Cybersecurity Action Plan

May 3, 2018

State of Connecticut

Contents

Foreword

Connecticut's Cybersecurity Action Plan calls on everyone in our state to defend against the growing menace of cybersecurity threats.

We are enjoying the immense benefits of the digital age. Through technology, we are creating new businesses and allowing all citizens, businesses and governments to become more efficient. In our rush to realize the benefits of technology, our society crossed the threshold into cyberspace with insufficient controls in place to manage our risks.

Regaining an appropriate balance of cyber risk and cyber reward requires awareness and disciplined plans of action to avoid potential downside in our digital lives. Some counter measures are relatively easy; others will require time, education and investment. We have no choice but to act. We cannot be complacent in face of the potential dangers the cyber world presents.

We launched our Connecticut Cybersecurity Strategy in July 2017, assessing the challenges Connecticut faces in state government, municipal government, private business, higher education and law enforcement. This Cybersecurity Action Plan builds on our strategic seven principles applicable to any group and calls for specific actions to build resilience to cyber intrusion. The plan itself does not make us safe; it gives us a way to work toward safety. We have a lot of work ahead of us. Connecticut will be a stronger, more resilient state with more competitive businesses if we can turn this plan into meaningful action.

We must advance our progress in cybersecurity, continuing to recognize that our goal of security will always be a process and not an end. Connecticut's motto holds that "he (or she) who transplants sustains." In that spirit, let us take action to earn a more secure future.

Dannel P. Malloy

Governor of the State of Connecticut

Introduction

In 2016, Governor Dannel P. Malloy called upon leaders in Connecticut to address and reduce the risks to our state from growing cybersecurity threats. A multi-disciplinary team of state government, local government, education and private business undertook the task. Governor Malloy announced the product of this effort as the first statewide Connecticut Cybersecurity Strategy on July 10, 2017. The strategy outlined the risks to our state, identified the imperative to improve and proposed seven fundamental principles through which all entities in the state, public or private, could reduce their cybersecurity risks.

This document, Connecticut's Cybersecurity Action Plan, follows the Strategy and sets forth specific steps necessary to strengthen the state's ability to defend against and recover from cyber compromise.

Connecticut's Cybersecurity Strategy and this Action Plan together are a call to arms to prepare for, prevent, respond to and recover from threats to our cybersecurity infrastructure at the state, local and private sector levels. The Action Plan's purpose is to effect coordination between government entities with focus on state and municipal government, the private sector, institutions of higher learning and law enforcement.

Seven Principles

1. **Executive Awareness and Leadership**
2. **Cyber Literacy**
3. **Preparation**
4. **Response**
5. **Recovery**
6. **Communication**
7. **Verification**

Five Sectors

1. **State government**
2. **Municipalities**
3. **Business**
4. **Higher education**
5. **Law enforcement**

Executive Summary

This Action Plan identifies goals for Connecticut's five critical sectors and applies seven principles for strengthening cybersecurity defense identified in our strategy:

- Executive awareness and leadership;
- Cyber literacy;
- Preparation;
- Response;
- Recovery;
- Communication; and
- Verification.

The single, most impactful way for any organization to reduce cybersecurity risk is to have informed and engaged leadership. Leadership positively influences the rest of the principles, flows through all sectors and throughout the action plan. While the leaders in each sector may have different titles such as CEO, Agency Head, Administrator, Board of Directors, or Elected Official, they all need to lead by example by increasing their own awareness and requiring regular risk reporting and communication.

A second theme in the plan is the need to improve every individual's level of cybersecurity awareness. Each employee, student and resident must understand how to operate technology safely. Without a basic knowledge level, it is simply too easy for cybercriminals to entice individuals into giving away access to systems and data. The Action Plan calls for education of employees in the workplace, students in our schools and teachers as they prepare to bring new skills into the classrooms. We must place special attention on addressing the cybersecurity skills gap in our workforce, estimated to be over 4,000 unfilled jobs. Two-year and four-year education programs must supplement employer-funded training to meet our state's need for cyber warriors.

It should not be a surprise that much of the feedback collected during creation of the Action Plan indicated a lack of information on where to start improvements. Cybersecurity risk reduction is a relatively new topic outside of the technology workforce. Fortunately, resources have been mustering to address this issue. All sectors stand to gain from work with a member of the National Council of Information Sharing and Analysis Centers ("ISACS"). These groups share information on threats and best practices to reduce risk. State- and national-level online resources are also available for businesses and individuals. A listing of resources is at the end of this Plan.

Our state has a rich history of responding to disasters through cooperation and mutual-aid. Cybersecurity risks present a new type of man-made disaster that requires attention. Connecticut state government, towns and cities need to prepare for the disruptive effects of cyber incidents

including prolonged absence of public utility services and to participate in statewide emergency response exercises. The Division of Emergency Management and Homeland Security (DEMHS) within the Department of Emergency Services and Public Protection, is charged with anticipating the new dimensions and challenges of a cyber attack on Connecticut's critical infrastructure and rehearsing recovery scenarios. DEMHS will complete and disseminate to appropriate tribal, local, state, federal and private sector partners Connecticut's Cyber Disruption Response Plan and conduct training and exercises to sharpen performance.

Private business must demonstrate that it understands its role and is prepared to protect citizen data and the critical services it provides. A key goal of Connecticut's Action Plan is for businesses to recognize the threats they face and to have serious, effective programs that distinguish Connecticut businesses as active partners in the state's cybersecurity efforts, thereby improving their security and helping give Connecticut a competitive edge.

It is especially important that company boards of directors and chief executive officers recognize the dangers of cyber compromise. Connecticut has been a pioneer in fostering a collaboration model for state officials to review annually cybersecurity defense capabilities in the electricity, gas and water sectors. Given strong public interest in the ability of companies to defend against cyber intrusion, a key question is how effective cooperation and collaboration between business, the public and government can be. The future path may be one of annual audits conducted by licensed firms chosen by each company. Where our preferred route of voluntary action does not achieve necessary goals, inevitably the political process will look to legislation and regulation. We offer at the end of this report some initial budgetary and management considerations to help start that discussion.

The Action Plan calls for strengthening our approach to law enforcement and security related to cyber crime. Recommendations to continue the progress being made begin with strengthening the Connecticut Intelligence Center's analysis capacity and increasing its ability to assist law enforcement to benefit from classified cybersecurity intelligence. The second step is creation and staffing of a dedicated state cybersecurity investigations unit to work with local and federal authorities. The third is training: a basic cybersecurity training program for cadets, programs for all troopers and assistance in cybersecurity education for municipal police. Finally, law enforcement will benefit from planning and rehearsing response to new challenges in the event of a critical infrastructure compromise.

"THERE ARE RISKS AND COSTS TO A PROGRAM OF ACTION—BUT THEY ARE FAR LESS THAN THE LONG RANGE COST OF COMFORTABLE INACTION."

John F. Kennedy

State Government

Goal

The Action Plan goal for state government is to make cybersecurity awareness and strengthening a top priority throughout Connecticut government. Connecticut needs to protect its extensive data, public processes and services covering the complete span of personal information, public safety and support, elections and the work of each agency. We should not wait for a large-scale cybersecurity incident to occur before we make this a priority.

Connecticut government needs to be a safe place to work, its communications and products difficult to compromise with a workforce aggressive in its efforts to enhance security. The state should be a national leader in cyber defense by creating a culture of cyber responsibility and hygiene in which every agency head is accountable for his or her own cybersecurity program and every employee becomes a cybersecurity defense agent.

Every agency head or equivalent in the Executive, Judicial and General Assembly branches of government needs to understand and promote Connecticut's seven cybersecurity principles. Agency heads should communicate the principles thoroughly, apply them to each job and incorporate them in annual performance reviews.

Executive Awareness and Leadership

The first priority is top-level leadership. A necessary initial step is for the Governor and his or her commissioners, Chief Justice of the Supreme Court and the House Speaker and Senate President pro tempore to communicate to their respective branches of government the need to adopt an enhanced culture of cybersecurity awareness and defense. Each should explain why such change is necessary and communicate expectation of positive behavior change consistent with the seven principles.

State government leaders immediately below these top officials should review the adequacy of technical and management defense systems, seek assistance from the Bureau of Enterprise Systems in the Department of Administrative Services (DAS/BEST) when needed, provide training as required and make every part of Connecticut government a resilient, flexible and active source of cybersecurity strength.

To manage and reduce cyber risks, each branch of state government needs to report quarterly the state of cybersecurity risks and the activities undertaken to reduce them. The Department of Administrative Services/Bureau of Enterprise Systems and Technology (DAS/BEST) will facilitate and collaborate with the Office of Policy and Management (OPM) and Department of Emergency Services and Public Protection (DESPP) in managing these reviews for the executive branch. Agency executives will be responsible for delivering these reports and a summary of results to top-level officials, including the oversight legislative committees.

