OFFICE OF LEGISLATIVE RESEARCH
Objective Research for Connecticut's Legislature

ResearchReport

Cyber Threats and Cybersecurity

By: George Miles, Legislative Analyst II

February 11, 2019 | 2019-R-0047

Issue

Provide (1) an overview of cyber threats; (2) a summary of Connecticut's cybersecurity strategies, action plans, and resources for public utilities, state government, businesses, and individuals; and (3) an overview of certain state cybersecurity laws.

Summary

Cyber threats are potential attempts to alter, disrupt, deceive, degrade, destroy, or gain unauthorized access to computer systems or networks or the information or programs contained in them. Cyber threats that successfully breach a computer network can steal system access or personal, financial, or commercial information. From viruses to malware, these threats are increasing in frequency, types, and sophistication.

The Department of Administrative Services (DAS) has grouped these threats into three broad categories: data breaches, disruptions of services, and failures to maintain information systems and networks. Internet users encounter the same types of cyber threats, whether personally or professionally, because they engage in similar online activities (e.g., sending and receiving emails, downloading webpage files, exchanging banking and credit card data, etc.).

Cybersecurity generally refers to the measures taken to protect against cyber threats. In 2014, the Public Utilities Regulatory Authority (PURA) produced a strategic plan to specifically address the cybersecurity of public utilities and then an action plan two years later. In 2016, then Governor Malloy created a state Chief Cyber Security Risk Officer position within DAS. Then in 2017, a multi-disciplinary team of representatives from state and local government, education, and private business produced a statewide cybersecurity strategy for Connecticut and followed up in 2018 with

a statewide action plan, which examined various challenges that different sectors faced, including the state government and businesses. Following the release of these action plans, PURA published annual cybersecurity reports for 2017 and 2018 and DAS recently issued a cybersecurity update at the start of this year.

The state maintains several cybersecurity-related websites, including the Connecticut Cybersecurity Resource Page, an Internet Fraud webpage from the Department of Consumer Protection, and a Cyber Security Awareness webpage from DAS. These provide resources to various groups, including tips for individuals to protect themselves from cyberattacks (e.g., using different passwords for important accounts, updating software, and being careful when choosing which websites to visit).

Beyond these strategies and resources, Connecticut has enacted several cybersecurity-related laws that, for example, require businesses to protect individuals' personal information and notify them of a data security breach.

Cyber Threats

Types

There are many different types of cyber threats that can produce a diverse range of effects. They take various forms with different methods of trying to gain unauthorized access. For example, "malware" are programs that can infiltrate a system and do a number of things such as generating pop-up messages, altering or deleting files, and taking control of a computer, while "spyware" can collect personal information without a user's knowledge or consent.

Categories

DAS has grouped cybersecurity challenges into the following broad categories:

1. data breaches, in which there is a loss of control over information stored on government or commercial systems, including credit card data, electronic medical records, Social Security numbers, or other personally identifiable information;

2. disruptions of business or government services that rely on information technology (IT) infrastructure (e.g., the unavailability of Twitter and PayPal for certain users in 2016); and

3. failures to maintain information systems and networks to minimize the occurrence and severity of cybersecurity incidents, including not training, employing, and managing a knowledgeable, qualified IT workforce.

PURA Cybersecurity Strategy and Action Plan

In 2014, PURA developed a cybersecurity strategic plan concerning the state's electricity, natural gas, and major water companies. Two years later, PURA produced a cybersecurity action plan containing standards, guidelines, and the creation of a Public Utility Company Cybersecurity Oversight Program to allow the utility companies the opportunity to demonstrate, through annual meetings with government stakeholders, that they are adequately defending against cyberattacks.

Under the oversight program, representatives of PURA, DAS, and the Division of Emergency Management and Homeland Security (DEMHS) hold voluntary annual cybersecurity review meetings with participating utility companies and discuss their (1) cyber defense programs, (2) cyber threat experiences over the prior year, and (3) anticipated corrective measures. For more information on the program, please see 2016-R-0274 and 2016-R-0267.

Statewide Cybersecurity Strategy and Action Plan

In 2016, then Governor Malloy convened a multi-disciplinary team of representatives from state and local government, education, and private business to produce a statewide cybersecurity strategy. Following the strategy, the team produced a statewide cybersecurity action plan to set specific steps to defend against and recover from potential cyberattacks. The strategy provides the foundational principles and the action plan applies them to different sectors, including state government and businesses. The principles are:

1. executive awareness and leadership, with leaders prioritizing cybersecurity in the same way they do such things as financial or market risk;
2. cyber literacy, with a strategy of citizens establishing a baseline knowledge to identify and prevent cyberattacks;
3. preparation, with regular risk assessments in accordance with industry standards;
4. response, with executing incident response plans and launching continuity operations;
5. recovery, with identifying damage from an attack and restoring operations;
6. communication, with fostering coalitions and information-sharing behavior; and
7. verification, with measuring and reporting progress.

