STATE OF CONNECTICUT

2018 Cybersecurity Update

Melody Currey, Commissioner
Mark Raymond, Chief Information Officer
Department of Administrative Services
January 1, 2019

Contents

Transmittal

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

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

Dear Governor & Distinguished Chairs;

The 2018 Connecticut Cybersecurity Action Plan proposed a series of activities to reduce cybersecurity risks for government, business, citizens and all stakeholders within the State of Connecticut. A fundamental finding of this Action Plan was the need for Executive Awareness and Leadership regarding cybersecurity threats. This report is the first in a regular series of updates to provide a view into the activities and status of state government activities in this field.

I extend special thanks to CIO, Mark Raymond, (DAS/BEST), David Geick, (DAS/BEST), Chief Cybersecurity Risk Officer, Arthur House (DAS) and state agency security and technical professionals for their efforts in developing this report for you and the Legislature. The coordinated effort of this group has led to the preparation of a substantive and comprehensive report. I am hopeful that in the months ahead the content of this document will be useful to the Administration and policymakers as they explore the issues surrounding cybersecurity preparedness.

Sincerely,

Melody Currey

Commissioner

Executive Summary

Connecticut has taken key steps to mitigate the basic cybersecurity vulnerabilities facing all states. We have raised awareness and understanding of the broad range of cyber threats facing the state, its government, businesses, organizations and individuals. We have a strategy and an action plan, we are executing annual reviews of critical infrastructure, we have both methodologies and metrics to use in strengthening defense, and we are revising our approaches to response and recovery.

Despite that work and progress, Connecticut, like all other states in our country, is vulnerable to cyber intrusion, breach and damage. We have seven principles to guide our action, but they are unevenly recognized and practiced. We have a "federated" system of cybersecurity management with varied levels of leadership and attention to strengths and weaknesses. For greater improvement, we must create a statewide culture of cybersecurity, widely recognized and seriously observed, with greatly enhanced action to promote the identified steps to enable greater security.

We need to review our federated cybersecurity management structure and commit to putting forth the discipline and effort to make it work, or we must optimize our limited technical resources in a more centrally accountable approach. Everyone in Connecticut is vulnerable to the effects of cyber disruption. Everyone needs to own the solution by changing behavior and erecting modern, effective barriers to cyber penetration. Connecticut has taken admirable, effective steps toward a more secure cyber environment. However, reaching the goal of adequate security will require making the goal a priority matter supported by continuous, dedicated and attentive work.

Introduction

The State of Connecticut Cybersecurity Action Plan advocated lowering cybersecurity risks in the state by building Executive Awareness and Leadership. This report is a product of that recommendation. While the Action Plan calls for quarterly reports, this initial report recognizes the burden on agencies of manually creating the report within existing resources and suggests an annual reporting cycle until additional automation and tools can streamline the process.

Background

The State of Connecticut has a measured program to reduce cybersecurity risks. Executive leadership and agency personnel are becoming more knowledgeable of the threats facing our state and the skills and tools required to protect our systems.

Connecticut first started to reduce cybersecurity risks by focusing on our critical utilities. A multi-agency team from the Connecticut Public Utilities Regulatory Authority (PURA), the Department of Administrative Services (DAS) and the Division of Emergency Management and Homeland Security (DEMHS) continue to perform according to the PURA 2016 action plan to strengthen defenses against cybersecurity challenges in the state's public utilities. The plan provides a process for PURA, DAS and DEMHS to review cybersecurity progress according to mutually agreed standards with electricity, natural gas and water companies. Annual reviews with participating utilities have been completed in 2017 and 2018.

In 2016, pursuant to Special Act 15-13, the Department of Administrative Services (DAS) conducted a study of cybersecurity issues facing Connecticut and recommended certain actions "to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness."

In July 2017, Governor Malloy announced a comprehensive vision for improving cybersecurity throughout Connecticut. This first of its kind document, the Connecticut Cybersecurity Strategy, presented seven principles for improvement and identified areas in the public and private sectors that occupy special significance based on their influence on the shared security of Connecticut residents.

While the Strategy set the direction for what needed to be done, further guidance was required to outline how the state would accomplish the strategy. In May 2018, Governor Malloy announced the release of the Connecticut Cybersecurity Action Plan. The Action Plan describes practical recommendations and actions to implement the cybersecurity strategy, including specific goals for Executive branch agencies.

Since that time, Connecticut has made significant progress. This report describes the continued and changing threats, our state's work to reduce risks from cybersecurity threats and recommendations for continued improvement.

