SPOTLIGHT

Sponsored by: Proofpoint

Improving state and local government cybersecurity posture starts with technology that supports the government workforce. Sophisticated targeting of government employees means that a protected employee is one of the best cyberdefenses.

Protecting Against Identity-Based Attacks in State and Local Governments

October 2023

Written by: Ruthbea Yesner, Vice President, Government Insights, Education and Smart Cities and Communities

An Environment of Constant Cyberthreats with High Stakes

Cybersecurity has been and continues to be a top priority for state and local governments in the United States, and with good reason. Cybersecurity incidents from malware, phishing, and ransomware continue to grow in state and local governments, and news of major public sector breaches continues to be reported with regularity. Globally, 57% of government organizations reported a ransomware attack in 2022, which is a similar number to the 56% of U.S. state and local governments that reported being a victim of an attack and/or being under constant attack.

The consequences of a successful cyberattack are severe and the stakes are high. In detail:

- **Public or confidential data is taken.** Among governments around the world, the 78% that experienced an attack had data exfiltrated that was public or confidential, and 21% of this data was considered valuable, sensitive. and/or secret data.
- **The cost of ransomware can be significant.** The average ransom paid by governments is approximately $185,000, which is a nonnegligible amount, especially in the context of more modest state and local government budgets.
- **Data exfiltrated may not be fully recovered.** One-third of organizations that pay the ransom do not fully recover exfiltrated data.

AT A GLANCE

KEY STATS

According to IDC's *2022 Government Buyer Intelligence Survey* of 986 U.S. state and local respondents:

- 56% of respondents have been the victim of an attack or reported "being under constant attack."
- 67% are researching or in the process of implementing email security, but only 20% have a solution in production enterprisewide.

KEY TAKEAWAY

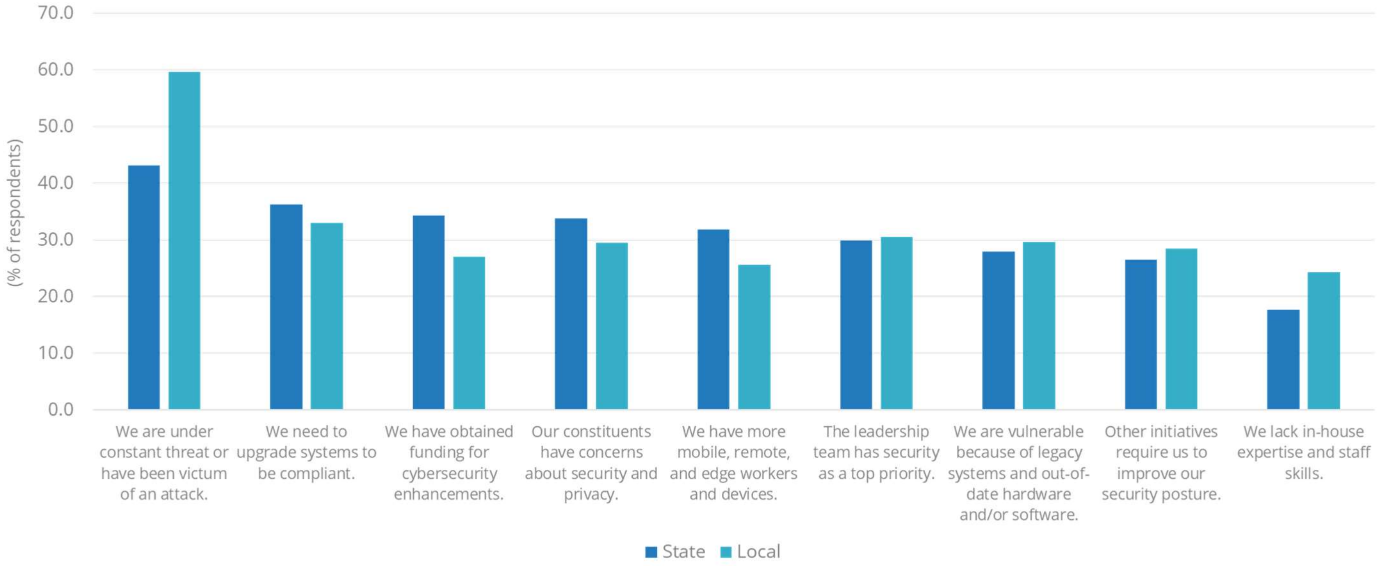
State and local governments in the United States are concerned about cyberattacks and the threat of malware and ransomware. The number 1 cybersecurity investment priority is to reduce the risk of ransomware/malware attacks (e.g., prediction, early detection, prevention).

