When the Weakest Link Is You: Cybersecurity Awareness Training for Georgia Employees

NASCIO 2020 State IT Recognition Awards

gta
GEORGIA
TECHNOLOGY
AUTHORITY

Category:	Cross-Boundary Collaboration and Partnerships
State:	Georgia
Contact:	Calvin Rhodes, State CIO (404) 463-2340 calvin.rhodes@gta.ga.gov
Project Initiation Date:	August 13, 2019
Project End Date:	November 13, 2019

EXECUTIVE SUMMARY

In the span of just two years, multiple state agencies in Georgia fell victim to cyber attacks. Destructive malware and ransomware significantly disrupted services. Despite best efforts to defend, phishing attacks were opening holes at the weakest link – employees.

“It’s frustrating, but you also have to be realistic…We might as well own it and be as prepared as we can and train our people so we can cut down on the number of instances,” stated Gov. Brian P. Kemp as he laid it bare (Atlanta Journal-Constitution article, August 2019). His words became the rallying cry for Georgia state agencies to up their guard against cybersecurity threats.

In response to the increased level of cybersecurity threats in the state, Gov. Kemp issued an Executive Order on August 13, 2019, that mandated (among other steps) cybersecurity awareness training for all Executive Branch agencies within 90 days, impacting more than 100 agencies and approximately 86,000 employees.

CYBERSECURITY AWARENESS TRAINING

REQUIRED WITHIN **90** DAYS

AFFECTED **100+** AGENCIES

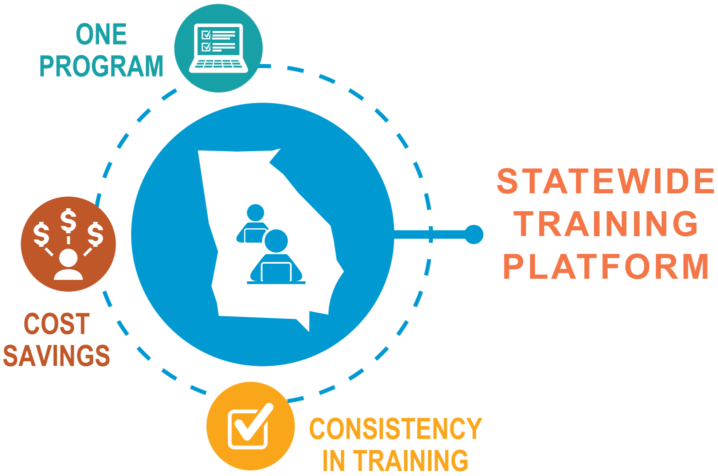
INVOLVED **86,000+** EMPLOYEES

The Georgia Technology Authority (GTA) took the lead to deliver comprehensive cybersecurity training in an efficient and cost-effective manner. GTA had already used the Proofpoint® Wombat Cybersecurity Training Platform for its own security awareness training program for several years and had extended access to the platform to some agencies via the state’s shared IT services program. It was clear this tool could help agencies comply with the governor’s training mandate. All Executive Branch agencies needed to be onboarded onto the platform swiftly so training could begin.

Training invitations were emailed, and by year’s end, all Executive Branch state employees completed the required training. Georgia state government demonstrated that, given the appropriate, scalable resources, state agencies could band together for a common cause, which also opened new channels of exchange among IT and information security leaders. State employees gained a fresh understanding of their critical role in cyber defense, promoting a sense of shared responsibility for cybersecurity across state government.

CONCEPT

Human error. It is why phishing works, and Georgia government was paying the price. Costly ransomware attacks were stacking up, and Georgia's governor responded. An August 2019 Executive Order addressing cybersecurity included a key provision aimed at what is too often the weakest link in defenses – employees. The state needed a way to better manage the problem, not a one-time security enhancement but a learning tool that could be used to strengthen its cybersecurity stance.



The state also needed to avoid having each agency figure out its own way to meet the training mandate, which would have taken longer, cost agencies individually, taxed the limits of many agency IT staffing levels, and led to inconsistency. Even though some larger entities, like the Technical College System of Georgia, had existing training programs in place, all agencies were asked to use the statewide platform for this effort to ensure a streamlined approach.

Having agencies come together to reduce human error and adding an ongoing learning component to employees' toolbox were the keys to effectively meeting the standards of the Executive Order. It was important to instill a sense of urgency in the employees so they, and therefore the state of Georgia, could fully combat the relatively new and continually evolving threat at hand. More than a learning tool, employees needed to gain a sense of responsibility for state systems and data.

