WHITE PAPER

Building a resilient government

The critical roles cybersecurity, AI and workforce development play in keeping government secure

December 2024

LUMEN®

Table of contents

Introduction

In today's rapidly evolving technological landscape, the resilience and adaptability of government operations are more crucial than ever. In fiscal year 2023, federal agencies in the United States reported over 32,000 cybersecurity incidents, marking a 5% increase over the previous year.[1]

This paper examines the essential role of robust cybersecurity measures, the significance of Zero Trust Architecture, the integration of AI in security, and the importance of effective talent management in supporting national security. It underscores the need for a well-prepared security workforce and advanced security frameworks to build a resilient government for the future.

Cybersecurity: the invisible battleground

The convergence of emerging technologies like AI, data management, multi-cloud infrastructures, and quantum computing presents significant security challenges. As a result, cybersecurity stands at the forefront of priorities for government CIOs with federal and state governments listing cybersecurity as their top priority. [2] The complexity of network architectures which are often spread between legacy, on-premise systems and modern cloud infrastructures – exacerbates these challenges and creates significant interoperability and security concerns.

In this landscape, governments face sophisticated cyber threats from nation-states, cybercriminals, and hacktivists, with attacks ranging from espionage and data breaches to ransomware. Protecting critical infrastructure requires robust security measures and thorough resilience planning.

With limited budgets, many agencies are optimizing resources by leveraging AI technology, securing operations, and engaging with third-party Managed Service Providers (MSPs). These strategies aim to address talent shortages and improve the efficiency and effectiveness of government cybersecurity efforts.

Building a comprehensive and robust cybersecurity framework

As the complexity, sophistication and frequency of cyberattacks continue to rise, the need for both state and federal government agencies to enhance their overall security posture with advanced security measures has never been greater. Government agencies should consider implementing a comprehensive cybersecurity framework that will be the foundation underlying all IT initiatives. This framework would have multiple components including implementing Zero Trust and Whole-of-State principles, expanding the use of artificial intelligence to improve secure data management and threat detections, upskilling and empowering their internal teams and engaging in partnerships with a managed service provider that can support agency missions across the entire cybersecurity infrastructure.

86%
of state chief information security officers (CISOs) reported that their responsibilities are growing – 2024 Deloitte-NASCIO cybersecurity study[7]

By adopting these strategies, government agencies can significantly bolster their defenses against cyber threats with protection of sensitive data and the continuity of critical services. In an era where cyber resilience is paramount, a proactive and comprehensive approach to cybersecurity is not just an option, but a necessity. Together, we can build a safer, more secure digital future for all.

> "Cybersecurity is literally the bedrock of any IT framework. IT leaders are treating cybersecurity as their most critical priority. It is superseding any discussion around IT priorities in general"
>
> ***– Vinod Brahmapuram,***
> *Lumen Senior Director of Security Sales, SLED*

Zero Trust architecture

A Zero Trust architecture is a powerful tool in preventing unauthorized access and data breaches, supporting the secure use of modern technologies, and providing better protection for national security and citizen privacy. In 2021, the Biden Administration set a bold mandate with executive order 14208 for federal agencies: adopt a Zero Trust architecture by the end of 2024. This directive is crucial for agencies that handle highly sensitive data. To embrace Zero Trust agencies must shift their security focus from response and mitigation to proactive protection.

Proactive protection operates on the principle of "never trust, always verify". Every user and device, whether inside or outside the network, must be continually authenticated and authorized through a variety of protocols including multi-factor authentication, least privileged access, and role-based access control, will help significantly reduce the risk of unauthorized access.

> "Adopting compre - hensive multi-layered security measures with continuous monitoring, strong access management leveraging benefits of adaptive trust and a strong security culture are crucial for protecting against high-velocity, multi-directional cyberattacks and ensuring digital sovereignty"
>
> – **Vinod Brahmapuram**
> Lumen Senior Director of Security Sales, SLED

55%

Of federal, state and local leaders cite cost as a top concern when implementing Zero Trust. – Market Connections Feb. 2024[5]

In addition, Zero Trust aims to provide 24/7 visibility to data wherever it resides, allowing IT leaders to manage identity risks, optimize data accessibility, and begin to ready their environments for the future. It is also essential for maintaining digital sovereignty and enables the integrity and security of government operations.

