Cybersecurity predictions for public sector in 2024

A guide for state and local governments to help protect their digital assets

verizon

New year, new opportunities

In 2023, cybersecurity took center stage for public sector institutions as ransomware and data breaches increased dramatically. Now a top target for hackers, government agencies and public infrastructure focused on ramping up information security budgets to combat escalating threats.

According to the 2023 Verizon Data Breach Investigations Report (DBIR), bad actors are increasing the variety of tactics they use in attempting to access government data. External adversaries are combining their forces like never before to steal information from public sector.

The DBIR also revealed that 74 percent of breaches were caused by the human element – e.g., error, privilege misuses, stolen credentials or social engineering. Mistakes by employees continue to be a major vulnerability.

Though challenges remained throughout 2023, the public sector did make significant strides to reinforce network defenses, adopt cloud-based threat monitoring, centralize data access controls, leverage intelligent technologies and prepare contingency plans. With proper strategizing, 2024 could be the year we see some relief in the explosive growth in attacks against government entities.

Predictions for 2024

At Verizon, we are passionate about our responsibility to provide customers with networks that are secure and resilient. Not only do we provide public sector with industry-leading cybersecurity solutions, we offer monthly threat briefings (for customers and non-customers), host cyber risk roundtable sessions and publish three preeminent, publicly-available annual reports: the aforementioned DBIR, the Payment Security Report and the Mobile Security Index.

Relying on the security expertise of Verizon, and the analyses of our own global network, we have compiled a list of issues we believe will be prevalent for the public sector in 2024.

1

Nation-state threats aimed at the public sector will intensify in 2024.

Threats and challenges are likely to heighten even though public sector resources and readiness will probably continue to lag. 2023 brought a noticeable uptick in attacks aimed at critical infrastructure targets across transportation, energy, water treatment and other vital services. This trend may persist into 2024, putting public sector groups responsible for infrastructure security on high alert. Sophisticated nation-state bad actors will likely remain active in scanning networks, identifying vulnerabilities and preparing strategic cyberwarfare tactics.

This isn’t to say that the government sector won’t be able to make progress in mitigating threats, but it doesn’t seem that the risks themselves will decrease.

2

Public sector entities will continue to struggle with inadequate staffing and insufficient budgets.

Funding and employment issues continually plague public cyber preparedness initiatives. Heading into 2024, budget shortfalls mean resource-strapped agencies simply can’t always implement best-practice cyberdefenses. Multi-factor authentication, advanced endpoint detection, improved network monitoring, routine penetration testing and modern data protections all carry costs many public groups cannot meet. Government entities also struggle to compete with the private sector when it comes to the infosec talent pool.

Until budgets grow, hackers may be better positioned to succeed in probing under-defended networks.

3

Government employees will remain highly vulnerable.

The human factor will continue to be pivotal in 2024’s cyber landscape. Public sector employees remain extremely vulnerable to social engineering attacks and phishing schemes, giving hackers access to sensitive systems.

Far too few public entities employ comprehensive security awareness training to help employees identify risks. Additionally, many public-facing agencies rely on outdated legacy computer systems riddled with unpatched vulnerabilities. Upgrading systems takes time and money, both of which are in short supply. This combination of untrained employees and antiquated technology widens the security gap attackers can actively exploit.

4

Antiquated, unpatched legacy systems will continue to provide easy attack vectors.

Progress in combatting public cyber threats will focus heavily on cloud adoption in 2024. While digital transformation is a focus for government agencies, legacy on-premises systems haunted by unpatched vulnerabilities persist across the public sector.

Transitioning services like email, data storage, and document management to reputable cloud providers will help boost security. Cloud companies may dedicate full teams of cybersecurity experts and employ the most sophisticated tools money can buy. This would provide a substantial upgrade over existing legacy defenses in the resource-poor public sector.

Federal initiatives incentivizing secure cloud migration as well as state-supporting programs like IIJA should assist more small localities, municipalities, community colleges, police departments and public health networks to break away from outdated on-premises systems.

5

Artificial Intelligence (AI) and Machine Learning will be even greater difference-makers.

Along with digital transformation efforts, AI-readiness is a mandate for many public entities. These technologies are pivotal for enhancing cybersecurity measures within the public sector. Trajectories suggest increased focus on leveraging AI and Machine Learning will better enable governments to detect and respond to sophisticated threats.