Updated Threat Landscape

Since the submission of the 2016 Cybersecurity Study, public awareness of the cybersecurity threat has been heightened by ongoing reports of data breaches, social media data gathering, and state-sponsored efforts to influence U.S. elections. Massive data breaches at Facebook, Google and Marriott continue to erode public confidence that any data that they share will be able to be kept private.

The recent Department of Justice indictment of two Chinese nationals reinforce the concern that nation-state actors continue to be interested in US-based businesses and data. The 2017 Verizon Data Breach Investigations Report provided this summary for the public sector: "Almost one half of attacks resulting in confirmed data disclosure are state-affiliated. Timeline for breach to discovery is over 50% in the "years" category."[1]

At the national level, elections systems have been designated as "critical infrastructure"; an effort supported by the creation of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The risks identified in 2016 have persisted and the trend towards increased digital integration in private and public services has continued. Detailed descriptions of these risks can be found in the 2016 Cybersecurity Study.

In March, the City of Atlanta was hit with the SamSam ransomware attack. This attack disabled critical systems for weeks, resulted in the loss of law enforcement evidence data and cost millions in response and recovery efforts.

The Connecticut State government experienced a moderately sized incident in February 2018. A computer virus, introduced through a third party, quickly spread across a small number of vulnerable state computers. This infection partially disrupted state business as agencies moved to patch infected computers. The vast majority of state computers were patched and protected by anti-virus technology and were not affected. While minor in impact, this incident serves as a reminder to the threats we face.

Later in the year, a Connecticut municipality was struck with a ransomware attack that disabled critical systems. The city paid $2,000 to the cyber criminals to unlock the systems.

Actions Taken

This 2018 report updates the current state of cybersecurity readiness for Executive branch agencies, and recommendations for continued improvements in this area. Actions accomplished during this period include:

- **State Agency Security Controls Survey.** DAS/BEST conducted a survey in the fall of 2018 to assess state agencies' cybersecurity readiness and progress made compared to the results of the first survey in 2016. This survey assessed security controls defined by the Center for Internet Security (the CIS 20 Critical Security Controls).

[1] (Verizon, 2018)

Adherence to the CIS controls are the fundamental way agencies demonstrate progress in securing their environments. These controls also help more quickly to identify intrusions when they occur by documenting and contrasting intrusions with normal, expected behaviors.

- **Monthly Cybersecurity Committee Meetings.** The Department of Emergency Services and Public Protection (DESPP) and DAS/BEST have instituted monthly meetings between national, state and local governments and private sector security leaders to share current threats and best practices. These meetings have grown in attendance and have been critical in building more trusted relationships across disparate communities of interest.

- **Establishment of State Police Computer Crimes Unit.** DESPP established a dedicated Computer Crimes Unit, fulfilling a recommendation called out in the Connecticut Cybersecurity Strategy and the Connecticut Cybersecurity Action Plan. This unit handles cybersecurity related crimes and is a resource for local law enforcement when activities escalate beyond local abilities.

- **Completion of the Cyber Disruption Response Plan.** A Cybersecurity Disruption Response Plan identifies the actions to be taken if a large-scale cybersecurity attack were to substantially disrupt activities in the State of Connecticut. This plan works in conjunction with the State Response Framework for handling emergency events of any nature.

- **Completion of the Cyber Incident Response Plan.** An Incident Response Plan identifies the actions to be taken if an organization experiences an incident worthy of note but short of designation as a cyber disruption. This plan was updated and published as a template for state agencies and local governments to develop their own local incident response plans.

- **State Agency Cybersecurity Leadership Discussions.** DAS/BEST held a series of cybersecurity readiness and awareness discussions with state agency commissioners and senior leaders in support of fulfilling the recommendation called out in the Cybersecurity Action Plan. These discussions covered intrusion and malware alert summaries, security awareness training completion statistics, email phishing training campaign statistics, and visualization of internet traffic to agency websites showing location, volume, and blocked traffic.

- **CT Secretary of the State joined Elections Infrastructure - ISAC as Critical Infrastructure –** The US Department of Homeland Security designated elections as “Critical Infrastructure” and established an Information Sharing and Analysis Center (ISAC) dedicated to the Elections area. The Connecticut Secretary of the State joined

the Elections Infrastructure ISAC in advance of the 2018 elections. Teams from the US DHS, SOTS and DAS/BEST monitored elections technology throughout the general elections and reported anomalies to the EI-ISAC. No breaches of state election systems were uncovered.

