Indiana Office of Technology

Powering a State that Works

Title:	Whole-of-State Cybersecurity – Improving the security and digital services of local government
Category:	State CIO Special Recognition
State:	Indiana
Contact:	Graig Lubsen, Indiana Office of Technology 317-268-8071; glubsen@iot.in.gov
Project Initiation Date:	2020
Project End Date:	Ongoing

Executive Summary

Under Chief Information Officer Tracy Barnes, the State of Indiana has made a concerted effort to work with local governments and improve the whole-of-state cybersecurity approach. This includes learning more information from our local partners, frequent in-person events and offering technology services to improve their security and digital government efforts.

Starting in February 2020, the Indiana Office of Technology (IOT) stepped up efforts to expand local government adoption of IN.gov domains and began offering the state’s award-winning website services to locals. In 2021 IOT worked with the legislature on a law that requires local government to report cyber security incidents to the state. IOT began visiting across the state to have conversations about local government's needs, raise awareness of the law, and promote engagement between the state and local government.

Idea

Tracy Barnes became Indiana's Chief Information Officer in March 2020 with a priority to improve technology across all bodies of government. The Indiana Office of Technology (IOT) statutorily provides central information technology support to the executive branch of state government and can provide services to local government, judiciary, legislature, and higher education. Until Barnes' appointment, nearly all of IOT's focus was on serving the executive branch.

Driven by a desire to enhance security and services, IOT made a rigorous effort to work with local governments with a focus on a whole-of-state cybersecurity approach. The state and local government networks are interconnected across various applications, including health and human services, child services, taxes, etc., meaning a vulnerability in one spot potentially places everyone at risk. Additionally, the state has invested in security and digital government infrastructure that some smaller local government bodies cannot match. It made sense to extend free or low-cost services across jurisdictions.

IOT developed a plan to work with local government by first understanding the need. To do so, state law was changed to require local government to report cybersecurity incidents to IOT.

Shortly after the state law change went into effect, the federal government passed the Infrastructure Investment and Jobs Act, which provides $1 billion in cybersecurity grants to states and local governments. Due to the requirement that 80% of the funding go to local government, IOT incorporated information gathering for the cybersecurity plan into its community conversations.

To support the state law and promote available resources, IOT began visiting communities.

Implementation and Impact

IOT approached the collaboration with local government through a phased approach.

In the summer of 2020, IOT began meeting with local government associations, including the Association of Indiana Counties (AIC) and AIM, the local municipality trade association representing cities and towns, to learn more about their approaches to cybersecurity and digital government. As expected, local government cybersecurity preparedness was all over the board – some were very well prepared and had invested; others, generally smaller municipalities, had bare-boned resources. Of course, the evaluation was primarily anecdotal, and more evidence was necessary.

IOT and the local government groups agreed that a law was necessary to better understand the scope of cybersecurity threats in government. As part of the negotiations, IOT agreed to begin actively offering and promoting state services that local governments could use to improve their security posture and digital government experience.

While IOT made plans to visit all 92 counties, the federal government passed the Infrastructure Investment and Jobs Act that provides cybersecurity funding to state and local governments. Some of the specifics on how to obtain funding are still unknown as of May 2022, but it is clear that at least States need to have a cybersecurity plan in place on how funds will be spent. Knowing this, IOT was able to incorporate gaining an understanding of local government cybersecurity needs into its county visit agenda.

Collaboration and law change:

Working with legislators and the associations, IOT jointly created a cybersecurity incident reporting legislation to understand government bodies' threat landscape. In all, the law covers more than 3,000 political subdivisions. Governments needed to report, using best professional judgment, threats in the following categories:

1) Website defacement
2) Distributed denial of service attack
3) Zero-day exploitation
4) Vulnerability exploitation
5) Business Email Compromise
6) Ransomware

Each political subdivision is required to have at least one designated incident reporter. Due in part to the support and collaboration of the local government trade associations, the bill became law without receiving a dissenting vote across the entire legislative process, becoming law on July 1, 2021.

Since taking effect, IOT has received more than 350 incident reports. Of those, approximately 70% of the attacks were unsuccessful. The data indicates that business email compromise is the most common attack, with ransomware beginning to tail off. IOT has also been able to distribute indicators of compromise from a ransomware attack against a political subdivision, allowing others to identify and thwart any efforts on their systems quickly.

