CONNECTICUT

Cybersecurity Strategy

DANNEL P. MALLOY
GOVERNOR

July 10, 2017

Photo: © User:Colin / Wikimedia Commons, via Wikimedia

Table of Contents

This page left intentionally blank.

Introductory Note

The digital age has put us in a tug-of-war with technology. Every part of our lives and our work is touched by—if not driven by—digital technology. We're not going to change that, nor should we. But the dangers that go with that digital exposure are relentless and escalating.

We have to confront and figure out this problem. Every person, agency, organization and business in Connecticut faces some degree of vulnerability.

You are affected whether you are a major corporation or the convenience store down the block, the General Assembly or part of our judicial system, a millennial or a senior who's off the grid, but whose health history and tax returns are sitting in government databases. And you must be part of Connecticut's effort to control the effects of digital exposure.

In 2014, I called for a cybersecurity strategy to cover our vital public utilities. We did that and launched an action plan now in operation. I am proud that our state got out front in that effort. In 2016 we went further to see what we could do to make Connecticut more secure and one of the most cyber-savvy states in the nation.

The Connecticut Cybersecurity Strategy that I announce today is a significant step. It specifically highlights state government, municipalities, business, higher education and law enforcement. But its principles apply universally, and will form a pathway to a more detailed, operational action plan.

This strategy makes it clear that we cannot ignore the problem of digital insecurity. We cannot wish it away. And we cannot wait for someone else to solve it for us. I firmly believe that, if we embrace cybersecurity as a perennial priority—as a daily responsibility—the safety and competitive advantage we can gain for our state could be immeasurable.

I am grateful to Chief Information Officer Mark Raymond and Chief Cybersecurity Risk Officer Arthur House, and to all those who supported them in crafting this strategy.

Security is not an end point; it is a process. I call on everyone in Connecticut to be part of the effort to turn this strategy into action.

Dannel P. Malloy
Governor of the State of Connecticut

Connecticut State Capitol
photo by Anthony Calabrese

Executive Summary

This strategy has a dual mission. First, it is aimed at putting the entire state on the same page when it comes to cybersecurity. We must be unified in understanding the nature, ubiquity, urgency and persistence of the cyber threat. Second, it is to put the entire state on the same path. The strategy sets forth seven foundational principles—executive leadership and awareness, literacy, preparation, response, recovery, communication and verification—that will lead the way to an action plan and adapt to any public or private entity.

Such an ambitious mission requires leadership. That is why the primary audience for this strategy is Connecticut's leaders—those who oversee our General Assembly, Judiciary, municipal governments, businesses, civic organizations, higher education institutions and law enforcement units.

This strategy discusses these principles and challenges from the perspectives of five sectors:

- Connecticut State Government;
- Municipalities;
- Business (emphasizing critical infrastructure, financial services, insurance, and defense);
- Higher Education; and
- Law Enforcement and Security.

These sectors were selected because of their statewide importance, as well as their special status as both prime targets and prime defensive players in the event of a major incident. They matter, and cyber adversaries know that.

However, the authors hope that all readers—individuals and representatives of other sectors—will see themselves in the issues raised, the principles offered and the path toward solutions.

Several themes are woven throughout this strategy:

1. Education and training are vital to the culture change Connecticut needs to optimize prevention and to be always "at the ready"—alert and prepared to manage response and recovery;

2. While respecting privacy and proprietary information, government and businesses must break down silos and embrace communication and information sharing. No one has a corner on insights and best practices;

3. Our state must adopt cybersecurity as a perennial priority—as immutable as essential services and public safety—and factor it into decisions about both short- and long-term resources and actions;

4. No one and no organization is immune. Everyone and every organization has a stake in this game and a role to play in making Connecticut more cybersecure and cyber-savvy.

5. Robust cybersecurity can become a Connecticut hallmark, making our state an even more sought-after place to live and work.

THE THREAT

Cyber attacks are different from information technology system break-downs or natural disasters, which can be remedied with standard, operational best practices. Cyber attacks are crimes—malicious acts intended to steal data, disrupt services or corrupt and disable systems. Attackers are stealthy, often "invisible" and able to strike from anywhere in the world. Methods of attack are so mercurial they can shift while an attack is underway.

Any data passed through the Internet and any Internet-connected device is susceptible to compromise. As a result, cyber attacks are potentially life-altering. We are utterly dependent on networked devices and systems, and for better and worse, our digital world is built for speed, access and information sharing—all qualities that are incongruous with the security principles needed to protect us.

Threats range from dissemination of embarrassing or false information about an individual all the way to use of cyber attacks as a weapon of war. In between is the growing industry of ramsomware, estimated by some to have harvested global revenue of over a billion dollars in 2016. Hackers paralyze systems and demand payment to release the computers, often requiring payment in bitcoin. Normally it is not possible to identify the hackers or to trace bitcoin transactions. Some insurance companies and law firms now have practice areas devoted to bargaining with hackers, arrange payment and ensure restoration of service, and understandably so.

Police departments have been forced to manage dispatch calls manually. San Francisco's public transit system was unable to receive fares during a Christmas shopping weekend. Attacks recently hit hospitals in England and Scotland. Business and municipal services in Connecticut have also been hit. Initial reaction to a ransom notice is often anger and defiance. But when one considers the impacts of losing police or fire services, shuttering a hospital or losing all of a law firm's client files, ransom is often paid. And ransoms tend to be deliberately calibrated to be affordable. The firm Symantec estimates that, while ransomware demands are rising, the average demand tripled in 2016 to $1,077.

The tension between enjoyment of online services and exposure to compromise is especially notable with the "Internet of Things." Companies are not just selling goods online, they are enticing us to have "smart" homes and offices, by enabling us to use devices remotely to adjust thermostats, activate cameras, open garages, even manage complex equipment.

The flip side of such innovation is that if we continue on the current track, by the end of 2018, a Business Insider report projects that the number of devices creating inadequately secured, potential attack vectors to our homes and businesses will grow from 6.6 billion in 2016 to 22.5 billion in 2021.

Connecticut and the country do not need an Internet of Things. We need an Internet of Secure Things. We need to reach a point where security is addressed at the design stage rather than as an add-on or correction, and when production standards for secured device technology are consistent among states. But we cannot wait. Connecticut must move to protect itself.

Where do threats come from? Powerful potential adversaries such as Russia or China could be perpetrators. But the concept of asymmetrical warfare—that a "weaker" opponent can best a stronger one with unconventional tactics and weaponry—certainly applies to cyber warfare. Aggrieved nations, such as North Korea or Iran could act. Individuals or groups for hire (cyber mercenaries) and even our own citizens are potential sources of attack. These adversaries have the ability to disguise their locations and identities, complicating attribution and retaliation.

Former President Obama warned that, at low cost, both state and non-state actors can "penetrate core functions in our society," and that ability "is moving faster than our defenses." Admiral Michael Rogers, Director of the National Security Agency and head of United States Cyber Command, warned in 2016 that, at some point, the United States will see an attack on our critical infrastructure. We have already seen such an attack, he noted, against Ukraine's electric grid.

The means of potential attack vary from simple phishing intrusions to the implantation of malware into corporate operating systems or public utility critical infrastructure. Larger scale regional or national attacks could involve shutting down a natural gas pipeline, coordinating events in several states or detonating a nuclear weapon from a satellite to trigger electro-magnetic effects that knock out electricity distribution. Whatever the intention of such attacks, their second and third order effects could be catastrophic.

The messages are clear: cyber dangers are diverse and serious; offense is outpacing defense; and our daily digital life is a threatened environment.

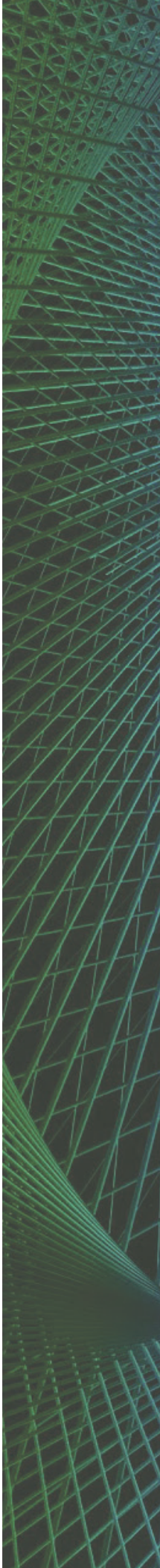
OUR SHARED VULNERABILITY

Connecticut must act with a sense of community. All individuals and entities face the potential for severe harm. We must collaborate to raise awareness of the dangers, strengthen our defenses and prepare to respond and recover. We are connected in this effort.

National experts confirm that almost everyone, including in rare instances the Intelligence Community and cutting-edge firms, has been or will be penetrated—banks, utilities, hospitals, schools, manufacturing and services firms and national, state and local governments. We saw it happen when the identities of Americans with security clearances were stolen from the federal Office of Personnel Management, and when some of our largest companies had devastating security breaches.

The Privacy Rights Clearinghouse estimates that, during 2016, all government and military in the United States had a total of 5,329,961 breaches; remarkably only 27 were made public.

Here at home, of the roughly 4.8 billion connection attempts per month to the state network from external computers, approximately 2 billion, or 42 percent, are blocked by perimeter security, based on known malicious Internet protocol addresses or threat signatures. In a typical month, state anti-virus



Connecticut State Capitol photo by Anthony Calabrese

protection catches about 2,400 malware infections before they install. Despite this protection, state third-party monitoring detects an average of 66 infected or compromised state systems per month.

The severity of potential harm and the fact that no one is immune must be heard loud and clear, not to stoke fear, but to prod us to act, particularly those involved in protecting the security and wellbeing of our state.

If the public and private sectors do not commit fully to this reality, strategies and action plans—developed by the state, individual agencies or private entities—will not be effective, and we will never realize the benefits and competitive power that come from living in a safer, more cyber-aware state.

OUR MARCHING ORDERS

There is no international or national governing regime for cybersecurity. Thus, we must defend ourselves, which demands new habits and sensibilities. At the same time, we can never stop inventing and investing in knowledge and systems that improve our lives and ability to compete.

To both embrace and protect our digital lives, and to make Connecticut a more resilient, safe, competitive state, Governor Malloy called for a statewide cybersecurity strategy. It will be followed by a more explicit cybersecurity action plan to execute the strategy.

Statue of Nathan Hale

Strategic Vision and Principles

VISION

Cyber attacks are different from information technology (IT) system breakdowns, which can be addressed with standard, operational best practices. Cyber risk management means preparing for and responding to deliberate, malicious acts designed to disrupt services, steal data, inflict terror or misuse IT systems.