A major cybersecurity threat is vulnerable employees. Employees let malware in — via email or texts/SMS — by way of an attachment or link. An IDC survey from March 2023 showed that the most significant sources of initial compromise for ransomware incidents in governments were an employee opening a malicious attachment in a phishing email (28% of respondents) or clicking on a malicious URL in a phishing email (18% of respondents). While networks, systems, and applications have become more secure, the following government workforce trends have been a major factor affecting cybersecurity posture for state and local governments in the United States:

- **Staffing issues such as staff shortages and hybrid and remote work** mean that employees may be burnt out, managing multiple roles, or distracted, and many may lack the skills or training around cyberawareness. Figure 1 shows that one-third of U.S. state and local government organizations are investing in cybersecurity because of the lack of in-house expertise and staff skills. Hybrid work also means that employees may work, at times, in isolation where they don't have easy access to check in with other employees if they are unsure of content.
- **Lack of automation and updated tools** means that manual processes, or siloed and fragmented processes, add to a lack of awareness when a breach occurs. In addition, few U.S. state and local organizations report having enterprisewide, unified sets of tools or processes that protect identities and access to systems.
- **Increased use of social media** is another set of data that bad actors can use to determine vulnerabilities. Just as someone may look to see who is posting online while on a vacation in order to burglarize their home, this data can also be used to assume an identity of someone not in the office.
- **Technical debt** — which includes legacy systems, out-of-date hardware or software, and highly customized systems — is also a major factor in introducing risks into IT systems.

FIGURE 1: ***U.S. State and Local Government Cybersecurity Investment Drivers***

Q ***What are the primary drivers of your organization's cybersecurity investments?***



n = 986

Source: IDC's U.S. Government Buyer Intelligence Survey, 2022

It's not easy to keep up with the increasing sophistication of bad actors as they exploit vulnerabilities in government employees, such as timing malware when employees are more distracted or busy during weather events or emergencies. And once malicious software is in, it can go unnoticed or be hard to find or remove. The first cybergoal of any government organization is to keep bad actors out of government systems. The second cybergoal is to quickly identify any breach and work fast to resolve it. Investment in identity threat detection and response technology for identity threat defense (ITD) is essential to reduce the risk and burdens (i.e., free up resources) on the workforce, protect valuable data, and improve community trust.

Common Terms and Definitions

As the variety and sophistication of cybercrime increases, new terms describing actions are created:

- **Technical debt** is the residual cost of technology tasks left undone — in the race to be agile or innovative or from a lack of funding or carelessness — which constrains the ability to innovate and sustain IT operations and adds risk, operational inefficiencies, and cost.
- **Malware** is software designed for nefarious purposes, including ransomware and cryptominers, which can be spread to users.
- **Ransomware** is malware that is specifically designed to hold devices, data sets, or infrastructure hostage by encrypting information or operating systems and threatening to destroy the data, sell it, and so forth if the target doesn't pay up. Ransomware can be downloaded via email or from malicious sites, among other places.
- **Spam** refers to the unsolicited messages that inundate inboxes in an effort to create chaos or infiltrate an organization. With spam messages, attackers are relying on volume to deliver unwanted content to the broadest audience possible and will often include payloads such as unwanted or objectionable content, social engineering, or even malware.
- **Phishing** is an attempt at social engineering designed to mimic something or someone that the target trusts, such as a boss or website, to ask an end user to put in ID credentials or trigger a link to a malicious site or file. With phishing, cyberattackers have crafted these messages to appear legitimate but typically include malicious links or code that could compromise the security of a device, account, or data. Moreover, the term *spear phishing* refers to targeted phishing and the term *whaling* refers to targeting executives.
- **Social engineering attacks** include spear phishing (i.e., phishing attacks targeted and tailored to specific individuals), fraud, impersonation, extortion, and other tactics. Extensive social engineering campaigns — called business email compromise (BEC) — employs a combination of these tactics, including account takeover, grooming, manipulation, and the use of email in an attempt to defraud an organization.