The Judicial Department and the General Assembly should establish their own annual review and assessment processes. DAS/BEST will be available to assist these processes if requested.

Annual assessment of all agencies' (executive, judicial and legislative) cybersecurity risk should be completed using National Institute of Standards and Technology (NIST) Cybersecurity Framework methodologies. Agencies with less sensitive data may assess cybersecurity risk against alternative frameworks such as the Centers for Internet Security Top 20 Critical Controls.

Cyber Literacy

All current and future state employees need to receive education in cybersecurity awareness in accordance with their roles and responsibilities, including the need to utilize multi-factor authentication (MFA) for critical or sensitive systems. Periodic refresher training will be required to reinforce solid security practices. DAS offers the ability for all Executive Branch employees to take monthly, self-paced cybersecurity training. Agencies should include in their risk reports descriptions of education programs including the percentage of employees participating in annual or refresher cybersecurity training.

Both central and agency personnel with technology, procurement and audit responsibilities need to receive cybersecurity training on subjects relevant to their work, with receipt of cybersecurity certification when available. By January 1, 2020, 20 percent of security personnel should have received the International Information System Security Certification Consortium's (ICS2) Certified Information Systems Security Professional (CISSP) or similar designation.

Connecticut's Department of Education should propose introduction of K-12 curricula materials designed to promote safe computing concepts and practices.

Connecticut's Department of Labor and Department of Economic and Community Development need to address public awareness programs and job training supports to help create and maintain a cybersecurity workforce commensurate with employment needs.

Preparation

Connecticut needs to take several specific steps to prepare for the disruptive effects of a cyber incident or attack:

1. The Division of Emergency Management and Homeland Security (DEMHS) in the DESPP needs to complete the State Cyber Disruption Response Plan as an annex to the State Response Framework and Disruption Response Plan and distribute it to all agencies;
2. Connecticut's participation in the national Cyberstorm VI exercise and its annual emergency management exercise for 2018 and beyond should include practice of the cyber incident response plan and the cyber disruption response plan;

3. DESPP should continue to review the state and local allocations for cybersecurity under the federal Homeland Security Grant Program and determine their applicability for Connecticut's state and local cybersecurity needs;
4. The DAS/BEST should encourage and track agency and municipality participation in the Multi-State Information Sharing and Analysis Center (MS-ISAC);
5. DAS/BEST should prepare, review and take remedial action pursuant to annual security assessments including external security reviews of security and penetration testing as called for by nature of function and sensitivity of data;
6. The state's Cybersecurity Working Group should continue to provide a forum for tribal, local, state and private sector officials and subject matter experts to communicate regarding emerging issues and proposed policies;
7. DAS/BEST should create an active threat-hunting team to identify swiftly threats that may cross security perimeter protections;
8. All state agencies should have documented compliance with at least the first five of the CIS 20 Critical Controls by December 31, 2018. Agencies with more strict requirements should follow the more strict required controls; and
9. All state agencies should complete data inventory and classification activities for all data in their care by December 31, 2018.

Response

All state agencies should complete and rehearse their incident and disruption plans and be prepared to execute them when required. The state agencies should record statistics for the number of times they have initiated their incident response plans and document outcomes, resolutions and recommended modifications to their plans for future use. In light of experienced use of their plans, agencies should submit suggestions for changes and improvements to the statewide template to DAS/BEST.

Recovery

All state agencies should have a recovery plan including continuity of operations planning based on worst-assumption scenarios and rehearse recovery steps in annual exercises. Integral to recovery is trouble-shooting capability, a broad array of problem management and root cause analysis capabilities applied to the full spectrum of possible intrusions. State agencies should maintain, update and review regularly their Continuity of Operations Plans. Among future challenges requiring attention is whether there should be state assistance to resident victims of cyber crime and identity fraud.

When incidents and disruptions occur, each agency should submit an after-action report reflecting its own lessons learned to inform other parts of state government how the agency managed its disruption.

Communication

Effective communication is necessary for successful management of all seven cybersecurity principles. In the event of a cyber disruption, agencies need to anticipate concurrent dissemination of false news and propaganda to aggravate the negative consequences of attack. Pre-planned messages, effective relations with the media and the ability to use social media may be required in response and recovery.

Specific steps to prepare for required cybersecurity communications include these:

1. Each agency needs to prepare a standard briefing format for cyber incidents and disruptions, compatible with the State Response Framework that can be used for communications with the general public;
2. DAS/BEST should create and maintain an easily accessed and readily understood cybersecurity public website. Agencies should visit the website frequently, provide feedback and ensure that information is fresh, relevant, helpful and appropriately comprehensive;
3. Each agency needs top-level attention to make communication regarding cybersecurity issues a priority. Important elements of such communications are educational meetings and dialogue with other state agencies, local government, private business, educational institutions and law enforcement and security;
4. Each agency should develop and test its cybersecurity communications plan to prepare for incidents or disruptions.

Verification

This action plan calls on all three state government branches to improve their respective cultures regarding cybersecurity and to take concrete action to protect Connecticut. Unfortunately, the state faces potentially devastating threat scenarios requiring profound change from top leadership to every employee and including all digital systems and use of the Internet. Presenting ways to strengthen defense and recover from compromise are not enough. Connecticut needs to verify that its action plans are working, both through formal reviews and by requiring state employees to cooperate and to report shortcomings and vulnerabilities they discover.

DAS/BEST with the Auditor of Public Accounts should determine how best to measure cybersecurity improvements through existing audits and incorporate such measures into the annual agency reporting process.

Agencies should identify capital improvements, action plans and expenditures that support the seven strategic principles in improving Connecticut's cybersecurity.

DAS/BEST should receive reports from each government agency and provide a summary annual report on the status of cybersecurity in Connecticut to the Governor, Chief Justice and General Assembly leadership. The report should assess progress on the seven cybersecurity principles -- and on any action that will result in more effective cybersecurity for Connecticut.

Municipal Government

Goals

Each Connecticut municipality needs to make cybersecurity awareness and cybersecurity defense top priorities, relevant to its distinct character. Our goal is for municipal governments to create serious, effective cybersecurity programs to protect citizens and municipal governments and to help make Connecticut a national leader in cybersecurity defense. We seek to have municipalities become active participants in the state culture of cybersecurity responsibility and hygiene and to create effective, local programs to enhance statewide security. Recognizing the value of shared experiences, templates and suggested municipal guidelines should be available and crafted to fit the needs of each distinct municipality. Simultaneously, appropriate local solutions may be most effective and affordable if managed within a regional context in cooperation with state law enforcement and management authorities.

Executive Awareness and Leadership

The critical first step is leadership. The top elected municipal official, the governing board and the head administrative officer all need to recognize the primacy of Connecticut's cybersecurity challenges and advocate for cybersecurity awareness and defense, underscoring the fact that effective cyber defense involves all citizens and is not simply a matter of information technology or management.

A key municipal responsibility should be determination of the adequacy of technical and management defense systems. Recognizing that cyber penetration is possible from any point of municipal communication or operation, both cultural and practice hygiene need to extend throughout local government.

Leadership applies to regional and association cooperation as well. To share lessons learned and best practices, Connecticut municipalities should have the benefit of cybersecurity expertise and practices from the Connecticut Conference of Municipalities (CCM), the Connecticut Interlocal Risk Management Agency (CIRMA), the Council of Small Towns (COST), Connecticut's nine Councils of Government (COGs) and the DEMHS Regional Emergency Planning Teams. These organizations should play leading roles in advancing action plans and supporting municipal cybersecurity defense and response.

Cyber Literacy

The use of shared education programs, adopted appropriately for local use, can help bring municipal employees up to appropriate levels of cyber literacy. All current and future municipal employees need to receive basic education in cybersecurity awareness. Some functions will require customized

training. Risk reports to municipal governing authorities should have descriptions of education programs including annual or refresher programs and assessments regarding the extent to which municipal employees have completed them.

Key to building a more secure cybersecurity environment for Connecticut's future is creation of effective education programs in K-12 curricula designed to promote safe computing concepts and practices.

