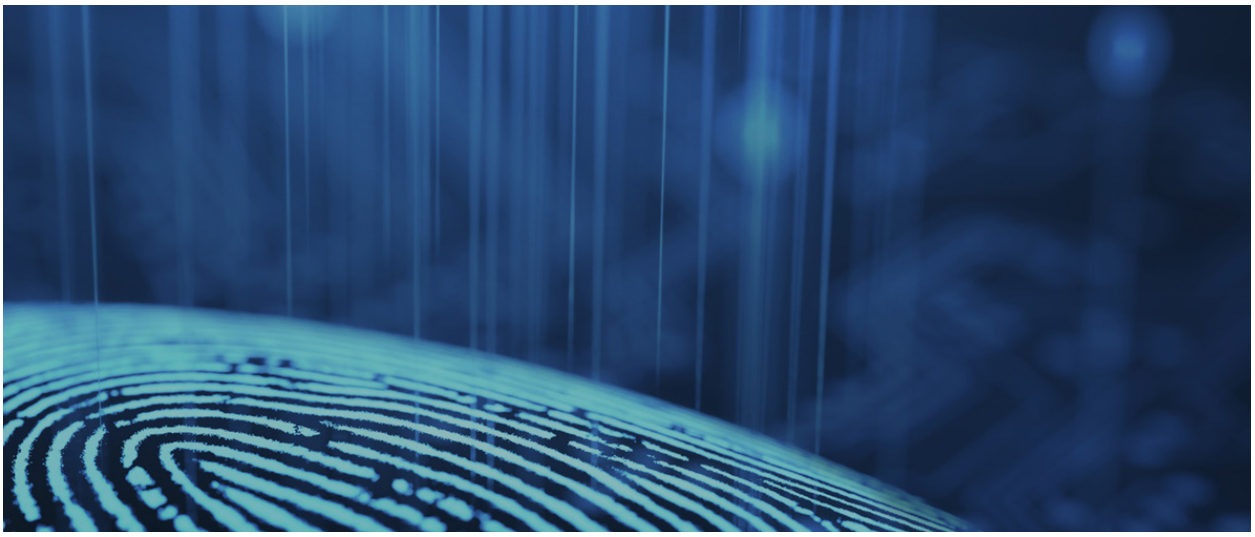

Taking a broad look at cyber risk

Modernizing risk management requires attention to people, process and technology

To mitigate cyber risk, agencies must improve the way they train employees, adopt technology and update processes that in many cases have existed for years – and they must do so holistically. Focusing on technology without bringing along people and process won't deliver desired business improvements.

"We can have a great technology, but we (also have to) find a way to change the mindset, win hearts and minds, and understand security cannot just be a punitive set of actions," said Jenn Fabius, director at KPMG.

Agencies are confronting a culture challenge, whether it's resistance to new ideas and processes or generational clashes that can occur when younger employees work alongside staff who are nearing retirement.

"The biggest challenge is how do we think differently and how do we change the culture mindset to do that," said Jason Martin, vice director of the Development and Business Center and acting director, Cyber Development Directorate, at the Defense Information Systems Agency.

Agencies would do well to foster a culture that is open to new approaches for securing work environments, reducing vulnerabilities and lowering risk. Getting there require a shift, from reactive to proactive, from simply protecting environments to ensuring that they are resilient.

Making the shift demands situational awareness, staying on top of threats and moving toward automated remediation, Fabius said. "It's a journey. You don't get there overnight."

Enterprise approach

The Department of Defense is taking a broad look at cyber security in order to reduce risk to mission at the combatant command level, said John Garstka, director of Cyber, at the DOD.

The focus is on securing different levels of the stack – including weapons systems and defense critical infrastructure – and teaching the workforce what cyber hygiene means in these different levels.

"We're finding that you can be really secure in your network space and lose a mission because an adversary has figured out that they can attack in one of those other layers of the stack," Garstka said.

