SPOTLIGHT
Sponsored by: Proofpoint

This Spotlight Paper highlights the importance of a human-centric cybersecurity strategy in government agencies, focusing on workforce empowerment and security awareness to mitigate risks and enhance organizational resilience.

Building a Human-Centric Security Program in State and Local Governments

April 2024

Written by: Aaron Walker, Research Manager, Government Trust and Resiliency Strategy

Introduction

Human error has long been the preferred weak spot for cybercriminals to attack. As the threat landscape evolves, attacks increase in sophistication, and the attack surface expands, organizations should shift their focus to empowering and securing workforce identity. This will help in addressing immediate risks and foster a proactive culture of security awareness and resilience. These weak spots may come from an unaware employee falling victim to phishing or a novice developer using code possessing a known vulnerability. Despite advancements in security technologies, attacks that rely on human error are increasingly targeting government organizations.

Malware attacks on state, local, tribal, and territorial government organizations rose by 148% from 2022 to 2023, according to the *Nationwide Cybersecurity Review* published in 2024 by the Center for Internet Security with help from the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers. In that same period, the report also documented a 313% increase in endpoint security incidents within government organizations, including data breaches, unauthorized access, and insider threats.

Current Situation, Attack Surface, and Risks

State and local government agencies must address the challenges that legacy technology, skills shortages, and budgetary constraints pose by investing in modern security solutions and fostering a culture that values continuous learning and adaptation to evolving cyberthreats. Human-centric security programs offer direct benefits, such as improved staff security awareness and reduced organizational risk, by educating employees on digital threats and implementing secure daily practices.

AT A GLANCE

KEY STATS

State and local government endpoint incidents increased by 313% in 2023, according to the Center for Internet Security. IDC's March 2023 *Future Enterprise Resiliency and Spending Survey, Wave 2,* found that:

- 45.8% of government-targeted ransomware is delivered via phishing email links and attachments.
- 34.4% of ransomware incidents in government saw the exfiltration of valuable sensitive or secret data.

KEY TAKEAWAYS

- Humans remain an organization's most vulnerable resource.
- Governments are a top target for cybercriminals.
- AI is enabling more sophisticated social engineering.

In detail:

- **Legacy technology:** State and local government entities often operate with less staff, fewer resources, and more legacy technology than private sector businesses. Organizations are often reluctant to modernize critical systems if they require staff with new skills and substantial financial investment. As a result, these outdated solutions and devices are full of vulnerabilities, increasing the organization's risk of falling victim to a cyberattack.
- **Skills shortages:** Globally, skilled cybersecurity staff is in short supply. For state and local government agencies that cannot afford to pay the high salaries that tech giants can, this shortage cuts even deeper.
- **Funding resources:** States and cities have numerous budgetary factors that significantly differ from private enterprises. State and local governments can be more easily influenced by economic uncertainty and political influence. Uncertainty and outside influence can complicate budget ownership and slow down acquisition processes, limiting the impact of organizational attempts to meet citizen needs while empowering numerous departments.