Preparation

Connecticut's towns and cities need to prepare for and rehearse responses to the disruptive effects of a cyber incident or attack ranging in severity from a ransom demand or compromise of personal information such as tax and medical information to the effects of prolonged absence of public utilities**.** Some specific steps can start the preparation process:

1. Assessment of the steps necessary to prevent a ransom attack and plans to manage an attack should one occur;
2. Plans to protect municipal tax and other sensitive citizen information and to communicate with victims and manage response should there be compromise. Larger cities would benefit from conducting data inventory and classification, while smaller municipalities could survey exposure by completing a data security plan, sometimes called a "written information security plan," or "WISP."
3. Confrontation of the reality that cyber exposure requires both financial and personnel resources while all Connecticut cities and towns face difficult budget constraints. Municipalities have to decide how to reduce risk to acceptable levels, how to reach cost-effective decisions and share regional solutions and whether to purchase cyber insurance. Sharing of common best practices can produce enhanced collective defense, including up-to-date patching, multi-factor authentication, frequent renewal of appropriately complex passwords and assignment of greater levels of personnel for the most critical functions.
4. Definition of municipal cyber crimes and plans to manage them. Decisions regarding municipal, regional and state police protection and investigation capabilities in the event of a cyber crime, and if municipal police are not able to respond, plans regarding guidance to municipal citizens;
5. Recognition that the consequences of a prolonged absence of public utility services would present unprecedented strains on local communities and require expansion of existing severe weather/mutual aid scenarios. Connecticut municipalities need to prepare for the consequences of long outages. Challenges could include heating or cooling shelters, requirement for extended first-responder duty, food, water and medicine shortages and public order disruptions;

6. Recognition that a cyber incident could bring public anxiety and panic. Unusual communication demands and channels, such as social media, need to be foreseen and planned; and

7. Awareness of how municipal governments will execute their Cyber Incident Response Plans as part of their Local Emergency Operations Plans and awareness of municipal roles in the State Cyber Disruption Response Plan.

Response

Among the specific intrusions requiring effective, professional response are management of cybercrimes against the municipality or its citizens, ransom attacks and compromise of sensitive citizen information. Municipal governments need to decide ahead of time what they will do in the face of such challenges and cover a full range of cyber emergency responses in their emergency response exercises.

Based on the state template of incident and disruption plans, municipalities would benefit from running scenarios and assessing what could happen in the event of a cyber attack, including population migrations out of or into a municipality or neighboring community. Municipal officials should participate actively in statewide cybersecurity emergency exercises to anticipate regional emergency response assets and to understand what assistance could be available from state agencies.

Recovery

Connecticut towns and cities need to imagine the difficulties and disruptions that could result from a range of cyber compromises or attacks and plan recovery. Plans should include:

1. Identifying the team that would respond to various threats and consideration of actions necessary if an attack such as a ransom demand were to close off access to communication and management of police, fire and other municipal operations;

2. Identifying a central facility to manage recovery with generation capacity and registered with utilities for priority response;

3. Recovering from compromised sensitive information or the closure of schools for a prolonged period; and

4. Managing the effects of prolonged absence of critical infrastructure services. Specific needs could involve managing triage operations from a central recovery center and proactive efforts to determine damage and to effect remediation.

Communications

Effective communication is necessary for successful management of all seven cybersecurity principles. Both the substance and means of delivery might be quite different from normal conveyance of municipal government information. Speedy, accurate, complete and relevant communications are necessary to sustain credibility and operational effectiveness in the face of a compromise of any sort.

Municipal authorities need to anticipate dissemination of false news and propaganda intended to aggravate the negative consequences of compromise or attack. Pre-planned messages, effective, established relations with the media and the ability to use social media are likely to be required for effective response and recovery. Citizens of a municipality should know ahead of time how to receive authoritative information in a compromise situation. Towns and cities should develop and test cybersecurity communications to prepare for a full range of incidents or disruptions.

Verification

Municipalities need to review changes required by action based on the seven principles to determine how well they work and how they can be improved. Facing cybersecurity challenges requires change, and change is difficult for any organization. The normal response is to do things as they have been done in the past – a response that may not work on a new set of problems.

Unpleasant as it is to confront, the United States including its individual states and municipalities faces potentially damaging cybersecurity threats with national security consequences. Effective defense requires that towns and cities be part of an integrated security effort. The steps outlined in this action plan need to be examined, supplemented and replaced through a process of verification and improvement.

Business

Goals

Connecticut's business community shares common perspective with Connecticut's elected officials and the public on several key points regarding cyber threats. All want businesses to thrive, to enjoy protection against intellectual property theft, and to afford employees, customers, shareholders and the communities in which they operate reasonable security from business interruption or destruction resulting from cyber penetration damage. Harm to a company from whatever source has public consequences.

All businesses that have computers and connect to the internet are vulnerable to compromise. Every private sector entity faces the continuing, difficult task of ensuring that its products and services are safe and that its communications and work with vendors and all outside parties remain secure despite constantly evolving threats. Operating in a state that educates cybersecurity personnel, seeks to create a culture of business cyber hygiene and openly discusses cybersecurity threats while seeking to contain them can have positive, reinforcing effects on individual company cybersecurity.

A key goal of Connecticut's action plan is for every company to recognize its threat environment, to have a serious, effective cybersecurity program and to help distinguish the state's business community as being an active partner in the state's cybersecurity efforts. The necessity of effective business cybersecurity to jobs, prosperity and even survival underscores that the national trend is to look to legislation and guidelines to strengthen cybersecurity practices. The Securities and Exchange Commission emphasized the importance of this goal in a February 20, 2018 unanimously approved set of guidance to assist companies in the disclosure of cybersecurity risks and incidents. The guidance also required controls that prevent insider trading of securities when in position of privileged information about cybersecurity risks and incidents. In a February 21 SEC press release, Chairman Jay Clayton urged "…public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

Connecticut's goal is to work with its business community through active collaboration to accomplish as much as possible before formal processes and legislation prove necessary. Two key results of collaborating can be increased security and lessons learned regarding what works and what does not. Absent active collaboration, it is entirely possible that the critical need for effective cybersecurity measures will result in legislation and regulation that do not effectively reflect the best interests of the state or of private business.

There are cybersecurity defense standards for different industries and services, including defense companies, banks and insurance companies. Larger companies can draw upon trade association and federal guidance to improve their security. Companies with operations in other states and countries

have a stake in Connecticut's efforts to strengthen cybersecurity. They need cyber-literate employees aware of a culture of cybersecurity who will support and reinforce company cybersecurity programs. They stand to benefit from information exchange with colleagues and competitors in similar businesses. They all face the threat of receiving supplier products and services reflecting inadequate protection and stand to benefit from receipt of products and services from companies with rigorous cyber programs. Less tangible but nonetheless relevant is the benefit of doing business in a state that emphasizes cybersecurity not only in business but also in state and municipal government, higher education and law enforcement.

Smaller companies that may not have the benefit of a network of peers or structured access to federal intelligence still need to measure their cyber risks against their defense systems to determine whether their cybersecurity maturity and applications are sufficient. A cyber compromise can have extensive consequences, reaching into many areas including operational integrity, financial vulnerability, business and brand reputation, public confidence in products and services, corporate branding and ability to hire. Cybersecurity is a business risk. At some point, with greater experience and more data, the insurance industry will be able to fill many existing gaps and offer counsel as it does with other risks. At present, many businesses, especially small ones, are learning about cybersecurity exposure and seeking guidance in constructing appropriate defense.

Executive Awareness and Leadership

Boards of directors and chief executive officers need to recognize how easy it is to penetrate and damage an inadequately protected business and lead the process of creating effective cybersecurity defense programs tailored to their companies. Business leadership recognition and application of Connecticut's seven cybersecurity principles would be a significant boost to our state goal of national cybersecurity leadership. The principles are general and flexible, given to different emphasis and relevance in different settings. Those leading and managing companies are welcome to take and use them, incorporate them in business mission statements, cultures and value propositions and then apply them actively as best practices. Today's business leaders need to manage cybersecurity both to avoid damage and to give their businesses a competitive edge.

The need for leadership extends beyond individual companies to Connecticut's municipal, regional and statewide business organizations. Connecticut's metro and regional chambers of commerce have communicated interest in both raising awareness and finding shared service solutions to strengthen small- and medium-size business cybersecurity. Such organizations can help make best practices, templates, new information and practical checklists available for individual business use rather than keeping them closed and proprietary. A safe business community is a welcome setting for a safe company.

Cyber Literacy

Every Connecticut business should be familiar with cybersecurity vocabulary, terms and issues, and cyber defense should be a core part of every corporate culture. Connecticut businesses need to bring together understanding of cybersecurity issues and their own risk management challenges to form strategies and action plans best suited to their own cyber defense posture.

