ATARC PRESIDIO®

Powered by GovExec

Achieving Cyber Readiness for 2025 and Beyond

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

In a recent roundtable discussion, Federal experts discussed the challenges and successes with developing and implementing data strategies. Participants shared insight into crafting data strategies, the evolving role of Chief Data Officers (CDOs), the importance of strong leadership, and leveraging data and Gen AI for mission outcomes.

Key Challenges with Cyber Readiness

"We can't continue down the same path we've always gone. We have to fundamentally change our perspective."

Quantum Computing

Panelists jumpstarted the conversation around cyber readiness by discussing quantum technology. The emergence of commercial quantum computing poses an existential threat to existing classical security models built on asymmetric encryption. Eventually, a quantum computer will be able to break today's asymmetric encryption protections, and as such, agencies must fundamentally change their IT security models.

Legacy Technology

"We have to change our infrastructure to be quantum secure, and that means being able to support those cutting edge technologies."

Due to the threats posed by quantum technology, one panelist suggests that agencies should stop modernizing antiquated legacy systems altogether, and instead focus on agile technologies built for the future. While most agencies do not have the capacity to engage in quantum research, there are groups working on initiatives to ensure agencies are prepared to transition to post quantum cryptography.

Workplace Culture

Panelists acknowledge there are still challenges surrounding workplace culture that must be resolved to achieve cyber readiness. One panelist noted a widespread resistance to embracing quantum key distribution, which has been accepted and implemented by European countries. Panelists caution that by delaying quantum key distribution further, the US will find itself with significantly more challenges.

Panelists shared another example of resistance where a senior leader had been advocating to take the government off the grid and back to an analog state. While this is an extreme response, there are still individuals in leadership thinking in these terms, which reflects the urgent need for the government to quickly introduce new cybersecurity solutions.

> **“We need to move quickly, because if we don't, there will be people that will take us back.”**

Despite needing to move quickly, agencies face delays in the decision-making pipeline. Often, the leaders who are accepting the risk are completely removed from the actual work, which disincentivizes them from moving quickly on a solution. Another panelist noted that the authorizing official is often not the same person who assumes the risk. Because there are multiple leaders involved in the decision-making process and are incentivized by different things, the process to acquire and adopt new technology is disjointed and slow.

Acquisitions

Panelists also discussed the importance of continuous education on evolving technology trends to ensure smart acquisitions. When engaging with vendors, suppliers, or contractors, agencies should inquire about security challenges the vendors face, and share any challenges the agency experiences that vendors may not know about. Agencies should also consider the infrastructure behind the technologies so acquisitions can be set up in a way to quickly react to changes in the future.

Protecting Data

Panelists also discussed the challenge with finding balance between reaping the benefits of new technology and ensuring information is protected, particularly with generative AI. Agencies are continually educating users on the risks and implications of using public generative AI models. Other panelists note the importance of maintaining public trust as the risk of data breaches increases with generative AI use. One panelist suggested treating generative AI like an intern, and providing the same level of oversight to generative AI as one would an intern.

Steps to Take Now

Conduct Inventory

Panelists concur the biggest threat to cybersecurity is quantum computing breaking classical encryption. However, not all algorithms used today are equally vulnerable, so it’s important for agencies to conduct cryptographic discovery and inventory of all systems, architecture and software.

During this inventory process, agencies should evaluate what data is protected by asymmetric encryption and where connections might exist in the infrastructure. By understanding existing systems, agencies can ask better questions of vendors as technology continues to evolve.

Prepare the Workforce

> **“We absolutely have to get workforce right.”**

Panelists emphasize the need for continued upskilling and reskilling of the existing workforce to achieve cyber readiness now. Agencies cannot wait a generation to hire quantum literate people. Identifying individuals who have the capacity to be reskilled and building expertise on U.S. soil is critical.

Preparing the workforce for future technology changes is also very important. Workers should know how their work fits into technology, and reassure them that while change is uncomfortable, technology is not designed to replace them. Panelists note that many people assume that working in quantum requires a PhD, but that’s not necessarily the case.

The types of in-demand skill sets and jobs in this field are vast. As one panelist stated, “we want people to stop thinking about quantum as a science fiction concept, and start thinking about it as the next development in AI.”

However, to keep these jobs in the United States first starts with creating demand for this new technology. As such, the onus is on IT professionals to demonstrate the potential of new technology to investors.

Improve the ATO Process

Panelists also emphasize the need for automation in software delivery and change management. Current ATO processes are often delayed due to manual processes and dependencies on individuals. Panelists suggest that the ATO process should be integrated into the development process in order to keep pace with the rapid emergence of new technologies.

Prepare Data

Panelists underscore the importance of understanding and preparing data to achieve cyber readiness. Panelists contend that to establish a strong data foundation, agencies must take the time now to understand and prepare their data so it is ready for future uses. Data scalability should also be considered.

Achieving Cyber Readiness for 2025 and Beyond

> **“We are in a situation where technology has created opportunity, but it's also created vulnerabilities.”**

Fail Fast

Panelists discussed the need for risk-tolerant environments to foster innovation. Decision-makers should define an acceptable level of risk and encourage experimentation within those parameters, specifically in innovation labs or lift cell environments. Doing so would allow solutions to be tested and gradually rolled out on a larger scale, thus reducing the risk while making progress.

De-Risk Decision Making

Similarly, panelists discussed the need to foster a more forward-leaning culture. The current cybersecurity workforce tends to be risk-averse, so it's important to demonstrate new technologies within a safe environment in order to generate empirical evidence and build confidence in stakeholders.

Increase Collaboration

Finally, it’s critical that agencies work amongst themselves and with international partners and allies with similar quantum missions to stay ahead of the drastic changes ahead.

Final Thoughts

Cybersecurity is changing, and agencies must address a multitude of challenges before achieving cyber readiness. Challenges posed by quantum computing and evolving cyber threats necessitate fundamental changes to cybersecurity models. To achieve cyber readiness, agencies must also work towards a more innovative and risk-tolerant culture, and take decisive actions to reskill the workforce, manage data, and streamline existing processes.