- **Cross-Sector Outreach.** DAS/BEST has actively engaged in outreach efforts within Connecticut, in the New England region, nationally and internationally. The goal of these outreach efforts are to improve cybersecurity through practical applications of actions both here in Connecticut and across the globe.

  In Connecticut, we have discussed cybersecurity threats and Connecticut's strategy and action plans with the Connecticut Business and Industry Association and several of the regional and metropolitan chambers of commerce, trade associations, professional associations, organizations representing corporate board members, programs sponsored by law firms, university and community college classes and seminars and groups of municipalities. There have also been many presentations to private businesses and community and civic organizations. We have made presentations to meetings of the Connecticut National Guard.

  Regional work has included participation in sessions sponsored by the New England Conference of Public Utility Commissioners and annual National Guard "Cyber Yankee" exercises. Some of the New England states have used Connecticut's Cybersecurity Strategy and Action Plan in launching their own cyber programs, and we have collaborated in such work.

  Nationally, Connecticut has supported several cybersecurity discussions. Among them have been financial summits in New York and meetings of the National Governors Association in Colorado, Virginia and Washington, D.C. Connecticut has consulted with the National Cyber Command in Washington, D.C., met with agencies in the U.S. Intelligence Community and worked with the Department of Homeland Security and the Department of Energy. In late 2018 Connecticut authored an op-ed regarding cybersecurity policy in The Washington Post.

  The United States State Department/Agency for International Development (AID) has a program to assist friendly countries to create cybersecurity strategies and action plans. Working with AID and the National Association of Regulatory Utility Commissioners (NARUC), Connecticut has supported programs in Vietnam, in the Black Sea Region (Ukraine, Armenia, Georgia and Moldova) and with the Balkan region countries. Work has also included meetings in Estonia and Latvia. In addition, Connecticut has reported on its strategic plan and action plan at a joint meeting of the American and French cybersecurity officials sponsored by the French-American Foundation.

Connecticut Executive Branch Metrics

Security Controls

Center for Internet Security Critical Security Controls

The Center for Internet Security (CIS) established twenty critical cybersecurity areas and published an assessment tool that details these controls and their implementation, including policy, automation, and reporting of each element. The first five[2] controls are considered basic, and analysis of breaches and other cybersecurity incidents have shown that proper implementation of these five basic controls would have prevented up to 70% of these incidents. The first five controls are:

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software

Assessment Methodology

In October 2018, the Department of Administrative Services/Bureau of Enterprise Systems & Technology (DAS/BEST) provided each Executive branch state agency with an assessment tool developed by the Center for Internet Security. Each agency performed a self-assessment using this tool to determine a rating for each security control. DAS/BEST collected these self-assessments and compiled them to determine statewide ratings. DAS/BEST then compared the 2018 results to the results from a similar statewide agency self-assessment using the same CIS Critical Security Control that was performed in August 2016. Additional information on the reporting methodology can be found in the Appendix.

2018 Agency Self-Assessment Survey Results

The focus for the Cybersecurity Action Plan is on the "Implemented" category of this survey for the first five Critical Security Controls. The results showed an average for the first five Critical Security Controls as follows:

- Control #1 (Hardware Asset Control) averaged 43% implemented, ranging from a low of 6% to a high of 96%
- Control #2 (Software Asset Control) averaged 34% implemented, ranging from a low of 5% to a high of 83%
- Control #3 (Vulnerability Management) averaged 37% implemented, ranging from a low of 0% to a high of 82%
- Control #4 (Controlled Administrative Privileges) averaged 32% implemented, ranging from a low of 0% to a high of 100%

[2] Note: In version 7 of the CIS Controls, a 6th control of "Maintenance, Monitoring and Analysis of Audit Logs" was added to the "Basic" category. This will be reported in the next version of the report.

- Control #5 (Secure Configurations) averaged 34% implemented, ranging from a low of 0% to a high of 100%

The data demonstrate that there is a wide variation in agencies use of security controls. Some agencies are bordering on fully compliant and others will need great assistance in tools and skills to become compliant in the most basic security controls.

The average, based solely on the "Implemented" status reported by each agency, along with the range of responses (highest to lowest), are shown in the plot below. This graph shows the averaged responses for all twenty Critical Security Controls.