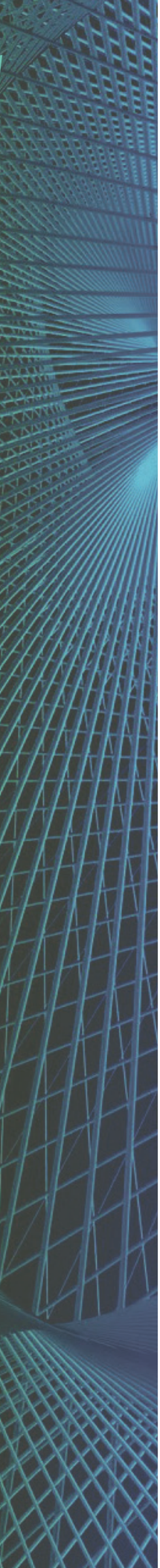
Our ability to connect anything to anything and anyone to anyone is now a cornerstone of our economy and lifestyle. Using the Internet is virtually effortless. Protecting ourselves from the Internet takes work, and that is what the Governor's directive and this strategy are all about.

The Connecticut Cybersecurity Strategy's goal is to strengthen the awareness and resilience of public and private entities to reduce the likelihood and severity of large cyber attacks. Achieving this goal requires making cyber defense a shared priority.

Americans are effective responders to tragedy and emergency but are less apt to act pre-emptively. If Connecticut's public, private and corporate citizens embrace cybersecurity as a unifying goal, and work together, we can be among the states leading the way to enhanced, nationwide cybersecurity.

In other words, managing cyber risks can provide a competitive advantage for Connecticut businesses, a more secure living environment for Connecticut residents and better stewardship of information and services by Connecticut state and local governments.

Achieving this vision—in which every citizen and organization has a stake and a role to play—will make Connecticut an even more sought-after place to live and work.



PRINCIPLES

The strategic path to this vision is built on seven principles:

1. Executive awareness and leadership
2. Literacy
3. Preparation
4. Response
5. Recovery
6. Communication
7. Verification.

These foundational principles apply to all five sectors highlighted in this strategy—Connecticut state government, municipalities, business, higher education and law enforcement and security—acknowledging that each has its own strengths and limitations. These principles are complementary and encompass the range of efforts required to build a secure cyber environment statewide.

In putting them into action, it is important, and heartening, to recognize that experience counts. Existing disaster recovery, continuity and contingency plans can and should be incorporated into cybersecurity planning. Lessons already learned about resilient design, redundancy, failover, clustering and network and application architectures have roles to play in cybersecurity response and risk reduction. There is no reason to reinvent defenses that are already compatible with cybersecurity.

Executive Awareness and Leadership

Executive awareness and leadership will largely define the success or failure of this strategic undertaking. Business and government leaders may have full plates and limited time, but there are ample reasons why cybersecurity should be one of their persistent priorities:

A single incident can be devastating. Virtually all organizations house large amounts of information on people and businesses. Cybersecurity losses can have serious, material effects on financial performance and personal security. Should this information be corrupted or stolen, those in charge potentially face loss of reputation and trust, financial reversals, fines and penalties and inability to focus on business, while recovery and remediation are underway.

There is No Status Quo. Today's firewall is tomorrow's soft spot. Cyber risks are inherently complex and changing. Attackers are stealthy, and their motives and tactics are in constant flux. Failure to recognize and address threats as they emerge or change escalates the impacts.

All eyes are on you. To mold organizational behavior into a cybersecurity culture, executives must attend security awareness training, practice safe computing and recognize that subordinates emulate their leaders.

This threat demands a wide-angle view. Often, only executives have a sufficiently broad view across an organization to ensure cross–boundary compliance. Leaders have a special responsibility to execute cyber policies based on their encompassing perspective.

Improvement requires attention. Items that executives keep at the top of the agenda receive staff attention. Cyber risk deserves the same attention executives give to financial and market risk. Asking about the status of cybersecurity—including requiring quarterly updates, annual dashboards and trend reporting—sustains a sense of urgency and leads to action.

Leaders ask critical questions. An effective executive can influence organizational behavior by asking:

- What are we doing to protect important data?
- How would we know if we had been breached?
- How quickly could we recover from a cyber attack?
- Are we leveraging our human and technical assets appropriately to protect our information?
- How complete is our understanding of current cyber threats?
- To what extent have we reduced our risks in the past year?
- To what extent have we reduced cyber incidents in the past year?

Literacy

Almost every major cyber intrusion, at home or work, starts when an individual unwittingly opens a door to attackers. Our strategy recognizes that we must both establish a minimum base of knowledge to identify and prevent cyber intrusions, and continue to build specialized skills to address the more complex cybersecurity tasks.

A literate, mindful citizenry and workforce create a strong cybersecurity culture.

To improve literacy:

- Training and educational programs should begin in grade school and build throughout one's life. Schools, libraries, employers and senior centers can all become hubs for the basics on fraudulent email and websites;
- All employees should have refresher and professional development training in cybersecurity;
- Workplace communications, professional development, accountability and training should emphasize that best practices, responsibility, security and risk mitigation are part of every function;
- Auditors should be trained to include cybersecurity as a priority focus; and
- Our educational systems should support the development of curricula for cybersecurity professionals and encourage post-secondary, advanced certifications in the field.

Preparation

This principle, like Response and Recovery, is based largely on the state's experience responding to emergencies—primarily natural disasters—through the State Response Framework.

Of course, a cyber incident differs from a natural disaster in that: 1) an attacker has intent to steal or harm, and 2) the technology environment changes every day. Still, preparation for cyber incidents, large or small, can benefit greatly from these known and understood structures.

Helpful, adaptable lessons learned include:

- Conduct regular risk assessments in accordance with industry standards. The State of Connecticut recently conducted an agency-by-agency self-assessment against Center for Internet Security (CIS) critical controls. There are also sector-specific tools for industrial control and financial systems.
- Use a credible information security framework from a source such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST) or the International Organization of Standardization (ISO) to create a proactive protection program.
- Include cyber risks and risk assessments in strategic and operational planning, including risk identification and assessment.
- Train constantly to hone literacy and technical skills, and to rehearse and modernize continuation of operations (COOP) and continuation of government (COG) plans. Well-planned training and exercises can enable local, state and federal partners to teach and mentor each other to enhance both situational awareness and their chances of avoiding or mitigating cyber threats.
- Share information with public and private entities via the State Cybersecurity Committee, through public service announcements and, when appropriate, with law enforcement and Connecticut's intelligence fusion center. Develop plans for use of a web portal and social media.
- Institute incident response plans aligned with the State Response Framework, following the National Incident Management System (NIMS). Planning should include continuity of operations and continuity of business plans. Rehearse on a stand-alone basis and with federal, state, local and private partners.
- Staff an incident response center and practice its use. The field of cyber defense and threat mitigation is in its initial stages. Connecticut needs to be part of the national discussion on how the federal government and states can collaborate to contain or eliminate harm from an active attack.
- Take advantage of mutual aid, if an incident warrants additional resources, via the Intra-State Mutual Aid Compact, state-to-state Emergency Management Assistance Compact or International Emergency Management Assistance Compact.

Response

Cyber events are virtually always complex because attackers will employ a variety of tactics and even change tactics during an attack. A common example is a denial-of-service attack that distracts from an actual system intrusion, until it is too late.

Response requires:

- Executing incident response plans;
- Activating a cyber disruption response team;
- Reporting to a sector-specific Information Analysis and Sharing Center (ISAC) for coordination and, when appropriate, to Connecticut's intelligence fusion center and/or the national level;
- Escalating authority and responsibility, when appropriate, to a multi-jurisdictional, multi-discipline response team following the State Response Framework;

- Providing situational awareness and subject matter expertise to the State Emergency Operation Center, if activated;
- Launching business continuity operations.

Recovery

Recovery operations must be as nimble as Response operations, because consequences of attacks are increasingly difficult to predict. The fallout could include financial, physical, reputation and/or other damage. Connecticut has a State Disaster Recovery Framework that provides a general recovery structure in the event of an incident affecting public safety. Cyber threats add new demands to that recovery structure.

Recovery requires:

- Identification of damage from the attack;
- Investigation and data collection;
- Root cause analysis;
- Eradication of the threat and restoration of operations;
- Creation and distribution of an after-action report that summarizes the event, lessons learned and follow-up remediation activities; and
- Follow-through to execute recommendations and mitigation actions.

Communication

Organizations and individuals do not enjoy equal access to threat intelligence about the extensive array of wily and pernicious cyber foes. That is why an important goal of this strategy, and the action plan to follow, is to foster coalitions and information-sharing behavior across Connecticut and with regional and federal colleagues.

Even recognizing the need, in some organizations, for discretion or secrecy, cybersecurity demands that organizations break down silos and embrace information-sharing habits. Vertical and horizontal information flows allow coordinated action and lead to better decisions about resource allocation within and among organizations.

In addition, formalized groups—such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), regional chambers of commerce or groups organized around common interests, such as insurance, finance, law enforcement and the Connecticut intelligence fusion center—enhance shared understanding of risk, response and recovery.

Leaders and their communications professionals should:

- Advocate common understanding of risks, threats, potential consequences, operating environments, goals and objectives;
- Use common terminology and measurements internally and with outside partners. Promote communication standards, such as TAXII (Trusted Automated eXchange of Indicator Information), STIX (Structured Threat Information eXpression) and CybOX (Cyber Observable eXpression) to automate situational awareness;
- Assure coordinated actions within and among organizations;
- Use the Connecticut Cybersecurity Committee for information exchange with judicial, legislative and executive branches of government, federal partners, state agencies, local governments and/or private sector leaders;

- Initiate or support industry and area-specific forums to foster regular dialogue and share policy templates and best practices. Recognize and support the role the non-profit Infragard plays as a communications nexus between the corporate world and the FBI in cyber matters;
- Support the use of social media and development of a cybersecurity website as a hub for Connecticut residents, businesses and public sector organizations to find information, report incidents and obtain access to resources.

In addition, in the event of a major incident, the importance of the media cannot be overstated. Crisis managers need to ensure that the media are able accurately and coherently to communicate the facts of a cyber crisis. National security officials warn that an attack by a nation state on state systems or critical infrastructure would most likely include disinformation, rumors and messages to instill panic and thwart order. The Governor must have considered, ahead of time, and perhaps already composed, messages to pre-empt "fake news" and/or reassure the public with instructions and updates. The media will be a critical ally and conduit in this effort.

Crisis communication plans must also include practical, technical considerations. Any intrusion that affects electricity will eventually disable devices that require recharging and backup. It used to be that if electricity went down, the landline system remained operational. No longer. Cable, broadband and other ways of sharing news are vulnerable to the disruption of electricity. Without the ability to recharge mobile phones and without secured management of generator fuel for cell towers, much of the population will need other ways to receive communications necessary for reassurance and potentially for survival.