Preparation

Recognizing that all computer, digital and communications systems are susceptible to compromise, each company should conduct its own data inventory and cybersecurity risk assessment. A defense plan could follow from such assessment -- regularly reviewed, updated and exercised -- to prepare for and deflect compromise attempts. Levels of attention to cyber compromise should be commensurate with the value placed on risk exposure. Substantial resources exist to help businesses understand how to start preparations in the context of their industry.

Information Sharing and Analysis Centers

Many medium-size and larger Connecticut businesses participate in Infragard, a partnership between the FBI and private business. The InfraGard program provides a vehicle for public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.

There is a national network designed to help any business seeking assistance and collaboration in cybersecurity. “Sector-based Information Sharing and Analysis Centers” (ISACS) work through the National Council of ISACS (NCI) to “collaborate and coordinate” with each other. They share information regarding cyber and physical threats and “mitigation strategies” among members and with government and private sector partners. ISAC council members have representatives on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor and can work with the National infrastructure Coordinating Center (NICC) during significant events.

The ISACs offer daily and weekly calls and reports, respond to requests for information and offer participation in cyber exercises. Small- and medium-size businesses looking for information, support and collaboration in cyber defense can affiliate with an ISAC. The NCI currently has sector organizations covering a wide range of private businesses:

Automotive ISAC	Aviation ISAC
Communications ISAC	Defense Industrial Base ISAC
Downstream Natural Gas ISAC	Electricity ISAC
Emergency Management and Response ISAC	Financial Services ISAC
Heathcare Ready	Informational Technology ISAC
Maritime ISAC	Multi-State ISAC

National Defense ISAC	National Health ISAC
Oil & Natural Gas ISAC	Real Estate ISAC
Research and Education Network ISAC	Retail Cyber Intelligence Sharing Center
Surface Transportation, Public Transportation and Over-the-Road Bus ISACs	Water ISAC

Businesses need to identify important cyber risks and design appropriate defenses. There is an ISAC for virtually every business.

Response

Every company should know what to do in the event of a cyber penetration and rehearse response protocols according to a reasonable variety of threat scenarios. Among the tasks to be completed are identification, assessment, containment, communication and repair. Response steps should be familiar and executed with use of reminder lists so that responses are thorough, effective and reassuring. Some responses may include customers, government officials and third-party vendors; their interests should be included in response exercises. Responses should never be ad hoc or lend themselves to enhanced anxiety.

Recovery

Recovery scenarios need to manage the most serious damage possibilities, including potential threats to the health and safety of personnel inside or outside the company; national security matters; financial and privacy compromises to employees, customers and others; and any threat that could harm a company's reputation. Effective recovery requires setting priority goals and understanding what receives the first and most intense attention including protection of lives, damage limitation, communication with affected parties, reputation defense and restoration of operations.

Communications

Communications with all affected parties need to be planned and at least roughly scripted in advance. Accounting for audiences potentially reacting with anxiety or panic and for the presence of rumors or false information, the need for authoritative, accurate and timely information is critically important. Relations with the media and public officials should reflect established trust and credibility. Emergency communications must be able to leverage familiar, positive relationships. Companies should conduct emergency exercises and rehearsals in a realistic setting, assuming a healthy dose of external chaos, competing priorities and confused messages. "Hot house" drills focused only on events within a company are of limited value.

Verification

Cyber threats and ways to counter them are constantly evolving. While this action plan and templates from trade associations and consulting firms are helpful starting points, businesses need to stop and take a fresh look at the dangers they face and their plans to thwart them. Clever and potentially devastating cyber weapons are being tested and used all the time. Leadership needs to take stock of its risk environment and think openly and candidly about possible gaps and ways to improve defense and recovery.

External risk assessments provide an excellent starting point for improvement activities. Businesses can also consider an application for cyber risk insurance. The application process itself brings insight into any organization's risks.

Cybersecurity is not a state of affairs; it is a process of staying ahead of the possible damage everyone and every business, organization and government entity face. After we construct serious defenses, we need to look back and verify that they are working as intended.

Priorities and Approaches

Connecticut needs to approach its action steps recognizing that cybersecurity is a relatively new threat, a potentially dangerous one that has already damaged Connecticut businesses, that all enterprises including small businesses are vulnerable, and that the business community is only in the initial stages of understanding and constructing its defenses.

Globally, cyber crimes are the fastest-growing form of business crime. The Hiscox Cyber Readiness Report of 2018[1] surveyed 4,100 businesses and public sector organizations in the United States, United Kingdom and three other Western European countries and found that damage to a firm's reputation and its standing with customers after a cyber attack can be significantly more damaging than economic loss. Seven percent reported lost customers as a result of a cyber attack, an equal percentage found it more difficult to attract new ones, and five percent said bad publicity had damaged the brand. Five percent lost business partners, and roughly the same percentage laid off employees.

Firms deemed "cyber experts" had clearly defined cyber strategies, were prepared to make changes after a breach, had incorporated training and awareness throughout their workforces, had conducted phishing experiments, and 60 percent had cyber insurance. The most frequently targeted sectors were financial services, energy, telecommunications and government organizations. Professional services firms were the least prepared. The most common types of attacks were virus/worm infestation, ransomware and distributed denial of service (DDOS).

[1] **Hiscox Inc., https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf**

In Connecticut, recent surveys indicate that one-third of Connecticut businesses report that the risk of cyber penetrations is increasing. Nonetheless, many Connecticut businesses take no defensive action, citing lack of financial resources and lack of expertise as the main reasons. Only about half of Connecticut businesses report conducting cyber risk analysis, vulnerability testing and penetration testing. Fewer than half of Connecticut companies provide cybersecurity training, and fewer than 30 percent report that they know the financial impact of a cyber incident or set aside funds for attack response. More than half do not plan to add a budget line for cybersecurity defense.

Cybersecurity is critical to business security. Employees, customers, local communities and governments at all levels are increasingly concerned that businesses take cybersecurity seriously and put meaningful defense programs in place. There is a parallel to public understanding the financial health of a company. Because the public cannot examine the books of companies, the law provides for annual audits of publicly traded companies.

The same may be required for cybersecurity. At present, there is no way the public can know whether a company has an effective cybersecurity program or is lax and ignores cyber threats. Certainly, Connecticut has examples of both. It is clear that government and the public increasingly demand to know what a company's cybersecurity program is and how effectively it is prepared to deter threats. Chambers of commerce, trade associations and individual companies could volunteer information regarding steps taken to enhance cybersecurity, offer descriptions of cyber defense enhancements or account for progress made in company annual reporting.

The coming years will answer questions as to how effective cooperation and collaboration between business, the public and government will be. Connecticut is receiving mixed signals. Some companies readily discuss cybersecurity initiatives while others bristle at the suggestion that the subject is appropriate for public discussion or legislative attention. The business community may find productive ways to collaborate and respond to the increasing demand for cybersecurity information. However, if defensive posture and resistance to engage in dialogue continue, the future may include more mandatory annual cybersecurity audits conducted by licensed auditors chosen by each company and managed according to generally accepted cyber assessment practices.

Application of Connecticut's seven principles is a basic starting point; each company can tailor application to fit its distinct needs. As companies design their defenses, they face increasingly complex and dangerous threats. Offensive capabilities and deployments frequently outpace the ability to defend. The movement to embed new technology into industrial products and services called the "Industrial Internet of Things," or "IIOT" offers attackers more ways to get inside of energy systems and penetrate complex cybersecurity measures bolted on to other programs. More attack path options provide more ways to compromise.

Connecticut's cybersecurity strategy identified four broad areas of private business priorities:

- Critical infrastructure;
- Defense industry;

- Insurance and financial services; and
- All Connecticut businesses and trade associations.

All four continue to face changing cyber threats. Their ability to stay ahead of those threats is critical both to them and to Connecticut. Our shared challenge is to see how much progress we can achieve together through collaboration and cooperation, and whether that progress will be sufficient to avoid use of legislation and regulation to ensure adequate security in the cyber field.

The critical infrastructure program defined by the Public Utilities Regulatory Authority (PURA) Action Plan of 2016 called for annual reviews of public utility cybersecurity programs in electricity, natural gas and major water companies, conducted by four Connecticut officials using standards selected by each utility. That plan launched in 2017 with positive results reported to the Governor, General Assembly and Office of Consumer Counsel in September 2017. The plan sets a standard for achieving results through collaboration and cooperation.

The defense industry has extensive experience in covering three core cybersecurity components: internal security, collaboration within the defense industry and structured work with national intelligence agencies. Security screening of employees, attention to the backgrounds of those working in sensitive areas and application of “need to know” filters all reinforce managed security cultures in defense company workforces. Secondly, defense industries participate in peer group collaboration to provide best practices, identify common threats and to share warnings of penetration attempts. Third, the established and structured practices of federal intelligence cooperation to identify and control intelligence information provides an effective outer shield. The defense industry can help other businesses through sharing of these practices and through more thorough supply chain verification.

