Q&A

Federal Agencies Press Ahead on IT Modernization, Creating Opportunities but Also Challenges

The Federal government is in the midst of a sweeping IT modernization, replacing outdated legacy systems and moving rapidly to the cloud and other cutting-edge technologies such as robotic process automation. Modernization presents a mix of innovation and opportunity, bringing enhanced overall security and heightened employee productivity while also posing new risks. MeriTalk recently spoke with Fortinet's CISO focused on the public sector, Jim Richberg, and Forinet Federal's Robert Imhof about how Federal agencies are navigating their IT overhauls, the vast opportunities and strategic pitfalls along the way, and how Fortinet Federal can help. Richberg is a former national intelligence manager for cyber at the Office of the Director of National Intelligence; Imhoff is an expert in engineering secure network infrastructure.

MeriTalk: What is the current status of the Federal government's IT modernization and transition from outdated legacy systems, and what kind of trajectory do you see unfolding in the coming years?

Imhof: The increasing threat landscape has made modernization paramount. I see modernization efforts increasing as technology plays a more central role in agency missions.

Richberg: I recently spoke with a top Federal cyber official, who told me he would probably give the government a B or B minus grade in its cybersecurity performance. That's probably where agencies are in their IT modernization efforts as well. Federal agencies are turning to the Technology Modernization Fund to support execution-ready IT projects, which is accelerating updates to legacy systems.

Two things are happening in technology that should help guide modernization efforts moving forward. The first is convergence of networking and security – one product can replace up to a dozen different legacy tools. The second is consolidation of vendors into families of interoperability. For example, the cybersecurity ecosystem is converging toward mesh architecture, and Gartner research has predicted that organizations adopting a cybersecurity mesh architecture by 2024 will reduce the financial impact of security incidents by an average of 90 percent. Both trends will enable modernization and give agencies bigger bang for their technology bucks.

MeriTalk: What are some of the top priorities for agencies today as they attempt to modernize their systems, and what are some of the biggest opportunities that modernization presents?

Imhof: Security is the top priority because Federal agencies offer a target-rich environment. Modernization gives agencies the opportunity to address outdated systems, and that can really improve their security posture. One of the biggest opportunities with modernization is improving employee productivity, which is especially relevant in today's tight labor market.

Richberg: Job No. 1 is executing your agency's mission. But you have to do that against the backdrop of presidential executive orders (EO). Two EOs in particular impact agency modernization efforts – EO 14028 on cybersecurity and EO 14058 on customer experience. Both have created a government-wide priority list for IT modernization with a focus on security. Overall, I see four big areas of opportunity for agency modernization: cloud, software-defined networking, support for mobile and remote workers, and robotic process automation.

MeriTalk: What are the legacy systems still in use across government that pose the biggest challenges, and what types of cloud-based and other solutions should Federal agencies be seeking as they're trying to improve upon those legacy systems?

Imhof: Many legacy systems still in use across the Federal landscape are mission critical. These systems are written in antiquated programming languages like COBOL, and it can be really difficult to find people who know how to support them. Modernizing these antiquated systems and securing them with the latest security infrastructure and threat intelligence helps bring agencies' technical capabilities up to par with the private sector.

Richberg: The recent outage of the Federal Aviation Administration's NOTAM system perfectly illustrates the problem with legacy systems. Parts of the NOTAM system are more than 20 years old. When the system went down, it caused 1,300 flight cancellations and nearly 10,000 flight delays across the country. Outdated technologies are intertwined in systems that have a real impact on government operations and the daily lives of the American people. Today, government simply cannot maintain legacy applications that require modern-day functionality like accessibility, security, scalability, and resiliency.

MeriTalk: What pitfalls in the modernization process should agencies watch out for, and what's your advice for addressing those?

Imhof: One of the biggest pitfalls is modernizing without a solid plan. That could lead to building infrastructures based on buzzwords rather than what truly makes sense for the mission. That's something we really look out for: Are agencies asking the right questions and getting to the heart of their requirements?

Richberg: Two other strategic pitfalls are funding and procurement. In the private sector, if you make a compelling case for a particular solution, the purchasing decision usually gets made promptly. In the Federal environment, with continuing budget resolutions in place for much of the past decade, agencies can't start new projects. And once the funds are appropriated, agencies face a very complicated procurement process. Because of these challenges, the Federal government is typically three to five years behind the private sector in IT and cybersecurity.

MeriTalk: How have you seen shared services and cloud solutions alleviate some of the pitfalls of modernization?

