FEDInsider

State & Local Governments are Bolstering Cyber Tools & Partnerships

In the wake of increasingly sophisticated cyber threats, governments at all levels are working together, upskilling talent and investing in advanced solutions to protect citizen data

Featuring:

- **Jeremy Wilson**
  Deputy CISO, Security Operations, Texas Dept, Information Resources

- **Michael Dent**
  Chief Information Security Officer, Fairfax County, VA

- **Terry McGraw**
  Senior Executive Consultant, Secureworks

Cyberattacks, ransomware, phishing attempts and information warfare — security risks of all sorts are on the rise and becoming more sophisticated by the minute. Security and IT professionals are working to understand how cybersecurity ties into their agencies' missions to properly protect systems and networks.

Government and industry experts spoke at a recent FedInsider event to share the cybersecurity threats and trends they anticipate taking precedence in 2022, and how to respond to them. The following are some of the most important aspects of their discussion.

The Current Threat Landscape

Cybercrime consumes most incident engagements and network events, according to Terry McGraw, senior executive consultant at Secureworks. The top attack vectors are unpatched servers, weak or stolen credentials and a lack of multi-factor authentication.

"It really doesn't matter what your password complexity is if you don't have multi-factor authentication for your externally accessible surface," McGraw said. "That unfortunately is still the Achilles' heel of a lot of groups. They'll implement controls, but not full implementation. It's either everywhere or it's nowhere." Even if one person isn't using multi-factor authentication and a bad actor has that password, they can enter the network. Secureworks sees this often.

But being brilliant with the basics of cyber hygiene still matters, as phishing attacks and compromised external web browsers continue to enable vulnerabilities. Identity access management and control, and the capability to detect adversaries inside the environment remain necessary.

Protecting Critical Infrastructure State and Countywide

Texas is tackling an ever-changing threat landscape with a cybersecurity strategic plan updated every five years according to Jeremy Wilson, deputy chief information security officer for security operations in the Texas Department of Information Resources. The strategy focuses on staffing, outreach and education. "That encompasses what we're trying to do to protect critical infrastructure here in Texas," Wilson said.

The state's Community Emergency Response Team is also partnering with a public university to establish a regional security operation center, in addition to more local SOCs. This allows the department to cover the vastness of Texas, while providing training opportunities to students in incident response, policy and planning. "We'll have actual boots on the ground that can go out in that region and work incidents," Wilson said. And his office is working with federal partners to mitigate cyberattacks from nation states attempting to steal data by sharing threat intelligence and briefings with the Cybersecurity and Infrastructure Security Agency, FBI and Department of Homeland Security.

To combat everyday threats like phishing attacks, Wilson said his office is working on a statewide multi-factor authentication program, which helps secure critical systems. Data breaches have been of conversation lately in the wake of the war in Ukraine, after all, but they were already on the rise. According to the Identity Theft Resource Center's 2021 annual data breach report, there were 1,862 data compromises in 2021, up more than 68% compared to 2020.

In Fairfax County, Virginia, preventing daily threats regardless of what is occurring in

the world day-to-day is a common occurrence. "It is an enormous feat for us to have to do that and then making sure we have the capabilities to do it is always what's critical," said Michael Dent, CISO for Fairfax County.

To effectively reduce the network attack surface on the county's critical applications and virtual servers, Dent said they implemented a zero trust microsegmentation capability. The solution uses a software identity-based machine learning model that provides protections with policies between servers and full visibility into lateral server-to-server communications.

The county also implemented a secure access service edge next-gen VPN with internet access for secure, private zero trust network access to private applications and systems. Dent said the network is supporting a 10,000-remote user workforce in a public cloud infrastructure, so this was necessary. "Both of these solutions provided authorized, validated, secure and fast internet experience, and private access for those 10,000 authenticated users we have," Dent said.

Cyber Incident Reporting and Collaboration

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 will require critical infrastructure companies to report substantial cybersecurity incidents or ransom payments to the government. McGraw said that while this is stirring up controversy, incident reporting is essential, particularly for municipalities. "When you've had compromise, I think that together we learn more and there has to be a mechanism to share that information," McGraw said.

Virginia, Maryland and Washington, D.C., formed a committee of CISOs to discuss and strategize around cybersecurity, information sharing and best practices. Dent said the committee helps to form a public fiber network for public safety, equipped with cable franchise agreements that are interconnected with firewalls. And both Wilson and Dent expressed advantages to the Multi State Information Sharing and Analysis Center, which provides cyber threat prevention, protection, response and recovery services between the nation's state, local, tribal and territorial governments.

Protecting state entities and localities requires a holistic partnership approach. Wilson said his department shares indicators of compromise across state partners and back to federal partners to ensure all are doing what needs to be done to stay protected.

Getting Leadership and Financial Buy-in for Cyber

Wilson said considering budget may be an issue, especially for state and local governments, but that low-cost, no-cost and open-source tools are available to help. Texas offers these to localities, and leverages federal partnerships when it can. But ultimately, it's not just about the technology.

"While cybersecurity can seem complex and very hard and can take time, at the end of the day, any effective cybersecurity program is a combination of tools, people and processes," Wilson said. Invest in people and staffing, and reconsider processes or build an effective incident response plan to meet security needs.

For Dent, along with implementing the right security solutions like a zero trust architecture, leadership accountability is also important. At the end of the day, it's the data that is critical to citizens, and protecting that data while providing IT services is key. And Dent said having the CISO be the one to explain the importance of this to leadership — especially chief information officers — is critical to getting the funds, tools and solutions needed to do so.

"Having your CISO be the one to explain to leadership what the risks are, what it's going to take to mitigate those risks and give them options, that's going to be a better thing for you in the long run because the leadership is going to finally understand where things go versus having the risks being buried," Dent added.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(888) 936-2246
Secureworks@Carahsoft.com
Carahsoft.com/Secureworks
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
Twitter.com/Carahsoft