INDIANA INFORMATION SHARING AND ANALYSIS CENTER

ISAC

Sponsor: Dewand Neely, Chief Information Officer; Paul Baltzell, past-Chief Information Officer

Program Managers: Nick Sturgeon, M.S.; IN-ISAC & SOC Manager

Award Category: Cybersecurity

Completion Date: October 8, 2015

Executive Summary

In a centralized IT environment like the State of Indiana operates, the network infrastructure is an appetizing target for hackers to attempt to infiltrate. Daily, thousands of spam and phishing messages are blocked and millions of IP packets and TCP connections are either blocked or denied. To help combat this growing threat, the Indiana Information Sharing & Analysis Center (IN-ISAC) was created.

Launched on Oct. 8, 2015, the IN-ISAC is a multi-agency initiative to reduce the overall cost of cybersecurity through the centralization of resources, leveraging of large-scale purchasing, improved prevention efforts and faster containment of threats. It focuses upon the sharing of threat information and collaboration on strategies. IN-ISAC provides real-time network monitoring, vulnerability identification and threat warnings.

These are somewhat standard features in any ISAC, what makes Indiana's operation stand-out is who is working at the Security Operations Center (SOC) and the collaboration with the public, private and public education sectors.

Students from Purdue University are employed at the SOC and have responded to thousands of security tickets since opening. On-site, McAfee staff provide guidance and allow insight into global data from their systems.

The ISAC has utilized its staff to assist local government units with cyber problems, assisted coordination on a public/private utility cyber exercise and daily defends the State of Indiana network against attacks.

Concept

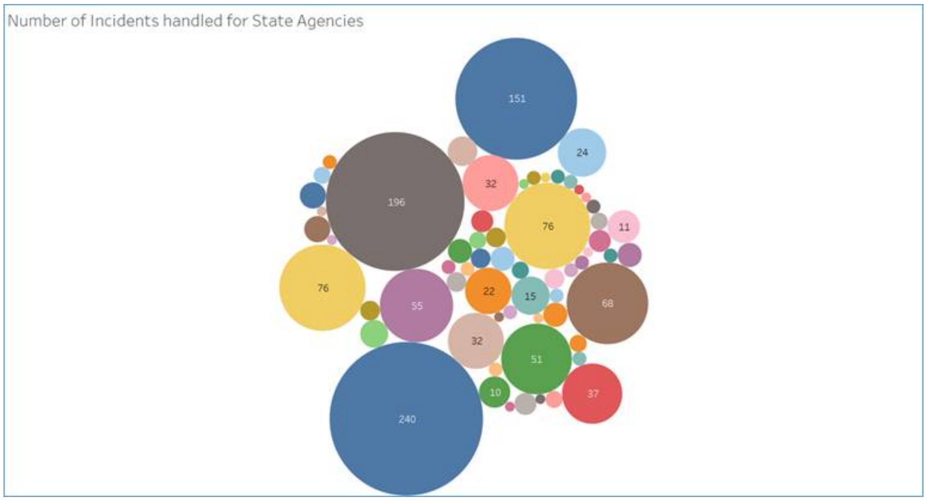
The landscape of cybersecurity has dramatically changed in the past few years. Breaches in the public and private sectors continue to rise, causing major concerns for identity theft, intellectual property protection, utilities, ransomware and botnets, to name a few. Indiana decided that a new approach was needed that incorporated all public sector units, the private sector and top researchers to combat these threats.

Prior to the IN-ISAC being formed, Indiana had several agencies that would work in the area of cyber defense, including the Office of Technology, Department of Homeland Security, State Police, National Guard and the Intelligence Fusion Center. While coordination was decent, there was not a centralized strategy across those entities, or clear delineation on who did what. Out of this, the IN-ISAC was formed.

The IN-ISAC is housed underneath the Office of Technology, but employees from multiple of the above listed agencies are part of the unit. The primary goal of the IN-ISAC is to better share and respond to threat information in a coordinated fashion.