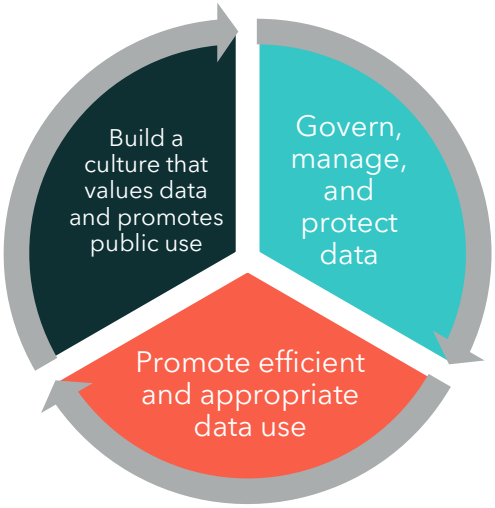
However, agencies must balance this priority with the need to maximize taxpayer value and responsibly allocate their limited resources. When mandates aren't backed with funding, it can create additional challenges. In these situations, partnering with vendors who provide security expertise and flexible management services for complex compliance environments is crucial, as they often offer cost savings, especially at scale.

SLED organizations should aim to follow the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). This framework will assist in enhancing their overall security posture, minimizing potential damage from cyberattacks, and ultimately helping improve citizen trust.

Data security and identity management

These new protections are essential, but there must be a strategy that guides the security of how data can be shared, remain accessible, and be appropriately used to create a data driven government that makes informed decisions, fosters innovation and maintains public trust. An effective data strategy will leverage all data to enhance mission delivery, serve the public and manage resources effectively while providing security, privacy and confidentiality. For federal agencies the "Federal Data strategy" calls for three main categories of practices that focus on culture, governance and appropriate use of data:

Federal Data Strategy – "The Practices"



These practices include establishing robust data governance frameworks, implementing tiered access controls, balancing risk and utility in data sharing and engaging stakeholders throughout the data lifecycle.[8] For SLED organizations, they can protect and secure their data through strategies like strong identity and access management (IAM), regular patching and updates, employee training on cybersecurity best practices, data encryption, periodic security audits, and using unified data management platforms. These measures help ensure data is safeguarded while allowing for secure sharing when necessary.

Identity management is a key particularly for SLED organizations. Robust identity management can be the first step in securing state and local systems. When data is spread across legacy on-premise and cloud systems, effective identity management is crucial. Every identity should be protected with the appropriate level of privilege control to then allow secure access for any identity into their environment from anywhere using any device.

To further mitigate risk, it is imperative to manage non-person traffic (zombie) and overprivileged identities which expand the attack surface. By enforcing the principle of least privilege for all identities and securing sensitive ones, agencies can prevent lateral movement by malicious actors, thereby protecting systems and data from potential attacks. Organizations can also lean into AI as an instrumental tool to effectively manage identities with its capability for speed that far exceeds human capacity. By continuously monitoring behavior patterns, access requests and network activity, AI can help ensure only authorized individuals and devices gain access to sensitive government systems supporting.

However, excessive barriers around data, even for authorized users, can create inefficiencies and degrade the user experience and ultimately negatively affect citizen experiences. That is why implementing strategic data management policies, public sector technology leaders can help ensure secure data sharing, enhance collaboration, protect critical infrastructure, and support the development of a resilient and adaptive government.

Threat detection and response

The importance of robust threat detection and response guidelines and strategies for government agencies cannot be overstated, as they are crucial in safeguarding sensitive information and maintaining national security.

One of the most significant challenges in this vital aspect of cybersecurity lays within the lack of the necessary personnel and tools to effectively manage the high-velocity, multi-directional cyberattacks prevalent today.

> "One of the good things about owning a large global network is that we can see more of what is going on over the Internet than others. We notice patterns as they develop. We can tell where some attacks are coming from even before the customer notices any impact."
>
> – **Jason Schulman**
> Vice President National Sales, Federal

Threat detection and analysis by experienced cybersecurity experts can help. At Lumen, it is the foundation of every Zero Trust and data strategy implemented. The Lumen threat research team, Black Lotus Labs, uses global visibility from the Lumen internet backbone to help agencies fortify their security posture. With complete network visibility, Lumen uses the Rapid Threat Defense platform to monitor 24/7, automate protection and proactively neutralize threats. This involves applying AI and machine learning to network data flows, which allows teams to detect, classify, validate and block bad actors before they strike—and continuously adapt as threat tactics evolve.

Artificial intelligence

IT leaders have witnessed artificial Intelligence emerging as a transformative technology with increasing importance for national security. By leveraging AI, government agencies can help keep constituents safe, healthy and engaged.

