PRESIDIO FEDERAL | IBM Gold Partner

TD SYNNEX Public Sector | IBM Distributor

Adapting Federal IT: Insights from 2023, Roadmap for 2024

The holiday season is officially over and the New Year has been ushered in, which means government IT departments are preparing their networks for a slew of federal cybersecurity mandates that must be met in 2024. But as they do so, they must take a moment to look back and reflect on 2023 and evaluate the successes, challenges, and lessons learned surrounding their cybersecurity infrastructures and the ever-evolving threat landscape they operated within.

The *GovCyberHub* recently had the unique opportunity to sit down with IBM's Security Sales Manager, Jon Whitman, and Presidio Federal's Vice President of Solutions and Services, Jon S Kim, to discuss the top cybersecurity trends of 2023, gain insight into the cybersecurity threats federal IT departments should prepare for in 2024, as well as examine the federal directives agencies must meet by year's end.

Here is what they had to say:

GovCyberHub (GCH): Looking back at 2023, what were the top cybersecurity trends federal agencies saw within their IT departments?

Jon Whitman: A prominent theme within federal agencies in 2023 was the strategic management of a secure remote workforce. This imperative spotlighted the heightened significance of mobile cybersecurity and the rigorous implementation of multi-factor authentication protocols across the enterprise.

Concurrently, amidst ongoing government modernization efforts, there emerged a critical need for cybersecurity solutions that span hybrid and multi-cloud environments seamlessly. Safeguarding vital assets in this dynamic landscape emerged as a pivotal focus for federal IT departments throughout the year.

GCH: In 2023, were there any new challenges within the cyber threat landscape that agencies came up against?

Jon Whitman: Due to global conflicts, there has been a notable increase in cyberattacks targeting government agencies. This surge extends beyond nation-state actors, encompassing a growing and increasingly sophisticated trend in hacktivism. As geopolitical tensions escalate, the cybersecurity landscape has witnessed a surge in both the frequency and complexity of attacks. Hacktivist groups have become more pervasive, employing advanced tactics to compromise sensitive information and disrupt government operations.

"OMB MEMORANDUMS HAVE MANDATED AGENCIES TO MEET SPECIFIC ZERO TRUST SECURITY OBJECTIVES BY THE CLOSE OF FY 2024. TO MEET THESE DIRECTIVES, AGENCIES ARE STRATEGICALLY PRIORITIZING ACTIONS AIMED AT ESTABLISHING A CONSISTENT ENTERPRISE-WIDE BASELINE FOR CYBERSECURITY." – JON WHITMAN

GCH: Zero trust is always a top-of-mind topic for federal cybersecurity. How much progress have agencies made in rolling out their zero trust architectures?

Jon Whitman: Throughout the past year, noteworthy advancements have been made as government agencies submitted their zero trust implementation plans to the Office of Management and Budget (OMB). These comprehensive

submissions not only outlined budgetary estimates but also the required resources for execution.

Several agencies issued technology-oriented solicitations that explicitly align with zero trust principles, referencing executive orders and OMB memorandums, underscoring the commitment to aligning with mandates through commercially available technology.

GCH: As federal IT departments begin their planning for 2024, what security areas should they focus on in the new year?

Jon Whitman: OMB memorandums have mandated agencies to meet specific zero trust security objectives by the close of FY 2024. To meet these directives, agencies are strategically prioritizing actions aimed at establishing a consistent enterprise-wide baseline for cybersecurity. This involves adhering to principles such as least privilege, minimizing attack surfaces, and framing protection under the assumption that agency perimeters should be treated as compromised.

"BALANCING TECHNOLOGICAL ADVANCEMENTS WITH A SKILLED WORKFORCE UNDERSCORES THE HOLISTIC APPROACH AGENCIES ARE ADOPTING TO MEET THE EVOLVING CHALLENGES OF CYBERSECURITY IN THE COMING FISCAL YEAR." – JON WHITMAN

An overarching priority for government leadership is the strategic utilization and investment in Artificial Intelligence (AI) and Machine Learning (ML) for enhancing threat detection, response capabilities, and the automation of security tasks. This approach not only contributes to workforce efficiency but also facilitates identification of anomalies and emerging threats.

Simultaneously, the critical importance of maintaining a proficient cyber workforce is recognized. Even as technology evolves, ongoing investment in the skills and expertise of cybersecurity professionals remains integral to ensuring a robust defense against dynamic and sophisticated threats. Balancing technological advancements with a skilled workforce underscores the holistic approach agencies are adopting to meet the evolving challenges of cybersecurity in the coming fiscal year.

GCH: There is a current cybersecurity workforce shortage within the federal government. How do you foresee that shortage affecting federal IT departments in the coming year? What can agencies do to overcome the challenges posed by the cyber workforce shortage?