The Importance of Identity Threat Defense as Identity-Based Attacks Rise

What Is Identity Threat Defense?

ITD is a discipline, beyond a class or category of security tools, that combines security tools, processes, and best practices to protect identities. It spans the entire life cycle of the attack — before, during, and after an attack. Preventative and detection capabilities offer a comprehensive solution for threat detection. Attractive deception targets can be deployed to draw a bad actor away from real targets, thus creating bottlenecks that make traversing the network more difficult. When a compromise is detected by ITD — whether from internal or external sources — remediation is initiated via actionable recommendations and alerts and is monitored by dashboards.

Anatomy of an Identity Threat Attack

To build a robust identity threat defense strategy, it is important to understand the fundamental steps in an identity threat attack:

- Discover credentials. Bad actors employ a number of approaches to steal users' credentials including social engineering, compromising Active Directory, and buying credentials on the dark web through access brokers.
- Breach the identity perimeter.
- Compromise credentials, and impersonate legitimate users.
- Escalate privileges.
- Move laterally to more valuable targets.
- Exfiltrate data, or do other damage.

Identity threat defense helps prevent initial attacks, breaches, or breach-like activities by identifying the users most susceptible to phishing emails, keeping emails secure, and providing continuous monitoring and updates so that if there is a breach, government organizations can be aware and respond as quickly as possible.

The Existing Situation in State and Local Governments Increases Susceptibility

There are major developments in recent years in state and local governments that contribute to the challenges around cybersecurity. Many of them also point to the need for an identity-based approach to threat defense. The foundation of vulnerability is people led, both in terms of staff that are overly busy coping with staff shortages and in terms of fragile, outdated systems that make work less efficient — thus leaving less time for cyberawareness training and leaving workers more susceptible to increasingly sophisticated bad actors and phishing schemes.

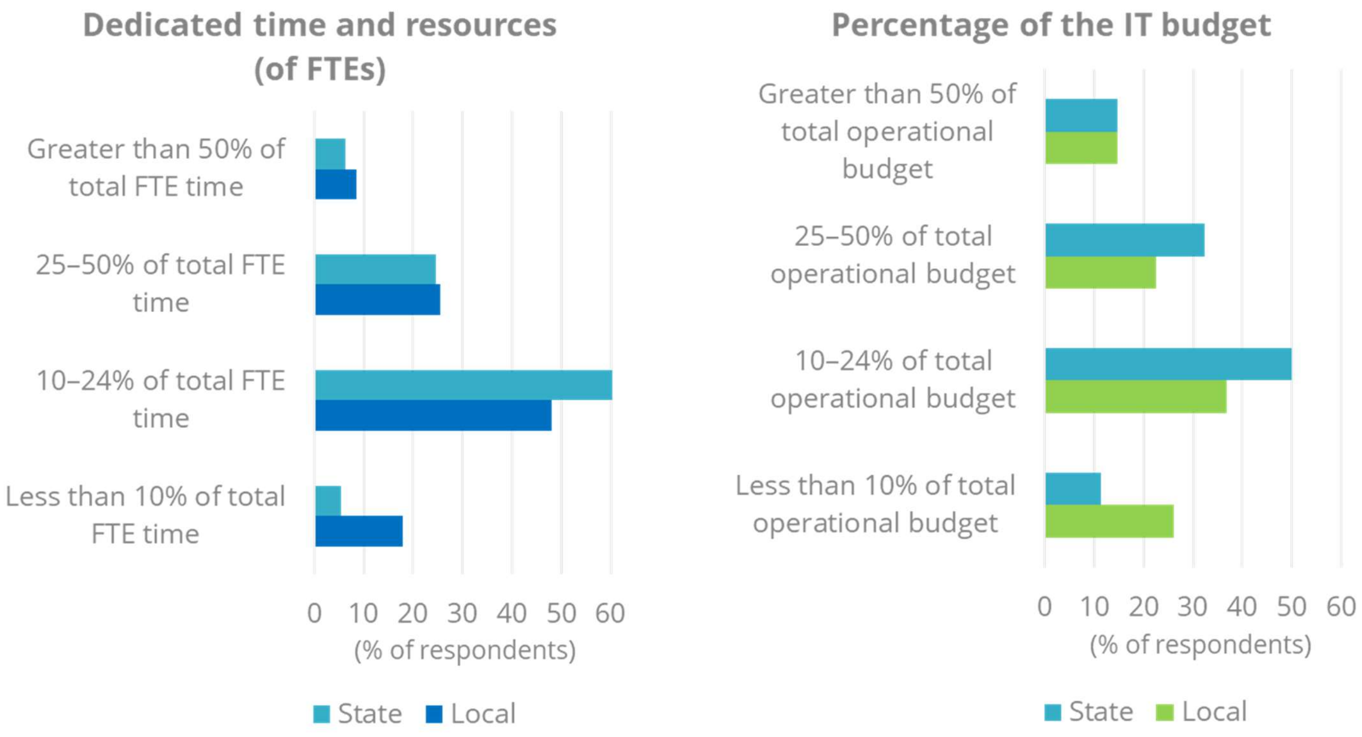
Technical debt introduces vulnerabilities and makes it harder for organizations to respond to cyberthreats. It is the cost of maintaining aging software and systems, particularly those that have been customized or patched or have added manual processes because of age or to provide a function beyond the original intent.