The insurance industry in Connecticut has started to cover cybersecurity vulnerabilities, but in some respects is a developing business, gathering experience data, learning how to measure risk and price the cost of coverage. Many businesses are unaware of the cybersecurity market. Others do not look to the insurance industry for cybersecurity protection and do not see insurers as presently able to provide company-specific, concrete information to avoid cyber compromise for their products and services. Clients also note that they would welcome more extensive and effective risk reduction advice. Not surprisingly, some insurers reject such characterization and defend their ability to reduce client risk. Insurers describe collaboration with national intelligence authorities to share threat information with the insurance industry as “event related” rather than systemic.

Connecticut insurers include large underwriters with extensive programs to protect their own data and educate their work forces. Smaller agencies face the challenge of offering advice in a relatively new field of coverage with staff needing education and training or being obliged to rely on external consultants. Connecticut insurance companies have expressed interest in creating best practices and threat-information sharing settings similar to those in the defense industry. There is room to become

more effective providers of risk advice and to offer business-specific, insightful and savvy counsel to customers seeking to improve their cyber defenses.

Financial services, including both retail and commercial banking, have extensive experience in data protection. As with defense, employee screening, the use of peer group information sharing and collaboration with federal authorities are all established practices. Financial service companies can help Connecticut by helping their customers to understand more fully the range and complexity of cyber threats and by offering practical defense advice. Relations with intelligence authorities tend to be more structured than in the insurance industry, but some bankers express desire for greater collaboration.

Action Steps

Connecticut's business community can take several specific steps to improve cybersecurity:

- The public utilities can continue their leadership in collaboration with state officials started in 2017 to conduct confidential, rigorous annual assessments of their cybersecurity programs;
- The defense industry can support trade associations and the business community by discussion of what works for them: their three-tiered approach to cybersecurity. Moreover, they can tighten their work with their extensive supply chain to verify more completely the full manufacturing process;
- Insurance companies can share best practices and threat assessments with each other and make progress in becoming more valuable business partners with their insured to defend against cyber threats;
- Financial services companies can work with their customers to improve customer defense. There is scope to improve protection of information systems in collaboration with third-party service providers. The areas of personnel training, operations monitoring, testing, management of incident response and reporting of an agreed level of cyber attack are always open to improvement. While some states (e.g. New York) have decided to pursue these challenges through legislation and regulation, Connecticut is agnostic at this point as to the means of achieving greater security. Nevertheless, greater security and sharing of information will be necessary. The Federal Financial Institutions Examination Council (FFIEC) working with other regulators including state banking regulators has developed methodology for banks and credit unions to use in assessing cyber risk. The business community may develop and effect such methodologies on its own with trade association guidance. If not, the future will likely involve further state or national templates to ensure broad business cyber risk assessment; and
- The state-level, regional and local trade associations and chambers of commerce have considerable scope to enter the cybersecurity field constructively and contribute to

progress in Connecticut. They need to make cybersecurity a visible, active priority and explore provision of shared services. They need to demonstrate energy, plans and engagement. There is extensive room for offerings: a basic cybersecurity "kit" for small businesses, descriptions of the core components of a cybersecurity team, communications of technical support and educational resources available, crisis training, financial systems monitoring and operations oversight. Small- and medium-sized businesses need to be cyber secure in order to win business from larger companies that will select the more cyber-advanced competitor.

Effective cybersecurity can give Connecticut businesses a competitive edge. The inspiration to do so ought to be positive and come from within before it becomes obligatory because of damaging experiences. Connecticut business should see cybersecurity as an inevitable frontier and recognize the potential gains from active leadership.

Connecticut business leaders concur on some basic points:

- Cybersecurity threats are serious, and there is growing recognition of the damage cyber compromise can inflict on a company and the state;
- Company engagement with business organizations, chambers of commerce and trade associations can help raise awareness and share defense costs;
- Businesses must take action to increase cybersecurity defense capabilities including risk assessment, addressing company culture, allocating financial resources and training; and
- The chances are that we will see significant damage to some Connecticut companies in the future. Companies must plan for and rehearse recovery from cyber compromise.

The business community is generally resistant to new legislation and regulation affecting business operations. Connecticut is recognized in other states and in some countries as having successfully launched a "collaboration model" between state authorities and public utilities through the voluntary Connecticut annual cybersecurity review process. It is possible that collaboration could be effective in the full range of unregulated businesses. Some cyber experts warn against regulation such as New York's required reporting of cyber penetration attempts, fearing that companies will not look for cyber compromise diligently in order to avoid reporting obligations, or will resist effective detection for the same reason.

Our recommendation is that business have an opportunity to come up with its own, voluntary cybersecurity defense system, applying the seven principles and any other measures that will strengthen deterrence effectively. Skepticism that voluntary solutions will work is warranted. Absent dramatically changed attitudes and organized efforts to create effective defense, the next step should be a system of required audits similar to financial audits. Rules to assess priorities and measure the effectiveness of company programs will need to be established, and ways to ascertain performance codified. An audit system could allow businesses to choose cybersecurity auditing firms, which would

render annual assessment letters reporting performance scores and indicating required remediation but not in such detail as to help potential hackers to recognize vulnerabilities. A system of cybersecurity auditing could avoid the burden and bureaucracy of state-imposed requirements and enforcement.

While many businesses would like to have a thorough and robust corporate culture of cybersecurity awareness and prevention, not all devote the resources necessary to have one. Most businesses concur that employee awareness and screening, collaboration with trade associations or other, similar companies to detect threats and share information would be productive. They want to operate in a state known for effective cybersecurity defense. All welcome the prospect of threat alerts from intelligence sources.

For many businesses, concern regarding new legislation and regulation dominates their thinking about cybersecurity, and they approach the subject with suspicion and resentment. Cybersecurity has become a public issue. Elected officials and the public no longer accept lack of information when asked questions about the effectiveness of cybersecurity in business; they demand answers. There are positive ways to raise a banner of cybersecurity culture and performance. Where progress proves possible through collaboration and cooperation, we need leadership and experiments. The business community itself knows best how to create an effective cybersecurity climate and how best to incorporate Connecticut's seven principles into their operations. Where necessary goals are not achievable by voluntary action, inevitably the political process will look to legislation and regulation.

Higher Education

Goal

Our goal in Connecticut higher education is twofold: to increase the safety of institutions of higher learning through enhanced cybersecurity defense and to enrich the state's cybersecurity talent by improving and expanding educational opportunities.

Our action plan is have higher education be a source of strength in our cybersecurity efforts -- aware of and engaged in the fight against cyber threats, difficult to penetrate, increasing our knowledge and educating students who will contribute to a safer, more productive digital economy and society.

Executive Awareness and Leadership

A critical first step is effective cybersecurity awareness and leadership starting with the executive leadership teams of the public and private in-state institutions of higher learning and extending to staff, faculty and students. It is difficult to change the culture of an institution; it takes time and effort, and the change starts with leadership.

The academic world by its nature benefits from sharing information and research. Academic institutions risk being inviting targets because they are custodians of personal information and resources. Making Connecticut higher education more resilient and creating both a sense of defense urgency and opportunity to improve Connecticut's digital life in the largest sense, must start with academic leadership.

Cyber Literacy

Education in cybersecurity awareness should be part of matriculation and emphasized throughout the academic year through the normal channels of academic communication. Staff, faculty and students should be educated about and reminded of the dangers of cyber compromise and the advantages of living and learning in a community that understands the reality of threats in our digital world.

As more education and research is conducted using online tools, academic leaders must reinforce the need to protect data and intellectual property using safe computing skills.

Preparation, Response and Recovery

All Connecticut higher education institutions should understand the consequences of cyber compromise, how cyber disruption can cause both personal and institutional damage and upset accomplishing basic goals of education. Cyber compromise cannot be a theoretical abstract and must be an understood clear and present danger. Staff, faculty and students need to know how to recognize the signs of cyber compromise, what to do when they encounter them and what their roles

are in recovery. Institutions of higher learning need to rehearse recovery and create a participatory culture in which everyone owns safety and everyone is responsible for responding to and recovering from compromise.

Communication

Connecticut higher education needs to create communications templates for basic sharing of information, for example in information given to incoming students at the start of the academic year, at the first lecture of a semester and at department meetings. While language need not be identical for every institution, leadership can recognize the opportunities and communicate similar, basic messages. Communication can create a healthy and rigorous culture of awareness, obligation and prevention to strengthen cybersecurity hygiene and practice in Connecticut's higher education.

