THUNDERCAT TECHNOLOGY

How Government Leaders Can Leverage Four Trends in Cybersecurity

The stakes of cybersecurity are high for government leaders, whether at the federal level or in a small municipality. More than protecting company secrets, government officials are responsible for the safety of their citizens, as well as securing critical infrastructure. Without a robust cybersecurity strategy, access to basic needs like electricity or clean water could be at risk. Technology leaders must stay apprised of the latest strategies and cutting-edge solutions to establish a comprehensive cybersecurity safety net.

Among the most-discussed cybersecurity topics at the moment are securing critical infrastructure, threat intelligence platforms (TIPs), external attack surface management (EASM) and 5G. With so many choices to make regarding tools and strategies, external partnerships can help government organizations assess their current cybersecurity landscape, as well as identify and deploy the right solutions to help them safeguard the needs of their constituents.

1. Protecting Critical Infrastructure

A key cybersecurity consideration that often sets government IT teams apart is the need to protect critical infrastructure. Worst-case scenarios in this field can lead to serious physical injury and loss of life — not typically the case in traditional IT systems. Even less physically threatening outcomes can be incredibly disruptive, such as major power outages or the consequences of the Colonial Pipeline ransomware attacks, for example.

Despite the high risk, protecting critical infrastructure is a complicated partnership between public and private entities. Government officials understand the importance of modernizing their security stack, however, most critical infrastructure is owned and managed by private companies. Those companies

must balance their own financial gains and losses, in addition to what Beau Nuanes, systems engineer at ThunderCat Technology, describes as “the push and pull between reliability and security.”

Upgrading security can require, or even accidentally cause, downtime and outages. Reliability is of utmost importance for companies providing essential services such as gas or electricity. They may be more reluctant to invest time and resources into upgrades that could cause interruptions when the status quo is working well enough.

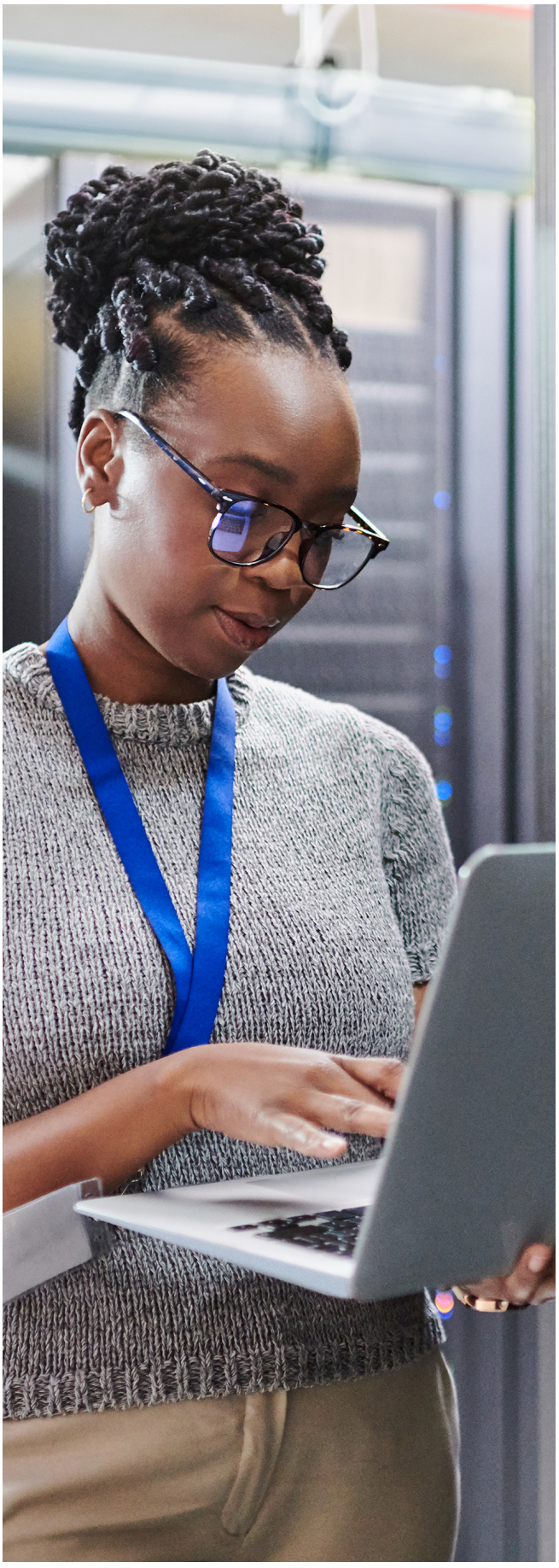
Historically, “because the community, and users, and folks buying the services weren’t asking for security, vendors weren’t building those features in,” Nuanes says. “But that’s started to change.”