In state and local governments that have a lot of legacy software, custom-developed software, or highly customized software, technical debt often means that developers create a workaround or add in custom code to try to get functionality out of an application that is beyond its original design or intention. Due to a lack of resources — such as staff skills, staff time, budget, and time to develop — state and local organizations cannot redesign or completely rearchitect systems and software to meet new requirements. So they create workarounds on top of workarounds that ultimately create fragility, a lack of interoperability, manual processes, and security risks and that result in more internal and external help desk tickets and other "debt services." Technical debt results in unfunded liabilities that inhibit state and local governments' ability to maintain normal operations, innovate, scale, and transform.

U.S. state and local government organizations are dedicating tremendous staff and budget resources to deal with cybersecurity threats. This puts undue pressure on existing staff and is an inefficient use of funds. The amount of resources that technical debt consumes makes a compelling business case for investing in a current ITD solution. As shown in Figure 2, for most U.S. state and local governments, technical debt related to cybersecurity is taking up 10-24% of staff time and the IT budget. Moreover, almost 3 in 4 organizations use 10-50% of FTE time to service debt. Figure 2 also shows that state organizations use more of total operational budget on debt, and the impact can be medium or high. Ultimately, technical debt introduces vulnerabilities and makes it harder for organizations to respond to cyberthreats.

FIGURE 2: ***U.S. State and Local Government Cybersecurity Technical Debt***

Q ***How much estimated time, budget, and resources does technical debt related to cybersecurity require from your organization?***



n = 782

Source: IDC's U.S. Government Buyer Intelligence Survey, 2022

Workforce challenges also increase the burden on IT staff. When asked about the workforce strategy related to cybersecurity, 48% of state and local organizations implement more cybersecurity training for employees and 43% train IT staff to acquire more cyberskills, demonstrating the challenges centered around employee risk related to cybersecurity. Workforce challenges include the following:

- Staff vacancies means that existing staff are covering multiple roles.
- Hiring under existing requirements makes finding employees a challenge, and onboarding employees can take several months.
- Training can be overly generic and not created using people-centric design principles that ensure that training formats and materials align with specific types of work and workflows and key vulnerability areas. Training that doesn't align with work needs can become a must-do item to check off rather than provide high-value new skills.
- Remote and hybrid work expand vulnerabilities, for example, when employees use personal devices without government cyberprotections.

