IoE Capabilities Help Delaware Deliver Award-Winning Cybersecurity and Disaster Recovery Training



EXECUTIVE SUMMARY

Objective

- Establish information security and continuity-of-operations governance plan for every state agency to protect against all threats, including data security breaches

Strategy

- Instituted extensive employee training, outreach, and education
- Applied uniform security strategy across all state governments

Solutions

- Online cybersecurity training program that is required of all Executive Branch employees
- Critical disaster recovery and continuity-of-operations planning initiative
- Specialized training events, including Cyber Security Conference and Cyber Security Exercise
- Certification programs for state's ISOs
- Penetration tests assess each state agency's preparedness to deal with possible cybersecurity attacks

Impact

- Number of incidents has dropped measurably as Education and Awareness program has matured
- Delaware is considered on the forefront of cybersecurity awareness, and has been recognized with a number of official awards and designations from the government and third-party organizations

Background

In January 2014, Cisco released the results of an in-depth analysis of the economic benefits of the Internet of Everything (IoE) for the public sector. Cisco's model revealed that some $4.6 trillion in "Value at Stake" would result from the adoption of IoE capabilities across 40 key public sector use cases over the next 10 years, including smart water, smart buildings, smart energy, smart parking, and more (http://bit.ly/1aSGlzn).

As a next phase of its analysis, Cisco engaged Cicero Group, a leading data-driven strategy consulting and research firm, to undertake a global study of IoE capabilities across these 40 use cases — how the best public sector organizations are "connecting the unconnected," as Cisco terms it. To that end, Cicero Group conducted interviews with dozens of leading public sector jurisdictions — federal, state, and local governments; healthcare organizations; educational institutions; and non-governmental organizations (NGOs) — to explore how these global leaders are leveraging IoE today.

The research examined real-world projects that are operational today, are being delivered at scale (or through pilots with obvious potential to scale), and that represent the cutting edge of public sector IoE readiness and maturity. The aim of the research was to understand what has changed in terms of the jurisdictions' people, processes, data, and things, and how other public sector organizations can learn from (and replicate) the trail blazed by these global IoE leaders. In many cases, these jurisdictions are Cisco customers; in others, they are not. The focus of these jurisdictional profiles, therefore, is not to tout Cisco's role in these organizations' success, but rather to document IoE excellence, how public sector entities are putting IoE into practice today, and to inform a roadmap for change that will enable the public sector to address pressing challenges on multiple fronts by drawing on best practices from around the globe.

About the State of Delaware

The state of Delaware has established an award-winning data security initiative to educate and train all state employees to recognize and respond appropriately to cybersecurity threats. It employs a uniform system of training, including monthly and annual events, security certification programs, cybersecurity breach simulations, and online education programs. Additionally, the state runs an active disaster recovery and continuity-of-operations planning program to help anticipate and prepare for cybersecurity threats.

"We had a really good focus on security ... but it was tactical and technical. We had the right firewalls in place, and antivirus tools and other technologies to keep us secure. What was missing was the holistic view. We didn't have many policies on the books. We didn't have any type of formal education and awareness of state employees. We had limited attention on business continuity and disaster recovery."

Elayne Starkey,
Chief Security Officer,
Delaware Department of Technology and Information

Chief Security Officer Elayne Starkey oversees the Delaware Department of Technology and Information (DTI) Security Office. Under the direction of Delaware's General Assembly and the governor, DTI services all state organizations, including the legislative, judicial, and executive branches, public schools, and various other governmental agencies.

Ms. Starkey works closely with DTI Chief Information Officer Jim Sills and the governor's office. Her team is responsible for the design and execution of the Delaware Information Security Program and the Continuity of Operations and Disaster Recovery Program.

Ms. Starkey became DTI's CSO in 2006 after serving a number of years as the state's chief technology officer, and as chief information officer for the Delaware Department of Public Safety. Ms. Starkey has private-sector software engineering experience at Xerox Corporation.

Objectives

In 2009, Delaware's governor issued an executive order requiring every state agency to establish a continuity-of-operations plan for protection against all threats, including data security breaches. Ms. Starkey described the state's previous program: "[We] had a really good focus on security ... [but] it was tactical and technical. We had the right firewalls in place, and antivirus tools and other technologies to keep us secure. What was missing was the holistic view. We didn't have many policies on the books. We didn't have any type of formal education and awareness of state employees. We had limited attention on business continuity and disaster recovery."

