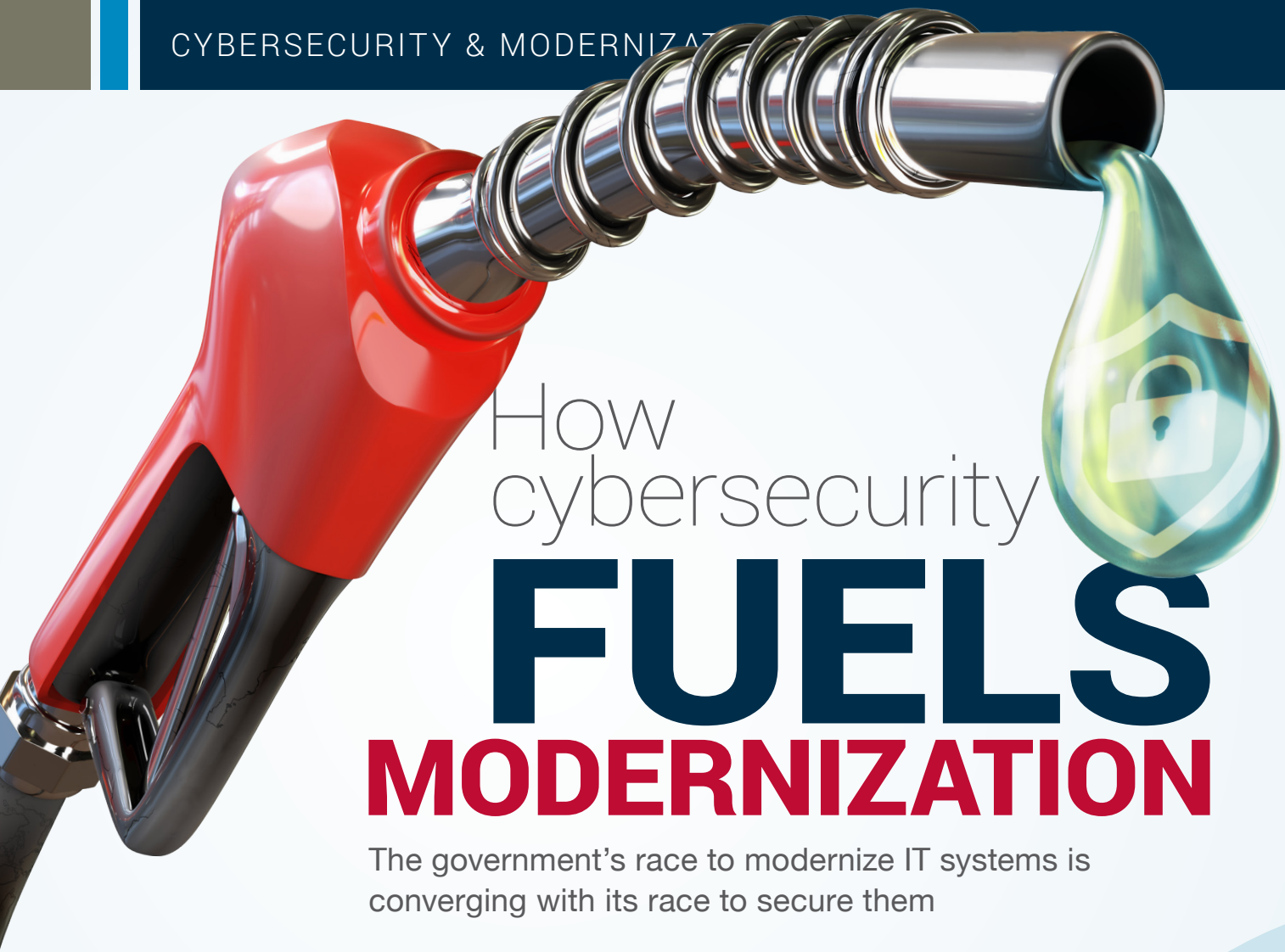

How cybersecurity FUELS MODERNIZATION

The government's race to modernize IT systems is converging with its race to secure them

SOME FEDERAL AGENCIES rely on IT systems that have 50-year-old components. Operating and maintaining those outdated systems have contributed to a $7.3 billion decrease in spending on development and modernization from fiscal 2010 to 2017, according to the Government Accountability Office.

Market research firm IDC predicted that annual civilian agency spending on IT would reach $52 billion by the end of the government's 2018 fiscal year, with 21.1 percent going to new systems and 78.9 percent devoted to operating and maintaining legacy ones.

