NAVIGATING UNCHARTED CYBER WATERS

Agencies are looking for innovative ways to plot a course through a seemingly limitless ocean of cyberthreats

NEXT-GENERATION technologies such as artificial intelligence, cloud and the internet of things have the potential to revolutionize the government's ability to fulfill its missions. But the tools that present such promise also create cyber risks.

Modern technologies challenge the perimeter-based security that agencies relied on for years when IT resources were on-premises and comparatively easy to contain. Today, mobility reigns, and cloud technology enables government employees to work from anywhere.

Consequently, agencies must continue to protect on-site IT systems while they also find ways to secure user activity that is happening far outside the data center.

Meanwhile, adversaries have modernized, too, and the growing sophistication of cyberattacks is making it harder for the government to stay ahead of threats. To avoid security blind spots, agencies must address a long list of challenges, including maintaining visibility into a complex mix of cloud and on-premises systems.

Aligning policies with today's IT environments

In a recent survey of FCW readers, 83% of respondents said their agencies had well-defined strategies for modernizing their approach to cybersecurity. In addition, 29% used AI/machine learning, 51% used automated threat response, and 29% said their agencies had adopted zero trust.

The National Institute of Standards and Technology defines zero trust as "an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets and resources."

The second draft of NIST's Special Publication 800-207 further states that the approach "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local-area networks versus the internet)." Authentication and authorization of users and devices must happen every time a connection to an enterprise resource is established, and the subsequent activity must be continuously monitored.

According to NIST, numerous policies have pushed agencies toward a zero trust mindset for more than a decade, including the Federal Information Security Modernization Act; Risk Management Framework; Federal Identity, Credential and Access Management; Trusted Internet Connections (TIC); and Continuous Diagnostics and Mitigation.

However, NIST notes that those programs typically reflected the technical capabilities of information systems at the time they were developed: "Security policies were largely static and were enforced at large 'choke points' that an enterprise could control to get the largest effect for the effort." Fortunately, advances in technology are making it possible "to continually analyze and evaluate access requests in a dynamic and granular fashion."

The government is making an effort to bring policies into alignment with today's IT environments. For example, the updated TIC 3.0 was released this year to allow agencies "to place security capabilities closer to the data using trust zones, policy enforcement points and use cases rather than force the rerouting of data to the inspection sensors,"

Shutterstock/FCW Staff

according to the Cybersecurity and Infrastructure Security Agency (CISA).

Furthermore, lawmakers have taken notice that technologies such as IoT have emerged and exploded since those first directives were issued. The IoT Cybersecurity Improvement Act, introduced in Congress last year, would ensure that such government-operated devices meet certain minimum security requirements.

"As these devices continue to transform our society and add countless new entry points into our networks, we need to make sure they are secure, particularly when they are integrated into the federal government's networks," said Sen. Cory Gardner (R-Colo.) when the bill was introduced.

Strengthening the role employees play in security

Even the best technology and policies can be undermined by a careless employee. That's why agency leaders must continue to educate workers to recognize — and avoid — phishing attempts, which have increased during the coronavirus pandemic as adversaries look for ways to steal privileged credentials at a time when even IT teams are working remotely. However, in the FCW survey, only 42% of respondents said their agencies conducted robust cyber-hygiene training for employees.

As soon as thousands of government workers went from on-site to online work in response to the coronavirus, cybersecurity experts began warning about an increase in cyberthreats. In early April, CISA said advanced persistent threat groups were using the virus as a lure: "Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised."

In May, CISA and the FBI issued an alert about malicious cyber actors targeting unpatched virtual private networks, among other commonly exploited — and easily patched — vulnerabilities. CISA offers a number of tools to help agencies improve, including cyber-hygiene vulnerability scanning and a six-week-long Phishing Campaign Assessment that "measures your team's propensity to click on email phishing lures."

In addition to educating employees across the enterprise, agencies must strengthen their cybersecurity teams, which can be a daunting task. According to CyberSeek: "From October 2018 through September 2019, there were 270,000 openings for information security analysts, but only 112,000 workers currently employed in those positions — an annual talent shortfall of 158,000 workers for cybersecurity's largest job." Furthermore, "the average cybersecurity role takes 20% longer to fill than other IT jobs."

CyberSeek is supported by the National Initiative for Cybersecurity Education — a NIST-led joint endeavor of government, academia and the private sector focused on cybersecurity education, training and workforce development. Among other tools, CyberSeek provides an interactive "heat map" that shows the supply and demand for cybersecurity professionals throughout the country.

In addition, the Federal Cybersecurity Reskilling Academy has helped non-IT federal employees build foundational skills in the field of cyber defense analysis. The CIO Council is evaluating the success of the first two cohorts of students who went through the program last year to determine what educational opportunities to offer in the future.

The National Cyber Strategy states that "a highly skilled cybersecurity workforce is a strategic national advantage." The strategy's plan to build and sustain a talent pipeline includes expanding reskilling and educational opportunities, standardizing the recruitment and talent development process, and promoting "appropriate financial compensation...in light of the competitive private-sector environment."

The strategy highlights the challenges that many agencies are grappling with, but some are finding solutions. When FCW asked survey respondents how confident they were in their agencies' ability to recruit and retain cybersecurity professionals, most answers fell in the middle to high range. Only 7% said they were not at all confident, while 30% said they had no problem attracting topnotch talent.

As agencies crest the latest wave of cybersecurity challenges, they are constantly being forced to change course in response to new threats. Staying afloat in those stormy seas requires embracing innovative approaches to securing and modernizing the government's IT infrastructure. ■

Emerging cybersecurity BY THE NUMBERS

346 out of 6,843

Federal security incidents with confirmed data disclosures in 2019

61%

Malware attacks against government entities that are ransomware

1.8M

Projected global cybersecurity workforce shortage by 2022

52

Distinct cybersecurity roles identified in the Cybersecurity Workforce Framework

Sources: Frost and Sullivan, National Initiative for Cybersecurity Education, Verizon