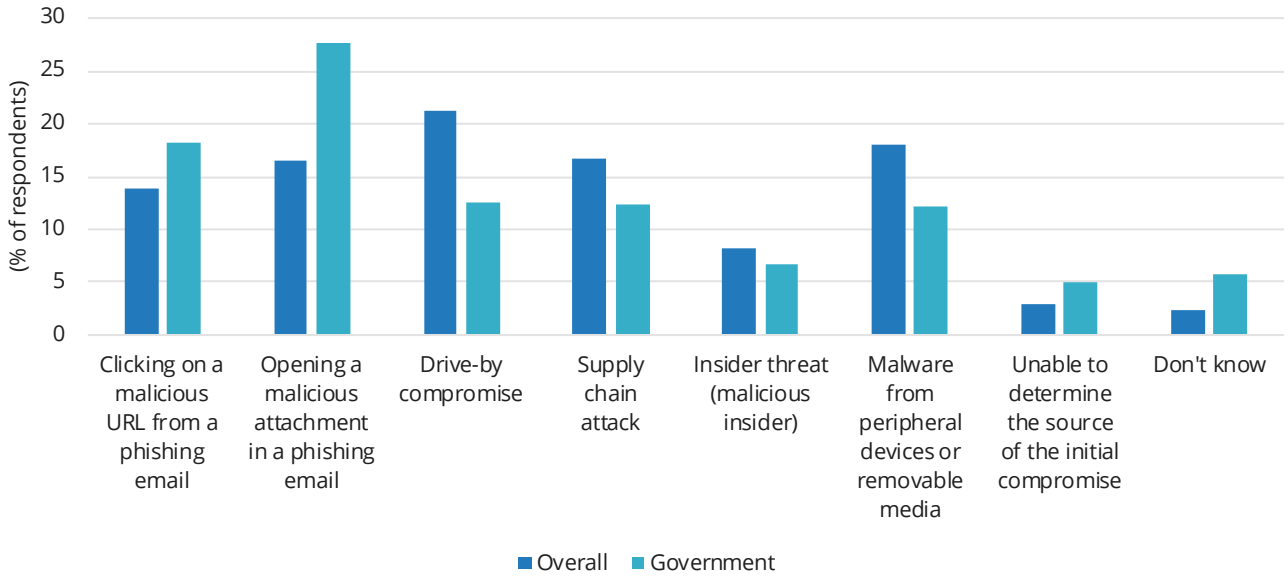
Consequences of an Attack

There are many forms of cyberattacks and many different consequences depending on the attacker's motives, techniques, and targets. Some attacks are more preventable than others, specifically those that result from mistakes made by individuals. These are typically in the form of phishing, business email compromise (BEC), and weak passwords, to name a few. Despite the increased adoption of security awareness tools that help identify risky behaviors and prevent employees from committing them, attacks continue to rise.

Ransomware, for example, is one of the most common attacks impacting government organizations. More than two-thirds (68.2%) of government organizations have experienced a ransomware attack, according to IDC's March 2023 *Future Enterprise Resiliency and Spending Survey, Wave 2*. These attacks result from infecting an organization through social engineering to lock down devices and networks after infecting a computing environment. According to the same survey, 45.8% of ransomware attacks in government organizations came from employees receiving phishing emails and clicking a malicious link or opening a malicious attachment (see Figure 1). While 46.5% of those organizations attempted to pay the ransom, only about one-third of those that paid were able to fully decrypt their compromised files and systems.

FIGURE 1: ***U.S. Government Ransomware Attack Vectors***

Q ***For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of the initial compromise?***



n = 577

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 2, March 2023

A successful attack has other consequences as well.

- **Financial:** In terms of the financial consequences of cybercriminal fraud and theft, BEC alone accounted for over $2.7 billion in losses in 2022, according to the FBI, a number that is sure to rise when accounting for 2023 attacks. Phishing, ransomware, and spoofing add nearly $200 million in losses to that total.
- **Regulatory:** Regulatory penalties can also impact finances in the form of fines for failing to protect against or disclose cyberincidents. Fines can vary from tens of thousands to tens of millions of dollars depending on the scope of the breach and the sensitivity of the exposed data. Other consequences can include litigation. Public sector organizations may open themselves up to private and class-action lawsuits if the cyberincident impacts citizens on a large enough scale.
- **Organizational:** Organizational impacts come in many forms. Skilled cybersecurity staff may become less productive because they must spend more time remediating and investigating the incident. Leaders such as CISOs and CSOs or team managers responsible for the incident may lose their jobs if found personally responsible. Breaches may also result in downgraded credit, increased premiums, and operational disruption.
- **Reputational:** Reputational consequences typically arise in the form of public perception and a loss of trust. Attacks may impact the delivery of services to constituents and have dire consequences if individuals cannot receive the

care or assistance they need. Breaches often result in the exposure of citizen data for use by cybercriminals, which many citizens will blame on the organization that exposed their data.

Common Terms and Definitions

- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** DMARC is an email validation system designed to detect and prevent email-borne threats by authenticating using the instructions the domain administrator sets. DMARC can help combat spoofing, BEC, phishing, and other messaging threats.
- **Phishing:** Phishing emails can inundate inboxes with unsolicited messages, hoping to create chaos and/or infiltrate a business. These emails include messages designed to appear legitimate but that typically include malicious links or code that could compromise the security of a device, account, or data.
- **Social engineering:** These attacks include spear phishing, a targeted form of phishing tailored to specific individuals, and tactics relying on human interaction to commit fraud, impersonate individuals, and/or extort their target.
- **BEC:** BEC refers to extensive social engineering campaigns that employ a combination of social engineering tactics, including impersonation, account takeover, grooming, manipulation, and fraud to defraud organizations and expose them to significant financial loss.
- **Telephone-oriented attack delivery (TOAD):** TOAD attacks are a form of social engineering that encourages the target to call a telephone helpline. The victim will believe they are speaking with customer service when they are actually talking to a cybercriminal. The attacker can then encourage the target to provide them with remote access and install malware.