> *You have to know what the threats are to your systems, or you can’t really look at risk. Threat intelligence gives you context for risk. And a threat intelligence platform is key in being able to disseminate that information and make sense of it.*
>
> ***— Beau Nuanes, Systems Engineer, ThunderCat Technology***

As organizations involved in protecting critical infrastructure, both public and private, look to ramp up security, comprehensive asset identification and full network visibility is essential.

“I’m a big advocate of tools like packet brokers,” Nuanes says. “When you have a large organization, they provide visibility into strategic places on your network.”

As network complexity increases, it becomes more difficult to monitor the full network in an organized and timely manner. Network packet brokers simplify and streamline the monitoring process by, as the name suggests, acting as “brokers” for the network — analyzing, filtering and routing network traffic and data from multiple network links to the appropriate monitoring tools.



And because the best defense is a good offense, Nuanes also highlights the importance of threat intelligence, or gaining an understanding of threat actors' strategies and behaviors, to securing critical infrastructure. Tapping into the adversarial mindset helps cybersecurity teams assess which attack vectors are likely to be exploited and shore up security accordingly.

2. Threat Intelligence Platforms

Research by Sophos found that 58% of state and local government survey respondents reported being hit by ransomware in 2021, a significant increase over the 34% of the previous year. To combat this increase, technology leaders should seek an effective threat intelligence platform (TIP) for organizing threat intelligence data. A TIP can give government technologists a way to create order out of chaos amid an overwhelming volume of threats.

"There are, I don't even know many types of threat telemetry and threat intel feeds out there," Nuanes says. "What a TIP does is it allows you to take and manage those, integrate them, look at them, and then automate actions based on them."

As the TIP simplifies the collection and aggregation of threat intelligence data, it works in conjunction with other security tools, such as security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions to enable faster analysis and automated threat response.

Think of risk as a function of threat, vulnerability and impact, Nuanes says. Without extensive knowledge about each key component of that calculation, it's impossible to have a comprehensive understanding of risk.

"You have to know what the threats are to your systems, or you can't really look at risk," Nuanes says. "Threat intelligence gives you context for risk. And a TIP is key in being able to disseminate that information and make sense of it."

> *Any device that's connected to my corporate network becomes another device that's potentially vulnerable. Another device I need to worry about, and something that, as a cyber defender, I might not even know is there.*
>
> ***— Beau Nuanes, Systems Engineer, ThunderCat Technology***

TIPs, like each piece of the cybersecurity ecosystem, are essential to establishing 360-degree security coverage and mitigating risk.

"You have your asset identification, you're using packet brokers to get data and send it to sensors, passively picking up assets — and identifying vulnerabilities on

and threats to those assets," Nuanes says. "You're sending that to your SIEM and SOAR and bringing it all together with threat intelligence. It's part of what we at ThunderCat call data-centric security."

3. External Attack-Surface Management

A data-centric security model must also protect the organization's external attack surface, which refers to all of its internet-facing assets and the vulnerabilities they create. The more assets an organization has, the larger its attack surface. And as the list of devices, operating systems, cloud providers and third-party vendors grows, so does an agency's attack surface.

A more expansive and variable attack surface makes it more difficult to maintain an accurate accounting of all assets exposed to the internet. This limited visibility often becomes apparent when an agency conducts an assessment of its attack surfaces.

"When we're talking to customers," Nuanes says, "sometimes they end up saying, 'Oh, wow, we didn't even know that was out there and facing the internet.' It's pretty eye-opening."

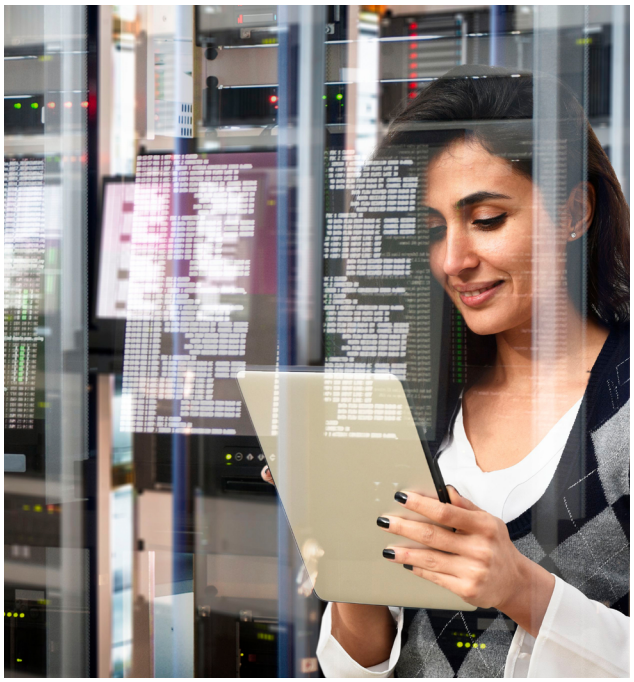
This doesn't inherently indicate a failure on the part of agency technologists but rather highlights why a specific external attack surface management (EASM) tool is helpful — because the attack surface is constantly shifting, making it difficult to monitor.