Beyond the financial costs, legacy systems severely restrict the government's ability to be innovative, provide efficient services and stay technologically up-to-date. They also constrain agencies' capacity to respond to a cyberthreat landscape that is constantly evolving and becoming even more treacherous, which is why cybersecurity has become one of the biggest drivers of IT modernization.

Updating and securing government systems represent a complex and time-consuming undertaking, however. As IT managers are assessing, planning and upgrading systems, they must ensure that security is incorporated every step of the way — an approach that also applies to the adoption of emerging technologies such as artificial intelligence and the internet of things. At the same time, they must continue fortifying existing systems with the latest patches and antivirus updates.

A slip in cybersecurity can have a lasting impact. The 2015 breach of the Office of Personnel Management's background investigations database, which exposed sensitive information on more than 20 million people, is still fresh in the minds of many government leaders. In fact, former CIA Director Michael Hayden said at the time that fallout from the incident could continue for decades, and former U.S. Chief Information Security Officer Greg Touhill said last year that the breach could ultimately cost the government more than $1 billion in identity management solutions over the next decade.

Updating policies to address the challenges

The importance of IT modernization and security is not lost on government leaders. After the OPM incident, agencies engaged in a cybersecurity sprint to administer software patches and institute multifactor authentication for privileged users.

And in a 2017 study, DHS officials spelled out the challenges of securing mobile devices such as smartphones and IoT sensors, which "extend enterprise borders outside of the physical walls, fences, guards and firewalls that previously protected the enterprise against physical attacks. Additionally, they have a full range of sensors not seen in previous computing devices, which enable new types of attacks on the devices as well as the systems they touch."

In response to such warnings, Congress has sought to pass legislation that would address the government's challenge of protecting modern and existing IT infrastructure while looking ahead to emerging technologies.

The 21st Century Integrated Digital Experience Act, which was introduced earlier this year by Reps. John Ratcliffe (R-Texas) and Ro Khanna (D-Calif.), would digitize government processes and

GCN Staff

establish standards for federal websites to include secure, mobile-friendly interfaces. And in 2017, the Modernizing Government Technology Act authorized a central fund from which agencies could draw to help pay for IT updates.

Furthermore, initiatives such as the Federal Risk and Authorization Management Program (FedRAMP), Trusted Internet Connections, Continuous Diagnostics and Mitigation (CDM) and the National Institute of Standards and Technology's Cybersecurity Framework remind agencies to consider cybersecurity in the context of new and existing technologies.

For example, to achieve FedRAMP certification, cloud solutions meet certain levels of cybersecurity. The Department of Homeland Security designed CDM to help agencies identify risks on an ongoing basis and then mitigate them according to threat levels. CDM's new Dynamic and Evolving Federal Enterprise Network Defense series of task orders supports enhanced security for cloud and mobile technology, a standardized approach to incident response and stronger boundary protections that align with IT modernization efforts.

Building a stronger workforce

There are other signs that the government's approach to cybersecurity is evolving. In the Trump administration's fiscal 2019 budget request, White House officials wrote that "although the federal government spends roughly $90 billion annually on IT, these systems remain outdated and poorly protected. The administration will increase the use of modern technologies, retire highly insecure and outdated systems, and direct modernization cost savings to mission-driven outcomes. The administration will improve its ability to identify and combat cybersecurity risks to agencies' data, systems and networks."

One tactic involves strengthening the government's cybersecurity workforce. In 2017, OPM launched CyberCareers.gov as part of the Federal Cybersecurity Workforce Strategy to help "build the cybersecurity workforce pipeline as well as recruit, hire, develop and retain top talent," a press release states.

In addition, DHS runs the National Initiative for Cybersecurity Careers and Studies, which includes the Federal Virtual Training Environment. FedVTE offers free courses on ethical hacking and surveillance, risk management and malware analysis for government employees and veterans who want to become cybersecurity professionals.

In a report released in May, DHS and the Commerce Department called for "immediate and sustained improvements in the country's cybersecurity workforce," in part by encouraging the public and private sectors to join forces. The report was prompted by the Trump administration's 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

Given the challenges, it's not surprising that digital transformation is the top-ranked business priority among government CIOs, according to Gartner. Fortunately, policies and resources are in place to help agencies make the transition.

CYBERSECURITY and IT MODERNIZATION by the numbers

$80B

Proposed spending on IT and cybersecurity in the Trump administration's fiscal 2019 budget

$100M

Approved by Congress in fiscal 2019 for the new Technology Modernization Fund, from which agencies can borrow to update their IT

$210M

The fiscal 2019 budget request for the Technology Modernization Fund

30,899

Information security incidents reported by federal agencies in fiscal 2016

$57B-$109B

Estimated cost of malicious cyber activity to the U.S. economy in 2016

Sources: CIO.gov, White House, Heritage Foundation