Verification

Verification answers the question: Are our efforts actually working to lower cybersecurity risks?

Public and private entities must measure and report progress, or lack thereof, against each of this strategy's other six principles. Without this introspection and candor, it will be difficult to determine if efforts are making a difference for the organization and for Connecticut.

For those concerned about cybersecurity, questions to pose:

Executive Awareness and Leadership

- Do leaders (Governor, legislators, mayors, CEOs, et al.) receive regular briefings on threats, incidents, risks, mitigation and workforce needs?

- Are policies and actions being updated or amended based on such briefings?
- Are leaders using their bully pulpits to reinforce cybersecurity awareness and risk reduction?

Literacy

- How many public service announcements have focused on cybersecurity?
- What percentage of school districts and libraries teach safe computing?
- What percentage of businesses and employers include safe computing and security awareness in their orientation and refresher protocols?
- How many post-secondary cybersecurity class options are available in the state?

Preparation

- Is a recent security risk assessment in place, and has management reviewed it?
- Is a Cybersecurity Incident Response Plan in place, updated regularly and available to those who need access?
- Have there been at least 10 meetings of the Connecticut Cybersecurity Committee within the past 12 months?
- Has cybersecurity threat been part of Connecticut's annual, statewide emergency response exercise in the past two years?

Response

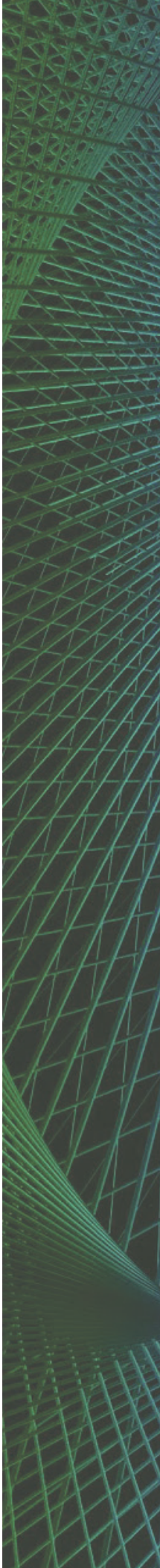
- Have all cybersecurity events been managed according to the Incident or Disruption Response Plans?
- Have all incidents been reported through the applicable ISAC, to law enforcement or to the Connecticut intelligence fusion center?
- Have changes been made to reflect lessons learned?

Recovery

- Are we experiencing similar cyber events repeatedly?
- Are all incidents scrutinized in after-action reports?
- Are all remediation steps followed to completion?

Communication

- Do all appropriate organizations, entities, disciplines and sectors have representatives participating in the monthly Connecticut Cybersecurity Committee meetings?
- Have inter-governmental and business cybersecurity forums been established, and are they ongoing?
- Have repositories for policy templates, best practices and tools been established, and who has accessed them?
- Are organizations sharing cybersecurity information using automated exchange standards?
- Are standardized terms used across documents and organizations, and are they boosting understanding and response?
- Has a website been established as an information hub, and does it provide accurate information and links to useful resources?



Connecticut Legislative Office Building

Sectors

A damaging cyber hit on any Connecticut office or business is unacceptable, and all of Connecticut needs to be proactive. While the points raised in each of the sections below can be extrapolated for other sectors, this plan highlights a select group of government and business entities because they occupy a special position relative to cybersecurity.

All are prime targets. An assault of sufficient magnitude on any of them potentially would have impacts that radiate beyond their walls, affecting most, if not all, Connecticut residents.

All are also prime defensive players. Each has essential resources and skills to help the state through a major cyber-induced emergency.

CONNECTICUT STATE GOVERNMENT

In the Crosshairs

Hackers actively attack Connecticut's state government daily.

Of the roughly 4.8 billion connection attempts per month to the state network from external computers, approximately 2 billion, or 42 percent, are blocked by perimeter security, based on known malicious Internet protocol addresses or threat signatures. The state receives close to 38 million emails per month, of which about 85 percent are blocked by the enterprise email gateway system. In a typical month, state anti-virus protection catches about 2,400 malware infections before they install.

Despite this protection, state third-party monitoring detects an average of 66 infected or compromised state systems per month.

As a target, the State of Connecticut, like all states, is a prize, because it is a trove of data that

can be exploited or sold. Due to its responsibilities for revenue collection, law enforcement, public health, including Medicare and Medicaid, among many other things, the state has information on virtually all 3.5 million residents and health records for about 1.2 million.

On The Right Track

Strategically, Connecticut has already taken positive steps by seeing cybersecurity for what it is—an existential threat—and for being proactive.

State government promotes cybersecurity defense in all executive branch offices and the five sectors addressed in this strategic plan. Oversight is consequential in the cyber arena, because the agencies with greater cyber awareness are those that are regulated by state or federal authority (or both). When Internal Revenue Service, Social Security Administration or state management and budget officials evaluate agencies, reveal weaknesses and explain how to improve, better outcomes result.

State initiatives have included:

- Operating the state intelligence fusion center, managed by the Department of Emergency Services and Public Protection;
- Operating as a clearinghouse for cybersecurity information sharing;
- Matching cybersecurity demands with training and personnel resources;
- Conducting network penetration tests, security assessments and cross-sector exercises;
- Negotiating contracts that balance the cyber-related risks and rewards of service providers;
- Monitoring for and responding to incidents;
- Designing active defenses and recommending statewide and agency-specific technologies, and issuing a strategy and action plan focused on public utility cybersecurity; and
- Collaborating with the National Governors Association.

In addition, the Connecticut Bureau of Enterprise Systems and Technology in the Department of Administrative Services (DAS/BEST) provides security standards for the executive branch and manages IT systems for the state. In 2016, DAS/BEST facilitated risk-assessments by each state agency, and plans to repeat them annually.

Each Connecticut agency is also responsible for its own awareness program and defense mechanisms, and for working with DAS/BEST on network perimeter safety and firewall management, employee access to unsafe websites, malicious email and antivirus measures and backups.

Enduring Responsibilities

The state must keep asking how every agency and authority can play a constructive role in cyber defense, just as they are obligated to act on fire hazards, fraud and drug problems.

Ways to improve:

- DAS/BEST must keep conducting assessments, and help, particularly smaller state agencies, to boost adoption of standardized technologies and security protocols, contracting standards and centralized approaches to multi-factor authentication for critical systems;

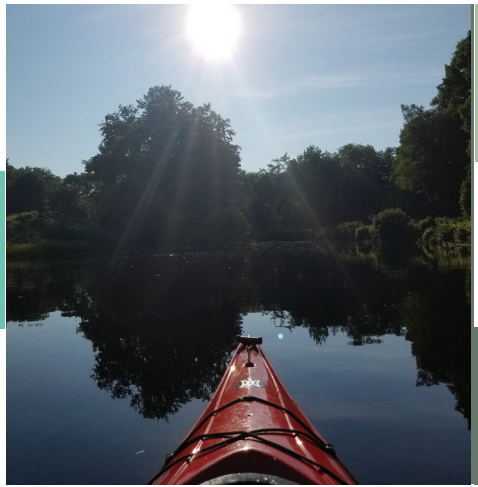
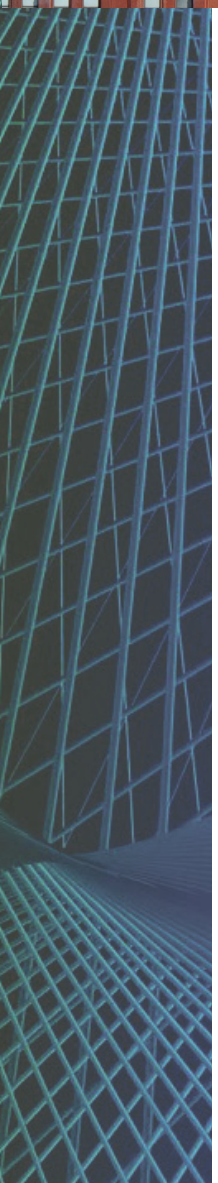


Photo by Kevin Nodwell

View of Hartford Photo by J. Carlos Velez



- The Office of Policy and Management must advance its work in classifying categories of data by risk level;
- The Department of Emergency Services and Public Protection (DESPP) Division of Emergency Management and Homeland Security (DEMHS) must continue to coordinate planning, training and exercises, and integrate cybersecurity issues in its work;
- Agencies, the General Assembly and Judiciary should cultivate cybersecurity cultures to underscore that cybersecurity is not simply an information technology problem. To ensure that it is part of every agency mission and job description, Human Resources must tailor recruitment to a workforce that lacks adequate cybersecurity skills, by seeking new hires with the talent and attitude to commit to cyber awareness amid resource scarcity;
- Agencies should examine critical systems requiring special protection and use centralized approaches to multi-factor authentication;
- State auditors should assess cyber culture in their evaluations;
- The Department of Consumer Protection, in managing citizen complaints, should direct people to investigation and prosecution authorities;
- The Attorney General, already active in cyber matters, should increase attention to potential damage to the state from cyber compromise;
- The State's Attorneys can increase their criminal awareness and prosecution activities, by working with a Connecticut cyber incident response team or task force to assist investigations;
- The state must encourage more municipalities to join, either directly or through trade association representation, Connecticut's Cybersecurity Committee, a venue for state and town representatives to discuss threats, priority concerns and best practices. Each of the five DEMHS Regional Emergency Planning Teams (REPTs) should have at least one representative on this committee;

- More municipalities should utilize the shared firewalls and other Internet protections available through the Connecticut Education Network (all school districts and roughly 100 municipalities currently participate); and
- Connecticut must take full advantage of federal, cyber-related grant opportunities available to state agencies and municipalities.

State and local officials must never stop working to improve preparedness by considering questions such as: What federal, regional and/or statewide coordination is required? What steps are necessary to maintain public order and distribution of vital supplies, such as food, pharmaceuticals and water? Have the media been included in crisis planning, since their credibility and ability to distribute news are essential to recovery?

Next steps for Connecticut state government will prioritize:

1. Working with agency heads to assess the current state of cybersecurity defense and law enforcement and identify gaps;
2. Offering the services of DAS/BEST to the General Assembly and Judiciary to assess the current state of cybersecurity defense and to identify gaps;
3. Helping smaller agencies lacking cybersecurity programs to identify basic needs, secure applications, manage contracting standards and pursue other initiatives to start building cybersecurity defense; and
4. Seeking federal grants to bolster Connecticut's efforts.

MUNICIPALITIES

Until recently, cybersecurity was not always recognized as a municipal issue or responsibility. It is not a common budget item in Connecticut cities and towns, nor is it a frequent agenda item at the Connecticut Conference of Municipalities.