Ephemeral IP addresses, for example, are being created and recycled. A third-party cloud provider might default to making its storage publicly accessible, while an employee's shadow IT software operates without the knowledge of IT leadership. Each scenario represents a potential hole in the protective layer around an organization's data and assets. Threat actors actively look for these holes, and with many employees working from home at least one day a week, visibility has only become more cloudy.

"Any device that's connected to my corporate network becomes another device that's potentially vulnerable. Another device I need to worry about, and something that, as a cyber defender, I might not even know is there," Nuanes says. "We've even seen things like an Xbox on a corporate network."

In fact, half of the companies surveyed by MIT Technology Review Insights and Palo Alto Networks said they have experienced a cyberattack "originally from an unknown, unmanaged, or poorly managed digital asset." An EASM tool defends against such threats by tracking all assets and moving parts.

"It shows you the things that — in your organization, in your IP space — are out there, that the world in general can see, and then ties that into, 'Here are some issues you might have with those things,'" Nuanes says. "If the tool is showing it, then I guarantee the attackers see it as well."



One such tool is Palo Alto's Xpanse, which is currently used by several government organizations. According to Nuanes, Xpanse offers comprehensive attack surface monitoring and risk mitigation. Despite the benefits of tools like Xpanse, the most important step is choosing the right tool that works for your specific organization and mission.

"It depends on the organization, and it's not always technical," Nuanes says. "It's important that you're using an EASM tool. If there's already an investment or an enterprise license agreement, and that's the one that's cost-effective, it might make sense to use that one."

Many factors can go into finding the best solution for a government agency or department, and partners like ThunderCat help sort through them all, from technical capabilities to cost to leveraging an existing technology portfolio.

4. 5G Security

Among more early-stage technologies, 5G has yet to see widespread adoption but is still a hot topic of interest among government leadership. A couple of use cases Nuanes highlighted are 5G campuses, where instead of WiFi, all devices on campus connect via 5G, and private 5G networks confined to individual buildings and spaces.

"With WiFi, it can be hard to do classified wireless, but if you could do wireless that's only available with the signal in that building, then that could be really beneficial," Nuanes says. "There are also some potential cost savings, in that they don't have to have all the cabling and infrastructure to physically plug in."

New use cases also raise new security concerns. At the most basic level, more technology means more attack surfaces. Agencies looking to prepare for the future of 5G should consider basics such as the infrastructure footprint required to introduce 5G in their spaces. But most importantly, leaders need to keep security front and center from the beginning of development.

"Security is very often an afterthought," Nuanes says. "It's not part of the design, it's, 'Let's build this thing,' and then, 'Oh, now we need to figure out how to secure it.'" Instead, security must be integrated into every step. One tool that has potential on a 5G-enabled campus is a software-defined radio, which provides observability of a facility's wireless spectrum by monitoring its radio space. It can detect wireless and cellular devices within the facility via the signals they emit — even if they aren't connected to the network — and can locate potential threats.

"It then provides the ability to block or limit those signals, so only the signals you want are able to be connected," Nuanes says. "If you start thinking about these tools up front, it's going to make your job easier later."

Accelerate Progress to Achieve Security Goals

Between the federal government and more than 90,000 state and local government units, there is a wide range in how modernized individual departments and agencies are. For government technology leaders looking to elevate cybersecurity programs, industry partnerships are crucial.

"While previously there was a lot of 'build your own' in government … I've seen more willingness to admit there's a lot of good work happening on the vendor side of things," Nuanes says. "And perhaps the focus should be on integrating those tools."

In addition to specific tools and solutions, Nuanes adds that this also applies to adopting strategies and developmental methodologies used by industry organizations, such as data-centric security operations and DevSecOps. Partnerships and modernized strategy enable government technology teams to expand automation capabilities and focus on more complex improvements and upgrades.

Agencies are increasingly clearing a path toward integrating commercial technologies by making the process faster and simpler. For example, the U.S. General Services Administration teamed up with the Defense Innovation Unit, part of the Department of Defense, to "enable both DoD and non-DoD entities to scale novel commercial technologies across the United States, including those needed at the federal, state, local, and tribal levels."

As government leaders take advantage of these opportunities, the ThunderCat team stands ready to help agencies develop a robust cybersecurity strategy by sorting through the seemingly endless tools for each security element or establishing a data-centric security operations center.

Nuanes, who has direct experience working for the government at the Sandia National Laboratories in New Mexico, says the focus on leveraging industry and commercial partnerships is growing. "My hope is that we start to see this willingness proliferate throughout the government."

THUNDERCAT TECHNOLOGY

Learn more about how ThunderCat helps higher education and government organizations identify and deploy the right suite of technology tools to support their missions.