Strategy

In response to the enterprise data breach security and prevention plan, Ms. Starkey instituted a plan of extensive employee training, outreach, and education. She sought to establish "a 50,000-foot view" across all state government and to apply a uniform security strategy "holistically – not just in our department, but across all state government."

Ms. Starkey indicated that the overall budget for DTI is $39 million, which includes IT infrastructure and software costs. She estimates that 2 to 3 percent, or approximately $1 million, of that budget is earmarked for security training and administrative expenses.

Solution

Cybersecurity Education and Awareness

One of the first steps was to establish a cybersecurity training and awareness program for all employees. This training provides employees with insights on how to avoid cybersecurity risks and vulnerabilities. It includes specific, actionable guidelines such as scanning files before opening them, best ways to avoid phishing attacks, and not clicking on suspicious links in an email.

State employees receive cybersecurity training annually, in addition to when they are first hired. Training to date has included the state's 15,000 Executive Branch employees, 18,000 K-12 school district employees, and special in-depth training for the state's 230 information security officers (ISOs). According to Ms. Starkey, the chief justice of the Delaware Supreme Court also recently mandated increased data security training for all Judicial Branch employees. Ms. Starkey termed education and awareness training the "cornerstone" of Delaware's "very aggressive outreach program."

"We recognize that they are not in the business of information security like we are, but it's the little things that they do every day while sitting at their computer, or handling paperwork, or handling thumb drives, laptops, and mobile devices, that really do make a difference in the security of our network."

Elayne Starkey,
Chief Security Officer,
Delaware Department of Technology and Information

The training is delivered via a 45-minute course, which includes instruction, quizzes, threat examples, and other content. Users move through at their own pace. According to Ms. Starkey, the training has more than 30 modules that are rotated each year to address specific challenges or threats. These modules include subject matter such as mobile device protection, social engineering, and staying clear of viruses. In addition, each agency can opt to include agency-relevant modules, such as a HIPAA module that the Delaware Department of Health and Social Services uses to train employees dealing with sensitive medical records.

The training modules enforce basic security procedures for daily operations. "We recognize that most employees are not in the business of information security like we are, but it's the little things they do every day while sitting at their computer, or handling paperwork, or handling thumb drives, laptops, and mobile devices, that really do make a difference in the security of our network," Ms. Starkey explained.

One particularly informative aspect of the training is regular "phishing" exercises conducted by DTI. "We carefully craft an email that looks like a phishing attack, but it's all coordinated through our office. It invites employees to either open an attachment file or click on a link," Ms. Starkey said. "If they do click, they are immediately presented with an education screen that says, 'Oops. We were hoping you would not click on that link. Here are all the reasons you shouldn't have clicked.' That's been very useful to give me some real meaningful metrics to measure how closely our employees are paying attention to all the education and awareness that we're sending their way."

To supplement this outreach, DTI also manages a scorecard program where ISOs in each state agency and school district are surveyed about their cybersecurity practices. Ms. Starkey explained: "We do this on a biannual basis. They complete a survey, which results in a numerical score and a one-page management-friendly Information Security Scorecard." Results are provided to both Information Security Officers and their senior managers.

To accommodate the growing need for trained data security professionals, Ms. Starkey's office also partners with the Cyber Aces program. This organization sponsors events and competitions encouraging youth to pursue education and employment in data security fields. Delaware is one of the first states in the United States to host Cyber Challenge Camps and Cyber Aces Competitions to attract young people to pursue a career in information security. The state also hosts an annual statewide cybersecurity training conference for state, local, county, military, and private-sector employees. Each year, state employees and outside partners also spend time in elementary schools educating students about Internet safety principles.

Business Continuity and Disaster Recovery Plans

In response to a directive from the governor, Ms. Starkey's team also assumed responsibility for assisting each state agency in establishing an all-hazards continuity-of-operations plan for protection. "My team is responsible for getting out there and working with each state agency to assist them in the preparation of their plan," Ms. Starkey said. Her work has included Executive Branch agencies, the Department of Education, and the Judicial Branch.

"Every plan is prepared in a consistent way so that in the event of some large-scale disaster, we could readily get to the COOP plans and provide information to decision makers in the midst of a disaster."

Elayne Starkey,
Chief Security Officer,
Delaware Department of Technology and Information

Initially, DTI worked with the Delaware Emergency Management Agency to identify "tier-one agencies," which are, according to Ms. Starkey, those that, if they could not deliver services, would risk either loss of life or significant property damage. Currently, plans have been completed for all tier-one agencies, and they have nearly finished plans for the tier-two agencies as well.

