would operate under the National Incident Response System (NIMS) and under the auspices of the State Response Framework (SRF),[6] an all-hazards framework prescribing the interaction of state government with federal, local and tribal nation governments, nongovernmental response organizations and private sector partners, the media and the public in implementing emergency response and recovery functions in times of crisis. Our work with the 2012 National Level Exercise reinforced the need to follow state and national response frameworks in the event of emergencies.

State Agency Capabilities

State cybersecurity capabilities include several disciplines that map to existing capabilities. For example, the DAS/BEST Security Services team is responsible for defense of the state's network perimeter, while the DESPP's Forensic Laboratory and Computer Crimes unit are responsible for investigating computer-related criminal events. Current agency capabilities are described in the following sections:

Department of Administrative Services (DAS)

DAS/BEST provides statewide IT services to executive branch agencies. Its Security Services group protects and monitors the state's network, manages central state security assets and is a resource for state agencies. This group also provides central administration of identity management and multi-factor authentication for the state's virtual private networking (VPN) and performs forensic analysis on state computers to support internal investigations.

Department of Emergency Services and Public Protection (DESPP)

- **The Connecticut Intelligence Center** (CTIC) resides in the Division of State Police, Bureau of Criminal Investigation, Counterterrorism Unit. The CTIC is involved in cybersecurity through the facilitation of information sharing with its federal, state

[6] (Department of Emergency Services and Public Protection, Division of Emergency Management and Homeland Security, 2014)

and local stakeholders and partners. CTIC provides monthly cybersecurity threat briefings to two state-designated entities that focus on state cybersecurity programs, strategies and protections. CTIC also works closely with State Police Computer Crimes and DAS BEST IT Security staff in dealing with cyber-related incidents across the State.

CTIC is able to analyze malware and phishing emails in order to provide timely indication of compromise for both mitigation and intelligence sharing to the intelligence community/intelligence enterprise through Intelligence Information Reports (IIR). CTIC is heavily involved with the National Fusion Center Association's (NFCA) Cyber Intelligence Network (CIN) and has a role with the NFCA CIN Cyber Threat Intelligence Working Group as the Northeast Regional Coordinator. CTIC also provides ad hoc cyber threat briefings and support to stakeholders that request assistance with cybersecurity matters.

- Connecticut's **Computer Crimes Unit** resides within the State Forensic Laboratory. The Computer Crimes Unit specializes in both proactive and reactive computer-related criminal investigations. The Computer Crimes Unit also works in close partnership with several federal, state and local law enforcement agencies and task forces including U.S. Immigration and Customs Enforcement (ICE), the Secret Service and the FBI on cyber-related investigations.

  The Computer Crimes Unit works in partnership with the United States Secret Service Financial Crimes Task Force and is regularly called upon to investigate point of sale system compromises and to conduct network intrusions analyses and vulnerability assessments. Additional areas of expertise include identification of suspects through email header content, IP address investigation and log analysis. The Computer Crimes Unit is also able to conduct in-depth computer forensic analysis of computer and electronic mobile devices related to cyber crimes.

- The **Division of Emergency Management and Homeland Security** (DEMHS), operating under NIMS and the SRF, directs and coordinates available resources to protect the life and property of Connecticut citizens in the event of a disaster or crisis through a collaborative program of prevention, planning, preparedness, response, recovery and public education.

Other State Agencies and Activities

Under the leadership of Governor Malloy, Connecticut actively promotes National Cyber Security Month through an annual gubernatorial proclamation designating October as Connecticut Cyber Security Awareness Month. The state also raises public awareness of cybersecurity through press releases and social media messaging.

All state agency personnel attend security awareness training to establish the fundamental responsibilities they have in handling state data. The training is annual with specific emphasis during National Cybersecurity Awareness Month.

Large agencies have designated security personnel; moderate to small agencies often combine security responsibilities with either information technology or other administrative management.