Verification

Each institution needs to determine which steps have the greatest success for its culture. On a regular basis, each institution should take responsibility for its own program and report progress and need for remedial action to the appropriate governance structure, summarized and shared with the Governor and General Assembly.

Action Steps

Increase the Safety of Higher Education Institutions

1. **Need to Increase Cybersecurity Defense**

Despite efforts to improve cybersecurity, Connecticut higher education institutions agree that aggressive steps are necessary to strengthen cybersecurity defense on campus. Making Connecticut higher education more resilient, and creating both a sense of defense urgency and opportunity to improve Connecticut's digital life in the largest sense, must become more visible institutional priorities.

2. **Institutional Flexibility**

Each institution of higher education should create its own cybersecurity awareness, prevention, defense and recovery programs, crafted to protect valuable personal information and verify the extent to which its programs succeed. Outside professionals from other Connecticut institutions or the private sector should inspect and test cybersecurity programs. To bring about the difficult cultural change required to understand the risks of cyber compromise and the steps needed to avert them, the leadership teams of the University of Connecticut, the Connecticut State Colleges and Universities and the independent institutions of higher learning must be actively engaged in promoting cybersecurity and extending that awareness to staff, faculty and students.

3. **The Scholarship of Cybersecurity**

Connecticut currently has academic centers of excellence examining and contributing to the advancement of cybersecurity's role in business, government and society. They are valuable contributors to the positive relationship between scholarship and practical operational challenges business and society face. Connecticut needs to determine whether more such institutions or additions to those currently at work can help to increase understanding of the state's cybersecurity needs and solutions. Connecticut higher education has an important role to play in general education and public awareness of cybersecurity directly through its students and staff and through teacher preparation programs and K-12 education.

Increase and Enrich the State's Cybersecurity Talent

Commitment and support from higher education is vital to a healthy, positive setting for increased cybersecurity. Student and faculty understanding of the serious nature of cyber threats, new habits supporting that understanding and development of skills in defense and response are key to Connecticut becoming more cyber safe. Positive change in education demands essential and difficult cultural evolutions necessary for a healthy, positive setting for cyber progress. Connecticut's student habits, their understanding of the profound nature of cyber threats and their skills in defense and counter-attacking are vital to Connecticut having a more resilient defense posture.

A full understanding of cyber issues requires not only Bachelor degree education, but also the faculty and graduate student support that accompanies such scholarship. The business community expresses less interest in the scholarship of cybersecurity and emphasizes urgent, pressing demand explicitly for two-year, Associate degree professionals. Effective community college programs, especially when combined with private sector mentoring and support, would be valuable for Connecticut students, the private sector that employs them, and Connecticut itself as a state seeking to enhance its cybersecurity defenses.

There is a serious gap between the need for cybersecurity professionals in Connecticut and the number of graduates qualified to assume those responsibilities. Some estimate about 350,000 unfilled cybersecurity jobs in the United States at present; Connecticut's share is roughly 4,000. The annual graduation of cybersecurity professionals from Connecticut's public community colleges is fewer than 40 -- less than one percent of the demand. Businesses point to the difficulty of strengthening cybersecurity because of insufficient education of cybersecurity professionals. They point out that education is not a market system: enhanced demand does not come close to producing greater supply of needed graduates despite attractive starting salaries for cybersecurity professionals. Deliberate, structural and budgetary actions are required to redress this imbalance and increase exponentially the number of Associate degree cybersecurity graduates Connecticut requires.

1. **Consultation with Employers and Professional Organizations**

Academic leaders and cybersecurity specialists must invest time and effort to understand the cybersecurity requirements businesses and other organizations express. Consultation should include

the Labor Department, the Department of Economic and Community Development, major business trade associations and employers to ensure a shared understanding of the educational requirements for cybersecurity professionals and to assess the need for curricular and programmatic changes. Higher education should also explore with employers and professional organizations opportunities for collaboration in developing and delivering innovative educational models to meet the urgent need for cyber professionals. One European model some companies recommend provides for companies to hire cybersecurity prospect students, pay them for three days of work and share the expense of two full days of education per week.

2. **Assessment of Capacity to Meet Demand for Cyber Professionals**

We need to have a candid discussion in Connecticut of whether we seriously plan to meet through our state higher education system the Connecticut demand for cybersecurity professionals. If so, we need concrete plans to address existing and projected demand for cyber professionals, the restructured and expanded cybersecurity curricula required and the geographic availability of the resulting programs.

If we do not plan to respond to the current gap through Connecticut state higher education institutions, the next logical assessment is the cost and effectiveness of relying on Connecticut-based private colleges and universities and out-of-state institutions or a combination of state and private higher education. A decision whether to meet the gap in unfilled cybersecurity positions should be explicit, thereby giving both prospective students and employers notice that Connecticut will meet demand, or that employers will need to address the education shortfall on their own. A helpful starting point would be to make available in a web site the options Connecticut's colleges and universities offer in the cybersecurity field.

3. **Commitment to Continuing Cybersecurity Education**

Connecticut higher education also needs to decide whether and how extensively it plans to provide retraining and refresher courses for cybersecurity graduates. If action were required, there would be considerable value in designing and offering such programs soon. If the decision is not to be active in retraining and refresher courses -- or to offer a limited set of courses, that decision should also be explicit so that private training can plan to fill the growing demand for continued training and recertification with a greater sense of what offerings will be in the marketplace.

Law Enforcement

Goals

Connecticut law enforcement has experienced pressure in the past few years affecting both budget allocations and force levels. On top of those constraints, cybersecurity challenges are an added dimension calling for attention. The Law Enforcement action plan identifies four principal goals, discussed more extensively in the sections below. The four are:

1. To strengthen the Connecticut Intelligence Center's intelligence analysis capacity, thereby increasing its ability to assist law enforcement through access to and use of classified cybersecurity intelligence;
2. To create a dedicated entity within the Connecticut State Police (CSP) responsible for investigating and pursuing the perpetrators of cyber crime, with adequate capacity to serve the needs of the CSP, manage effective liaison with regional and federal authorities and to assist municipal police in cybersecurity investigations;
3. To review and enhance CSP cybersecurity training programs to equip the members of the dedicated unit to perform their duties; to ensure that existing basic training in cybersecurity skills for all troopers is up-to-date and sufficient, to establish a modern cybersecurity training program for cadets; and to help provide municipal police with updated cybersecurity skills; and
4. To use the interdisciplinary skills of DEMHS, CSP and the Police Officers Standards and Training Council (POST) to prepare for and to rehearse emergency recovery from cyber compromise to Connecticut's critical infrastructure.

Executive Awareness and Leadership

The Department of Emergency Services and Public Protection (DESPP) is aware of and shares responsibility for managing cybersecurity threats facing Connecticut. The Connecticut State Police (CSP), the Connecticut Intelligence Center (CTIC) and the Division of Emergency Management and Homeland Protection (DEMHS), all within DESPP, have established command structures and leadership traditions that will help them manage cybersecurity threats and incidents.

Challenges for the several parts of DESPP working on cybersecurity include making cybersecurity a top priority and directing awareness and leadership efforts to specific actions. That work is underway with executive awareness and leadership of the CSP, CTIC and DEMHS focused on enhanced intelligence collection and analysis, creation of an investigations unit, rigorous cybersecurity training and aggressive efforts to plan and rehearse emergency services related to cyber disruption. The CSP

has established a cybercrimes unit within the CTIC and a statewide cybercrime task force in partnership with local Connecticut police departments. CSP has begun participation in the FBI's recently created Connecticut Cyber Task Force. Connecticut's Cyber Disruption Response Plan (discussed below) presents a multi-jurisdictional plan to address cyber crime proliferation and the effects of cyber attack on critical infrastructure.

Inclusion of cybersecurity metrics in DESPP reports will assist leadership to measure the volume of intelligence analyzed, the number of cases handled by an investigations unit and results of exercises based on cyber disruptions.

Cyber Literacy

Creation of a cybersecurity curriculum for new CSP cadets and a program of in-service training for CSP sworn officers delivered through the Police Officer Standards and Training Council (POST) would both standardize terms and vocabulary and provide a reference for ongoing education. Refresher courses would benefit both specialized investigations officers and the entire force, as is the case with update education in other security fields. Increased officer training and literacy would set a positive example for municipal and regional law enforcement units seeking to increase their ability to fight cyber crime.

Preparation

Law enforcement involves managing cyber crime and preparation for the unusual demands of a cyber attack on Connecticut's infrastructure.

Cyber crime is not geographically limited, making state collaboration with tribal, local, regional, state and federal authorities both necessary and productive. Connecticut's goal in preparation and execution is to earn and sustain a reputation for responsiveness and professional skill.