Things are changing.

Some cities and towns now have information technology officers, and some retain IT vendors. A recent briefing on cybersecurity threats by the Connecticut Interlocal Risk Management Agency (CIRMA) raised alarm about the potential damage

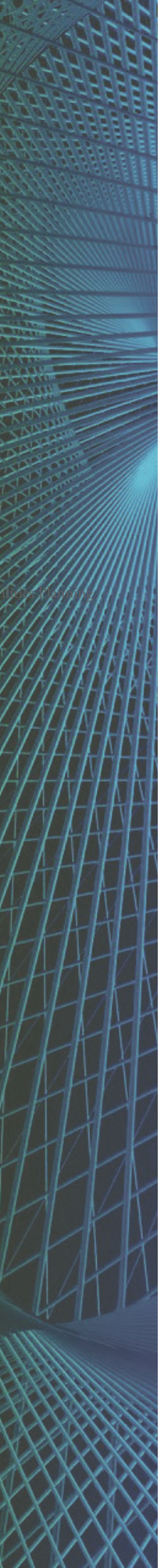
an intrusion could bring. CIRMA now provides cybersecurity insurance coverage for Connecticut municipalities.

In 2015, Governor Malloy signed legislation expanding protections for personal data. In the event of a breach involving residents' personal information, municipalities are subject to Connecticut's Data Breach Statute, Connecticut General Statute Section 36a-701b, requiring notice to both the affected residents and the Attorney General. In response, many municipalities have implemented written information security plans (WISPs), documenting the measures they are taking to protect the integrity of the information they collect and maintain.

Thus, Connecticut's municipalities are taking positive steps to identify, prevent and manage cyber threats, and they are motivated to build defense programs and join together to identify common vulnerabilities and best practices.

To build on this momentum, some initial strategic objectives for municipalities should be to:

- Increase civic awareness of cyber dangers to municipal government, citizens and local businesses; identify prevention measures; investigate compromises; and prosecute cyber crimes when possible;
- Join together to make defense a shared learning experience and reduce costs. Shared work with CIRMA and through the existing DEMHS Regional Emergency Planning Teams (REPTs) and their Emergency Support Function (ESF) groups provides a framework for communication and action plans;



- Embrace collaboration with DAS/BEST to strengthen network defenses; and
- Assess municipal work underway in other states and consider tapping other existing resources, such as the Connecticut Center for Advanced Technology.

Next steps for Connecticut's municipalities will prioritize:

1. Identifying steps each municipality can take to begin effective cybersecurity defense programs;
2. Investigating how best to use CIRMA as a resource and clearinghouse to share useful information and best practices, and participating in the Connecticut Cybersecurity Committee; and
3. Encouraging participation in the free services of the Multi-State Information Sharing and Analysis Center (MS-ISAC).

BUSINESS

Cybersecurity has emerged as a top business concern, receiving serious attention in business publications, at trade association meetings and through the difficult experience of cyber compromise.

Government and business share the responsibility to enhance the state's and the nation's cybersecurity defenses, and they depend on each other to do it well.

Thomas Bossert, Assistant to President Trump for Homeland Security and Counterterrorism, in March 2017, suggested a role for the federal government is to urge business leaders to "think through the cybersecurity challenge." The goal, he explained, is not to intrude on business operations, or "to ask businesses how secure they are, but rather to ask: how can we help you be more secure?"

By and large, Connecticut is in sync with this position. Our state government generally asserts that it should not and cannot regulate all the ways business responds to cybersecurity challenges.

That said, Connecticut General Statute Section 36a-701b, referred to above, includes the requirement that any business holding electronic personal information on Connecticut residents must report to the Attorney General and affected residents if the business experiences a security breach.

The state has also vested interests in maximizing the financial wellbeing of companies, the safety of their employees and the integrity of their products, and in giving Connecticut businesses a competitive edge. Therefore, it has a responsibility to engage the business community, and vice versa, about how to defend against disruption. In addition, should issues resistant to or not addressed by voluntary solutions emerge in the future, legislative or regulatory approaches have to be considered.

However, as is clear in the discussions below, it is encouraging that Connecticut's business community is taking the initiative to embrace cybersecurity.

For example, Infragard Connecticut, a partnership between the FBI and the private sector, is a non-profit organization that seeks to protect local, state and national infrastructure. Many Connecticut businesses, as well as academic institutions and state and local law enforcement agencies, have sought Infragard assistance to prevent and respond to exploitation of cyber vulnerabilities.

There are still chief executives, primarily in small and mid-market companies, who believe that cyber problems can be solved with software or by hiring a security vendor. However, they are fewer in number every day, and in the industries highlighted below, cybersecurity is clearly and appropriately top of mind.

Critical Infrastructure

Critical infrastructure includes a broad array of structures and services, beyond the public utilities addressed in this report. Effective cybersecurity defense compels attention to highways, rail networks, seaports, airports, dams and any other facility or service that affects lives, safety and economic activity in Connecticut.

Public utilities—electricity, natural gas, telecommunications and water supplies—are

highlighted here because their cybersecurity is more than a matter of health and wellbeing; it is a matter of survival and national security.

Utilities are susceptible not just to phishing and other "social" intrusions but also to penetration through their supervisory control and data acquisition (SCADA) systems, because SCADA systems can be reached through the Internet, supply chain devices and other vectors.

Because of the potentially profound consequences, even devastation, of an attack on public utilities, Connecticut issued a dedicated strategic plan for public utility cybersecurity in April 2014 and an action plan in April 2016. Both are available on the website for Connecticut's Public Utilities Regulatory Authority (PURA). Governor Malloy and members of the General Assembly requested the plan, reflecting their increasing desire to understand the state of public utility cybersecurity and how it could be improved. The time had passed when constituent questions regarding critical infrastructure cybersecurity could go without informed responses and assurances that designated officials were responsible for overseeing defense.

(See Appendix for a discussion of the impact and response a catastrophic utility attack could unleash.)

The public utility action plan called for "technical meetings" in which the electricity and natural gas utilities, major water companies and telecommunications companies would work outside the formal docket/regulatory framework to establish a process to review progress in cybersecurity defense.

Negotiating in the public interest, PURA and utility officials agreed on three basic points:

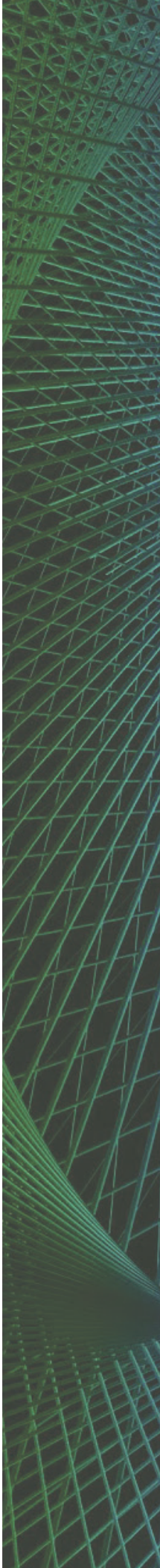
- Annual meetings would review the state of cybersecurity for each participating utility;
- Participating utilities would bring to these annual meetings whomever they wanted, internal or external to the company, and four State of Connecticut representatives would attend—two from PURA and two from the Division of Emergency Management and Homeland Security (DEMHS); and
- There would be mutually agreed standards to measure progress on cybersecurity defense. PURA asked the participating companies which standards they preferred, and all selected the Cybersecurity Capability Maturity Model (C2M2), a voluntary evaluation process using industry-accepted practices to measure the maturity of an organization's cybersecurity capabilities.

There were further "rules of the road" agreements regarding non-disclosure, protection of confidential information and concurrence on language used to report results to the Governor and General Assembly.

Both of Connecticut's electric and natural gas distribution companies (Eversource Energy and Avangrid) and its two main water companies (Aquarion Water Company of Connecticut and Connecticut Water Company) agreed to proceed. Major telecommunications companies refused to participate. Broadband and cable communications are vital to effective cybersecurity, and PURA has left the door open for these companies to join the process in the future.

The 2017 annual reviews started in February and were completed in April. A summary report by the state and utility participants will be forthcoming. The consensus assessment is that the reviews were very successful and that the decision to pursue a process designed by mutual agreement rather than formal docket decision produced an excellent model for future years. A spirit of responsible corporate citizenship, and a desire to respond to the public's need to understand the state of cybersecurity defense, have produced thorough, educational, professional reports and candid discussion of progress and areas where performance could be improved. Critical infrastructure in Connecticut is more secure, and regulators' and emergency managers' understanding of that security is materially advanced because of this new program.

Energy industry leaders have called for measures to close the gap between the need for cybersecurity threat intelligence and the scarcity of employees with top secret security clearances.



Connecticut's critical infrastructure public utilities have some access to threat intelligence, but need to rely on specialized vendors with access to such intelligence to try to fill information gaps.

During a U.S. Senate hearing in April 2017, a number of energy representatives stated that the U.S. Department of Energy should facilitate such clearances so that companies and government can share valuable information. Their plea was supported by Colonel Gent Welsh of the Washington State National Guard, who underscored the need for the National Guard to work with the private sector, saying that "there can be no partnership without access" to needed intelligence.

Financial Services

The financial services industry encompasses investment banking, asset management, pension fund management, large commercial and small community banks and credit unions, and businesses with significant financial components, including mortgage, property development and real estate firms. Other businesses, such as accounting and law firms, also deal with financial transactions.

While each firm faces its own cyber challenges, all must treat cybersecurity as a priority and ensure that public authorities are aware of major threats. The cyber threat is serious in financial services, as is the ardent desire to avoid publicity about it. The Privacy Rights Clearinghouse estimates that during 2016, for both financial services and insurance firms combined, there was a total of 1,009,897 data security breaches, of which 33 were made public.

There are understandable reasons for wanting to keep cyber breaches secret. Breaches with legal or regulatory implications can involve loss of records and damage to a brand name. An April 2017 study of 65 firms by IT consultant CGI and Oxford Economics found that, since 2013, share prices fell on average 1.8 percent on a permanent basis after a disclosed breach, with financial services companies being the most adversely affected.

Financial services businesses have the advantage of long-time experience protecting their processes, data and money. Before cybersecurity was a recognized problem, the industry was managing computer records and responding to problems with electronic information and systems caused by deliberate or accidental interruptions. In some ways, traditional financial crimes—skimming, over-invoicing and automated clearinghouse network fraud—have been adapted to the cyber world.

Financial services firms, in general, and especially banks, consistently underscore that they are already thoroughly regulated and do not want further regulation of any sort. Many emphasize that they are willing to cooperate in strengthening cybersecurity, but want to do so voluntarily rather than through new laws or regulations.