Thwarting Identity Attacks

Desired Outcomes

The top desired outcomes for U.S. state and local government cybersecurity investments, in order of priority, according to IDC's *Government Buyer Intelligence Survey* are:

1. Reduced risk of ransomware/malware attacks (e.g., prediction, early detection, and prevention)
2. Maintaining uptime/integrity of mission-critical applications/infrastructure
3. Improved trust in public services and technology
4. Faster response times to incidents
5. Protecting constituent privacy

As discussed previously, reducing the risk of ransomware and malware attacks is essential, given the high stakes of a breach. Ransomware or malware attacks also impact the other four priorities listed. To meet these outcomes, governments must not only reduce breaches but also ensure that small breaches don't become major enterprisewide events. The main goal is to keep malware out; it's always more difficult to detect and remove than to prevent its entry in the first place. To do this, state and local organizations must consider how ITD provides the following:

- **Protects the new perimeter.** ITD identifies vulnerabilities in identity management systems and mounts a response, in case a breach occurs. Coverage areas include configuration, modeling/anomalies, indicators, and behavioral analytics.
- **Places obstacles to limit or prevent lateral movement.** ITD makes it difficult for bad actors to traverse the network to gain further access and cause more extensive damage, in case they breach the identity parameter.

- **Monitors data handling.** ITD monitors how data is being manipulated by all users to identify anomalies that suggest that data exfiltration is occurring. For example, are files being chopped up into smaller sizes to make them easier to upload to another system or application? Is this user commonly online at this hour to access this IT resource?

Considering Proofpoint

Founded in 2002 by former Netscape CTO Eric Hahn, Proofpoint Inc. is a leading cybersecurity company headquartered in Sunnyvale, California, and serves 8,000+ enterprise customers worldwide. On average, Proofpoint analyzes 2+ billion emails, 26+ billion URLs, and 17+ million attachments per day. Proofpoint also monitors 17+ million cloud accounts per day using advanced artificial intelligence and machine learning to improve their clients' security posture, including people-centric risk.

In December 2022, Proofpoint acquired Illusive Networks, a company that was founded in 2014 by Ofer Israeli and the cybersecurity incubator Team8 and is headquartered in Tel Aviv, Israel. Illusive's identity risk management products provide prevention, detection, and response capabilities.

Challenges

Proofpoint and its customers face many challenges in protecting state and local government organizations against cyberthreats. At the same time, these challenges present opportunities for government organizations to make the case to invest in a partner, such as Proofpoint, that has strong state and local government experience and a broad product portfolio. Challenges that need to be continuously addressed include the following:

- Cybercriminals are constantly evolving their craft to exploit new vulnerabilities.
- Identity-based attacks are on the rise.
- Heightened demand for security products and professionals means that the government has a skills and staff shortage in cybersecurity.

Conclusion

IDC believes that identity-based attacks on U.S. state and local governments will continue to be pervasive and ongoing. State and local governments are up against national foreign actors that have vast resources to maintain a constant threat level. State and local governments need to provide the necessary solutions — including frequent employee training and investments in cybersecurity automation tools — to reduce identity threats, reduce technical debt, and protect the staff (and by extension the public) from constant cyber-risk. Identity threat defense offers a key set of security tools, processes, and best practices to protect identities, prevent and detect threats, and provide immediate remediation in cases of a compromise. It should be considered as a solution for U.S. state and local governments as they work to improve their cyberposture.

State and local governments need to provide the necessary solutions, including frequent employee training and investments in cybersecurity automation tools, to reduce identity threats.

About the Analyst

Ruthbea Yesner, *Vice President, Government Insights, Education and Smart Cities and Communities*

Ruthbea Yesner is the Vice President of Government Insights at IDC. She manages IDC's U.S. Federal Government, Education, and Worldwide Smart Cities and Communities practices. Ms. Yesner's research discusses the strategies and execution of relevant technologies and best practice areas — such as governance, innovation, partnerships, and business models — that are essential for government and education transformation. Ms. Yesner's research includes analytics, artificial intelligence, open data and data exchanges, digital twins, the Internet of Things, cloud computing, and mobile solutions in the areas of economic development and civic engagement, urban planning and administration, smart campus, transportation, and energy and infrastructure.

MESSAGE FROM THE SPONSOR

About Proofpoint, Inc.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.