The Executive Order also included the oversight of the State Government Systems Cybersecurity Board, an established entity widely recognized as the state's authority on cybersecurity. The board was bolstered and given responsibility for defining a program for statewide use, leading to the involvement of the Georgia Technology Authority (GTA) in the training. The State Chief Information Security Officer (CISO), a member of the Cybersecurity Board and part of GTA, took steps to identify resources to deliver the training.

Looking for internal resources readily available, GTA turned to the Georgia Enterprise Technology Services (GETS) program. GETS, the state's shared IT services program which delivers computing, network, and telephone services for state agencies, already included the managed security service Proofpoint® Wombat Cybersecurity Training. The training tool was flexible, scalable and ready – it was the right fit.

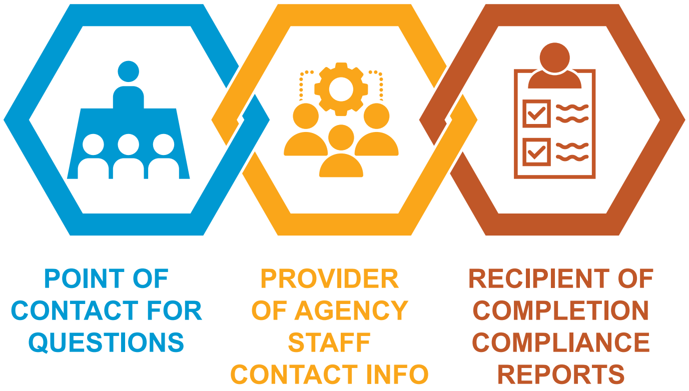
Working on an accelerated timeline, Georgia's Executive Branch agencies had to mobilize quickly to extend the cybersecurity training to all their employees. First, GTA and its vendor partner, Capgemini, worked to identify a training coordinator at each Executive Branch agency. The coordinator developed a list of email addresses for all staff at his/her agency so that information could be loaded into the training platform.

CONCEPT *(continued)*

By appointing a coordinator to this role, each agency created a point of contact for administering the training. GTA worked closely with these coordinators to ensure that the training was available to all employees, and Georgia's CISO provided memos that agencies could use to announce the new training program to staff.

Coordinating with Atos, the security services provider within the GETS program, GTA provided regular reports to the agency training coordinators to show them which staff had completed the training. The notifications for employees were not one-and-done; the training platform sent alerts, reminders, and completion confirmations, so each employee was kept well informed of his/her progress. GTA and Atos also provided a means for agencies to add new staff to the platform as they joined state government, giving a level of autonomy to agencies through the program. The Cybersecurity Board remained a presence as well, with the State CISO reporting updates on progress that could be given to the governor.

MERITS OF DESIGNATING AGENCY COORDINATORS


POINT OF CONTACT FOR QUESTIONS
PROVIDER OF AGENCY STAFF CONTACT INFO
RECIPIENT OF COMPLETION COMPLIANCE REPORTS

Required online training segments addressing phishing and ransomware were the initial offerings of the program. Organizers certainly appreciated that those alone wouldn't safeguard Georgia. But, they were putting the machinery in place for a sustained defensive campaign. Additional training would be delivered subsequently, thus capitalizing on the training platform and administrative processes implemented in fall 2019.

Every Georgia employee is on the front lines of cyber defense. The state's cybersecurity training platform arms employees with the knowledge to better hold off attackers.

SIGNIFICANCE

State agencies are already stretched to the limits to meet constituents' needs. It was essential that the training tool be effective and efficient, and that the training program not disrupt agency operations. Time required of agency employees needed to be kept in check, and agency budgets couldn't be rewritten. It had to be manageable.

Convenient

GTA and its managed security services partner, Atos, worked to ensure the time demands for training were kept reasonable. Delivered a few times a year, with each online module requiring less than an hour for completion, the training modules allowed participants to maintain their work schedules. An employee would work through a series of slides, some with short interactive videos, and a quiz to follow. And because the training could be accessed anytime via any Internet-connected computer, staff could fulfill the requirements from the office, home, or elsewhere. With many employees working remotely, at least occasionally, flexible access to the training made things easier.

Cost-effective

The Proofpoint® Wombat Cybersecurity Training Platform provided Georgia an attractive choice for a training tool, cost-wise. Extending the tool to the full set of just more than 100 Executive Branch agencies could be done without imposing new financial burden on them. And that remains true beyond the initial round of training prompted by the governor's August 2019 Executive Order.