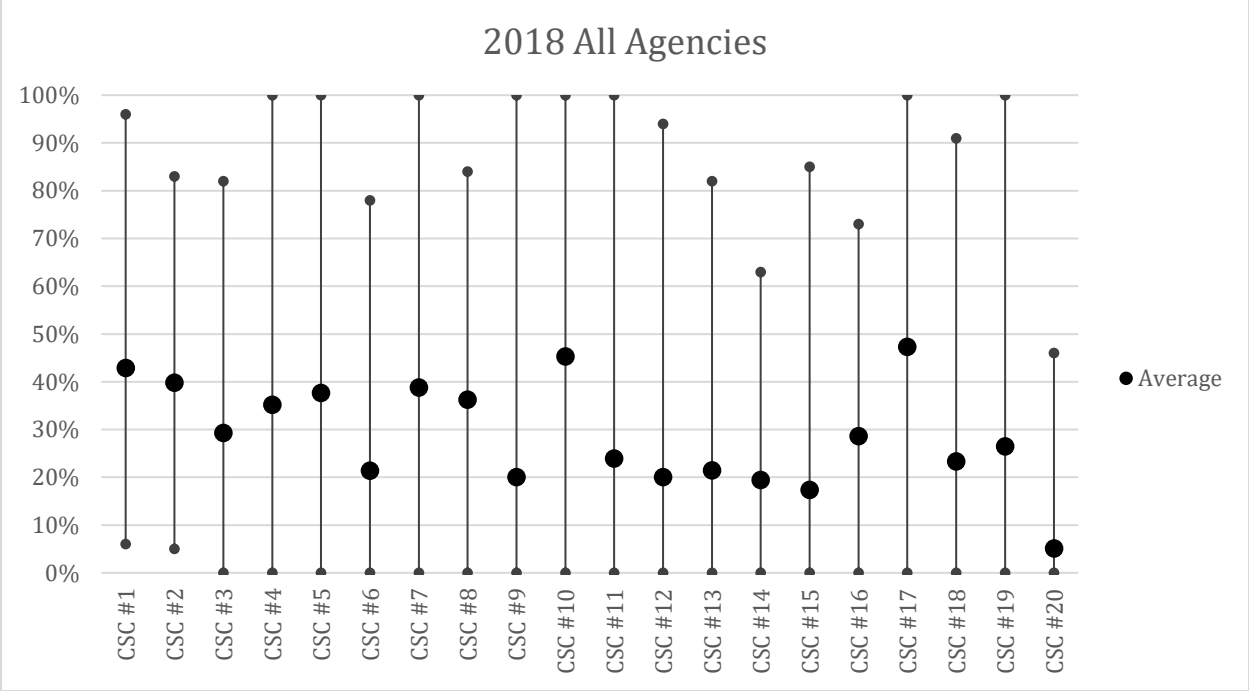

Figure 1 2018 Critical Controls - All Agencies

2016 Self-Assessment Survey Results

The 2016 survey result averages, with high and low ranges, for all 20 Critical Security Controls are shown on the plot below:

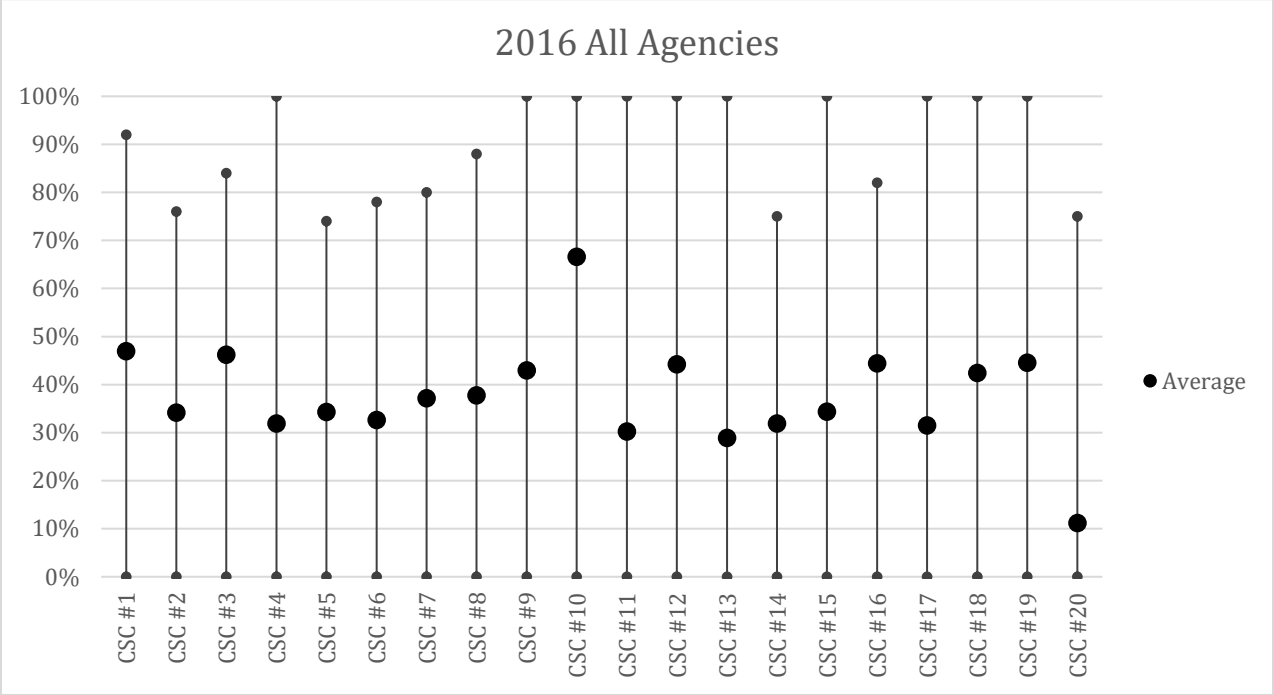

Figure 2 2016 Critical Security Controls

Comparing 2018 results to the 2016 survey results shows slight improvements in controls #2, #4, and #5, with slightly lower results for controls #1 and #3. These variations are most probably due to the changes in the reporting process and manual collection of the data.

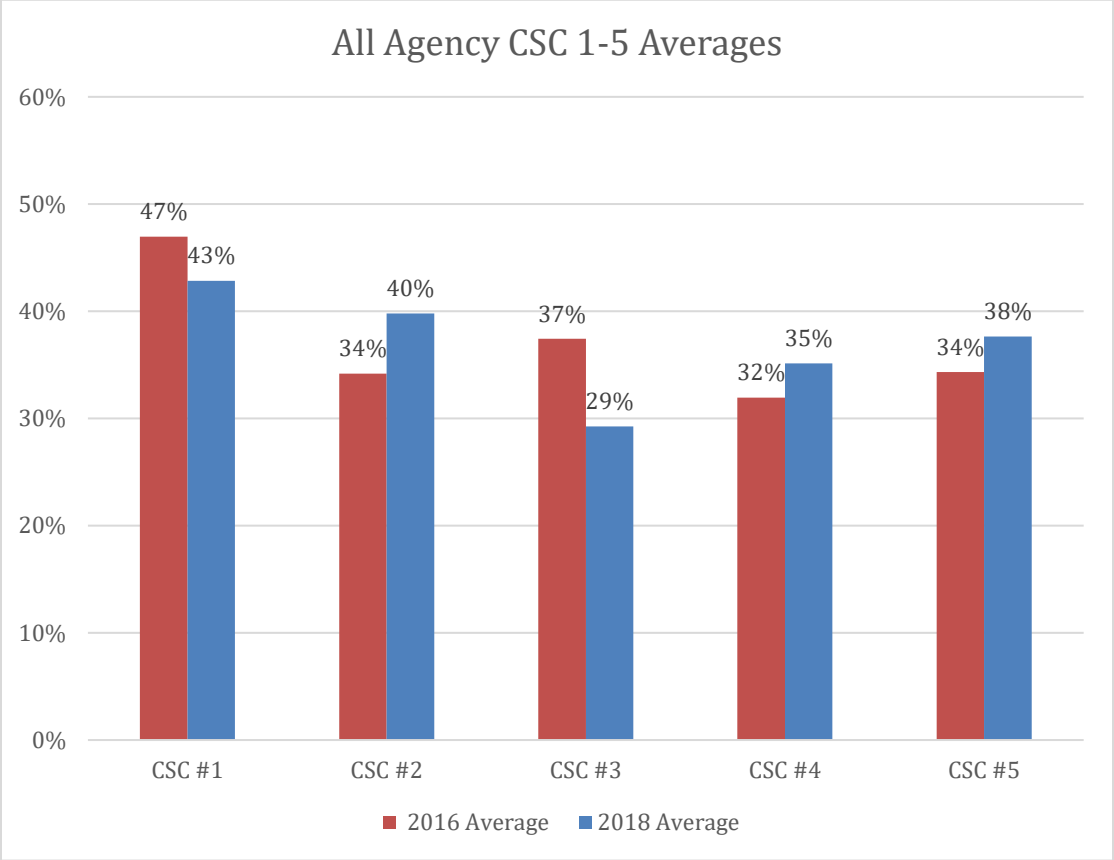

Figure 3 2016-2018 Critical Controls Comparison

State agencies have not made significant gains during the last two years in moving towards a more secure posture. There is room for greater effort to realize continued progress.