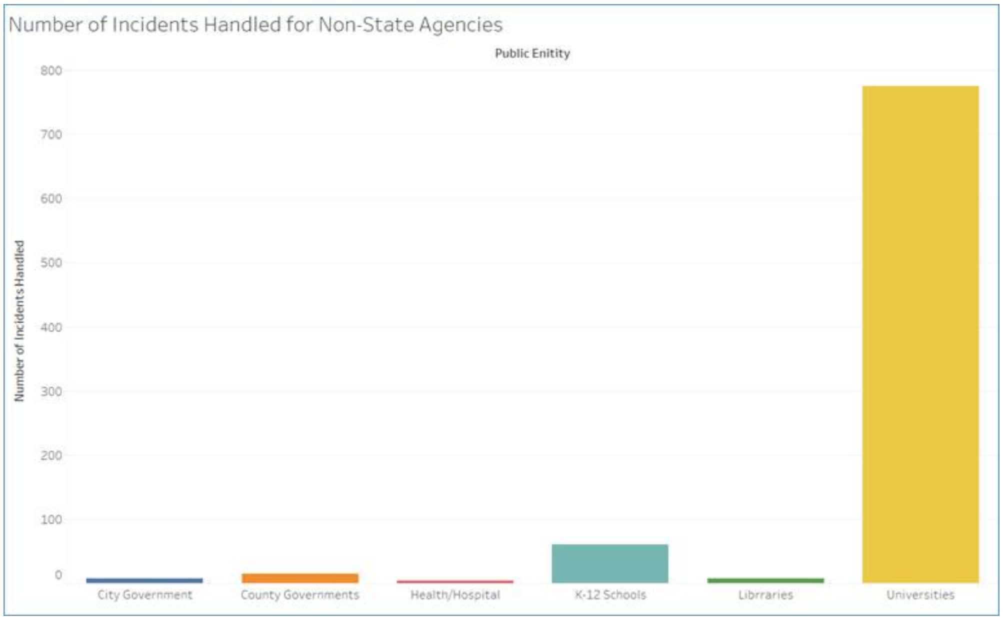
A major component of the IN-ISAC is the SOC, housed at Purdue University Research Park, about 70 miles northwest of the state capital. Purdue was chosen to house the SOC to utilize the talents of the technology students and the expertise of the facility. A couple full-time staff, as well as approximately a dozen students are employed at the SOC as Tier 1 support for the State, as well as towns, cities, counties, K-12 schools, and universities of Indiana.

Overall, the SOC has handled more than 3,000 requests for support.


Number of Incidents handled for State Agencies

The arrangement with Purdue University helps the State by providing greater support coverage, while incurring less expenses for staffing. In turn, the students benefit by receiving real-world experience and good compensation. The students earn $16.50 per hour and in 2016 the State paid $109,109.53 for their work. In comparison, if the state hired three additional full-time Information Security Analyst Senior positions making the mid-salary point at $73,918.00 or $37.91/hour would have cost the state $221,773.50, plus benefits; a savings of $112,000. This is a huge savings and provides 15 students with an opportunity to have hands-on experience.

The IN-ISAC also helps K-12 schools, colleges & universities and local government by providing MS-ISAC notifications and other services. Prior to the IN-ISAC, these alerts were unable to be actioned upon because of bandwidth. Now, there is staff time to identify a contact and pass along the alert. This has also led to more opportunities to provide services to these entities.



Additionally, the IN-ISAC was created to form partnerships and relationships with private sector companies. The private sector has staff that can lend its expertise to the State, which ultimately benefits the citizens.

Significance

There were three central problems that the IN-ISAC was created to solve. 1) The overall cybersecurity risk(s) posed to the State of Indiana network infrastructure systems, 2) as well as the risk to the private sector and citizens and 3) to try to create the next generation of cybersecurity personnel.

1) The IN-ISAC, through its Security Operations Center (SOC), helps mitigate cybersecurity risks among state agencies through the sharing of threat information and collaboration on strategies. It provides real-time network monitoring, vulnerability identification and threat warnings.
2) IN-ISAC has a website and newsletter that serves as a repository of information for security awareness for businesses and citizens. One of the goals is to educate citizens about ways they can better protect themselves from cyber risk. Ultimately, the more educated businesses and citizens are about existing cyber-threats, the less likely they are to fall prey to the traps.

   The IN-ISAC also has worked with local government to provide services. While the state information needs to be secured, so too does local government data. Outside of large cities, local government does not have similar technical resources and support as the State.

   Additionally, work has been completed to analyze vulnerabilities with utility companies.

3) Finally, through the partnership with Purdue University, the SOC employees Purdue students to help monitor the state network. This benefits the students to help them prepare for careers, while also serving the State by responding to lower priority risks. The state receives more than a dozen notifications of cyber-threats regarding town, city, county or state government computers, networks or websites within Indiana each day. Students at the SOC are now responsible for beginning mitigation efforts for things such as website defacement, computer/laptop reimages, possible account compromises, virus notifications and bot-net activity.

   While students focus on lower impact cyber notices, the more senior specialists continue to provide application support, provide system support, be responsible for system maintenance and conduct proof-of-concept tests on new technologies. They function as the subject -matter experts on the specific security systems IOT has in place.