According to Ms. Starkey, these plans are crucial to state operations. "Every plan is prepared in a consistent way so that in the event of some large-scale disaster, we could readily get to the COOP plans and provide information to decision makers in the midst of a disaster."

"We have a consistent, repeatable methodology that the team developed and tweaked along the way," Ms. Starkey indicated, adding that her team has been recognized for their efforts. "Last year, Governor Markell presented this team with the Governor's Team Excellence Award, and they have also been recognized by Disaster Recovery Institute International with the 2012 Strategy of the Year Award."

Conferences and Training Events

Ms. Starkey's team organizes specialized training events throughout the year, which she describes as "key parts of our Education and Awareness." She also hosts two large-scale training events: the Cyber Security Conference for both public and private representatives, held each spring; and the autumn Cyber Security Exercise for government employees. She and her colleagues create a large-scale cybersecurity breach simulation, in which participants practice emergency plans, including detection, remediation, and recovery techniques.

Certification Programs

Ms. Starkey offers certification programs for the state's ISO team: 230 information security officers consisting of one or two representatives from each area of state government. While establishing elements of the program, Ms. Starkey discovered

that the ISO program's existing education was outdated and did not take into account "how the world has changed in the last seven years." She noted, "Security wasn't such a headline then as it is today. It didn't require a lot of attention."

To rectify this, Ms. Starkey encourages ISOs to obtain their CISSP certification, which Ms. Starkey termed the "gold standard" in worldwide information security training. While the certification is voluntary, DTI actively supports the program, providing a week-long "boot camp" opportunity for each ISO. "We've asked them to step up in a major way, and I am not a big fan of asking our employees to step up without offering training to go along with that," she said. The camps are run with the assistance of (ISC)2, a professional certification organization, and the University of Texas. "This prepares the students to sit for the exam to achieve their certification," Ms. Starkey said.

The program was recently awarded the Cyber Innovation Award from the SANS Institute. In addition, Governor Markell has been highly supportive of the DCISO program, inviting those receiving the certification to his office for a recognition ceremony and presentation of credentials.

Ms. Starkey and her colleagues instituted an additional certification training program for Delaware public employees: the Delaware Certified Information Security Officer (DCISO) designation. This program is conducted through a series of online training courses and other activities, including various electives such as helping with exercises or doing presentations at regular ISO meetings.

Employees enrolled in the DCISO training receive credits for each area completed, which Ms. Starkey described as "an incentive program in its simplest form, something to aspire to and to demonstrate to their management how seriously they are taking information security." The program was recently awarded the Cyber Innovation Award from the SANS Institute. In addition, Governor Markell has been highly supportive of the DCISO program, inviting those completing the certification to his office for a recognition ceremony and presentation of credentials. Ms. Starkey described the executive-level support as "huge" for her department in motivating employees.

Additionally, Ms. Starkey indicated, "Throughout the year, we offer other types of training for our information security officers, and technical training for the IT staff."

Penetration Tests

Ms. Starkey described her agency's efforts at conducting penetration tests as an important way to assess each state agency's preparedness to deal with possible cybersecurity attacks. These tests involve simulated attacks orchestrated by DTI staff in conjunction with trusted vendor partners. Because Delaware's IT network is highly centralized, it is relatively easy for DTI to conduct such tests and to monitor and analyze results.

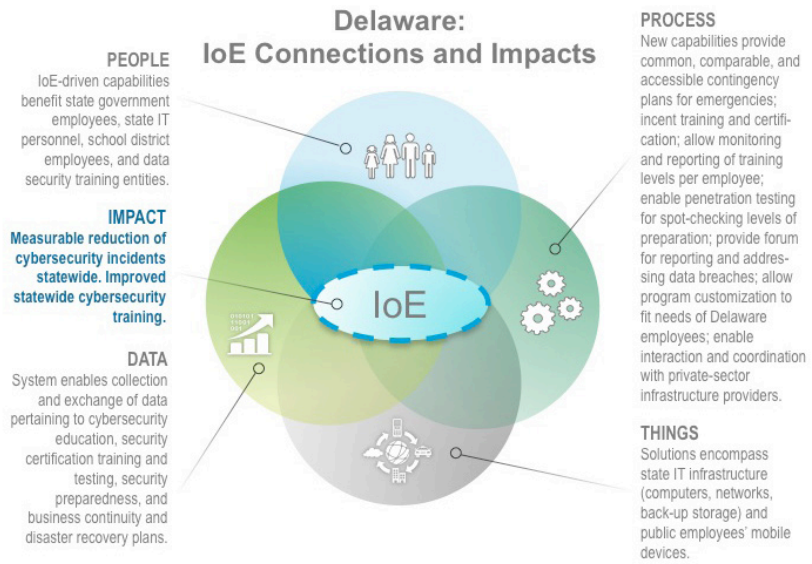
Ms. Starkey indicated that DTI will oftentimes conduct such tests or deeper analysis activities with agencies that did not score particularly well on the annual scorecard exercise. This is helpful in identifying and addressing vulnerabilities that might affect the statewide network.