Meet with local governments

The next phase to improve local government security and services was to visit counties across the state to meet face-to-face with the goal of:

1) Put a face on the state’s outreach efforts
2) Inform people about the cybersecurity law and register them as incident reporters
3) Learn about local cybersecurity awareness
4) Share best cybersecurity best practices and offer IOT services

Over the past 18 months, IOT held over 60 meetings with representatives from all 92 counties – half covered twice – and presented at 11 conferences and numerous city and county council meetings. During these engagement opportunities, IOT has met with nearly 1,000 local officials ranging from IT professionals to elected officials, such as county council, county commissioners, trustees, hospital staff, K-12 IT staff, and emergency managers to have a dialogue about improving the whole-of-state cybersecurity and government experience.

Meetings began in November 2021 and are continuing through the rest of 2023, culminating with a statewide cybersecurity conference in December. Billed as cybersecurity conversations, the initial agenda was to hear from locals about their needs, how IOT could help, and encourage adoption of an *.in.gov domain. The domains are important because they convey a sense of trust from the public. Indiana frequently conducts user testing sessions on its IN.gov websites and services. Our research has shown that trust in a .gov domain is significantly higher, with one research participant stating, “I know that if it’s .gov then it’s legitimate and has proven resources. It is not going to be spam. Medicare.com is not official. Medicare.gov is.”

IOT, for some time, has offered local governments free domains on the in.gov directory, but the footprint has grown to nearly 900 local in.gov domains existing across websites, email and applications (QA, Test and Prod).

Collect Feedback, Adjust & Offer New Products

Websites

As IOT held more meetings, local government leaders offered ideas on how IOT could best collaborate with them and which services were needed. Indiana had in earnest begun offering websites to locals through its award-winning IN.gov Program. Locals could take advantage of low-cost pricing options ($50/month, $100/month or $250/month) to use the same design templates as state agencies. This includes access to the state’s enterprise content management system, cybersecurity protections, accessibility checks, and analytics. The higher-priced packages come with additional benefits.

With the website, locals automatically receive an in.gov domain. During the pandemic, the trust of online information, especially for health departments, was vitally important. IOT saw many local health departments operate on .com, .org or through unverified Facebook pages. The state provided optional free websites to health departments to counter this, and 26/92 took advantage. Additionally, the State has paid engagements with a variety of local government offices, including sheriffs, towns, cities, townships, and a county prosecutor – in all, **more than 60 local governments are using IN.gov-developed websites.**

Office Productivity

One service that IOT heard about in meetings that locals wanted was an email solution. IOT brokered a discounted contract in March 2022 with Google and Carahsoft to offer Google Suite, starting at $5.50/user/month. This service became even more beneficial as we learned during our sessions from federal government representatives that grant applications submitted from non-.gov domains were sometimes being discarded. IOT has helped issue hundreds of Google Suite accounts.

Cybersecurity Training

The other major service IOT made available to locals was its cybersecurity training program. Using an industry-leading platform, IOT tests and trains its 30,000+ employees every month. After hearing about the need out of these meetings, IOT offered free access to its platform (April 2022). Since the announcement, 49 counties, 51 cities/towns, 2 townships and 29 libraries have signed up to use our shared cybersecurity training module. Of those, 33 already used the same training platform as the state and switched to our already paid-for licensing, saving those locals $183,134 in costs.

Cybersecurity Assessments

Another service request IOT frequently heard about during our conversations was the need for cybersecurity assessments. During the 2021 biennial budget session, the state set aside money for IT projects and security upgrades, and IOT used it to fund cybersecurity assessments. IOT negotiated with Purdue University and Indiana University (IU) to create an unprecedented and unique agreement to provide cybersecurity assessments for local governments across the state. Under the arrangement, Purdue's cyberTAP and IU's Center for Applied Cybersecurity Research (CACR) staff and students will analyze the cybersecurity posture of local government entities and provide a blueprint on how they can further secure their environments.

The agreement pays the universities to develop and conduct a cybersecurity assessment methodology for local government that incorporates evaluations from the Trusted CI, CIS and NIST frameworks. Overseen by IOT, the universities will complete at least 342 assessments over the next four years. So far, 82 local governments are in the assessment queue.

Summary

IOT's approach to working with local government has improved the overall security posture of the entire state. It provides good stewardship of already spent state dollars to allow local governments to receive no-cost or low-cost services. Additionally, scores of local governments now have user-focused, secure and accessible websites, while the employees running local governments are increasingly being trained on avoiding cybersecurity threats.