Merging CYBERSECURITY and MODERNIZATION

Agencies are speeding up efforts to modernize and become more resilient and innovative at the same time

CYBERSECURITY AND MODERNIZATION have a complex relationship in government. The two priorities must work together for agencies to move forward, but at the same time, they complicate each other's progress. For instance, government agencies must upgrade their IT systems to operate efficiently and meet customer demands, but those changes can introduce new vulnerabilities. And even as the transformation is happening, agencies must continue protecting mission-critical legacy systems.

That balancing act is challenging but not impossible. Success hinges on adopting robust tools and strategies that can support both goals.

Today's cybersecurity landscape is nearly unrecognizable from 10 or even five years ago, when agency officials worried mainly about networks and desktop computers. Today, they contend with cloud, mobility, the internet of things and emerging technologies that are finding footholds in government, such as artificial intelligence and automation.

As a result, the focus has shifted from protecting the perimeter to protecting data wherever it resides. Furthermore, ransomware has evolved to attack frontline systems and backup drives, malware kits are readily available on the darkweb, and cryptocurrencies such as bitcoin are complicating law enforcement, according to the Department of Homeland Security's 2018 Cybersecurity Strategy.

Attempted intrusions into government networks happen on a daily basis, and the number of cyber incidents that federal agencies reported to DHS increased more than tenfold from 2006 to 2015.

The Cloud Smart Strategy issued last year offers this straightforward advice: "Agencies might consider moving or adding security and privacy controls to the data layer itself, rather than just where they have historically resided at the network perimeter."

A vision for modernization

The White House and Congress have taken steps to ease agencies' transition to modern infrastructures and modern cyber environments. In November 2018, President Donald Trump signed into law the Cybersecurity and Infrastructure Security Agency Act, which established CISA at DHS to centralize the country's efforts to defend against cyberattacks.

Just months earlier, the White House had released the National Cyber Strategy, which seeks to protect national security, promote U.S. prosperity, preserve peaceful cyber behavior and advance America's global influence.

Around the same time, the Government Accountability Office released a report on high-risk cybersecurity challenges that require urgent action. Those challenges include securing federal systems and information, protecting critical cyber infrastructure, and protecting privacy and sensitive data. GAO first designated

joker1991/Shutterstock/FCW Staff

information security as a governmentwide high-risk area in 1997, then expanded it to include critical cyber infrastructure in 2003 and the protection of personally identifiable information in 2015.

Almost a year before the most recent security policies were handed down, the Modernizing Government Technology Act established the Technology Modernization Fund (TMF) from which agencies can borrow money to fund IT upgrades and replacements.

Modernization has been a top focus of the Trump administration, as evidenced by the subtitle of the 2018 President's Management Agenda: "Modernizing Government for the 21st Century." It explains how silos, outdated regulations and a lack of data-driven decision-making "prevented agencies from seamlessly transitioning services to meet the needs of the 21st century."

It also sets a long-term vision that emphasizes data sharing and modernized IT, and it identifies 14 cross-agency priority goals for achieving those objectives.

Innovative approaches at all levels of government

The progress on modernization has been swift. In March, the White House issued an update to the President's Management Agenda that highlights efforts in which the dual focus on modernization and cybersecurity has made a difference. It points to the $90 million that TMF loaned for seven projects at five agencies to enhance security, and it cites the migration to cloud-based email that more than 70 percent of Chief Financial Officers Act agencies achieved, thereby boosting security through standardization.

In addition, the U.S. Digital Service worked with the Department of Health and Human Services to enable 53 million Medicare beneficiaries to authorize third-party apps to access claims. The team created a standard, machine-readable format for health data and persuaded six technology companies to use it.

State IT leaders are also focused on modernizing IT and cybersecurity. On the National Association of State CIOs' list of its members' top priorities for technologies, applications and tools in 2019, cloud solutions was No. 1, followed by security enhancement tools and legacy application modernization/renovation.

Minnesota IT Services took an innovative approach to sharing information about IT and security by presenting business and technology leaders with a user-friendly inventory of state IT assets via Security Risk Scorecards. MNIT relied on a single framework, common business software, color coding and nontechnical language to create the scorecards, which were so well received that they are now part of everyday cybersecurity operations and decision-making.

"The dashboard for scorecards allows business leaders to see at a glance exactly what information and technology they have, what the security risks are, and how their business decisions and investments impact those risks," according to MNIT officials.

Some federal lawmakers recognize the benefits of supporting state and local agencies' modernization efforts. Those initiatives could get a helping hand if the Digital Service Act becomes law. Introduced in March by Sen. Kamala Harris (D-Calif.), it would authorize $15 million annually in seed grants for state and local governments to establish and grow digital services.

The need for flexibility and resilience

Cybersecurity and modernization are not one-off efforts. Instead, they require constant tweaking. The challenges are numerous and varied, but so are the benefits. Besides bringing government operations and services into the 21st century, the two initiatives will have a profound impact on the government's ability to innovate.

Currently, the roughly $90 billion in annual federal IT funding is largely spent on operating and maintaining legacy systems, some of which are 50 years old. The need to support those systems led to a $7.3 billion decrease in spending on modernization from fiscal 2010 to 2017, according to GAO.

In addition, the DHS Cybersecurity Strategy states that "cyberspace is an evolving domain with emergent risks. Although the proliferation of technology leads to new risks, it also provides an opportunity for innovation."

One way to make cybersecurity and modernization thrive in government is to take a community approach, said Jeanette Manfra, assistant director for cybersecurity at CISA, at an event in July.

The key to success is "trying to get everybody to think about what do we really care about," Manfra said. "What are really the high-value assets? How do we prioritize resources? How do we take actions to make ourselves overall more secure? And how do we become more flexible and resilient as a government?" ■

35,277
Information security incidents at civilian agencies in fiscal 2017

38%
Federal cybersecurity incidents for which the method of attack could not be identified in fiscal 2016

83%
Federal officials who said their agencies' future mission success depends on IT modernization

69%
Federal officials who said their agencies are working on IT modernization in a more integrated, holistic way

$617M
Savings the U.S. Digital Service could achieve through its current modernization projects

Sources: ACT-IAC, Government Accountability Office, White House