Benefits of Human-Centric Security Programs

The most direct benefits of human-centric security solutions are employee awareness of digital threats and the implementation of safe, secure daily activities. Reducing risky actions taken can be a key metric to implement across the organization. Regardless of whether the organization has adopted a new technology or whether employees are in the process of security awareness training, it reduces employees' likelihood of committing risky acts such as engaging with malicious links, sites, and files. This, in turn, reduces the overall risk throughout the organization.

While careless employees put organizational data at risk, skilled staff who control critical systems and infrastructure have an even greater responsibility to minimize risk. Teams managing IT, security, and development projects control some of the most vulnerable digital assets of an organization. Developers need training to avoid pushing flawed code; security teams need education on the latest, most secure operational processes; and IT staff need to understand security policies, patching, monitoring, and maintenance.

Leaders bear some of the greatest responsibility for championing a culture of security. They also face some of the greatest consequences when failing to practice what they preach. Depending on the organization, certain leaders can be found liable for cybersecurity incidents, even if they had no direct participation in the incident. Organizational leaders are responsible for developing policies that encourage secure behaviors and providing employees with the tools they need to develop and maintain modern security programs.

Desired Outcomes of Human-Centric Security Solutions

- Reduced risk
- Improved security awareness of staff
- Increased uptime
- Improved trust

Trends in Email Security

Organizations should be aware of the following trends in email security:

- **Interactive training:** Interactive security awareness training tools are emerging to provide employees with more realistic simulated threats. These tools integrate with an employee's day-to-day SaaS tools to automate simulated threat delivery within the environment most familiar to them. They have emerged after decades of security analysis tool solutions based on generic training videos and documents and without a visual representation within a familiar environment.
- **Data privacy platforms:** After the passing of GDPR in the European Union and the rise of privacy legislation in the United States, data privacy solutions will be necessary to properly govern the collection, storage, and use of sensitive and personally identifiable information. These regulations include terms that require the maintenance of email consent compliance, such as providing options to unsubscribe, getting positive opt in, and keeping consent evidence.
- **Generative AI (GenAI) risks and protections:** The expanding digital attack surface and critical infrastructure targets make cybersecurity management difficult because they add thousands of new internet-enabled endpoints and connections to secure. GenAI can help hackers generate personalized phishing emails, crack passwords, and poison open source code. However, GenAI-powered solutions also can improve reporting, standardize playbooks, and bolster security rule effectiveness. AI analytics will improve security monitoring, risk analysis, and time to respond.

By 2026, cyberattacks and crimes caused by weaponized GenAI will impact 90% of local and regional governments, driving the adoption of new human-centered cybersecurity and public safety approaches, according to *IDC FutureScape: Worldwide National Government 2024 Predictions* (IDC #US50296223, October 2023).

Considering Proofpoint

Founded in 2002, Proofpoint Inc. is a leading human-centric cybersecurity company serving more than 510,000 customers worldwide. On average, Proofpoint reports that it scans and analyzes 3.1 trillion emails, 21 trillion URLs, and 0.8 trillion attachments and monitors 45 million cloud accounts for takeover detection per year using advanced AI and ML. It uses these insights to improve its clients' security posture.

Proofpoint offers end-to-end email protection across the entire predelivery, click time, and postdelivery email attack chain. Its core email security packages include advanced AI-based predelivery detection and comprehensive protection powered by NexusAI, Proofpoint's proprietary AI engine built on trillions of data points, capable of stopping various payloadless social engineering threats like advanced email fraud and malicious links. In addition, Proofpoint offers adaptive email security with behavioral AI defense postdelivery to counter targeted threats like internal phishing, specifically for high-risk employees, with seamless API integration with Microsoft 365. Proofpoint organizes its product portfolio into four families: people protection, information protection, human risk mitigation, and premium services. Under people protection, the focus of this Spotlight, are the product packages shown in Figure 1. Each package builds on the company's Core P0/P1 solution and subsequently each other to provide comprehensive protection:

Core P0/P1 delivers essential email threat protection: There are multiple modules within Core P0/P1. Targeted Attack Protection (TAP) detects, analyzes, and blocks advanced email threats involving social engineering such as BEC, phishing emails, malware and ransomware, and spam. Threat Response Auto-Pull works with TAP to protect users from incoming malicious emails. Closed-Loop Email Analysis and Response streamlines the evaluation of emails users report as potentially malicious to an abuse mailbox. People Risk Explorer analyzes and segments the risks that internal and external users pose to identify the users most likely to pose a threat.