Richberg: Shared services and approved product lists are streamlining procurement. Cloud solutions can simplify modernization or, in some cases, complicate it. In many cases, security is implemented differently in one cloud than it is in another, which poses a challenge to the user to maintain consistency of security capabilities and policies across clouds. Our adversaries are looking for gaps they can exploit, and inconsistent agency security across cloud environments is one area threat actors often target. One of Fortinet's strengths is our cloud-native presence in all of the hyperscale clouds.

This means our next-generation firewall, FortiGate, can be configured the same way across Amazon Web Services, Google Cloud, Microsoft Azure, and Oracle Cloud.

MeriTalk: While modern technologies improve efficiency and the customer experience, they also pose security risks by expanding the cyberattack surface at the network edge. How can agencies mitigate those risks?

Richberg: The expanding attack surface is a modern-day reality. By adopting a mesh architecture, agencies can turn the size and complexity of that surface from a liability into a potential strength. By instrumenting that surface – at least the critical parts – with sensors that generate data and coupling that with artificial intelligence (AI) -powered automation at the back end, agencies can see what's happening across the attack surface in real time. They can characterize normal behavior, which makes it easier to spot and respond to abnormal and potentially malicious activity.

MeriTalk: Given the global shortage of cybersecurity talent, how important is it for organizations to employ automation solutions to amplify the efforts of their IT and security teams?

Richberg: Automation is vital. When you instrument the attack surface to collect cyber data for analysis, you're potentially ingesting trillions of pieces of data a day. People can't handle that volume. This problem inspired Fortinet to develop AI and machine learning capabilities more than a dozen years ago. We set down the path to automate rote tasks, let machines identify anomalies, and give people time to do things that require the human mind and human judgment.

MeriTalk: What challenges are agencies experiencing as they try to modernize branch or remote offices, and what is your advice for overcoming those specific challenges?

Imhof: Unfortunately, many organizations get a bit of sticker shock when they modernize remote locations for more bandwidth, especially if the sites have MPLS or TDM connectivity. Most telecommunications service providers are no longer supporting TDM, and they may have really expensive last mile buildout costs for MPLS. Software-defined wide-area networking enables agencies to use any combination of transport services, including 5G and cheap broadband, without compromising security.

Richberg: With SD-WAN, organizations become strategically resilient in three areas – connectivity, service, and security. SD-WAN offers multiple avenues for connections to be made – MPLS, broadband, satellite, etc. It enables agencies to define service levels for specific activities. And it supports zero trust because it enables connectivity between users, data, and compute resources, and then ensures those connections are innate and secure.

MeriTalk: As agencies migrate to cloud-based applications and services, visibility, control, and protection across hybrid and multi-cloud environments becomes especially important. How can Federal IT managers maximize the benefits of cloud computing while defending attack surfaces and ensuring data center integrity?

Imhof: The most important thing Federal IT managers can do is examine traffic flows and security posture for each application to determine if the application should be hosted within the cloud or on premises.

From there, they can work with a security vendor like Fortinet Federal, which offers both on-premises and cloud-based solutions and a single platform to manage all environments. Fortinet Federal gives agencies visibility across the enterprise without having to log into each security tool individually or have separate tools for on-premises and cloud-based infrastructures. One single pane of glass view helps ensure a consistent security posture and regulatory compliance and reduce human error.

MeriTalk: How can Fortinet Federal help Federal IT leaders achieve IT modernization and legacy technology transformation?

Richberg: We're a cybersecurity and networking company that doesn't force agencies to accept tradeoffs between connectivity, performance, and security. We also don't force agencies to reinvent the wheel when they're modernizing.

I joke that the box for our FortiGate appliance should say "I'm a next generation firewall," on one end and "I'm a third-generation SD-WAN device" on the other end. All joking aside, though, the same device does both beautifully – and up to a dozen other functions. It's like the Swiss Army knife of security. If you want to use it in your router refresh, not as a firewall, that's absolutely fine. When it's time to update your firewall, you simply turn on that functionality.

Imhof: Fortinet pioneered the cybersecurity mesh architecture concept a dozen years ago with an open architecture designed to connect disparate security tools into a unified solution. Our mesh architecture is called the Fortinet Security Fabric. It's a portfolio of more than 50 Fortinet security and networking technologies that leverage AI to share threat intelligence, correlate data, and automatically respond to threats as a single, coordinated system. It's an open ecosystem that also integrates more than 500 products and services from other security and IT vendors. And, because we leverage a REST application programming interface, we're able to integrate seamlessly into most agency environments.

FORTINET
FEDERAL®