Progress

The past few years have seen some dramatic cultural changes in financial services firms to harden defense against phishing—one of the most widespread threats to the industry. Also known as "business email compromise" or BEC, this growing activity has triggered active CEO and board of director involvement, in-house "town hall" meetings, onboard training of new hires and regular training and testing for all employees.

Intelligence assistance is available from the FBI and for subscribing members of the Financial Services-Information Sharing and Analysis Center (FS-ISAC), a global resource for intelligence analysis. While the extent and quality of cybersecurity defense vary among banks, some have robust programs, including twice-yearly penetration tests (both physical and network) and "red teaming" (designating a group to attempt penetration and compromise). Some engage external security services to provide constant surveillance.

One interesting innovation that could be adapted to other banks is the Mid-Atlantic Automation Group, a coalition of about 12 mid-sized, non-competing banks, organized to share threat information and best practices, and to offer members alternate facilities capable of backup outside their operating areas.

More to Do

Beyond these promising steps, cybersecurity in financial services can be enhanced by:

- Adopting a shared communications plan to disseminate information and updates among financial institutions in the event of a cyber incident, possibly through a common website or defined protocol managed by the FS-ISAC;
- Creating a cyber incident response team in Connecticut that banks and their customers could use. At present, the only such service is the FBI, which is normally not able to respond to retail, individual compromises; and
- Expanding the availability of cybersecurity personnel, who are in intense demand; positions in Connecticut are going unfilled, forcing some banks to poach experts from competing institutions, which favors large players that can offer higher salaries.

The Regulatory Balancing Act

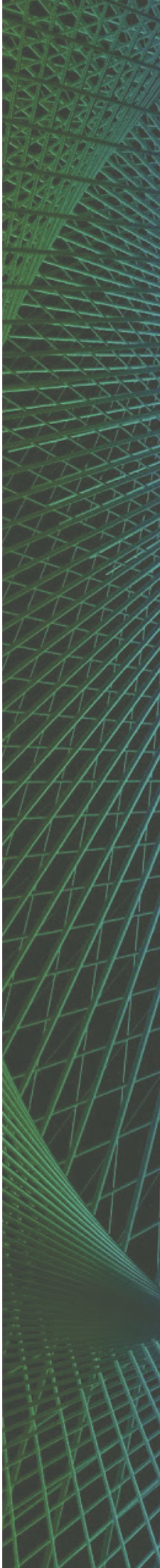
A question facing all states is whether, and to what extent, regulatory authorities should insert themselves into business affairs. A prominent example is New York State, which established first-in-the-nation regulations that took effect on March 1, 2017, requiring banks, insurance companies and other financial services regulated by the New York Department of Financial Services to institute:

- Governance controls requiring that a cybersecurity program be adequately funded and staffed, overseen by qualified management, and reported on regularly to the most senior governing body of an organization;
- Risk-based minimum standards for technology systems, including access controls, data protection and encryption, and penetration testing;
- Minimum standards to address cyber breaches, including an incident response plan, preservation of data to respond to such breaches and notice to the New York Department of Financial Services of material events; and
- Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certification of regulatory compliance.

Connecticut and other states, including Rhode Island, Illinois and Kansas, have passed broad but flexible statutes requiring entities that deal in personal information to institute reasonable security programs.

However, New York's regulations are more far-reaching creating new, cyber-related standards in financial services. While the efficacy of these regulations has yet to be determined, they may well prove to be appropriate in New York, which is the nation's (some would argue, the world's) foremost financial center.

However, Connecticut must pay attention. The effects of New York's regulations reach into Connecticut and affect our business community. Our institutions work with those in New York and face the same cyber threats. If financial cybersecurity risk rose to the point that it warranted special regulatory attention from the State of New York, Connecticut needs to consider the conditions under which it could make sense to take similar action.



Insurance

Not surprisingly, the insurance industry and the State Department of Insurance are active members of the Cyber Security Committee.

For itself and its clients, this industry faces a huge, dual challenge. Given that cyber breaches are among the most dangerous assaults on a company's value and reputation, insurance companies not only must protect their own data and security, but some in the property-casualty business are also responding to the growing demand for cybersecurity insurance coverage.

Travelers Insurance, Hartford

Protecting Themselves

Insurance companies differ in their views regarding the value of external security vendors. Some use them to supplement their own security programs. Others are so sensitive to the integrity of their data, they resist outsourcing. The larger insurance companies in Connecticut have designated senior-level cybersecurity officers; teams of support staff, on which at least one member has intelligence security clearance; and security programs that include trade association collaboration, such as with the FS-ISAC.

Given their avid attention to data security, insurers have paid great attention to the breaches that have beset government agencies and companies, such as the Office of Personnel Management, Sony and Target. Such reviews have resulted in risk assessments and heightened security measures.

Because the insurance industry is regulated, cybersecurity is an important facet of state oversight. There are several basic assessment mechanisms available, such as the International Organization for Standardization's (ISO) information security management process, which tracks security trends over time.

A common industry theme is a desire for cooperation with government regarding cybersecurity, but with as little publicity as possible—in other words, data protection with no public attention beyond that required by regulators or other legal requirements.

The insurance industry has, in fact, identified ways to expedite such collaboration:

- Some national organizations provide forums for information exchange regarding threats, defense and best practices. A few Connecticut insurers have expressed interest in the state helping to organize a forum of insurance company Chief Information Security Officers to exchange information about threat traffic, the evolving nature of penetration attempts and defensive best practices. Connecticut should be available to initiate such discussions if there is sufficient interest;
- This cybersecurity strategy and the push to establish Connecticut as a leader in this field—through business-to-business collaboration, government-business forums, drills and exercises—could provide a competitive benefit for insurers and all other businesses; and
- Insurance companies could step up the use of their macro-level, settled claims data to perform risk and trend assessments that determine, more precisely, how companies are breached, the most targeted industries and the kinds of data sought.

Underwriting Others

The business of providing cybersecurity insurance is in the early stages; it's a relatively new market. According to a February 2017 report from Deloitte, of the total $505 billion in all insurance premiums in the United States in 2015, cyber insurance premiums comprised less than $3 billion. The report also estimated that only 29 percent of businesses in the United States have cyber insurance.

There are several reasons for coverage being low for such a widely recognized risk. Defining the challenges, products and market segments

has not fully matured. There is lack of sufficient cybersecurity data regarding both expected frequency and severity of loss. The field also needs more attention to standard definitions of terms and hazards, which can hamper precise underwriting. And customers report that they are not receiving enough risk mitigation guidance. None of which is surprising in a new market.

There is ample precedent and experience in other areas of property-casualty coverage. The public hears admonitions not to drive while drinking or using smart phones. Medical doctors receive guidance from underwriters about how to avoid malpractice suits. The same goes for fire prevention and accidents in the home. Just as the industry has specialized experts in the range of commercial sectors, so too can it provide cybersecurity insights.

The bottom line is that insurers will surely emerge as critical cybersecurity underwriters and mentors. What better place to foster such growth than Connecticut? Underwriting cybersecurity insurance could be a growth area for our state, both in terms of business and jobs.

Defense

In reviewing exposure to potential cybersecurity threats in Connecticut, national security officials focused on three areas: critical infrastructure, financial services/insurance and defense. The defense industry must be part of the discussion for reasons that go beyond its size and employment level.

While most businesses are penetrated by invaders in search of valuable data, Connecticut's defense companies—such as General Dynamic's Electric Boat, United Technologies' Pratt and Whitney, Lockheed Martin's Sikorsky and their related and supplier companies—have the added attraction of manufacturing advanced weaponry and other defense hardware and systems. Nation states and non-state actors have long sought to steal information, plans, designs and other data related to the ships, aircraft and other products manufactured and overseen here in Connecticut, as well as potentially to corrupt or disable the information systems the defense industries use. Today, such actors use cyber penetration in addition to more traditional means of extraction.

Connecticut's defense companies face ongoing probes and penetration attempts from the full spectrum of attack vectors, including human compromise, technical intrusion and supply chain weakness. Cybersecurity, for them, is an immediate and dangerous threat.

Supply chain management is a particular concern. Defense companies rely on thousands of suppliers who have varying degrees of competence in cybersecurity. One company noted that there are many small, sole-source suppliers whose products are essential but whose cybersecurity protections are limited. Others point out that, given the industry's constant acquisitions and spin-offs, an inadequate level of cybersecurity can complicate or even doom acquisitions.

Forewarned is Forearmed

Yet another complication for this industry is that, due to its ties to national security, guarding secrets is integral to defense operations. That means sharing as little

information as possible externally, only voluntarily sharing information with colleague companies and establishing vigorous internal programs to limit communications. Defense companies also resist cybersecurity legislation and regulation, preferring to manage security on their own and receiving threat intelligence from the federal government.

Photo by By PA2 Sarah Foster-Snell - USCG

Despite this concern about secrecy, external collaboration and access to intelligence are critical to defense industry cybersecurity. The main vehicle for both is the Defense Industrial Base-Information Sharing and Analysis Exchange Organization (DIB-ISAO), created pursuant to the 2015 President's Executive Order 13961. It has about 70 members, including Connecticut's defense industry. Working with the FBI and Departments of Defense and Homeland Security, it encourages voluntary partnerships with government organizations so members can alert each other to threats, share mitigation and protection strategies, exchange actionable intelligence, consolidate analysis and develop tools to address emerging threats.

Defensive Role Model

Connecticut's defense companies recognize the value of state focus on cybersecurity and express willingness to help. A brief look at how those with a vital stake in cybersecurity protect themselves is instructive. Other U.S. companies are well advised, and likely, to move in their direction in coming years.

The effort starts with extensive employee training in threat awareness, phishing tactics, use of social media and the need for vigilant suspicion and verification. Defense companies combine information technology, employee communications and operations to enforce knowledge and habits, starting at employee onboarding. Efforts also include elements common in the military and intelligence community, including "need to know" enforcement (restricting information to personnel whose jobs specifically demand it), penetration testing, security exercises and careful vendor management.

Help Wanted

As in all other sectors, finding cybersecurity professionals in the defense sector is difficult because of a scarcity of talent. One corporate officer confirmed the challenges of dealing with the serious national shortage of cybersecurity professionals and noted that the United States does a bad job of training cybersecurity manpower. It is often necessary to recruit talent from other companies or hire infrastructure or network server specialists and train them to be security professionals.