How? It's possible thanks to the enterprise nature of services, cybersecurity training among them, available to state and local government agencies through the GETS program. GTA offers these technology services through a public-private partnership. Across the portfolio of GETS IT infrastructure and managed network services, there's a common theme of scalability and adaptability of services, well-suited to broad-ranging needs of varied agencies. As champions of an enterprise approach to IT in state government, GTA delivers the full range of IT services to 14 core agencies in the state's Executive Branch. Many more agencies consume a subset of GETS services. And, GTA has the capacity to extend services more broadly where there's demand. The cybersecurity training service is another example of matching the best service from the IT marketplace to meet fast-changing business needs of state agencies.

Scalable

Without overlooking necessary administrative legwork, training via the Proofpoint® Wombat platform was opened up to dozens of agencies and tens of thousands of their employees, all in a matter of just weeks. Agencies didn't need any in-house training specialists or additional hardware. They benefitted from the quality of service available via the GETS program, and they had the help of GTA every step where needed. The strong connections to agencies fostered through the cybersecurity training program illustrate what has been a guiding principle for GTA and GETS: To effectively deliver IT services that meet agencies' needs, you have to involve those agencies, engage with them, and build an understanding of what they're trying to accomplish.

IMPACT

Since the governor's Executive Order on cybersecurity in August 2019, more than 86,000 state employees have been loaded into the platform for cybersecurity awareness training. Benefits have been both immediate and enduring.

Year-round training program

Following the successful initial round of training in 2019, a full-year program for 2020 is underway. It features semiannual security training, complemented by mock phishing exercises to keep employees on their toes and alert to suspicious emails. In addition, new hires are required to complete the ransomware and phishing awareness training segments, so all new state employees start out cyber-prepared. Also, employees benefit in their lives outside of work thanks to the cyber care and vigilance promoted by the program.

Program momentum continued into the current year. In Q1, two additional training segments were assigned, and reached an even deeper pool of state employees. The 86,000 boarded in the Proofpoint platform from fall 2019 had grown by a bit less than half. And despite the COVID-19 challenges that arose early this year, 86 percent of those employees completed their training. Roughly calculated, that's better than 200,000 additional training segments completed by employees, helping protect Georgia.

Culture of shared responsibility

The training has helped build a culture of shared responsibility for cybersecurity in the state of Georgia. For employees, taking responsibility for being on guard against suspicious emails and other cyber threats is a big part of it. Employees better understand their role in an agency's security strategy, becoming cyber defenders themselves.

Inter-agency information exchange

The cybersecurity awareness training program has also promoted better information exchange to and from the state's Information Security Office (ISO) at GTA. The program has been a springboard for introducing state agencies to other useful services and support the ISO and GTA make available. These are the types and caliber of IT services many state agencies, especially smaller operations, might otherwise struggle to secure on their own.

And it doesn't end with state agencies. GTA's cybersecurity awareness training service is now available to all public entities across Georgia. That includes new subscriber Electric Cities of Georgia, a non-profit serving power companies and municipalities statewide. Other public entities are shopping the GTA service now.

ENDURING ELEMENTS OF TRAINING PROGRAM

SEMIANNUAL SECURITY TRAINING

MOCK PHISHING EXERCISES

NEW HIRE TRAINING

“I am a cyber defender.” That’s a new philosophy for many state employees, and it’s taking root thanks to training.

Quick-response capability

GTA demonstrated its ability to meet state agencies’ IT service needs in a timely manner, and on a broad scale. State and agency leaders witnessed that through the emergence of the cybersecurity awareness training program. In the future, as other technology service needs arise, or agencies are asked to come together to strengthen state government, leaders can point to the cybersecurity awareness training program as proof that an expansive, rapidly mobilized and effective effort is achievable.

To err may be human, but it comes at too high a price. Georgia is training its employees to take extra care and to beware of cyber threats.

Georgia recognized a vulnerability – not one uniquely its own. Every state needs to enlist its employees as cyber defenders and train them for the role. Georgia’s approach offers a model. Designate a central board to define a training regimen shared across all agencies. Look to the state’s central IT agency to deliver training via a single enterprise platform serving all agencies. Establish coordinators at each agency to act as liaisons with the central IT authority. Then, motivate employees to complete the training, and practice what they’ve learned. Hard work, yes, and necessary.

Security awareness training alone will not keep agencies out of hot water when it comes to cyber threats. However, Georgia has developed a robust training program built around a convenient, cost-effective, scalable training service. The program is a significant addition to the state’s cyber defense. Human error (a true cybersecurity liability) may not be neutralized, but through the cybersecurity awareness training program, it *is* managed and minimized.