State Government

The action plan lists many items that state government needs to protect, including its personal information data, public safety and support resources, elections, and the work of each agency. The plan argues that Connecticut should adopt a culture of cyber responsibility towards becoming a national cyber defense leader.

Executive Awareness and Leadership. The leaders of each branch of government (i.e., executive, legislative, and judicial) need to adopt an enhanced culture of cybersecurity awareness and defense. The plan believes each branch should annually assess its cybersecurity risk based on National Institute of Standards and Technology Cybersecurity Framework methodologies.

Cyber Literacy. All current and future state employees should receive education and refreshers in cybersecurity awareness based on their role and responsibility. Agencies should include in their risk reports descriptions of education programs, including the percentage of employees that attend trainings.

Preparation. Connecticut needs to take certain steps to prepare for a cyberattack or incident, including:

1. DEMHS completing a state cyber disruption response plan;

2. DAS encouraging and tracking agency and municipality participation in the Multi-State Information Sharing and Analysis Center; and

3. the state's Cybersecurity Working Group continuing to provide a forum for tribal, local, state, and private sector officials, and subject matter experts to communicate regarding emerging issues and proposed policies.

Response. All state agencies should complete and rehearse incident and disruption plans, document outcomes, resolutions, and recommended modifications to their plans for future use, and be prepared to execute them when required.

Recovery. Each state agency should (1) produce recovery plans; (2) rehearse recovery steps in annual exercises; (3) maintain, update, and review regularly a continuity of operation plan; and (4) draft and share an after-action report if an incident or disruption occurs, reflecting lessons learned to inform other parts of state government how the agency managed its disruption.

Communication. The plan suggests certain steps to provide effective communication, including preparing a standard briefing format for cyber incidents and disruptions along with creating and maintaining an easily accessed and readily understood cybersecurity public website.

Verification. Each state agency should provide a summary annual report on the status of their cybersecurity based on the seven principles. DAS and the Auditor of Public Accounts should incorporate cybersecurity improvements determined through existing audits into the annual agency reporting process.

Business

The plan notes that cyberattacks have public consequences, and as such every business should recognize its threat environment and have an effective cybersecurity program. The plan's goal is to accomplish as much as possible through active collaboration rather than formal processes or legislation.

Executive Awareness and Leadership. Business leaders should apply the plan's seven principles as best practices. Chambers of commerce can help create best practices, templates, and practical checklists, and make them widely available.

Cyber Literacy. Companies should be familiar with cybersecurity vocabulary and issues, and cyber defense should be a part of their cultures.

Preparation. Each company should inventory its data and assess its cybersecurity risk, and prepare a defense plan to deflect compromise attempts. Substantial resources, including InfraGard (a partnership between the FBI and businesses) and Sector-based Information Sharing and Analysis Centers (ISACS), exist to help businesses.

Response. Every company should have a plan to identify, assess, contain, communicate, and repair in the event of a cyber penetration. Companies should consider customer, government official, and third-party vendor interests.

Recovery. Businesses should prioritize recovery goals including protecting lives, limiting damage, communicating with affected parties, and restoring operations.

Communication. The plan notes that the Securities and Exchange Commission recently approved guidance to assist companies in disclosing cybersecurity risks and incidents.

Verification. Companies need to reflect and verify what they have is working as intended and consider external risk assessments and cyber risk insurance.

State Cybersecurity Law

Connecticut requires everyone, except the state and its political subdivisions, to safeguard data, computer files, and other documents in their possession containing personal information (e.g., driver's license or passport numbers), and destroy, erase, or make unreadable that data, computer files, and documents prior to disposal (CGS §§ 42-470 to 42-472d).

Another state law generally requires businesses in the state to (1) notify Connecticut residents of a data security breach within 90 days after discovering it and (2) offer at least two years of free identity theft prevention and mitigation services (CGS § 36a-701b). Following a data breach, consumers are encouraged to check or place a security freeze on their credit report. Under state law, credit rating agencies are prohibited from (1) charging a fee to place, remove, or temporarily lift a security freeze; and (2) requiring a consumer, as a condition of placing a freeze, to limit claims he or she may have against the agency (CGS §§ 36a-701 and -701a).

Several other laws require certain agencies, entities, or individuals to limit or restrict access to information they hold with varying degrees of specific technological considerations (e.g., CGS §§ 4e-70, 10-234aa to -234ff, and 38a-999b).

GM:kl