There was a substantial period of time between the collection of the 2016 data and an effort to focus on improving the outcomes with agencies. Central cybersecurity resources were working on centralized compliance and the creation of the Strategy, Action Plan, Incident Response Plan, and Disruption Response Plan. This diversity of effort may also explain some lack of progress in these metrics.

Additional Cybersecurity Statistics

Security Awareness Training (57% complete) – DAS provides periodic online training of state employees on the basics of security awareness. These short training exercises are delivered bi-monthly to continuously reinforce the topic. For 2018, 57% of employees are current on their training.

Connection Attempts Blocked (89%) – The State of Connecticut is a very active internet property with significant interest both nationally and internationally. Over a two month period in 2018, there were 2.1 billion connection attempts to the state network. Just over 400 million (19%) were allowed to pass the network boundary as legitimate traffic. The next three graphics show traffic being blocked, traffic attempting to access the network, and, the originating countries of the traffic allowed.

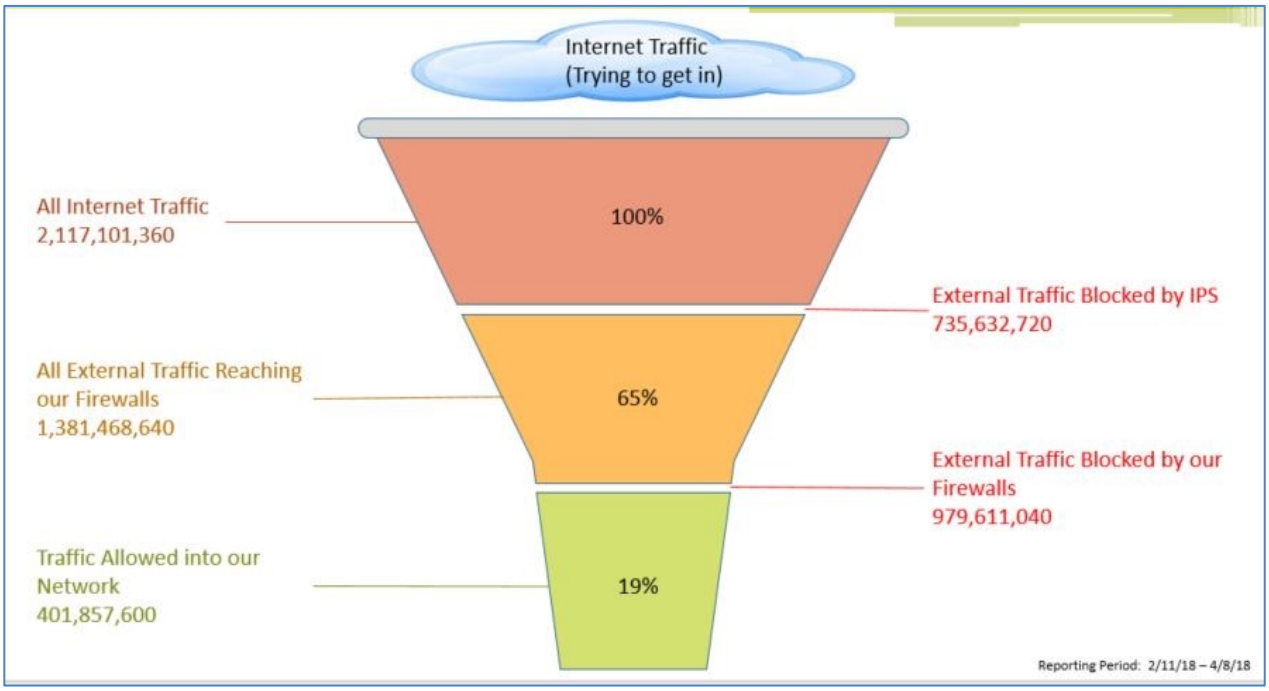

Figure 4 Internet traffic blocked by state enterprise boundary system

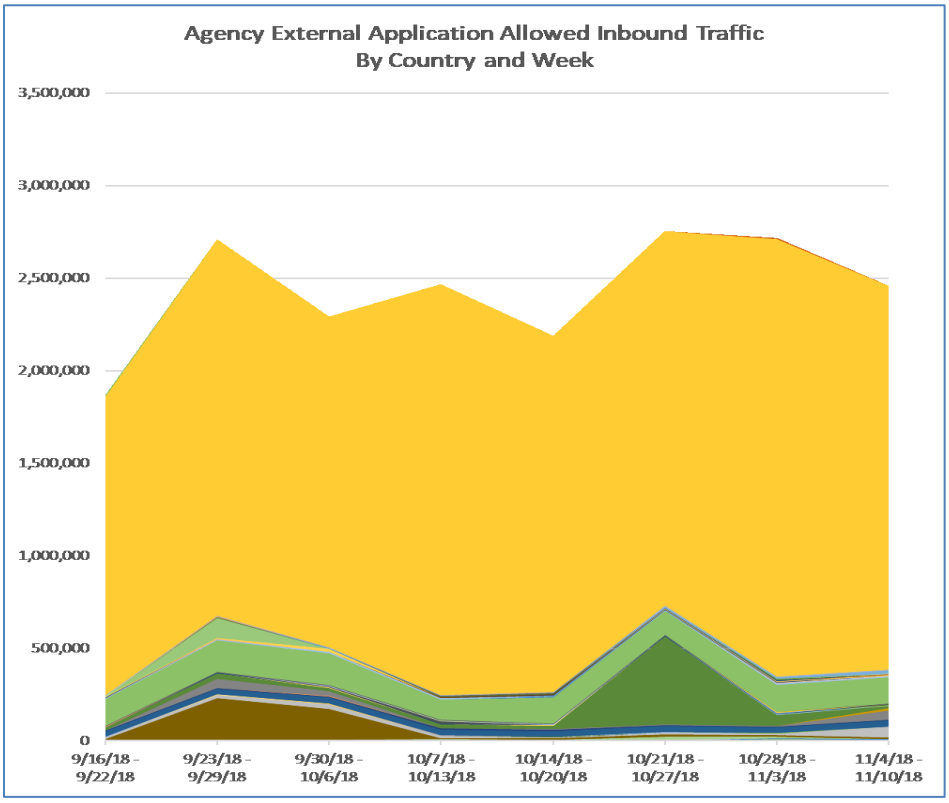

Figure 5 Internet Traffic allowed by Country (including US)