The IN-ISAC has had much success because of strong executive support. Indiana Gov. Eric Holcomb recognizes the role that cybersecurity plays within the state. In January, newly sworn-in Gov. Holcomb issued an executive order continuing a council on cybersecurity, which had been started under previous governor, Mike Pence. Gov. Holcomb understands the need for a cyber-strategy, and the IN-ISAC is to carry out the policies created by the council.

Impact

The IN-ISAC has provided true impact for Hoosiers in the realm of cybersecurity. The program has benefited students, state government, local government and private sector, with citizens as the ultimate beneficiary.

A few examples:

Students/private sector: The collaboration with Purdue University also helps to train and fill the next generation of cybersecurity professionals. Intel estimates that there are 200,000 unfilled cybersecurity positions in the United States. Students are able to get real-world experience, while also providing a civic duty. Thus far, of the five students that worked at the SOC and graduated, two are now working in the cyber-field and directly attribute their career to their SOC experience.

State government: On July 5, 2016, the IN-ISAC provided assistance in combatting a virus outbreak, dubbed “Locky.” These efforts were essential in minimizing the negative impact of the virus to the Indiana Office of Technology and to the State of Indiana Network. The IN-ISAC was able to help contain the virus to approximately 40 devices within one agency. Had this virus not been so swiftly contained, the damage would have spread through the entire network and created a severe impact upon business operations. Once infected, the malware uses the workstation’s contact list to spam others and expand the number of infected. The malware also typically encrypts the data on the local and mapped drives of those infected. Fortunately, security protections prevented data from being encrypted and held for ransom. The quick work of the IN-ISAC and security team prevented data loss, ransomware and a massive spread of the virus.

State government: On May 24, 2016, the IN-ISAC assisted several agencies with a security issue involving the possible compromise of personal and/or private computers used by individuals interacting with the State of Indiana through their personal accounts with agencies such as the Department of Revenue and/or the Bureau of Motor Vehicles. The IN-ISAC confirmed the information as legitimate that it had received from a private-sector source, which prior to the IN-ISAC would have remain unreported to the state because the source would not have known whom to contact. The IN-ISAC then helped with getting crucial information to affected state agencies so that they could notify their customers of the problem. The IN-ISAC also immediately took other needed steps to address the root causes of the issues. This incident demonstrated the need for continued information-sharing between the private and public sectors. It also demonstrated that the Internet-surfing habits of individuals at home or work put State of Indiana networks at risk.

Local government: In early November 2016, an unidentified cyber attacker targeted the Madison County, Indiana computer network with malware and demanded monetary ransom to release stolen files. As in all ransomware cases, once the ransom was paid, the cyber attacker pledged to release the encryption code to restore the stolen files. Very early on in the incident, the IN-ISAC, along with the Indiana State Police (ISP), was notified. The IN-ISAC took an active role in assisting the ISP Cyber Crime Detective with logistics, research and technical support through the entire case. The IN-ISAC took the lead in coordinating with the MS-ISAC and US-CERT. At the conclusion of the case, the IN-ISAC and the Indiana Intelligence Fusion Center released a joint sealed assessment of the ransomware attack. This bulletin was widely distributed throughout Indiana to public and private entities."

Local government: The IN-ISAC has worked with the City of South Bend on multiple occasions to provide vulnerability assessments of their public facing website. This service was requested by the City of South Bend after they made several upgrades to their website. Originally, the request came as a result of the monthly MS-ISAC website fingerprinting report the IN-ISAC forwarded to them. Since the MS-ISAC reports are only monthly, the IN-ISAC is able to provide this service on demand which is an enhancement to Indiana local and county governments."

Private sector/public sector: The IN-ISAC helped organize Crit-Ex, a cyberattack exercise against a water utility, that brought together all the ISAC partners, plus the Indiana Utility Regulatory Commission, US DHS and the FBI. Six private sector cybersecurity companies, seven public utility companies and Indiana and Purdue Universities also participated in the exercise.

Crit-Ex was conducted in two exercises, table-top & real-world, at Muscatatuck Urban Training Facility, a self-contained community once home to a state developmental center, to conduct a real cyberattack against a water utility. Using the working water system, including a functional Supervisory Control and Data Acquisition (SCADA) system, which is representative of approximately 70% of water utilities in the nation, cyber teams conducted two separate attacks against each of the seven participating utilities.

Crit-Ex brought more awareness to the ability of utilities to handle cyberattacks and assisted in developing best practice responses.

The IN-ISAC has transformed how Indiana is dealing with the growing cybersecurity threats. It has reduced redundancy, expanded state services to local government and education, is helping train the next generation of cyber employees, and assisted the private sector through coordination. This approach has benefited the State, citizens, businesses and students.