Next steps for all Connecticut businesses will prioritize:

1. Supporting the newly-created, critical infrastructure annual assessment program involving electricity, natural gas and water utilities managed by the Public Utilities Regulatory Authority;
2. Promoting collegial discussions among financial services and insurance companies, using non-attribution procedures (Chatham House rules) to share information regarding threats, defenses and best practices;
3. Assessing the benefits of participation in the Financial Services Information Sharing and Analysis Center (FS-ISAC);
4. Sustaining communications with Connecticut's defense companies to be aware of any assistance the state can provide

and to request assistance from the defense industry as needed; and

5. Working with Connecticut business representatives to find solutions to the personnel shortage in cybersecurity, including, as explained below, increasing continuing education/certificate programs to renew and upgrade the skills of current cybersecurity professionals.

HIGHER EDUCATION

Education is key to creating an effective cybersecurity culture in the state, and the effort must start in kindergarten. Limiting the scope of this strategy to higher education is not meant to diminish the full range of educational activities the cyber challenge demands.

This strategy has repeatedly noted the need for cybersecurity experts throughout the public and private sectors. Higher education in Connecticut has the potential to support state efforts to strengthen cyber defense and to assist response and recovery.

Higher education takes cybersecurity seriously. Private and state institutions have security programs and pay attention to staff training, monthly security updates and designation of personnel responsible for checking inventories of confidential data and reviewing access to sensitive personal data. They also conduct risk assessments of common controls and perform analyses, including "heat maps" to identify and prioritize cyber risks. Larger institutions retain outside vendors to detect and deflect penetration attempts.

Significant Exposure

Despite these efforts, operations are incompletely protected. Higher Education in Connecticut has a tough row to hoe, given its extensive financial and medical data on employees and students, need to protect proprietary research, large number of personnel who use common systems, constant turnover of students and faculty and limited cybersecurity cultures.

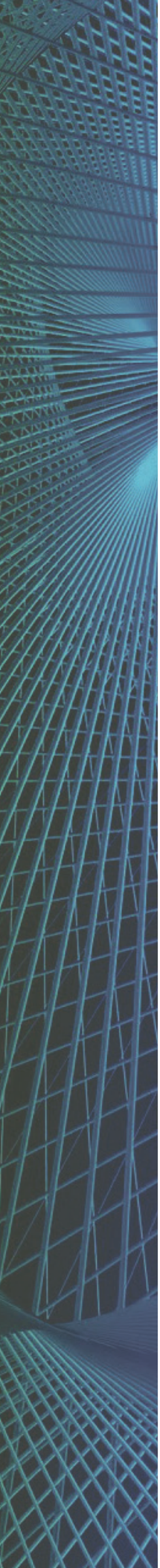
Academic culture, like the Internet itself, is designed for discovery and sharing. Thus, colleges and universities, particularly when it comes to students and faculty, may lack the level of cybersecurity urgency and awareness that one finds in the business community, especially in finance, defense and critical infrastructure. For this reason, Connecticut's cybersecurity strategy underscores the inherent vulnerability in higher education.

Penetrations continue, despite efforts to train rotating cadres of students and faculty regarding the damages of cyber compromise. Universities report that personnel are subject to the same tricks that endanger the non-academic world, and too often respond to phishing attacks with compromising behavior. There are warnings and notices regarding cybersecurity at state institutions, but security programs continue to fall short.

Nationally, the Privacy Rights Clearinghouse estimates that, during 2016, all educational institutions had 64,989 data breaches, of which 19 were made public.

Colleges and universities also cite the reality of budget pressures and the need for skilled personnel and vendors.

Southern Connecticut State University photo by Anthony Calabrese



Tightening Internal Discipline

Connecticut colleges and universities need regular exercises, agreed measurement standards, penetration testing and evaluation of new protection systems to boost their security efforts.

As in other public and private sectors, higher education would benefit greatly from cybersecurity collaboration. Academic institutions can help each other with both systems protection and recovery plans. There are ample grounds for academia to expand its relationships with business, government and civic organizations. For example, the University of Connecticut has announced partnerships with two corporations to pursue work in detection, prevention and analysis of cyber compromise.

Knowledge Transfer Opportunity

Strategically, it is in Connecticut's interest to capitalize on its relatively large number of higher education institutions to build its contributions to cybersecurity. As already discussed, there is a wide gap between the pool of qualified cyber professionals and open jobs.

In the United States, CyberSeek, part of the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology and the U.S. Department of Commerce, keeps a running estimate of cybersecurity jobs filled and unfilled. In March 2017, it reported 778,402 employed in cybersecurity in the United States, job openings for 348,975 and 4,153 unfilled positions in Connecticut.

The National Governors Association reported in 2017 that every state faces a cybersecurity workforce shortage. Some are trying innovative ideas to compete with higher-paying private sector jobs. Virginia offers two years of tuition for two years of state service, as an incentive to attract technical professionals to state service. In late 2015, Virginia estimated its cyber-related employment gap at 17,000; in February 2017 that number had ballooned to 36,000.

The federal government also faces the problem of not being able to hire enough cybersecurity professionals. One Congressional committee estimated that, in 2015, there were 209,000 federal cybersecurity jobs unfilled. One subcommittee chairman raised the idea of creating a "Cyber National Guard" that could "pull" workers from private business for short periods of time when their services were required at the federal level.

Non-academic entities look to colleges and universities for personnel and knowledge to help them build cyber defenses. Information technology professionals are always seeking to hone their skills and learn new ones through courses and seminars. Business leaders report that the availability of continuing education and efforts to bring cybersecurity professionals up to speed on current challenges are inadequate.

In their educational offerings, private universities, the University of Connecticut and the Connecticut State Colleges and Universities are starting to pay attention, especially to the theory and science of information technology. But there is no comprehensive effort to meet the growing demand for cybersecurity professionals.

At the University of Connecticut, about 150 freshmen enroll as majors in computer science; the degree offers a cybersecurity concentration.

Four Connecticut Community Colleges offer degrees or certificates in cybersecurity studies: Capital, Gateway, Naugatuck Valley and Norwalk. Manchester Community College offers training in information system security. Charter Oak State College offers a Bachelor degree and has a certificate program. Three Connecticut State Universities (Central, Southern and Western) offer Bachelor or Master of Science degrees in computer science with cybersecurity concentration. Adding all of these programs together, 13 students completed cybersecurity studies during 2015-2016 and 149 were enrolled in autumn 2016.

There are cybersecurity programs at private colleges and universities in Connecticut. Yet, combining currently enrolled students at UCONN and Connecticut's Community Colleges and State Universities plus Charter Oak State College, the total of enrolled students is about 300, less than one percent of the estimated 4,153 unfilled cybersecurity jobs in the state. Addressing this discrepancy needs to be a priority of our cybersecurity action plan.

Easier Said Than Done

The nature and pace of the cyber world pose difficulties for curriculum development. It takes up to a year or more for course material to be considered, organized, vetted and assembled into presentation form. With an associate's degree taking two years and a bachelor's degree four, cyber-related material introduced in the first year of instruction may be out of date by graduation.

Still, cybersecurity can have a greater presence in higher education as a concentration in other fields and as certificate programs for non-matriculated students. Certificate materials are not developed more quickly than normal curricula but can be more tightly focused. Either type of program would prepare graduates to be more immediately productive than graduates with general technical or professional degrees.

Training the Trainers

Higher education also faces a scarcity of educators in cybersecurity and questions regarding how to develop new ones. There are, at this writing, three nationwide searches underway for computer science faculty at the University of Connecticut. As other institutions create cybersecurity programs, the challenge will grow more acute.

Developing teachers of cybersecurity is difficult because:

- People with technical skills, who can prevent and diagnose cyber threats, prescribe response and recovery steps and exercise the seven principles discussed earlier, are scarce;
- Instruction needs to cover both pedagogy and the demands of the latest technology; and
- Credentialed cybersecurity professionals tend to find careers in business more attractive and lucrative than careers in academia.

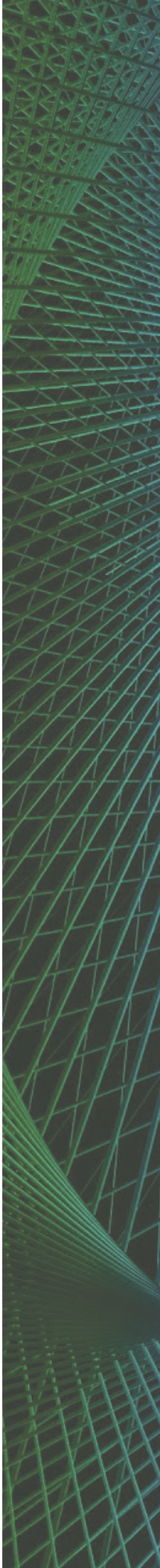
On this last issue, some academic leaders have proposed attracting professionals nearing or in retirement to join the academic world to train the next generation. Retired military personnel are also a good resource for such training.

Emergency Action

There is one other area—specifically related to response and recovery—in which higher education institutions can play a special role. Should there be a major cyber incident disabling critical infrastructure in Connecticut or a neighbor state, Connecticut needs to be ready to manage dislocation and out- and in-migration of populations. Colleges and universities manage large populations, with resources that cover workspace, housing, food, medical care and other essentials. At present, Connecticut has no plans to manage large numbers of migrants or dislocated residents. That challenge needs to be examined. Our higher education institutions can and must contribute to this important aspect of strategic contingency planning.

Next steps for higher education in Connecticut will prioritize:

1. Supporting collegial discussions among Connecticut's higher education institutions, using non-attribution procedures (Chatham House rules) to share information regarding threats, defenses and best practices;
2. Addressing the cybersecurity personal training gap in Connecticut.



LAW ENFORCEMENT AND SECURITY

Connecticut State Police

The Connecticut State Police (CSP) within the Department of Emergency Services and Public Protection (DESPP) has critical roles to play in helping the state respond to and recover from cyber intrusion.

CSP leadership is aware of the growing array of cybersecurity threats facing Connecticut and of the requirements to address them. It also recognizes that the time and attention of its force, totaling approximately 1030 troopers, must constantly address changing threat scenarios. While CSP has a unit focused on Internet issues related to child exploitation, it does not have a dedicated cybersecurity crimes unit addressing network intrusions.

The CSP has adapted with speed and skill to developments in areas such as organized crime, terrorism and drugs. Cybersecurity is one of the most critical new challenges it faces. A citizen reporting threatening individuals at a home or business, demanding money or private information, would trigger a police response. There are no comparable, assigned responsibilities for cyber threats.

Most cyber crimes do not have specific statutory definitions and are often grouped with charges that require a less complex response. An example is "data hostage taking" (ransomware). We need to consider policies and capacity to manage situations in which data is held hostage and ransoms are demanded from vital entities, such as hospitals. The action plan to follow this strategy should convene a study group to consider possible codification of cyber crimes.