A successful cybersecurity critical infrastructure attack on Connecticut would present demands on law enforcement beyond those experienced in hurricanes, snow and ice storms and floods. Law enforcement needs to work with DEMHS to anticipate the unprecedented demands and prepare to meet them.

Response – Routine Events

Law enforcement faces a range of cyber crimes including theft of financial records, personal information, ransom demands and other disruptions. Effective response requires identification of threat and skilled deployment of resources. Threat identification starts with CTIC having an adequate number of both top-secret and secret cleared personnel and being able to review all cyber intelligence relevant to Connecticut. After receiving and analyzing intelligence, the investigations unit then seeks to determine appropriate response and to recommend action.

A Connecticut citizen, business or organization perceiving an entry threat to home, factory or office wants to receive speedy police response. We will eventually have similar protocols and practices with

regard to criminal digital invasions. CSP and its cooperating partners will benefit from establishing and rehearsing operational patterns identifying personnel roles and response procedures.

In December 2017, Connecticut elected to be one of the participating states in FirstNet -- a public safety wireless broadband network. Rapid rollout of this communication capability will provide public safety first responders an interoperable, private network to assist response and recovery activities.

Response – Widespread Events

A wide-ranging, directed cyber attack against critical infrastructure may require responses not previously experienced. A prolonged outage of critical infrastructure presents a set of challenges local and state law enforcement need to anticipate and practice, including assessment of security demands resulting from prolonged absence of electricity, food, water and fuel. Law enforcement needs to be prepared to ensure safe delivery of scarce supplies, and if banking systems no longer operate, to anticipate and manage new law enforcement demands. Cyber threats extend beyond police departments to other government functions including but not limited to consumer protection, health and elderly services and banking and insurance regulators.

With an estimated 76 percent of Americans using some form of electronic payment, a disruption in the digital economy could present unique challenges when access to cash becomes constrained. Unusual requirements could include protection of grocery stores, gasoline stations and hospitals. Extended shortage of potable water might oblige law enforcement to assist large out-migrations, or the opposite effect: large numbers of people coming into Connecticut from other states seeking relief. Response to widespread cybersecurity disruption presents new situations that require fresh thinking and scenario testing to understand and prepare for new challenges.

Recovery

Recovery from cyber crimes also presents new law enforcement challenges. After a critical infrastructure attack and recovery, security hot points might continue as communities seek to replenish supplies and return to normalcy. Effective security operations need to help restore public confidence and enable disrupted communities to move to normal settings of reassurance and secure availability of necessities.

Communication

Common terminology, language, procedures and values among law enforcement agencies can serve to enhance effectiveness and public confidence. As Connecticut cybersecurity officers in a dedicated investigations unit work together and with other law enforcement entities, effective communication has the same effect as in any security operation: understanding problems, priorities and orders and facilitating speedy and effective action. Knowledgeable, disciplined rule adjudication and action are

invaluable in sustaining public order and promoting public confidence in and support for law enforcement.

Verification

Retrospective assessment is always healthy to discover what works and to consider opportunities to enhance, amend or drop certain innovations. Connecticut law enforcement currently includes intelligence, investigations and training. Given the Governor's direction to improve our cybersecurity defense and create a new culture throughout the state, the question is how well law enforcement can build on its current levels of cybersecurity work to create a more effective intelligence unit, a dedicated cybersecurity investigations unit and a more extensive and rigorous training program.

Reports to the Governor and General Assembly on the effectiveness of cybersecurity law enforcement will help both those preparing the reports and the recipients to verify the extent to which action plans have succeeded.

Action Steps

1. **Intelligence.** Supplementing municipal and federal intelligence, a key starting point for Connecticut is focus on the kinds of information CTIC needs and from what sources in order to make cybersecurity a more integral part of law enforcement's ability to protect Connecticut. CTIC will need to affirm with its law enforcement partners the information it needs to receive and concurrently communicate what intelligence it intends to provide.

A basic question is what staffing levels of top-secret and secret cleared professionals are required to manage the full flow of projected cybersecurity intelligence with effective screening, analysis and referral of actionable intelligence. The intelligence function needs an explicit plan to address mission, leadership and sources of support. Prior allocation of one full-time, top-secret cleared officer to this task was not sufficient to manage effectively the growing volume of cyber-related intelligence available. Additional CTIC personnel could come from current or additional resources within the State Police, on loan from federal agencies such as the FBI or the Department of Homeland Security or from Connecticut municipal police. The plan should include guidance as to what structural and procedural changes are required to enable such a unit to operate effectively.

The structure to strengthen Connecticut's ability to receive, analyze and refer for action cybersecurity intelligence is in place. Growth and enhancement can focus on these areas:

- More extensive monthly cyber products from the Connecticut Intelligence Center;
- Robust and effective communications flow to and from local, state and federal law enforcement partners, including prosecutorial arms such as the United States Attorney for Connecticut and Connecticut's Office of the Chief State's Attorney; and

- Continued collaboration with the FBI, including contributions to the FBI Unified Crime Report.

2. **Investigations.** The Connecticut State Police is currently standing up and starting operations of a cybersecurity investigations unit to perform vital cybersecurity work for the state and to work with municipal and federal resources, possibly forming a statewide cyber crime task force. Critical to effective launch are a fresh look at how Connecticut law defines cyber crimes, and then statement of what the mission and priority concerns of the CSP investigations unit should be.

Three steps are basic to Connecticut's effort to strengthen Connecticut's cyber crimes investigations capacity:

- Establishment of a Connecticut State Police Cyber Crime Unit;
- Enhanced collaboration with the Connecticut Police Chiefs Association and the Office of the Chief State's Attorney; and
- Collaboration with the FBI and participants in the FBI cyber crime task force.

As it progresses, the CSP will be better able to determine the appropriate size and composition of its dedicated investigations unit. The unit will benefit from available intelligence to conduct investigations into current and projected instances of cyber crime in collaboration with municipal, state and federal authorities. Guidelines will define how the unit will operate with other agencies in advancing their cyber investigations. Further determinations include command, structural, and procedural changes required to enable such a unit to operate most effectively and whether the unit is to be financed by reallocation of current resources or provision of additional resources.

3**. Training.** Increased attention to cybersecurity will require at least three kinds of increased training:

- Core cybersecurity training for incoming cadets and all sworn officers;
- Specialized training for the dedicated investigations unit;
- Periodic, updated training, continuing education and recertification to keep up to speed with changes in cyber crime and cyber challenges.

The constantly evolving range and sophistication of cybersecurity threats requires ongoing revisions to curricula for training all audiences and levels of instruction.

4. **Outreach.** With these intelligence, investigations and training changes effected, Connecticut will be better able to ensure maximum benefit in collaborative work at tribal, municipal, regional and federal levels. All Connecticut government agencies, businesses, organizations and individuals need to understand these new intelligence and investigation and training capacities and be encouraged to work with them.

Response and Recovery

Goals

The goal of Connecticut's cybersecurity response and recovery plan is to anticipate the new dimensions and challenges a cyber attack on or cyber failure of Connecticut's infrastructure would have on the state. Connecticut emergency management's goal is to prepare to meet the new dimensions and challenges and rehearse recovery scenarios with all likely participants, while following the all-hazard tenets of the existing State Response Framework (SRF) and State Disaster Recovery Framework (SDRF).

Seven Principles

All of Connecticut's seven cybersecurity principles apply to response and recovery.

Priorities

Connecticut's essential priority is to ensure that it is able to anticipate, plan and prepare for, respond to and recover from the unprecedented challenges that a cyber attack on critical infrastructure could present. For Connecticut's Governor and DEMHS to ensure effective response and recovery from a cyber incident, the state requires additional procedures, practices and planning in addition to execution of more familiar duties associated with previously experienced emergencies.

Specific Actions

1. DEMHS needs to complete and disseminate to appropriate private sector, tribal, local, state and federal partners the State's Cyber Disruption Response Plan and conduct training and exercises consistent with it;
2. DEMHS will review existing protocols and work with other state agencies to ensure that public messaging and communications processes enable the Governor and emergency managers in the event of a cyber attack to start communications immediately and work to control rumors and/or counteract any misinformation that an adversary might include as part of an attack. DEMHS, the Governor's Office and other state agencies will prepare and approve statements before an attack, thereby enabling response to the unprecedented situations a cyber attack or catastrophic cyber incident could present. Communications training should include use of social media and involve Connecticut reporters and editors in training and exercises related to cyber disruption response and recovery;
3. In accordance with the State Disaster Recovery Framework, DEMHS will work with state and local agencies to prepare for long-term recovery, including management of prolonged absence of public utility services lasting from two weeks to a few months. This preparation

will include identifying potential private sector, local, state and federal sources of emergency supplies of gasoline and diesel fuel, heating oil, food and water;

4. DEMHS will use the Emergency Support Functions outlined in the State Response Framework (SRF) and the National Incident Management System (NIMS) and work with its related task forces and working groups to identify and exercise the unusual demands likely to be placed upon several entities, including:

    a. The state's first responders, including local and state law enforcement, fire services, emergency medical services, and the Connecticut National Guard in the event sustained services are needed for several weeks or months;

    b. Local and state social service agencies and public works; and

    c. Government and private sector agencies including those involved in payroll, benefits and grant management, banking and insurance.

