MOVING FROM **CYBERDEFENSE** TO **DIGITAL RESILIENCE**

Why government agency IT leaders are moving beyond network protection and focusing increasingly on how to sustain operations during attacks.

By FedScoop Staff

A quiet shift is underway in federal cybersecurity that holds the promise of one day altering the strategic balance now in favor of the defender and allowing agencies to contain and respond to attacks without having to shut down operations.

At its core, the shift is about moving beyond cyberdefense — and the constant struggle to keep up with emerging threats — to a state of cyber-resilience in which agencies can act with agility to contain attacks and continue to operate unimpaired.

More and more agencies are beginning to embrace the change. The U.S. Army's Program Executive Office for Enterprise Information Systems, for instance, is in the process of acquiring automated network mapping and modeling tools to improve cyber-resilience, including tools to monitor, quarantine, emulate and counter threats.

The initiative is part of broader efforts to deploy sensor systems, infrastructure and remote cyber-maneuvering capabilities to protect the Army's tactical communications network during cyberattacks. It also reflects a shift in approach by PEO-EIS leaders: The focus is now on "capability drop decisions" rather than "traditional milestone decisions," to more effectively address the rapid changes in cyberspace the rapidly changing cyber landscape, according to an unclassified document presented to industry.

THE DEFICIENCY OF DEFENSE

The Army isn't alone in realizing that its dependence on largely manual processes for determining what actions to take when under attack is no longer adequate for ensuring sustainable network operations.

Nearly 7 in 10 federal civilian agency IT leaders — and more than half (55 percent) of their defense and intelligence agency counterparts — say their agencies aren't keeping pace with evolving threats, according to a recent study from CyberScoop and FedScoop, and underwritten by RedSeal.

While 2 in 3 federal IT executives in the study rated their agency's cybersecurity resilience maturity as moderate-to-high, only 18 percent of civilian agency executives and 30 percent of defense/intelligence executives in the study said they were "very confident their organization will continue running as usual" when facing a cyberattack.

Improving cyber-resilience is really about making sure you have choices — what the military refers to as freedom of action. And ensuring you have choices in the cyberspace means visualizing, identifying and measuring security risks in a way the enables your cyberdefenders to take the right actions at the right time.

"Achieving digital resilience begins with knowledge. The less you know about your networks — where they connect, how they connect, to whom they give access, and what they expose — the less resilient your networks and the organizations they support," says RedSeal CEO Ray Rothrock in his new book, "Digital Resilience: Is Your Company Ready for the Next Cyber Threat?"

"Point cyber security solutions are necessary but insufficient to really get control of the new risk demands of the digital world," says Rothrock. Organizations need effective analytics to quickly and objectively "compare the present state of the network with any number of future state scenarios," Rothrock says. That also "enables non-technical decision makers to evaluate the bang for their cybersecurity buck in increased resilience."

IMPROVING RESILIENCE

While the shift toward resilience is not about abandoning the basics of cybersecurity, such as firewalls, antivirus software and intrusion detection systems, the reality is

that these point products largely produce what some refer to as "busyness metrics" — they tell agencies how many attacks have taken place and how many patches have been applied, but they don't necessarily provide insight into how effective your responses have been.

Resilience is really about having choices the instant you detect an attack, Rothrock says. And the attacks will come — and inevitably some will succeed. Organizations "need to maintain a high level of awareness informed by multiple intelligence sources. Collect the data, analyze the data and adjust countermeasures accordingly," he says.

According to Rothrock, there are specific steps agencies should take to improve the resilience of their digital networks.

Get a real-time picture. The first step is to acquire a real-time picture of your network and all of its connections to the outside world. Network documentation can often be many years old, Rothrock warns. "Unless you can visualize your network accurately and in real-time, you cannot begin to take effective steps to improve its resilience," he says.

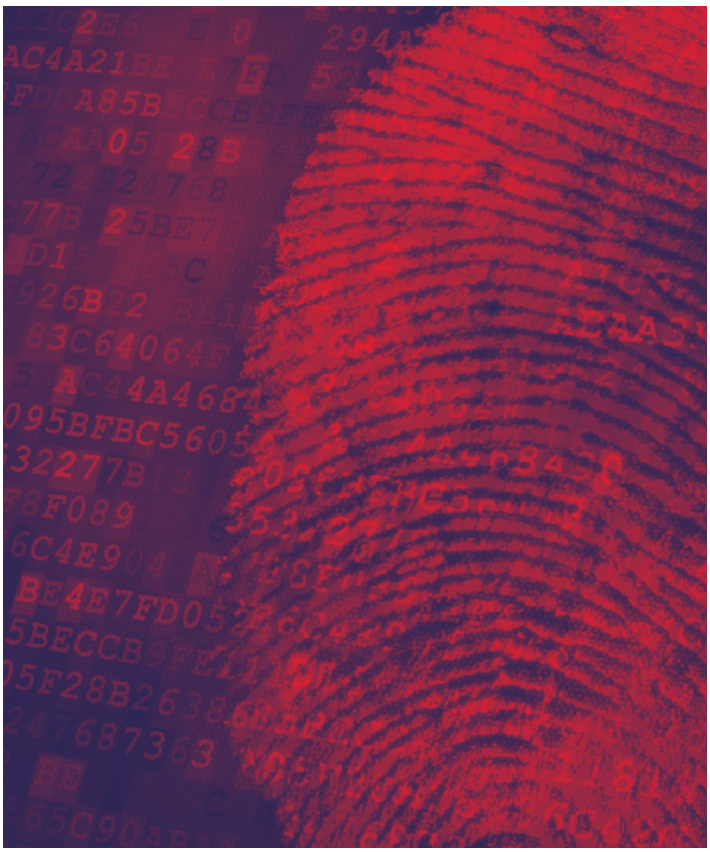
Verify configuration. Network devices often harbor default passwords and insecure services. "You need to determine whether any of your configurations violate your policies and standards, those of your industry, contractual obligations, or government regulations," Rothrock says.

Verify all possible access. This requires conducting an end-to-end analysis, including a what-if analysis, to determine the range of consequences of unauthorized access. Look for proper network segmentation and security zones.

Prioritize vulnerability remediation. Identifying your highest risk vulnerabilities and making them a priority for patching will increase your network resilience. "You need to be able to see these high-priority problems before you can patch them," says Rothrock.

PREPARING FOR THE NEXT THREATS

One of the most important pieces of cybersecurity, however, remains having the ability to quantify the resilience of your existing network and data structures. Yet, this remains a significant challenge for federal agencies.



The reality is that cybersecurity threats are evolving quicker than most agencies can respond. Automating more monitoring and mitigation activities is critical to enhancing security and resilience in the face of attack.

Executives are investing most heavily in fiscal 2019 into data and network protection tools and threat intelligence. But more than 3 in 4 respondents in the CyberScoop/ FedScoop survey said there's more that their agency could do to fortify their cyber resilience.

"Mere survival is not a sufficiently ambitious objective," writes Rothrock. "Intensively connected enterprises need to thrive in high-risk environments and even under attack. Thriving under attack is not a radical proposal. It is a function of digital resilience."

Find out more on the best ways to measure your Digital Resilience Score, and prepare your organization for greater cyber resilience.

This article was produced by CyberScoop | FedScoop for, and sponsored by, RedSeal.

cyberscoop | fedscoop REDSEAL