CSP also needs to provide incoming recruits with a basic understanding of detection of cyber crimes and reporting requirements. A dedicated cyber crimes investigation unit, whose services would be available to assist municipal police, would considerably strengthen Connecticut's efforts. There should be a central cyber incident response team with the tools to investigate, collect evidence, share intelligence and assess whether further police action is required. The action plan should consider the appropriate size, structure, composition and management of such a unit.

Federal resources lack jurisdiction and personnel to address many state and local cyber crime challenges, and they face monetary thresholds

before investigating others. But developing cybersecurity skills in a dedicated CSP unit, similar to the Major Crimes Units, could leverage their effectiveness statewide.

An alternative approach would be for the CSP to lead the establishment of a task force, including municipal police chiefs and other participants, as has been done for organized crime, terrorism and drugs. Such task forces have been used effectively by the Connecticut Intelligence Center (CTIC).

In the event of a cyber attack on critical infrastructure, the CSP, and with local police, other first responders and the Division of Emergency Management and Homeland Security within DESPP, would be heavily involved in response and recovery. Its duties would cover maintaining law and order, responding to emergencies, protecting critical facilities and helping to manage out- and in-migration of people and vehicles.

While the CSP has plans for virtually all contingencies, a cyber attack could present new short- and long-term challenges, including acute public insecurity, prolonged absence of critical infrastructure and CSP personnel facing competing responsibilities for public duty and care of their own families. While none of these problems is new, cyber disruption could present management issues quite different from those of other emergencies. Examining and gaming the possible new scenarios would be instructive and prudent.

Intelligence

At all levels of law enforcement, a dimension of the cyber crime challenge is to establish intelligence capacities. Procedures for businesses, citizens and civic organizations to report cyber intrusions, and for protecting the confidentiality of such information, need to be part of our defense efforts.

Connecticut has a state fusion center, known as the Connecticut Intelligence Center (CTIC), which is part of the Department of Emergency Services and Public Protection. The fusion center is the only state facility collecting and analyzing cyber intelligence from Connecticut, federal sources and other states.

CTIC is an all-crimes fusion center focusing on intelligence related to such activities as organized crime, gang violence, human trafficking, drug trafficking and terrorism. In several states, including Connecticut, fusion centers have seen a dramatic increase in the volume of information about threats and actors in the cyber domain.

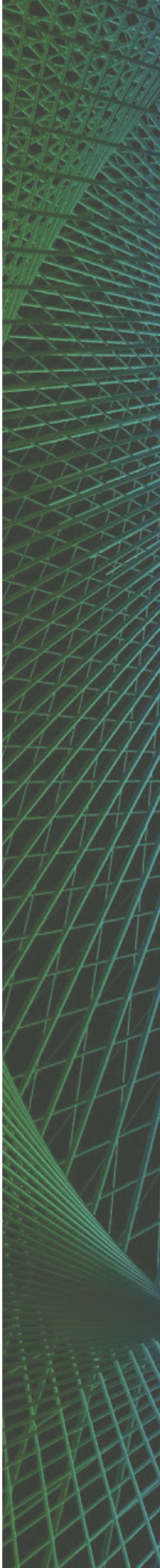
Today, when CTIC learns of a cyber crime or threat, it may refer that information to a federal agency, the CSP or a municipal police cyber crime unit. CTIC staff work with federal, state and local partners to maximize quite limited resources in order to perform intelligence and investigative duties related to cyber issues.

There are three challenges to enhancing the operational strength of the CTIC:

Staffing. Despite its reputation for helpful, professional work, the cyber function at the CTIC is sparsely staffed, relying on the services of several analysts, one of whom is a professional with cybersecurity expertise and other duties. That analyst holds federal security clearance and works with others in the CTIC and the CSP with federal security clearances, enabling the center to draw sensitive intelligence from national sources. The action plan to follow this strategy should consider the appropriate staffing requirement for current and projected volumes of work to receive, analyze and distribute cybersecurity intelligence to the CSP, municipal police or their federal partners (FBI, Secret Service, Department of Homeland Security).

Investigative Capacity. At present, intelligence findings are offered to federal, state and local authorities, yet often nothing happens because those who look into cybersecurity problems are not organized into a coordinated system with effective, consistent communication. A cyber incidence response team capable of taking intelligence and using it for appropriate police action would fill a major void.

Confidential Reporting. There is an understandable fear of embarrassment, reprisals and reputation damage if government



entities, businesses and citizens report cyber crime, and it becomes public knowledge. There are currently no standard instructions or suggestions for how individuals or organizations should deal with cyber intrusions. A properly staffed intelligence operation could receive and manage cyber threat information and warn others in similar situations to be aware of the threat, without divulging who had been compromised. Connecticut would also benefit from having an anonymous reporting system managed through a web portal, which could be tied to federal reporting as well.

An innovative New Jersey program, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), is worth exploring as a useful model. It is a one-stop shop for cybersecurity information sharing, threat analysis and incident reporting intended to promote shared, real-time awareness of cyber threat challenges for New Jersey residents, local governments, businesses and critical infrastructure. It offers small and medium-sized businesses an open door to bring cybersecurity problems to state law enforcement authorities. Reports are that the program is well received by the business community, and enables law enforcement to be aware of problems as they develop.

Municipal Police

Consistent with Connecticut's home rule form of municipal government, each city and town manages its own police function, with either municipal police or, in smaller towns, the State Police through the local barracks or Resident Trooper program. These forces are the front line in most citizen and business law enforcement interactions.

Cities and towns with their own police belong to the Connecticut Police Chief's Association (CPCA), but the CPCA has no cybersecurity strategy. Each police force addresses cybersecurity on its own, and normally contributes relevant information to the Connecticut Intelligence Center and other federal centers, such as the FBI and Secret Service, which share information with the law enforcement community.

Municipal police forces may offer advice about cybercrime prevention, but they are not equipped to prevent intrusions. Some aspects of cybercrime, such as ATM skimming and organized credit card theft, are treated as fraud cases.

Municipal police cite three familiar obstacles hindering their efforts to fight cyber crime and assist citizens:

Inadequate Authentication. Citizens too often use standard, easy-to-guess passwords, or they write down passwords and leave them unsecured. They also do not know how to recognize and defend against social engineering or information gathering via subterfuge.

Inadequate Resources. Police lack the skills, money and infrastructure to participate in resisting cyber crime, including data communication systems and software tools. Some police frankly admit that they are "outgunned" in fighting cyber crimes. When faced with ransom demands against their own operations, some have understandably negotiated settlements, rather than lose the ability to protect their citizens.

Inadequate Procedures. Unfortunately, many citizens do not call the authorities to report cyber crimes. When they do, local police forces often lack the type of guidelines and standard operating processes they have when dealing with other crimes. A publication or other guidance to all law enforcement regarding how to handle cyber problems would help to clarify procedures. It might also help to have a central website to report cyber crimes and threats.

Regarding their own response to and recovery from intrusions, municipal police are more focused on physical security and maintaining order than on the consequences of prolonged outages. Some smaller towns without IT staff have no plans for defense or recovery.

Each town also has its own emergency management capacity, distinct from the police department, and the strength of that capacity varies by town. It is common to find

emergency shelters and police, fire and emergency medical stations relying on redundant power sources, especially natural gas. There are normally no rules or regulations regarding emergency operations of private enterprises.

To strengthen police capabilities to be partners in cyber defense, strategic attention should focus on:

- Skills and training to respond to cyber crime and to help citizens defend themselves against intrusions;
- Codification of certain crimes into state law and strengthened ability to track and manage cyber crime;
- Infrastructure in the form of software and data communications;
- Capacity to determine attribution and bring charges, or to refer intrusions to those who can;
- Best practices, through CPCA or another organization; and
- Drills to rehearse responses to prolonged utility outages.

Connecticut National Guard

Internally, like all organizations, the Connecticut National Guard's (CNG) primary focus in the cyber domain is to protect its network and employ countermeasures if an attack or disruption occurs.

While in-state cyber capability is relatively small, utilization of the Emergency Management Assistance Compact gives the Guard access to cyber warrior capabilities from across the nation. It coordinates with the National Guard Bureau, Department of the Army, Department of the Air Force and United States Cyber Command.

The Guard also frequently participates in multi-service, multi-agency, regional and national cyber exercises; Cyber Yankee and Cyber Shield are two such recurring drills.

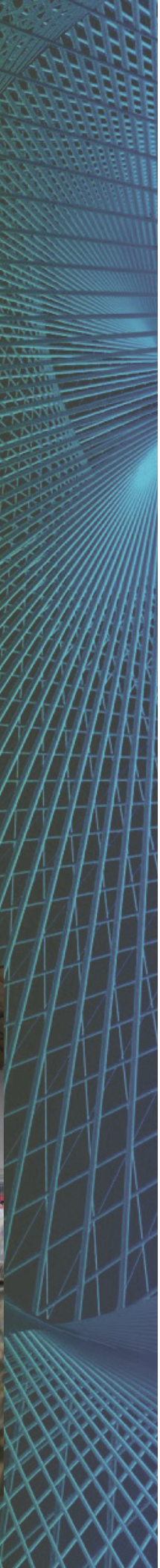
National Guard as Mutual Aid Partner

Externally, the Guard does not play a direct role in the detection and prevention of cyber intrusions. But in the event of a catastrophic disruption, it would be one of the most valuable players in the state's response and recovery.

If a critical infrastructure outage, for example, were to last beyond 10 days, with breakdowns associated with water, sewage, food, medicine, heat, shelter and/or law and order, the Governor could turn to the National Guard for a number of vital tasks. One of them is logistics, under the State Response Framework (SRF). The SRF includes a resource support/commodities distribution annex that outlines the state's plan to obtain and distribute commodities coordinated with state agencies and the National Guard.

Whenever an emergency exceeds the resources of municipalities, the state's Division of Emergency Management and Homeland Security manages requests for assistance, which can include the capable forces of the National Guard.

It has personnel dedicated to public service and prepared to go into harm's way. It has equipment able to respond, as well as the command structure and organizational discipline to sustain integrity, during crisis situations. It has access to intelligence, communications, public relations, transportation and reinforcements from other



states and the federal government. It has lists and plans of Connecticut's vital facilities—everything from hospitals and health care facilities to airports, trains and train stations, highways and bridges, ports and ferries and power generation facilities. And like municipal and state agencies, the Guard has "all hazard" responsibilities covering the sobering range of natural disasters, terrorism, chemical spills, radiological and nuclear attacks and pandemics.

All-Important Integration

It would be productive for the National Guard to hold exercises with state authorities on postulated cyber attacks, including prolonged power outages. The task facing the state is to articulate the demands the Guard could face, then to "game out" potential scenarios. Connecticut's strategy must include planning the National Guard role in the state's management of prolonged critical infrastructure outage.