Jon S Kim: The cybersecurity workforce shortage within the federal government presents a significant and growing threat to its IT infrastructure in 2024, potentially jeopardizing the security of vital infrastructure and sensitive data.

With a diminished pool of qualified personnel, agencies may struggle to adequately defend against cyberattacks, potentially leading to data breaches, system disruptions, and operational setbacks. A lack of manpower can also hinder incident response capabilities, prolonging the time it takes to contain and mitigate cyberattacks, which could potentially amplify the damage caused. There also may be a hampering of adoption and integration of new cybersecurity technologies due to limited expertise, which in turn will hinder the government's ability to keep pace with evolving cyber threats.

"IN 2024, FEDERAL AGENCIES WILL FACE A COMPLEX CYBERSECURITY LANDSCAPE, MARKED BY EVOLVING THREATS AND RAPIDLY CHANGING TECHNOLOGIES." – JON S KIM

While this talent gap presents a significant challenge, addressing it is not insurmountable. By prioritizing workforce development, embracing automation, and revamping recruitment practices, agencies can fortify their cybersecurity posture and protect critical infrastructure and sensitive data.

GCH: Are there any emerging security threats or cybersecurity trends that you predict federal agencies will see in 2024?

Jon S Kim: In 2024, federal agencies will face a complex cybersecurity landscape, marked by evolving threats and rapidly changing technologies.

The heightened geopolitical landscape has been increasing the risk of state-sponsored cyberattacks targeting critical government systems and infrastructure. Agencies will require strong incident response capabilities, robust network

segmentation, and international collaboration to mitigate these threats.

Furthermore, continuing cyberattacks from state-sponsored actors targeting critical infrastructure and information systems are likely. Agencies must strengthen cyber defenses and incident response plans. Also, bad actors will increasingly leverage AI and machine learning for automated attacks, reconnaissance, and social engineering. Agencies will require robust AI security practices and continuous monitoring to identify and mitigate these threats.

This year, AI-powered deepfakes and personalized social engineering tactics will likely lead to more sophisticated phishing attacks, potentially bypassing traditional email filters and fooling even vigilant users. Agencies must prioritize employee cybersecurity awareness training and implement multi-factor authentication for critical systems.

"THE POTENTIAL FOR QUANTUM COMPUTING TO BREAK CURRENT ENCRYPTION ALGORITHMS COULD ALSO POSE A SIGNIFICANT RISK TO SENSITIVE DATA IN 2024."– JON S KIM

Expect ransomware attacks to continue to evolve, with bad actors targeting critical infrastructure and supply chains to maximize disruption. Agencies should prioritize operational resiliency, incident response plans, and diversification of critical IT vendors.

The potential for quantum computing to break current encryption algorithms could also pose a significant risk to sensitive data in 2024. Agencies should explore quantum-resistant cryptography and data security solutions.

In response to these evolving threats, the federal government is likely to implement stricter privacy regulations and security compliance requirements. Agencies must prepare for increased compliance burdens and invest in tools and processes to demonstrate adherence to new regulations.

GCH: Are there any cybersecurity deadlines or federal directive mandates that agencies must meet or comply with in 2024?

Jon S Kim: Federal agencies are entering 2024 faced with several significant cybersecurity deadlines and mandates looming. Several of these deadlines and mandates necessitate proactive implementation of enhanced security measures to safeguard critical infrastructure and sensitive data.

September 2024 marks the looming deadline of the federal government's Zero Trust Strategy. This initiative mandates a shift from perimeter-based security to a "never trust, always verify" approach, requiring agencies to authenticate every user and device attempting access to sensitive resources.

"BY PROACTIVELY ADDRESSING THESE MANDATES AND LEVERAGING INNOVATIVE CYBERSECURITY STRATEGIES, FEDERAL AGENCIES CAN BOLSTER THEIR DEFENSES AND PROTECT CRITICAL ASSETS AGAINST EVOLVING THREATS IN 2024." – JON S KIM

Under the Cybersecurity Incident Reporting for Critical Infrastructure Act (CISA Act), agencies must report cyber incidents affecting critical infrastructure to CISA within 24 hours of discovery. This timely notification facilitates rapid response and mitigation efforts.

The National Institute of Standards and Technology Cybersecurity Framework serves as a dynamic roadmap for federal agencies to improve their security posture. In 2024, agencies are expected to continuously monitor and adopt updates to the framework as they become available.

Another mandate is the Federal Acquisition Regulation, which includes stringent cybersecurity clauses for government contracts. Agencies must ensure their contractors comply with these requirements, such as implementing multi-factor authentication and conducting regular vulnerability assessments.

By proactively addressing these mandates and leveraging innovative cybersecurity strategies, federal agencies can bolster their defenses and protect critical assets against evolving threats in 2024.

To learn more about how Presidio Federal and IBM can serve as strategic partners for your agency in 2024 and beyond, click HERE.