When implemented correctly, AI can bolster cyber defenses with adaptive security that continually adjusts to the evolving threat landscape. It can analyze vast amounts of data in real-time to identify potential security threats, automate threat detection, and provide actionable intelligence. AI-driven solutions enhance the ability to prevent, detect, and respond to advanced cyber threats by identifying patterns of malicious activity, predicting potential attack vectors, and automating defensive measures. This enables a robust cybersecurity posture for federal agencies. The speed at which AI executes these functions surpasses human capabilities, saving precious time and potentially preventing costly and dangerous breaches.

But if misused, even the White House agrees, AI could threaten United States national security, bolster authoritarianism worldwide, undermine democratic institutions and processes, facilitate human rights abuses, and weaken the rules-

based international order. Harmful outcomes could occur even without malicious intent if AI systems and processes lack sufficient protections.[3]

> "No one can solve complex problems in isolation. We need to foster a culture of collaboration and innovation across agencies and sectors and leverage the best practices and expertise from different domains"
>
> — **Jason Schulman**
> Vice President National

Public-private partnerships

Public-private partnerships will play a crucial role in the effort to effectively and ethically deploy AI in government. Collaboration between government agencies and private sector entities strengthens cybersecurity defenses through the sharing of threat intelligence and best practice governance. For example, the federal Department of Homeland Security (DHS) has released a set of recommendations for the safe and secure development and deployment of AI in critical infrastructure. This framework was developed in collaboration with private sector industry specialists to provide guidance on how each layer of the AI supply chain can ensure the safe and secure deployment of AI in critical infrastructure.[4]

For SLED agencies, adopting a whole-of-state cybersecurity approach and working with a single vendor for their networking and security needs can be significantly beneficial when developing cybersecurity frameworks that include AI. This approach can pool the strengths of state, local, education, and tribal partners to help improve cyber posture and reduce risk for everyone. It helps IT security leaders align their standards while sharing threat intelligence, best practices, and lessons learned—so organizations at all levels can collectively stay ahead of emerging threats.

Collaboration for success

As we have established, to achieve cybersecurity mission success, public-private partnerships are essential to government agencies. By collaborating with private sector entities, government agencies can tap into a wealth of expertise and resources, significantly enhancing their security posture and closing expertise gaps. These partnerships provide access to advanced technologies, specialized knowledge, and innovative solutions that might not be available within the public sector alone. The most valuable partnerships educate both parties, improving skill sets and provide an environment for learning. Through these relationships with the private sector, government can bridge technology and talent shortages, enhance efficiency and reach their mission to provide a secure national infrastructure that secures all data and processes, creating a formidable defense against cyber threats.

An excellent example of collaboration at work is the Lumen Integration and Enablement Lab, where Lumen co-innovates with industry partners to solve specific IT challenges for government customers. In the Zero Trust Integration Lab, Lumen and partners demonstrate integrated solutions for various scenarios defined by the Defense Information Systems Agency (DISA), including AI, quantum computing, hybrid environments, and inter-agency data sharing. This collaboration helps create proof of concept for future solutions that agencies can apply in their Zero Trust strategies. Lumen leadership also actively participates in the ATARC IT forum and its Zero Trust Working Group, offering expertise while also gaining new knowledge from other members.

Lumen has a very specific approach when partnering with a government agency. The belief is that it is vital to have a holistic view of each customer's requirements. Lumen consultants work closely with agencies from day one to understand their budget, IT environment, risk profile, compliance requirements, organizational goals, and user needs.

This collaborative and transparent process helps ensure agencies play an active role in determining their ideal networking solution. Lumen positions itself as a "side-source" for agency IT teams, working alongside them to identify, train, and educate IT teams so they can control their cybersecurity framework effectively.