The challenges of having National Guard units respond to a cyber attack are receiving national attention, because Congressional committees have expressed concern that neither federal agencies nor state emergency management agencies are adequately prepared to manage crises they have not experienced, and because the role is relatively new to Guard units.

In his April 2017 testimony to the U.S. Senate Energy and Natural Resources Committee, Colonel Gent Welsh, commander of Washington State National Guard's cyber unit, the 194th Wing of the Air National Guard, saw a need for the federal and state governments to plan for recovery from a cyber attack, rather than focus on prevention. Colonel Welsh emphasized that, while a cyber attack starts in the virtual world, it is likely to have physical impacts on pipelines, electric grids and other parts of critical infrastructure. His unit is working with Washington State on how to respond to such attacks.

Next steps for law enforcement and security in Connecticut will prioritize:

1. Strengthening Connecticut's cybersecurity intelligence gathering and analysis capacity and sharing this work with the Connecticut State Police and municipal police;
2. Creating a cyber incident response team with the ability to investigate, collect evidence and assess the need for police action, and to make its services available to municipal police; and
3. Working with the Connecticut National Guard, state and local police, emergency management and other first responders to rehearse scenarios of a cyber attack on Connecticut to enable the Guard to plan for all dimensions of such a crisis.

Conclusion

Cyber threats are a fact of life. Cybersecurity must be a universal priority for every public and private entity in the state. If Connecticut accepts cybersecurity as a mandatory, daily responsibility, it will realize measurable economic and quality-of-life gains.

The strategy's seven foundational principles—executive awareness and leadership, literacy, preparation, response, recovery, communication, verification—form a logical, progressive pathway to this vision of a cyber-secure, cyber-savvy state. They are adaptable to any individual or organization.

The next step is to engage each of the highlighted sectors in active dialogue, in order to follow this big-picture strategic plan with more operational action plans. Those plans will clarify the steps we need to take and the resources we will require to: protect our networks and critical infrastructure; implement information-sharing mechanisms that also respect privacy and secrecy; address the cybersecurity talent gap for our state and nation; support the efforts of our legal and law enforcement communities; and activate our citizenry to be life-long learners, when it comes to protecting themselves against cyber crime.

A basic question is whether Connecticut will press forward, continually creating and updating its protection and recovery measures, or wait until after a truly debilitating cyber event. In other words, do we have the will and vision, not only to regard cyber threats as a fact of life, but also to realize that committing energy and resources to cybersecurity must become a fact of life?

Given the severity and breadth of the cyber threats we face, Connecticut must proceed with its strategy and action plans, not because work to date has been inadequate, far from it. Our state's efforts have been important and impressive. Rather, we must act because cyber crime is a relentless foe, evolving virtually every day. We cannot run from this problem, wish it away or hope that someone else will solve it for us.

By facing our responsibility head-on, Connecticut can enrich its quality of life and economic competitiveness, and help lead the way for other states in our national cyber defense effort. True to our motto, Connecticut must adapt to sustain.

Appendix

A CYBER DEFENSE PRIMER

Small businesses express the need for information about how best to defend against cyber attack and what to do to recover. A "primer" with basic information and solutions might help them, and any organizations becoming aware of cyber threats, to learn from the experiences of others.

A business association might find it valuable to write such a primer for its members. State participation would also be helpful.

Here is a sample of the issues the primer might address:

- What basic perimeter defenses are necessary?
- Why should defense begin with a general risk assessment, and how is one conducted?
- What assets should a business protect?
- How does cybersecurity extend beyond the IT function?
- What is the role of corporate culture in cyber defense?
- Why is phishing the most basic threat to cyber integrity?
- What are "entry threat vectors"?
- Why are supply chains a potential vulnerability?
- Is cyber insurance necessary?
- What do we do if our business is hacked or we receive a ransom notice?
- How do we communicate with employees, customers, shareholders and the public after a compromise?
- What role do the police play in cyber crime?
- What legal protection does our business need, and are we obligated to disclose, based on state breach laws?
- How do we find the right vendor to provide defense?

THE CATASTROPHIC ATTACK

No cyber incident is out of the realm of possibility. For that reason, this section addresses the type of incident—a major attack on critical infrastructure—we have, fortunately, not yet experienced, and one that we dismiss at our peril.

Also of concern would be an attack timed to amplify the effects of a natural disaster, that is, a hurricane, tornado or extreme cold or heat spell.

Right from the start, a cyber attack alone or in conjunction with another emergency would be a challenge far different than anything the state has seen. Unlike a natural disaster, which has a defined end, a cyber attack could involve not knowing the extent of damage, when the attack is actually over and whether it might return.

Critical Infrastructure: The Achilles' Heel

Government and private experts have called our electric grid the glass jaw of American industry. In addition, national security officials note Connecticut's vulnerability to severance of natural gas transmission pipelines from the Pennsylvania/New Jersey area to Eastern New York and New England.

There are many ways to attack the grid and other utilities, from employee compromise through phishing and social engineering to take-over of operational controls, supply chain compromise and unsynchronized generators that cause kickback or an "aurora" effect that knocks out generation.

Cascading Consequences

Direct consequences could be a shutdown of roughly half of the electricity generation in New England and cessation of the ability to refine and transport gasoline, diesel and propane fuel. Indirect consequences could be depletion of reserves and liquefied natural gas and, over a few days, a shutdown of electric service, followed by depletion of gasoline, diesel and propane reserves.

Such an event would likely require authoritative communications to the public and potential declaration of emergency by the Governor, which could include an invocation of his or her powers to suspend statutes and take emergency actions to ensure public order, safety and health.

Transportation in and out of the region would become difficult; generators would cease to function; and ports would close. Remaining assets, including Connecticut's Millstone nuclear plant, producing 2,100 megawatts of electricity, and other generation facilities, such as fuel cells and renewable energy systems, would be pressed to provide electricity, but their combined capacity falls just short of 50 percent of the electricity generated in New England.

Other emergency management triggers, after about eight days of no electricity, could be lack of capacity to purify and deliver potable water and process sewage, resulting in forced dumping into waterways.

The result, from those who have examined such scenarios, would be attempted out-migration of possibly hundreds of thousands of people to reach safe areas with functioning utilities. Conversely, should an attack affect areas to the east, north or west of Connecticut, our state could be on the receiving end of these migrations.

There are other scenarios worth noting that would require response and recovery efforts beyond what Connecticut, indeed the United States, has previously managed. One study conducted by the Chinese military, subsequently declassified, concluded that a military engagement with the United States would be difficult for China to win. However, the study found, should parts of the United States be crippled by a critical infrastructure cyber attack, and should the U.S. military be forced to dedicate resources to response and recovery, China could prevail.

The point is, there are potential attackers, vulnerable places they could attack and many ways to amplify the effects of a cyber attack by combining it with other emergencies.

Prepare, Prepare, Prepare

We can never adopt the attitude that "it cannot happen here." Connecticut needs strategic plans to confront situations it has not experienced.

The following is a partial list of challenges we must address:

Communications. Given the unknown consequences of a cyber attack, the Governor and state and local leaders must anticipate scenarios and prepare communications ahead of time, with scripts pre-written that can be tailored to fit circumstances.

The Governor and Connecticut's emergency management team must ensure their ability to communicate securely, under stressed conditions, with: emergency management services; appropriate federal, regional and state authorities; local and private sector partners and national leadership, including the President.

Planning and preparation need to involve the media and use of social media. In times of crisis, people turn to trusted sources. Reporters and editors need to know, through planning and rehearsal, how authoritative news will be conveyed, and understand the vital role they would play in reporting the truth and correcting rumors.

It is possible that a cyber attack could include disinformation from a state or non-state actor. All the more important that official information be prepared and delivered credibly, directly by the state and through the media.

Emergency Management. In the event of a cyber attack, emergency management professionals and first responders would need to manage new levels of anxiety and panic. Municipal police, State Police, National Guard, the Federal Emergency Management Agency and other state and federal players need to plan for fear-driven behavior that could exacerbate the difficulties of emergency management. Public messaging would be a critical component of maintaining order. Partners such as United Way 2-1-1 would be especially important. Lack of food, medicine, fuel, electricity, potable water and the ability to communicate requires alternate planning to direct people to those services. In addition, it may be necessary to maintain public order and prevent harmful, desperate acts.

The December 2016 Liberty Eclipse Energy-Cyber Incident Exercise, sponsored by the United States Department of Energy, postulated a cyber incident affecting the energy infrastructure of the Northeast and Mid-Atlantic regions. Two of its key findings deserve special attention.

One is that, "The public will face a great deal of uncertainty following a significant cyber incident that causes physical damage (such as a long-term power outage or petroleum disruption), creating a considerable challenge for public information and expectation management, particularly around restoration times." Social media would be an important mechanism to reduce misinformation, provide response and recovery information and communicate measures to ensure safety.

The second is that, "While the consequent management activities for the physical impacts caused by a cyber incident are largely the same as they would be for any other hazard….the unique conditions of a cyber incident pose additional challenges that necessitate new capabilities and the use of new authorities."

Emergency Powers. Cyber aggression could present a dimension not present in storm management: the possibility of electricity outage beyond 10 days and the consequences described above. Storms have a natural end; cyber attacks do not.

There are extensive protocols for assigning emergency command and control authority, tapping emergency supplies, alleviating shortages from reserves and coordinating information and resources. But once the resources are depleted, the Governor's extraordinary powers may be the only option for relief and might come into play.

Early morning view of the Connecticut River photo by Kevin Nodwell

Section 28-9 of Connecticut General Statutes gives the Governor the authority to declare a state of emergency, which in turn gives the Governor extensive powers regarding vehicles and routes for evacuation for all or part of a stricken population, and states in part (b)(7):

> *The Governor may take such other steps as are reasonably necessary in the light of the emergency to protect the health, safety and welfare of the people of the state, to prevent or minimize loss of destruction of property and to minimize the effects of hostile action.*

Section 28-11 conveys the power to take possession of land, buildings, vehicles, fuel and provisions to protect the welfare of the state or its inhabitants.

Game plans. Clearly, Connecticut has civilian, police and military players and adequate special authority vested in its Governor to take extreme measures in case of prolonged damage to its critical infrastructure. Connecticut also has a detailed State Response Framework and State Disaster Framework that provides structure to response and recovery. However, it lacks a game plan for the various, possible needs discussed above involving prolonged outage of electricity, natural gas and the lack of potable water.

Connecticut must have an action plan to identify potential sources of emergency supplies and their allocation to allay the most vital public needs and assign roles to emergency responders. And various scenarios need to be rehearsed with all players, including private sector representatives and the media.