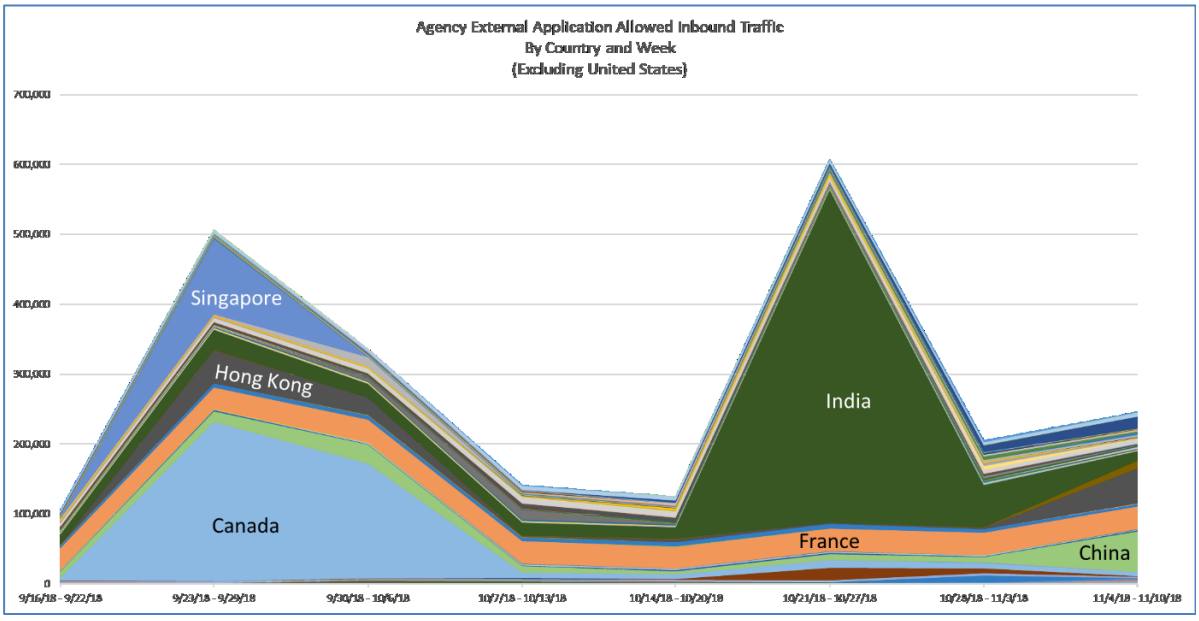

Figure 6 Inbound Traffic Allowed from Sources outside US

Denial of Service Attacks Blocked (>500) – The State of Connecticut, through the Connecticut Education Network, protects state agencies, public schools and most municipalities from Distributed Denial of Service (DDoS) attacks. A DDoS attacker attempts to make systems inaccessible by flooding the systems with more network traffic than they can handle. In 2018, CEN blocked over 500 attempts to disable school, town and state agency technology.

Recommendations

DAS/BEST should administer this same survey on an annual basis, each October, to track progress across Executive branch agencies in reaching the goal of full implementation of the Critical Security Controls. Agencies should use the 2018 self-assessment survey results to focus improvement efforts on their respective priorities.

Agencies have requested support from DAS/BEST in improving cybersecurity. A program of targeted improvements requiring additional funding has been defined and proposed in the DAS budget request. It calls for investments in:

- Identity and Access Management for state employees and citizen services
- Increased use of multi-factor authentication to reduce misuse of credentials
- Increased off-hours security monitoring and incident response
- Enterprise solutions for administrative credential management
- Enterprise solutions for software and hardware management
- Incremental technical assistance to identify and remediate specific vulnerabilities in processing, automation and policy.

Additionally, agency leadership must make security remediation a higher priority within their respective organizations. There is little reason why the state should have any less than 100% compliance with security awareness training.

Appendix A - Resources

Resource	Link
2016 Cybersecurity Report	https://portal.ct.gov/-/media/DAS/Communications/Communications-List-Docs/Special-Reports/2017-DASCybersecurityReport-SA-15-13.pdf
2017 Cybersecurity Strategy	https://portal.ct.gov/-/media/Office-of-the-Governor/Connecticut-Cybersecurity-Resource-Page/Connecticut-Cyber-Security-Strategy.pdf?la=en
2018 Cybersecurity Action Plan	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en
Cyber Disruption Response Plan	https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en
Cyber Incident Response Plan	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Incident-Response-Plan-template.doc?la=en
CT Cyber Library	https://portal.ct.gov/Connecticut-Cybersecurity-Resource-Page
