PUBLIC TECHNOLOGY INSTITUTE

A DIVISION OF FUSION LEARNING PARTNERS

Best Practice Brief:

CYBER INSECURITY, AI AND THE RISE OF THE CISO

October is Cybersecurity Awareness month, and a time to reflect on what is new. Based on the Public Technology Institute's (PTI) latest Cyber Survey of Cities and Counties, it comes as no surprise that cyber security once again tops the list of concerns. This year we find the threat landscape with increased dread as cyberattacks continue to rise in all sectors providing a sense of greater cyber insecurity. This also comes at a time when states are still mulling over the best methods to distribute the federal funds aimed at helping local governments better defend against attacks.

Adding to cyber insecurity is the unease in the use of artificial intelligence not only by public employees but by cyber criminals too. It comes as no surprise that artificial intelligence (AI) is being used by cyber criminals to further exploit cyber weaknesses and vulnerabilities. In PTI's City and County AI Survey, AI was listed as the No. 1 application to help thwart cyberattacks. They recognize how AI can actively scan for suspicious patterns and anomalies as well as assist in remediation and recovery strategies. What's more AI systems continue to learn and act.

Also new this year is the renewed focus on zero trust frameworks and strategies. Zero trust has never been more critical and unfortunately, it takes both time and talent to fully comprehend all its dependencies leading towards deployment. This year also saw for the first time in years the National Institute of Standards and Technology (NIST) has modified its Cybersecurity Framework to include an underlying layer of governance in each of its traditional five pillars. This too takes time to plan and implement for those who follow the voluntary guidelines.

The issue of staff capabilities continues to be of great concern to chief information officers (CIOs). As in the past several years, finding and keeping well trained cyber professionals remains a challenge. Nearly half of the states have removed the requirement for a four-year college degree in hopes of expanding this specialized labor pool.

Taken as a whole, zero trust, AI, workforce development and adapting to NIST's modified Cybersecurity Framework, adds to the ever-growing load to the CIO. This leads to the growing recognition that every local government needs someone who can remain laser-focused on cyber and all the moving parts, hence the rise of the chief information security officer (CISO).

Each year, the Public Technology Institute's Annual Cyber Survey of Cities and Counties asks how many local governments have a CISO. While the number is increasing, less than 40 percent have one. The state of New Jersey has passed legislation that requires that every local government have a CISO by 2025. Adding to such a challenge is the fact that while the legislation is well intended it does not currently provide any direct funding to pay for having a CISO.

As CIO demands and responsibilities increase so does the need for greater management and leadership development. The emerging CIO executive requires a complement of deputies to help manage the enterprise and chief among them is the CISO.

Today's local government CISO plays a pivotal role in protecting the digital assets and services of a local government, ensuring that its operations are secure, compliant, and resilient against cyber threats. For those who remain uncertain here are but a few key roles that a CISO plays. For those without a CISO, it should be understood that each of the following responsibilities is already performed by someone (possibly an overburdened CIO) in some form or fashion.

1. Strategic planning:

Develop and maintain the information security strategy, ensuring that it aligns with local government objectives and addresses the evolving threat landscape.

2. Policy development:

Draft, update and enforce information security policies, procedures and standards to ensure compliance with regulations and best practices.

3. Risk management:

Conduct regular risk assessments, identify vulnerabilities and prioritize security initiatives based on potential impact and threat probability. Risk management includes cyber insurance applications, requirements and appropriate policies.

4. Incident response:

Develop and maintain an incident response plan to address potential security breaches. Lead the response team during and after security incidents.

5. Security awareness training:

Create and deliver training programs to educate employees about security best practices and the importance of protecting government data.

6. Vendor management:

Evaluate and ensure the security of third-party vendors that the local government does business with, ensuring that they meet necessary security standards.

7. Technology oversight:

Evaluate, recommend and oversee the deployment of security technologies, including firewalls, intrusion detection systems, encryption solutions and endpoint security tools.

8. Regulatory compliance:

Ensure that the local government's IT systems and processes comply with applicable laws, regulations and standards.

9. Budget management:

Prepare and manage the information security budget, ensuring that adequate funds are allocated for necessary security measures and technologies.

10. Collaboration:

Work closely with other departments, such as IT, legal, human resources and emergency management, to coordinate security initiatives and ensure that security considerations are integrated throughout the organization.

11. Reporting and communication:

Regularly communicate the security posture of the organization to executive leadership and elected officials, providing them with updates on threats, vulnerabilities, and mitigation efforts.

12. Continual learning:

Stay updated with the latest security trends, threats and technologies to ensure that the local government's security posture remains robust and ahead of potential adversaries.

With the rise of the CISO, there is a temptation for over-reliance on one individual to be supremely in charge and lose sight of the fact that no individual—no matter how qualified—can truly be responsible for every vulnerability and the inevitably of human failings. There will always be someone who is "too quick to click." Even with the best CISO, public managers at every level must recognize that cybersecurity must be a whole of government approach.

This year, well over 60 percent of U.S. cities and counties lack a CISO, either because senior managers fail to see the need, have difficulty in recruiting a CISO, or simply lack the financial resources. The overall need and rationale for greater cybersecurity protection is ever-present and requires action. An example of an innovative approach is found with Texas creating Regional Security Operation Centers (R-SOCS) through partnerships with participating universities and technical schools aimed at providing assistance to local governments and as well as K-12 schools.

So, this October we not only recognize the ever-changing threat landscape and growing list of challenges, but we also salute the rise of the CISO as a noble start in better protecting our cities and counties and combating cyber-insecurity.

Dr. Alan R. Shark is the executive director for the Public Technology Institute (PTI), a division of Fusion Learning Partners; and associate professor for the Schar School of Policy and Government, George Mason University, where he is an affiliate faculty member at the Center for Advancing Human-Machine Partnership (CAHMP). Shark is a fellow of the National Academy of Public Administration and co-chair of the Standing Panel on Technology Leadership. Shark also hosts the bi-monthly podcast Sharkbytes.net. This first appeared on americancityandcounty.com in October 2023.