5. All emergency response participants will need to understand and rehearse the Connecticut Governor's emergency management authority so that his or her legal actions are understood and actions likely to be necessary can be anticipated;

6. Emergency management participants will need to anticipate unprecedented shortages and be prepared to identify actions necessary to alleviate them, including collaboration with the private sector, municipal governments, Connecticut state agencies, other states and federal agencies. Critical considerations include shortages of basic resources such as fuel, water, and food and the need to support priority functions such as public utility services and medical needs;

7. Emergency management participants need to discuss and plan with local, state and federal authorities the possibility of large-scale (potentially greater than 500,000) out-migration of Connecticut residents or in-migration of citizens from other states in the case of a major cyber incident in Connecticut or the New England region driven by various circumstances, especially the absence of potable water supplies;

8. DEMHS and the Governor's office need to exercise existing communications assets and explore extraordinary means of communication between the Governor and federal authorities including with the President of the United States; and

9. DEMHS and emergency management participants need to continue design and execution of exercises that identify cyber and long-term recovery issues in order to increase awareness and identify new challenges such a catastrophic event might present.

Legislative, Regulatory and Budget Considerations

Facing the demands of strengthening cybersecurity in Connecticut -- as with all change involving government, business and society -- is difficult. Existing structures and procedures have their defenders; disruption often meets resentment and resistance. The threats and potential damage brought by the cyber world require action, and this report has sketched some of the action Connecticut requires. We cannot continue to reap the advantages of the digital economy without protecting the digital assets required to make it successful.

We should try to accomplish as much as possible through positive initiatives, collaboration, adjustment and reallocation of existing resources and seek to legislate, regulate and allocate new budget resources as little as possible. That said, there are legislative, regulatory and budget issues requiring attention. Here is an initial list of items for consideration:

1. A General Assembly joint resolution affirming that Connecticut is vulnerable to cyber compromise and that action to strengthen cybersecurity is a state priority. The resolution should call on every agency to create its own action plan consistent with Connecticut's cybersecurity strategy and this action plan.
2. Cybersecurity affects all of society and understandably relates to the concerns of several legislative committees, including and not limited to Appropriations, Banks, Commerce, Energy and Technology, Higher Education and Employment, Insurance and Real Estate, Public Safety and Government Administration and Elections. Progress in effecting this action plan and guiding future cybersecurity work suggests the need for a recognized oversight committee to facilitate policy options and resource requirements.
3. Substantial improvement to the state's security apparatus will require each agency to decide whether to meet expenses through internal budget adjustments or through new appropriations. A dedicated security improvement program should fund the initial two years of program startup. This program would request funding from the Enterprise IT Investment Program. Moreover, the federal government has outlined the possibility for cybersecurity funding for states. A combination of agency chargeback, direct appropriation and federal grants should fund ongoing support for the program. Having a program ready to use and manage these funds in program-ready form will increase the chances of securing funds should they become available.
4. Municipal governments face budgetary constraints, and few enjoy the full complement of cybersecurity professionals they would like to have. Considering the broad array of cybersecurity initiatives required, municipal governments will need to determine where to find the personnel and resources needed for effective cybersecurity programs. Cybersecurity

challenges are consistent with the long history of Connecticut municipalities adjusting priorities to meet the most pressing issues before them.

5. For many businesses, fear of and opposition to legislation and regulation dominate their thinking about cybersecurity, and they approach the subject with some suspicion and resentment. Yet cybersecurity has become a compelling public issue. Elected officials understandably no longer accept lack of information as a reason for being unable to respond to questions about the effectiveness of cybersecurity in both government and business. They demand answers. There are positive ways to raise a banner of cybersecurity culture and performance. Where progress proves possible through collaboration and cooperation, we need leadership, experiments and joint effort. The business community knows best how to create an effective cybersecurity business climate and how best to incorporate Connecticut's seven principles into their operations. Where necessary goals are not achievable by voluntary action, inevitably the political process will look to legislation and regulation as has New York State with its promulgation of cybersecurity requirements for financial service companies.
6. Regarding higher education, for several years Connecticut colleges and universities have not met the demand for cybersecurity professionals in the state. It takes years to develop curricula, hire faculty and launch classes with enrolled students. We have lost years of valuable time and need to act now, with a sense of immediate urgency, to expand the availability of cybersecurity education to Connecticut students, whether from existing resources or additional funds.
7. The law enforcement cybersecurity action plan identifies needs for strengthened and enhanced intelligence capacity, investigations, training and collaboration. It does not appear likely that existing personnel and existing resources can meet all of these changes. A fresh review of Connecticut statutes regarding cyber crimes will help sharpen the focus of the cyber crimes investigations unit.
8. Emergency management faces the possibility of unprecedented demands, some of which will be clearer after completion of cybersecurity exercises. Connecticut's municipalities, state agencies and the Connecticut National Guard will all have new roles to play and will need to assess consequential personnel and financial costs.

Acknowledgements

The principal authors of this action plan are Connecticut's Chief Cybersecurity Risk Officer Arthur House and Chief Information Officer Mark Raymond. The core team engaged in its preparation included Director of Security Services David Geick, Office of Personnel and Management Director of Information Technology Policy John Vittner, University of Connecticut Vice President and Chief Information Officer Michael Mundrane, DESPP Deputy Commissioner William Hackett and Principal Attorney in the DESPP Division of Emergency Management and Homeland Protection Brenda Bergeron.

In addition to this core team, contributors from Connecticut's municipalities and state government, education officials and from businesses and professional service companies provided information, perspective and wisdom for which the authors are sincerely thankful.

Resources

The following is a partial list of resources for cybersecurity information.

National Cyber Security Alliance

The National Cyber Security Alliance is dedicated to providing resources to help individuals and businesses become better digital citizens. These resources provide initial steps to begin reducing cybersecurity risks.

- Stay Safe Online - https://staysafeonline.org/
- CyberSecure My Business - https://staysafeonline.org/cybersecure-business/
- StopThinkConnect - https://www.stopthinkconnect.org/

Center for Internet Security - https://www.cisecurity.org/

The Center for Internet Security, is a non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. The CIS Controls and CIS Benchmarks are a global standard and recognized best practice for securing IT systems and data.

CyberSeek - http://cyberseek.org/

Provides data on cybersecurity careers and employment needs for employers, job seekers, students, and policy makers.

Law Enforcement

National - https://www.fbi.gov/investigate/cyber

Standards

National Institute of Standards and Technology - https://www.nist.gov/cyberframework

InfraGard

https://www.infragard.org/

Information Sharing and Analysis Centers (ISACS)

National Council of ISACS - https://www.nationalisacs.org/

AUTOMOTIVE ISAC - www.automotiveisac.com

AVIATION ISAC - www.a-isac.com

COMMUNICATIONS ISAC - www.dhs.gov/national-coordinating-center-communications

DEFENSE INDUSTRIAL BASE ISAC - www.dibisac.net

DOWNSTREAM NATURAL GAS ISAC - www.dngisac.com

ELECTRICITY ISAC- www.eisac.com

EMERGENCY MANAGEMENT AND RESPONSE ISAC - www.usfa.dhs.gov/emr-isac

FINANCIAL SERVICES ISAC - www.fsisac.com

HEALTHCARE READY- www.healthcareready.org

INFORMATION TECHNOLOGY ISAC - www.it-isac.org

MARITIME ISAC- www.maritimesecurity.org

MULTI-STATE ISAC- www.ms-isac.org

NATIONAL DEFENSE ISAC - www.ndisac.org

NATIONAL HEALTH ISAC- www.nhisac.org

OIL & NATURAL GAS ISAC - www.ongisac.org

REAL ESTATE ISAC - www.reisac.org

RESEARCH AND EDUCATION NETWORK ISAC - www.ren-isac.net

RETAIL CYBER INTELLIGENCE SHARING CENTER - www.r-cisc.org

SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS - www.surfacetransportationisac.org

WATER ISAC - www.waterisac.org