CIS Critical Controls	https://www.cisecurity.org/controls/
2014 Public Utilities Cybersecurity Strategy	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Cybersecurity-and-Connecticuts-Public-Utilities.pdf?la=en
2016 Public Utilities Cybersecurity Action Plan	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Connecticut-Public-Utilities-Cybersecurity-Action-Plan-April-6-2016.pdf?la=en
2017 Public Utilities Annual Report	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/2017-Connecticut-Critical-Infrastructure-Cybersecurity-Annual-Report.pdf?la=en
2018 Public Utilities Annual Report	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/2018-Connecticut-Critical-Infrastructure-Cybersecurity-Annual-Report.pdf?la=en

Appendix B - Agency Assessment Methodology

The 2018 assessment tool uses a series of questions in each Critical Control area that are rated for the following areas (possible answers in parentheses):

- Policy Defined (No Policy, Informal Policy, Partial Written Policy, Written Policy, Approved Written Policy, External Responsibility)
- Control Implements (Not Implemented, Parts of Policy Implemented, Implemented on Some Systems, Implemented on Most Systems, Implemented on All Systems, External Responsibility)
- Control Automated or Technically Enforced (No Policy, Informal Policy, Partial Written Policy, Written Policy, Approved Written Policy, External Responsibility)
- Control Reported to Business (No Policy, Informal Policy, Partial Written Policy, Written Policy, Approved Written Policy, External Responsibility)

The "External Responsibility" option allowed agencies to identify functions that are not performed by agency employees, consultants or vendors. While this option indicates where other organizations outside the agency (central IT, cloud, etc.) may have delivery responsibility for a particular element of a control, primary responsibility for each control remains with the agency.

The 2018 survey converts the answers to an implemented percentage for each control, which is the metric that was used for comparison. It also provides separate breakouts for Policies, Implemented, Automated, and Reporting for each Critical Control. The 2016 survey used a different tool, which allowed agencies to respond that a specific control element was either Not Implemented, Partially Implemented, Implemented, or Not Applicable. DAS/BEST recompiled the 2016 answers for each agency to allow comparison of both sets of data using the 2018 framework.