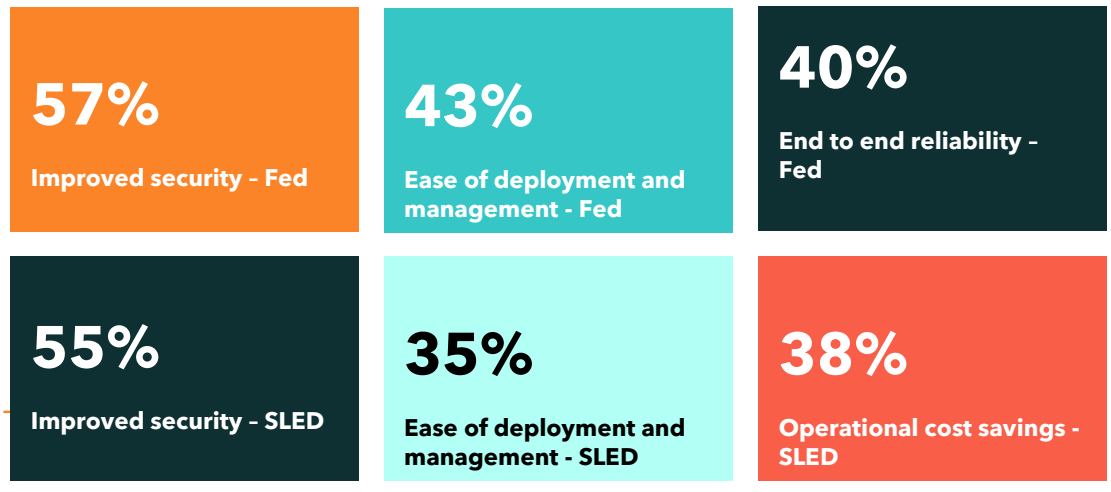
> "Many government customers face challenges in designing, implementing, and managing various capabilities. That is where we step in to deliver managed services and alleviate the burden on government agencies. Lumen not only has the dedicated people and qualifications to support agencies, but we also have the critical element—the network—that underlies everything. Everything rides on the network." — Jason Schulman, Lumen National Vice President Sales, Federal

For agencies requiring more intensive and ongoing guidance, Lumen's professional services team can help transition to a managed environment smoothly. With Lumen® Managed Network Services, agencies have full-time access to a dedicated team of Lumen experts who provide 24/7/365 network management.

This support helps agencies simplify and secure their operations, allowing them to focus on other areas of their mission.

Figure 1

The business benefits cited by respondents of choosing an integrated connectivity and technology services from a single communications provider*



Talent Management: the human element

Sourcing highly skilled, dedicated talent is a challenge for every sector but currently the public sector is grappling with a significant shortage of skilled cybersecurity professionals. According to the World Economic Forum, 52% of public organizations cite a lack of resources and skills as their biggest challenge when designing cyber resilience.[6] This talent gap is further widened by an aging workforce proficient in legacy systems and the difficulty in attracting younger talent, who are often lured by the commercial sector's higher salaries and modern office environments.

Managing large-scale, complex datasets and maintaining productivity with limited staff are ongoing hurdles. Additionally, the swift pace of technological and security changes demands continuous upskilling. These factors collectively create a challenging environment for government agencies to effectively manage their cybersecurity and IT workforce needs.

The perception that the government is behind the times due to its reliance on legacy technology persists. However, understanding that government agencies are partnering with private sector companies who are providing agencies with cutting edge technology can offer an attractive enhancement to procuring talent.

Public sector agencies struggle to implement digital transformation. Private sector IT partners with the right expertise can help close the gaps.

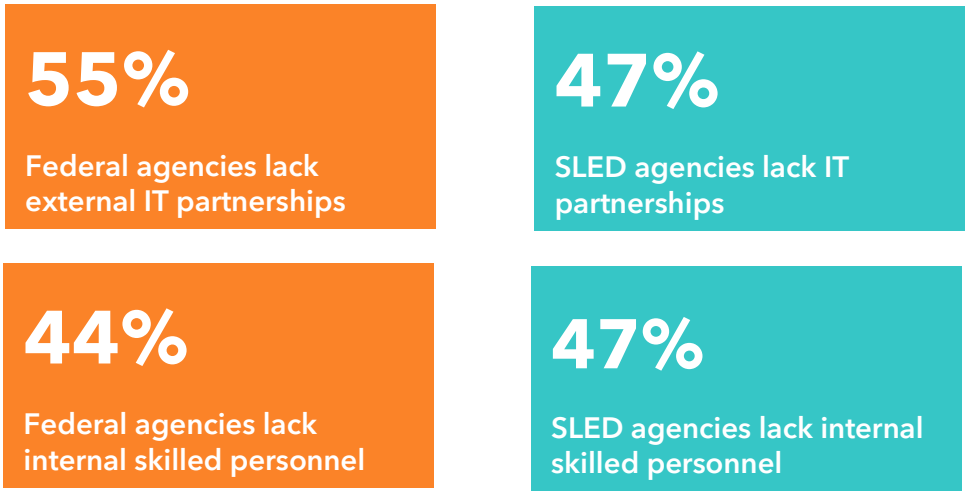


Figure 2

The percentage of respondents who reported difficulties in implementing digital transformation due to a shortage of skilled personnel, both internally and externally*