National Guard

The Connecticut Army National Guard maintains a Defensive Cyber Operations Element (DCOE) that protects and defends the military networks used by National Guard forces. The DCOE mission includes incident response and infrastructure support. Members are trained in investigation and cyber incident analysis. The element may be used in response to national, regional or state incidents.

Education

The University of Connecticut

The University of Connecticut is committed to advancing academic programs in cybersecurity at several levels. Through its academic plan, UCONN supported the launch of "C3", the **Connecticut Cybersecurity Center**, which is home to work in cybersecurity at the School of Engineering and is also an umbrella for existing centers working in computer security areas.

The Center for Voting Technology Research (VoTeR Center http://voter.engr.uconn.edu), founded in 2006, supports Connecticut efforts to ensure security and integrity of electoral processes that rely on electronic election systems. The Center works in collaboration with the Secretary of the State to evaluate voting solutions and define safe-use processes related to electronic voting.

The Center for Hardware Assurance, Security and Engineering (CHASE Center http://chase.uconn.edu), established in 2012, focuses on hardware-related research issues including detection of counterfeit devices, hardware Trojans, functions that cannot physically be cloned, secure supply chains and other hardware security subjects.

The Comcast Center of Excellence for Security Innovation (CSI Center http://csi.engr.uconn.edu), founded in 2014 focuses its research and development on Internet of Things devices as well as Comcast network and software infrastructures. Specifically, it considers penetration testing, hardening steps and holistic resource management that directly address cybersecurity threats.

In October 2016, C3 welcomed Synchrony Financial with the creation of the **Synchrony Financial Center of Excellence in Cybersecurity** with the aim to counter growing threats, whether domestic or foreign, directed against financial organizations.

Through these centers and industry partnerships, the University is establishing its authority in cybersecurity. The industry engagement led to two named endowed professorships – one by Comcast and one from Synchrony Financial -- that will substantially enhance the ranks of researchers devoted to rapidly growing and evolving areas of cybersecurity.

The recent growth of the **Computer Science & Engineering** (CSE) department with a doubling of its student population in recent years is complemented by a commitment to educate a new generation of professionals well-equipped with cybersecurity skills. CSE recently created a cybersecurity concentration for undergraduate degrees and is developing a Master of Engineering program with a cybersecurity focus at the School of Engineering.

Connecticut State Colleges and Universities (CSCU)

The Connecticut State Colleges and Universities have several programs at the Associate, Bachelor and Master's levels to prepare students with cybersecurity skills.

Capital Community College - Computer Networking: Cybersecurity Option - Associate in Science

This degree program is designed to take a student with little or no information technology experience and prepare him or her for entry-level work in cybersecurity. The degree prepares students for the foundational CompTIA Security Plus certification and provides the skills needed to implement, maintain and administer secure local and wide area networks. Curriculum in this program is based on topic areas, learning objectives and goals for educating the workforce prescribed by the cybersecurity community, including the National Institute for Standards and Technology (NIST) and the National Initiative for Cybersecurity Education (NICE).

Charter Oak State College - Cyber Security - Bachelor of Science

The cyber security major prepares individuals for careers as a security professional. This curriculum includes IT Security, Cyber Security, Information Assurance and Information Security Systems Security. It is designed for students with some background in computers.

Gateway Community College - Computer Science: Data Security Specialist Option - Associate in Science

The Computer Science: Data Security Specialist program prepares students to be employed as specialists in information technology data security and addresses the security specialist's everyday tasks of configuring, monitoring and repairing areas of security breach potential. Such tasks include data, internet, network and email security, client and server forensics,

and security for database users. Instruction includes recognizing and intervening to counter malware.