Core Plus provides impersonation protection: Impersonation targets can be internal employees or third parties such as customers and suppliers with whom employees would typically communicate but who may have been compromised or spoofed. Email Fraud Defense secures email channels, mitigates email fraud, provides visibility into fraud risks posted by external parties, and simplifies domain-based message authentication, reporting, and conformance (DMARC) authentication. Secure Email Relay protects application-generated email and supports the migration of on-premises email relays to the cloud. Supplier Threat Protection looks for suspicious emails from suppliers and third-party accounts to detect potential phishing, malware, and business email account compromise attacks. Analysis of patterns across Proofpoint's customer base enables alert notification before threat actors launch their email attacks.

Advanced offers adaptive email data loss protection: Building off the capabilities of Core and Core Plus, the Advanced package uses behavioral AI to detect anomalies, prevent email from being delivered to the wrong recipient or the right recipient but with the incorrect email attachment, and detect data infiltration in real time. Email Data Loss Prevention detects sensitive or confidential data within an email so that it can be further tracked and safeguarded. Email Encryption automatically encrypts emails and attachments, thus ensuring more secure email communications. The Advanced package mitigates the risk of data loss at the hands of the careless, compromised, or malicious user.

Complete ensures identity protection: There are two modules in the Complete package. Identity Threat Defense and Response continuously scans for identity threats to stop privilege escalation and lateral movements of threat actors to their ultimate target of extremely sensitive — and lucrative on the dark market — data assets. TAP Account Takeover identifies the diverse types of threats targeting email accounts, including business email compromise, brute-force attacks, and data exfiltration. It automates alerts for them and accelerates email threat investigation and account remediation.

FIGURE 1: ***Four Key Proofpoint Packages for Protecting People***

Source: Proofpoint, 2024

Cloud Email Security Use Cases

Deployed together, Proofpoint's extensive offerings address the following use cases:

Increased prevalence of human social engineering: Threat actors are taking advantage of AI to launch more sophisticated attacks involving human social engineering. They use GenAI to quickly generate phishing emails that mirror the targeted organization's communication style or translate effective phishing emails into other languages to attack targets in other countries. The Core P0/P1 package protects against BEC, ATO, credential theft, and financial fraud attacks.

Increased reliance on third-party vendors: Healthcare organizations are leaning on third-party email services to send emails on their behalf for marketing campaigns, customer support, and other administrative workflows. The Core Plus package protects against vendor email compromise through its Supplier Threat Detection module.

Data loss: Misdirected email by careless users is as much a problem as data exfiltration, if not more so, because users have logged in with legitimate credentials and may be misdirecting email to validated recipients (e.g., wrong customer or colleague). Proofpoint's inaugural edition of its *2024 Data Loss Landscape Report* (January 2024) revealed that more than 70% of respondents across industries identified "careless users" as a cause of their data loss, while fewer than 50% cited technical issues. The Advanced package offers protection against both forms of data loss.

Identity compromise: Active Directory (AD) identities are a common target for theft. Once AD has been compromised, threat actors can use legitimate credentials to move laterally through the network or escalate privileges to gain

access to more sensitive information. The Complete package offers identity threat defense and detection and identifies potential account takeover events.

Challenges

Proofpoint and its customers face many challenges in protecting against cyberthreats. However, 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. There are several challenges that need to be continuously addressed.

- State and local government organizations are a top target for email-based threats, including BEC, ransomware, and TOAD attacks.
- Government organizations can struggle to recruit and maintain skilled security staff, requiring as much security awareness and automation across organizations as possible.
- GenAI is increasing the sophistication of social engineering attacks, making AI-generated email content, photos, voices, and videos more believable.

Conclusion

IDC believes that human-centric security will continue to be important, and to the extent that Proofpoint can address the challenges described in this paper, the company has a significant opportunity for success. Human error remains a considerable vulnerability that phishing or the use of compromised code can exploit, despite advancements in security technologies. As cyberthreats become more sophisticated and the attack surface expands, the focus must shift to securing workforce data and identities through developing human-centric security programs that prioritize employee security awareness and implementing secure practices. Despite the challenges government organizations face in protecting themselves from cyberthreats, this paper views these challenges as opportunities for Proofpoint to demonstrate its expertise and broad product portfolio in addressing the needs of state and local government agencies.

Empowering and educating the workforce is key to fortifying cybersecurity in state and local government organizations against the evolving threat landscape.

About the Analyst

Aaron Walker, *Research Manager, Government Trust and Resiliency Strategy*

Aaron is a research manager for IDC's Government Trust and Resiliency Strategies program. His research focuses on innovations in security, privacy, and resiliency impacting U.S. federal government agencies. His primary focus is analyzing how innovative security and resiliency solutions can help modernize infrastructure and protect data, with the goal of building trust in government institutions by preserving privacy.

MESSAGE FROM THE SPONSOR

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 more than half of the Fortune 1000, rely on Proofpoint for human-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 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