In terms of specific firewall and antivirus technology, Ms. Starkey indicates that the state of Delaware utilizes a combination of industry tools to ensure protection of the network. This is in addition to the specific user and IT specialist training that she sees as critical to combating threats and addressing vulnerabilities.

"Here is what happened. Our incident count increased dramatically. We were scratching our heads and thinking, 'We're trying to lower our exposure, and here we are getting more incidents than ever.' We concluded that those incidents were going on before the Education and Awareness – we just didn't know about them. Knowledge is powerful. You can't fix something until you know about it."

Elayne Starkey,
Chief Security Officer,
Delaware Department of Technology and Information

Figure 1. Delaware: New and Better Connections.



Source: Cisco Consulting Services, 2014

Impact

Ms. Starkey admitted that, initially, measuring results of her work was difficult. "Not all of the benefits are easily quantifiable," she related, "but I will mention one in particular that caught us by surprise. We track the number of security incidents reported to our central service desk. Then, along comes our Education and Awareness program to increase people's knowledge and ensure they know who to contact. If they see something unusual or they've lost a laptop or a USB drive, they need to know what's expected of them in a case like that."

Ms. Starkey explained the initial numbers following implementation of her office's Education and Awareness activities: "Here is what happened. Our incident count increased dramatically. We were scratching our heads and thinking, 'We're trying to lower our exposure, and here we are getting more incidents than ever.' We concluded that those incidents were going on before the Education and Awareness – we just didn't know about them. Knowledge is powerful. You can't fix something until you know about it."

Ms. Starkey acknowledged that "on the surface, that might look like a negative metric," but as proof of increased awareness and reporting, her office interpreted the spike in incidents as a success. She indicated that as the Education and Awareness program has matured, the number of incidents has dropped measurably.

Due to the work of Ms. Starkey and her colleagues, Delaware is considered on the forefront of cybersecurity awareness, and has been recognized with a number of official awards and designations from the government and third-party organizations, including the Center for Digital Government and Disaster Recovery Institute International. Ms. Starkey was selected in 2012 as one of the 10 Most Influential People in Government Information Security by GovInfoSecurity.com.

Lessons Learned / Next Steps

Ms. Starkey mentioned that one challenge of her work is securing cooperation from so many different state agencies and their employees. "We have to look for creative and interesting ways for them to get on board with the program, to incent them to pay attention to security, and to take the necessary steps to protect the data within their organization."

"We have to look for creative and interesting ways for them to get on board with the program, to incent them to pay attention to all this, and to take the necessary steps to protect the data within their organization."

Elayne Starkey,
Chief Security Officer,
Delaware Department of Technology and Information

Ms. Starkey described the scorecard program as one such creative method of both vesting employees in learning and quantifiably measuring the success of the program. "That's been very helpful," she stated. "We've gone through three rounds now, on a biannual basis. We always put the previous scores at the top of the scorecard after the first round. That allows them to gauge how they are improving their overall security posture over the years. It also gives them a way to demonstrate to their management areas where they're not doing so well, and to help them lobby for the funding, or the resources, or the time, or whatever is needed to improve their score in the next round."

For each training event, Ms. Starkey tracks results and conducts analysis, noting possible areas of improvement. She said, "In the simulations that we go through, there's a list of lessons learned, and things we can tweak, and things we can do better. We document all those findings."

When asked what she considers the most frequently occurring area of improvement, Ms. Starkey replied, "This probably sounds generic, but it's communication. There's always a category for communication improvement. Participants often realize, 'I forgot to let so and so know,' or 'I forgot to loop this organization into the process.' We go back to the COOP plan and amend the checklist to make sure that they are not missed the next time. Because when you're in a crisis situation, much of your commonsense thinking goes out the window, and it is incredibly helpful to have a template and guidelines to follow."

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**