Naugatuck Valley Community College (NVCC) - Criminal Justice/Public Safety: Computer Crime Deterrence Option - Associate in Science

NVCC's program provides preparation for students to obtain entry-level positions in cybersecurity and computer crime deterrence and preparation and assistance to students to transfer to other institutions of higher education. It provides essential skills to gain and maintain employment at entry-level positions as computer crime investigators, computer security specialists and federal law enforcement officers. This new program combines elements of both NVCC's Criminal Justice and Computer Information Systems programs to offer students grounding in understanding the investigative nature of cybersecurity in the criminal justice realm and to gain technical skills in computer science networking and programming.

Norwalk Community College - Computer Science: Computer Security Program Option - Associate in Science

The A.S. degree program prepares graduates for careers in Computer and Information Security, equipping them with marketable skills and a targeted knowledge of the infrastructure that supports IT in business. The hands-on labs built into this program ensure that graduates go far beyond just theoretical studies.

Southern Connecticut State University - Computer Science: Networking & Information Security Option - Master of Science

The M.S. degree program in Computer Science educates next generation leaders in the field: technologically competent, capable of implementing the latest research and theory and prepared to meet the upcoming challenges of the information age. Program graduates program are prepared to advance their careers in any technology-rich field requiring advanced analytical skill or to pursue a doctoral degree in a computing-related field. The program is intended for computer professionals and those who wish to move into the computer field from other areas of study. The Network & Information Security Option is a cybersecurity concentration designed to prepare students with a solid foundation of information assurance along with skills to install security software, monitor networks for security breaches, respond to cyber attacks and gather data and evidence to be used in prosecuting cyber crime.

Western Connecticut State University - Cybersecurity - Bachelor of Business Administration

This degree builds upon student understanding of information systems security to develop additional understanding of cybersecurity issues faced by several kinds of organizations. The degree program covers both behavioral and technical aspects of security and develops student skills to learn how to conduct and prevent cyber hacking. Students are encouraged to take compatible courses in Justice and Law Administration and Computer Science as well

as courses in the Ancell School of Business core curriculum to enhance understanding of the critical importance of cybersecurity.

Connecticut's Cybersecurity Challenges: Findings, Recommendations and Key Tasks

Findings

1. Every state in the United States has serious cybersecurity challenges. Those facing Connecticut's government, businesses, educational institutions, civic organizations and citizens share both the common national intensity and also some threats designed and configured to affect Connecticut people and institutions. The range and sophistication of threats change constantly.

   For analytical purposes, the threats can be broadly grouped into three areas:

   - **Data breaches**: The loss of control over information stored on government or commercial information systems and databases. Such breaches can include credit card data, electronic medical records, Social Security numbers and a variety of personally identifiable information. There are scores of recent examples. One privacy rights website lists twenty-nine *reported* data breaches from Connecticut organizations since 2005, with over half a million privacy records potentially compromised.

   - **Disruption of services that rely on IT infrastructure:** The denial of business or government services through damage to networks and computing infrastructure, including the compromise or shutting down of vital public services. Such damage has several potential points of entry including connection of Internet and operating systems, supply chain compromise, human error or action and compromised Internet of Things devices. IoT devices were identified as the source of a disruption to commercial internet services experienced in October 2016, wherein websites including Twitter and PayPal were unreachable by much of the East Coast of the United States for several hours.

   - **Failure to maintain information systems and networks to minimize the occurrence and severity of cybersecurity incidents:** System maintenance involves designing, implementing and maintaining secure networks, systems and applications as well as training, employing and managing a knowledgeable, qualified IT workforce. It includes strong organizational controls, application of compliance standards such as HIPAA, FTI, and Payment Card Industry (PCI) controls and effective audit programs to verify adherence to security standards.

2. The DAS survey of state agencies confirmed that state IT systems follow basic security practices but require additional attention to be fully compliant with foundational

controls. Identified areas for improvement include automation of hardware and software inventories as well as remediation of known vulnerabilities. The "20 Critical Security Controls" developed by the Center for Internet Security were used to provide common evaluation criteria across agencies. Some agencies require compliance with multiple audit regimens, such as HIPAA or FTI. Many operate public-facing websites and applications, some operate internal applications for employee use and all use IT services such as email and network storage to conduct daily business. Funding for cybersecurity is not specifically identified or centralized, leading to fragmented efforts to address cybersecurity needs among state agencies.