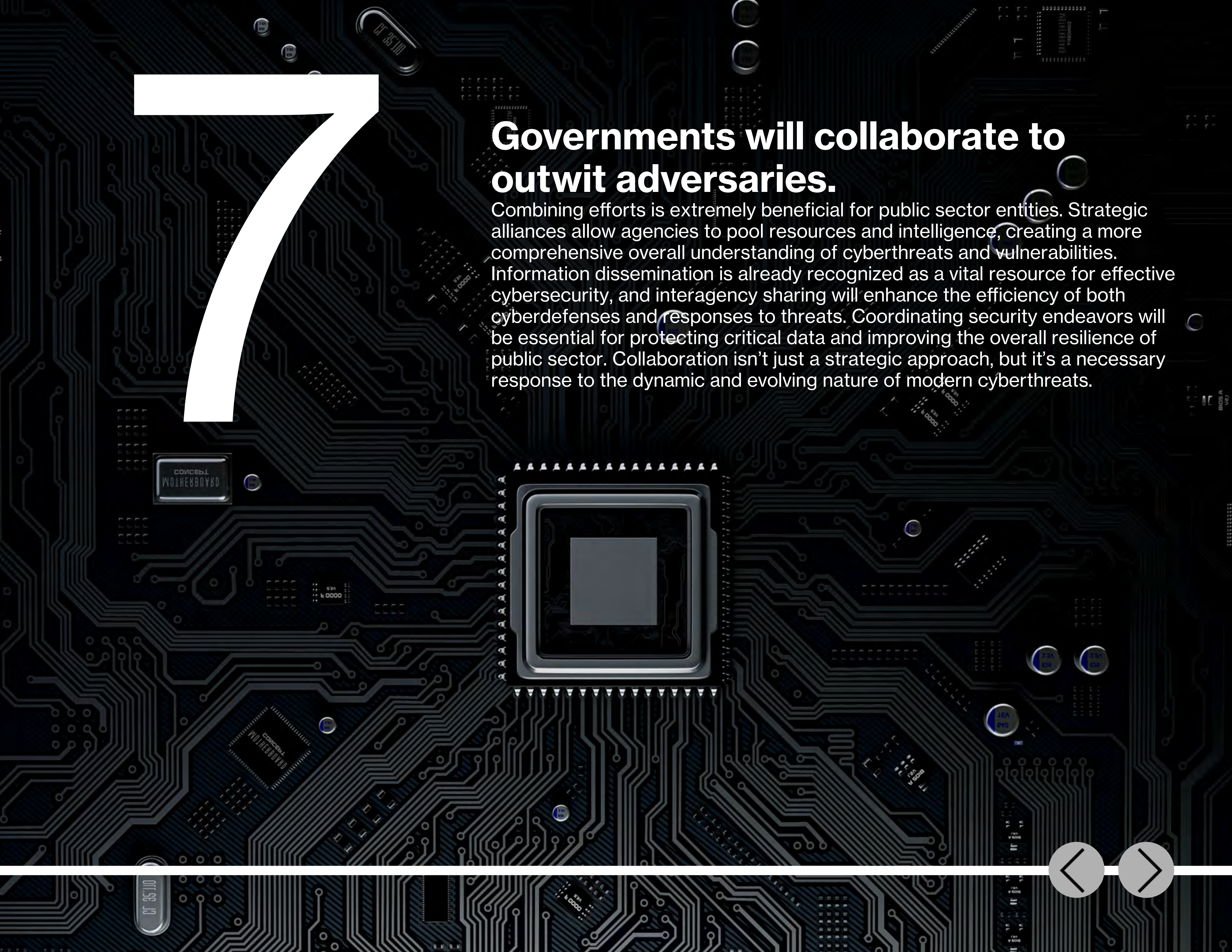
From a staffing standpoint, chief AI officers are rapidly becoming the norm for government bodies. As AI and Machine Learning grow in usage for cybersecurity to automate threat management, seek anomalies, and execute rote log administration, an AI security team will become necessary. In fact, in the next two to four years, it’s likely that at least half of our government agencies will appoint a Chief AI Security Officer to their leadership.

6

Internet of Things (IoT) security becomes paramount.