*Fed Gov: (n≈102) Public Sector (SLED/Higher Ed n≈113. IDC Resource Map for Lumen, sponsored by Lumen, doc US52124324, May 2024

Upskilling: education and partner support are key

Upskilling is an ideal avenue for supporting agency workforces. There are several strategies agencies have at their disposal. By incorporating education and training programs, organizations can raise awareness and foster a cybersecurity culture within their digitally focused environments. Job satisfaction and retention can be significantly improved through continuous learning, skills training, and opportunities to implement cutting-edge technology and innovate new programs.

As a single communications provider, Lumen can play a pivotal role in this process. By providing opportunities to work with advanced technologies that automate tedious tasks through AI frameworks, Lumen can help make daily work more efficient and flexible, boosting morale and even potentially attracting talent. The balanced AI and automation solutions Lumen provides enhance productivity without overwhelming human workers, and can help close talent shortages and gaps, especially in understanding and deploying AI and older systems.

By being able to offer robust cloud orchestration tools and pay-as-you-go network models, Lumen enhances control over workload deployments, to help improve and simplify governance and reporting. The intuitive and intelligent data protection solutions Lumen has built directly into the network, provide continuous monitoring and immediate defenses, minimizing compliance risks and bolstering security, to help ease employee stress over managing these tasks.

Empowering employees to further their training and education and encouraging them to use that knowledge within their teams helps build a culture of continuous improvement. This is particularly impactful in government work, where the mission often involves protecting national security and public safety. Offering extensive training and development opportunities, such as certifications and advanced degrees, enables employees to grow their skills and advance their careers.

Additionally, Lumen's experience with remote work can help government agencies offer flexible, secure work arrangements, which can be a significant draw for younger talent seeking work-life balance. By adapting hybrid work environments and offering alternative workplace solutions, including remote and hybrid work models using cloud-distributed tools and AI technology, along with flexible schedules, and project/task autonomy, can make government roles more appealing.

Conclusion

Building a resilient government is not just about implementing the latest cybersecurity measures; it's about creating a culture that values and prioritizes security and talent, and a framework that has cybersecurity and a Zero Trust architecture as its foundation. As we navigate the complexities of the digital age, the integration of advanced security frameworks like Zero Trust and AI-driven defenses becomes crucial. But equally important is our approach to data integrity and talent management. By fostering a culture of continuous learning and collaboration, we can attract and retain the best minds in the field. Public-private partnerships, like those between Lumen and the DoD and DISA, along with innovative technologies will play a pivotal role in this journey. Together, these efforts can help us safeguard

critical infrastructure, ensure efficient service delivery, and build a government that is not only secure but resilient and adaptive to future challenges. The proactive steps outlined in this document are the Lumen roadmap to achieving this vision.

To learn how to partner with Lumen to further enhance your agency's cybersecurity posture and workforce development, we invite you to explore Lumen's comprehensive suite of public sector solutions. Visit our website to learn more about how we can support your mission and help you build a resilient government. Contact us today to schedule a consultation and discover how our expertise can drive your agency's success, call us today at **800 871 9244 or visit us online**.

Footnote(s)/Disclaimer(s)

1. Statista.com, Cyber Crime & Security, Oct. 2024
2. Government Technology, "2024, SLED IT Spending Takes a Whole-of-State Focus", B. Harris, Feb. 2024.
3. Memorandum on Advancing the United States' Leadership in Artificial Intelligence, Oct. 2024
4. Groundbreaking Framework for the Safe & Secure Deployment of AI in Critical Infrastructure, Dept. Homeland Security, Nov. 2024
5. Navigating challenges and seizing opportunities. the state of zero trust in federal, state and local government, February 2024
6. World Economic Forum; State of Cybersecurity 2023, ISACA; A Closer Look at the Cyber Talent Gap, Trellix
7. Deloitte & NASCIO, 2024 Deloitte-NASCIO Cybersecurity Study
8. Federal Data Strategy, Federal government, 2018

Why Lumen?

Lumen connects the world. We are a trusted partner for public sector agencies seeking to modernize their technology ecosystems to provide outstanding citizen experiences. Our expertise in procurement processes helps agencies navigate government contract vehicles with ease. With our help, agencies can transform their technology, provide excellent service experiences for citizens, and accomplish their missions time and again.

866-352-0291 I lumen.com I info@lumen.com