3. The public online survey found that most businesses have personnel dedicated to securing IT systems against cybersecurity threats. Three out of four large businesses indicated that they received enough effective information to address cybersecurity concerns, but only half of the small and medium businesses reached the same conclusion. Both small and large businesses supported the suggestion of increased public warnings or a public website to provide additional threat information.

4. "Home Team" discussions confirmed the need to address two key elements: information sharing and a broad-based effort to increase cybersecurity awareness. The perception of "stovepipes" of information that interfere with coordinated and effective responses to cyber incidents was common. There was a recurring theme, in threat briefings and in the Home Team discussions, that people are the biggest threat to our cybersecurity infrastructure. Violations of security protocols circumvent even the strongest security posture. Lack of understanding of risks and of efforts to mitigate risk hamper effective executive support.

5. Demand for cybersecurity skilled resources is high in Connecticut and across the country.

6. Recovery from cyber compromise and damage is an area of growing concern and complexity. Connecticut, like other states, has an emergency management and homeland security authority capable of directing emergency operations and coordinating recovery. The longer the effects of a cyber attack continue, the more strain is placed on recovery capacity. At some point assistance from the federal government, regional authorities and the private sector would be required to supplement Connecticut's efforts to manage scenarios not previously experienced in our emergency management history.

Recommendations

Information systems and the data they convey permeate every facet of Connecticut citizens' lives and Connecticut organizations' functions. Critical systems rely on networks that are

vulnerable to a variety of rapidly changing exploits. In this environment, response and recovery are as important as preparation and mitigation. The recommendations below are aimed at enhancing Connecticut's cyber security, reducing the frequency of cyber incidents and minimizing the potential severity of incidents.

1. Creation and maintenance of a Connecticut cybersecurity webpage, hosted on the ct.gov portal. An easy-to-find and remember web page should be a hub for current cybersecurity information applicable to state and local agencies, small and large private businesses, public and private organizations and citizens. It should concentrate on organizing existing cybersecurity content and Internet resources rather than developing new content. The goal would be to create a clearinghouse for people and organizations to find information and tools to improve their readiness with online resources and training organized for user convenience.

2. Creation and maintenance of a cybersecurity library of tools and documentation available to anyone in Connecticut. This library could include standard operating system configurations, risk management templates, incident response plans, audit checklists and other tools developed by community members that can be used in an "open source" model.

3. Continuation of information sharing and professional exchange in the Connecticut Cybersecurity Committee and encouragement of similar regional and business organizations to share information and best practices. There may be value in sharing coordinated responses to cyber incidents between committee member organizations.

4. Institution of an annual program wherein state agencies audit themselves with the results reported to the Connecticut Chief Information Officer to promote focused, incremental improvements to information system security. An initial goal should be to have all state systems fully compliant with the foundational first five CIS 20 Critical Controls within two years.

5. Improvement of central utilization of funds for state cybersecurity efforts to strengthen efficiency and consistency across state agencies.

6. Review of workforce needs for cybersecurity skills and development of workforce strategies to improve the pipeline of skilled workers.

Key Tasks

Crafting a cross-agency, cross-sector state cybersecurity strategic plan involves at least nine basic tasks:

1. Creation of a Connecticut cybersecurity strategy to focus on and reduce the frequency and severity of cybersecurity incidents affecting Connecticut residents, businesses and government;

2. Establishment of plans to set clear, understandable cybersecurity standards for Connecticut government agencies, to break down silos among the stronger agencies and to help the smaller ones create effective cybersecurity programs;

3. Establishment of an approach to work with Connecticut's businesses to strengthen defense and to enhance cybersecurity in Connecticut enterprise with special attention to four major business clusters:

    - Health care and biosciences
    - Defense
    - Financial services and Insurance
    - Public Utilities

4. Establishment of an approach to higher education to enhance understanding of cybersecurity threats, strengthen defense and to educate cybersecurity professionals to fill both business and government job demands;

5. Establishment of an approach to collaborate with law enforcement to strengthen communication and intelligence sharing with and among state and federal authorities to enhance cybersecurity defense;

6. Establishment of an approach to Connecticut's municipalities to help them create and strengthen their cybersecurity defenses, exchange best practices and create and hone communications channels to manage disruptions;

7. Planning and execution of statewide multi-sector cybersecurity emergency planning including one or more tabletop exercises;

8. Planning and exercise with the media to understand shared challenges in conveying timely, accurate, authoritative and constructive communication in the event of a cybersecurity incident or disruption; and

9. Bringing all this work together. Integration of the common efforts of Connecticut government, business, higher education, law enforcement, municipalities and the media to understand, prepare for, respond to and recover from threats to Connecticut's cybersecurity infrastructure.

Appendix

Cybersecurity Strategy Core Team

- Mark Raymond - Chief Information Officer, DAS
- Arthur House – Chief Cybersecurity Risk Officer, DAS
- William P. Shea - Deputy Commissioner, DESPP/DEMHS
- David Geick - Director IT Security Services, DAS
- Dr. Michael Mundrane - University of Connecticut Vice Provost for Information Technology (VPIT) and Chief Information Officer (CIO)
- John Vittner – Director, IT Policy, OPM

Cybersecurity Strategy Home Team

- Board of Regents for Higher Education
- Department of Administrative Services
    - Bureau of Enterprise Systems and Technology
- Department of Banking
- Department of Children and Families
- Department of Corrections
- Department of Developmental Services
- Department of Education
- Department of Emergency Services and Public Protection
    - Division of State Police
    - State Forensic Laboratory
    - Division of Emergency Management and Homeland Security
- Department of Energy and Environmental Protection
- Department of Insurance
- Department of Mental Health and Addiction Services
- Department of Public Health
- Department of Revenue Services
- Department of Transportation
- Connecticut National Guard
- Connecticut State Police
- Connecticut General Assembly
- Connecticut Judicial Branch
- Connecticut Technology Council
- The Office of Policy and Management
- The Office of the Governor
- United States Coast Guard – Sector Long Island Sound

- United States Coast Guard Academy
- United States Secret Service
- Federal Bureau of Investigation
- City of Hartford
- Town of Manchester
- Town of Newington
- Town of South Windsor
- University of Connecticut
- University of New Haven
- Capital Community College
- Travelers Insurance
- Infraguard
- The United Way of Connecticut
- The Metropolitan District Commission
- Connecticut Information Technology Security Officers Roundtable

Cybersecurity Reports and Resources Bibliography

Center for Cyber and Homeland Security. (2016). *Into the Grey Zone: The Private Sector and Active Defense Against Cyber Threats.* Washington.

CyberSeek. (2016). *Cybersecurity Supply/Demand Heat Map*. Retrieved from Cyber Seek: http://cyberseek.org/heatmap.html

Department of Emergency Services and Public Protection, Division of Emergency Management and Homeland Security. (2014). *Connecticut State Response Framework.* Retrieved from Connecticut State Portal: http://www.ct.gov/demhs/lib/demhs/srf_v_4_1.pdf

Mandiant Consulting. (2016). *M-Trends 2016.* Milpitas, CA: FireEye.com.

Richard Kissel, Editor . (2013, May 1). *Glossary of Key Information Security Terms.* Retrieved from NIST.GOV: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913810

Robinson, D., & Subramanian, S. (2016). *2016 Deloitte - NASCIO Cybersecurity Study.* Deloitte University Press.

Verizon. (2016). *2016 Data Breach Investigations Report.* Verizon.