With the proliferation of IoT and smart technologies, a growing emphasis on enhancing cybersecurity measures around intelligent devices will be necessary. Allied Market Research reports that the global IoT in the public safety marketplace was valued at $11.87 billion in 2019, and is projected to reach $29.68 billion by 2027. The number of IoT devices is expected to reach 30.9 billion by 2025. Every second of every day, 127 new IoT devices go online.

While IoT postures can decrease costs and increase efficiencies for the public sector, the massive growth comes with massive cyberrisks. Each connected device represents an endpoint vulnerability. So as the IoT ecosystem grows, so must efforts around protecting it.



7

Governments will collaborate to outwit adversaries.

Combining efforts is extremely beneficial for public sector entities. Strategic alliances allow agencies to pool resources and intelligence, creating a more comprehensive overall understanding of cyberthreats and vulnerabilities. Information dissemination is already recognized as a vital resource for effective cybersecurity, and interagency sharing will enhance the efficiency of both cyberdefenses and responses to threats. Coordinating security endeavors will be essential for protecting critical data and improving the overall resilience of public sector. Collaboration isn't just a strategic approach, but it's a necessary response to the dynamic and evolving nature of modern cyberthreats.

8

Hacktivism will increase.

With divisive global conflicts like those between Russia/Ukraine and the war over Gaza stirring up emotions in the U.S., cyberattacks focused on issues rather than financial gain are surging. Public sector organizations will probably see enhanced risks from politically motivated adversaries, especially with 2024 being a presidential election year.

Also contributing to hacktivism – escalating capabilities, including tactics around generative AI and weaponized deepfakes, could incite online actions. The anonymity of the internet grants freedom for online protesters to organize disruptions against targets.

9

Remote security measures should expand.

2023 saw several standoffs between leaders and government employees – while the White House ordered federal employees to scale back on telework, the employees resisted. Other levels of government experienced similar struggles with efforts to return workforces to the office. In fact, nearly half of government employees reported they would look for another job if their agencies were to reduce remote and hybrid flexibility, according to a survey from Eagle Hill Consulting.

Nevertheless, hybrid and remote work persist as the norm. Experts from the Future Forum research consortium declared in late 2023 that the “five-day commute is dead.” Though convenient, telework opens up vulnerabilities to cyber risks. With the proliferation of home networks and devices, updated VPNs, multi-factor authentication, the adoption of ZeroTrust practices, endpoint monitoring and access controls are crucial for all endpoints. By proactively strengthening policies and workforce vigilance, cyber resilience can be improved despite the distributed operations.

10

Solutions for State and Local agencies should become more customized.

There is no one “right size” for cybersecurity. While solutions like firewalls and VPNs should be standard, government entities will likely see an increasing need for tailored security frameworks to address their specialized data assets, unique infrastructures and individual staffing organizations. Compared to the federal level, state and local governments operate with tighter budgets and more public-facing infrastructure. These frontline public agencies manage extremely sensitive constituent data across expansive, interconnected systems. Yet their dedicated IT resources are much more limited. A federal agency’s robust and costly cyberdefense architecture simply doesn’t filter downward. Therefore, local governments may continue to follow the best-practices put forward by federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Government Accountability Office (GAO), but state and local organizations will probably be required to increase their efforts around precise, priority-focused cybersecurity custom-built for their particular establishment.

With increased focus and improved technology, 2024 could see government entities better able to mitigate threats, even though the risks are expected to amplify. Budget and personnel shortages mean vulnerabilities will persist as hackers grow more sophisticated. AI and Machine Learning solutions may help bridge staffing and budget gaps and migration to cloud platforms should help, but proactive planning will be needed for 2024 to stem the tide of threats against public sector.

Why Verizon:

As an award-winning leader in cybersecurity, Verizon keeps up with the rapidly changing nature of cyberthreats by processing billions of security events every year. We continually analyze evolving threats at our global security operations centers, performing forensic investigations for companies around the world and sharing our knowledge through industry-recognized collateral like the Data Breach Investigations Report (DBIR).

We differ from other security service providers because our substantial risk and incident experience allows us to understand real-world threats and vulnerabilities faced by public sector and other industries across the globe. Our years of practical experience in developing and implementing security programs across all verticals demonstrates our priority for long-term success in the cybersecurity space.

Learn more about Verizon solutions for public sector and IT security at verizon.com/business/solutions/public-sector.

verizon