Navigating Cyber Challenges: Federal Agencies in the Digital Age

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Fortinet Federal, March 2024

In a recent roundtable, Federal experts discussed the various challenges and opportunities of navigating a rapidly evolving cyber landscape. Cyber threats are increasingly complex as technology advances.

Agencies are constantly challenged with striking a balance between implementing strong security measures and enabling agency missions. Leaders are continually weighing the risk to security for the sake of better service delivery. One panelist encourages their team to accept calculated risk in order to support the mission by countering the risk with additional security measures elsewhere.

As technology continues to advance, agencies cannot face cyber challenges alone. Partnerships with the private sector are essential for agencies to learn about emerging technologies and to prepare against new threats. In many cases, mitigating certain threats may require industry-wide adoption of new technologies, security features, or supportive services, which underscores the need for collaboration.

"We have to get it right 100% of the time. Adversaries have to get it right once."

One panelist recommends approaching cyber complexity by going back to basics: knowing a system's inventory, employing tools like pen testing and red team exercises, promoting multi-factor authentication, and ensuring robust identity management solutions.

Once these foundational practices are in place, agencies can take more proactive security measures. Agencies should also pay close attention to procurement language when procuring cloud and hardware vendors, and prioritizing data-driven decision making in Security Operations Centers (SOCs).

Panelists also highlight the challenges surrounding cloud computing, particularly in the post-Covid world of remote work. This rapid shift has made securing personal and organizational data in the cloud with Zero Trust practices a high priority for agencies.

Measuring Cyber Resilience

Agencies are measuring cyber resilience in several ways. Some analyze the authentication process to determine if the agency is successfully preventing unauthorized access or hindering legitimate users from accessing the system.

Panelists stressed the challenges of measuring resilience against the unknowns of social engineering and insider threats. Adopting a culture-wide Zero Trust mindset is key to adequately address the risk associated with the human element. Agencies should spend time preparing their response to breaches caused by insider threats.

Other agencies focus on business-level metrics, such as how long it takes to deliver services to customers after they initiate a requirement. They may also examine the efficiency of resolving issues, and whether delays are caused by the cloud or internal processes. Additionally, many panelists agree the authorization to operate (ATO) process is tedious and begs improvement.

Similarly, panelists are shifting towards quantifiable metrics that directly support business objectives and foster accountability, such as incident resolution and remediation times. By quantifying data, senior officials can more effectively make risk-based decisions to support the mission.

Some agencies on the panel conduct yearly assessments to evaluate authorized access. Others provide robust cybersecurity awareness training to improve cyber resilience. In the midst of constant change, agencies are focusing on the synergies of people, processes, and technology to move government IT forward.

"The technology will do whatever the process tells it to do, and in order for the process to work, you need to have people that are trained to know what to do."

According to one panelist, modern cyber resilience requires more than simply adopting new technology. It requires a collective mindset shift from protecting the network behind a firewall to taking a Zero Trust approach to cybersecurity. Soon, it will be unsustainable for agencies to react to incidents due to the sheer number of threats emerging. Panelists emphasize the need for agencies to take preemptive measures to prevent threats from emerging to begin with.

To aid in this culture shift, panelists encourage incorporating bite-sized training into daily work routines. Continually reminding employees of cyber security best practices can help make cyber security a part of the workplace culture. Ultimately, agencies need to cultivate a culture of vigilance, where every employee is a 'see something, say something' type of person.

Cyber Skilled Workforce

Panelists ended the roundtable by discussing the critical challenge of attracting, training, and retaining a skilled cybersecurity workforce. All agree the government simply cannot compete with the private sector for skilled IT talent on salary. Not only is salary a deterrent to Federal employment, so is the lengthy hiring process. One panelist hopes for a reform of the hiring process to improve onboarding.

Because there is such a disparity in pay, skilled tech workers must be motivated by public service missions to seek Federal employment. One panelist remains optimistic that more Americans will approach Federal employment as a way to serve their country as cyber threats continue to threaten national security.

Final Thoughts

Panelists encourage agencies to stay creative amidst these challenges and approach these obstacles with innovative solutions while maintaining a laser focus on security outcomes. This means embracing compliance, not as a roadblock, but as a tool to be leveraged to achieve the mission while ensuring robust security.