The DOD is giving particular focus to situational awareness in cyberspace, particularly mission awareness that helps agencies understand the relationship between mission and elements of the stack, Garstka said.

"At the end of the day … if the combatant commands can't execute the mission because the adversary has done something in cyberspace, then we have a problem," he said.

To improve cyber hygiene and bolster security, defense organizations must understand what is in their environment – not just what is on their network, Fabius said.

"We need to … look at what is actually in my environment, whether I invited it in or not, and how the things I want in my environment

connect, interact, interface with each other," she said. Creating this "smart baseline", she added, is essential to building a strong foundation for cyber security.

To get there, agencies can use predictive analytics, automation and security orchestration. Security Orchestration Automation and Response (SOAR) develops the "connective tissue" between different layers of the stack that makes the technology work together, Fabius said. "That integration piece is absolutely essential."

Data governance is essential. Agencies must consider how data is stored, transferred and processed. "If I don't know its origins, I can't really trust it," she said.

The National Geospatial-Intelligence Agency seeks to improve its supply chain risk management by pulling together "pockets of excellence' within the agency, including hardware, software and acquisition under a common governance structure, said Monica Montgomery, chief for risk management, Office of Cybersecurity, at the NGA.

"We can have a great technology, but we (also have to) find a way to change the mindset, win hearts and minds, and understand security cannot just be a punitive set of actions."

– JENN FABIUS, DIRECTOR AT KPMG.

The DOD is developing a cybersecurity maturity model certification, a five-tier structure based on existing standards that will help the department's acquisition community to protect critical unclassified information. "This is really an effort to keep people from stealing our lunch money in cyber space," Garstka said.

The NGA's cyber hygiene program includes a plan to remediate any problems that occur, Montgomery said. "Having automated incident response and processes in place in order to remediate those things in a timely fashion is also a key aspect for what we are trying to do," she said.

At DOD, cyber security efforts extend to the supply. The department has launched pilots and initiatives to help it better understand the elements of the supply chain, where along the line the risk is most significant and if the potential for systemic risk.

"We're really trying to understand how the combination of our traditional intelligence sources and commercially available data analytics can help us with that," Garstka said.

Technology is reducing risk for DISA, which provides enterprise services to the DOD. The agency plans to develop a zero trust network architecture, launch a mobile workforce pilot, build identity credential and access management and software-defined enterprise capabilities, and create global orchestrators to ensure synchronization throughout the department.

DISA is also considering where to apply artificial intelligence in the agency and has launched a new innovation organization directorate to look at how automation can help it do business differently. This includes reviewing how automation can help employees do their jobs better because humans today "don't need to do every single task" they were doing in the past, Martin said.

Focus on the workforce

Recruiting, hiring and training the workforce plays a central role in mitigating cyber risk at agencies.

The Defense Information Systems Agency is promoting careers at the DOD to high school and college students because recruiting and retaining a new workforce is essential for the department's future success. It also encourages job rotations that promote valuable learning experience and serve as a retention tool.

"I highly encourage people to circulate throughout the agency, throughout the department, throughout our partners space to learn to grow and to identify and share information they think is relevant across the board," said Jason Martin, vice director, Development and Business Center and acting director, Cyber Development Directorate, at DISA.

Agencies should have a plan for how to recruit and retain skilled cyber workers, in part by offering them interesting work and using automation to relieve them of mundane tasks, said Jenn Fabius, director at KPMG. If companies want to remain competitive, they have to keep their workforce trained and certified, she added.

The National Geospatial-Intelligence Agency is actively realigning its workforce toward the NICE framework and is promoting training programs so that its employees, including its cyber workforce, can maintain their certifications.

Continuous training is essential, said Monica Montgomery, chief for Risk Management, Office of Cybersecurity, at NGA. It's not enough to just maintain a certification. "We are actively looking to make sure that people continue to take training every year," she said.

Article Source: FCW Summit: Cybersecurity | August 7, 2019