Innovating on the Frontlines of Cybersecurity & AI

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

Artificial Intelligence (AI) is rapidly transforming the cybersecurity landscape. While AI is advancing threat detection and response and helping agencies manage risks in real time, it's also enabling threat actors and adversaries to launch more sophisticated attacks. This roundtable discussion brought together Federal experts to share insights on emerging best practices and current challenges with AI integration in cybersecurity.

Current AI Landscape

Since the issuance of OMB's M-24-10 memo regarding governance and management of AI innovation, agencies now have an official roadmap to guide AI implementation and use. Agencies are now mandated to appoint a Chief AI Officer (CAIO), develop AI strategy, convene agency AI governance bodies, and develop AI use case inventories, which panelists predict will have significant impacts on AI adoption across government.

Roundtable participants discussed organizational structures that could best utilize Chief AI Officers. However, where the Chief AI Officer sits largely depends on an agency's budget. Many small agencies will not be able to meet this mandate, which is concerning to many panelists. According to one panelist, the CAIO would ideally report to the Chief Technology Officer, and because of AI's dependency on data, a CAIO should work closely with Chief Data Officers, or assume the same role.

While having AI leadership at the Chief level is important, panelists emphasize the need for AI talent in all levels within a department. However, panelists often experience challenges with funding and obtaining security clearances that prevent agencies from effectively hiring, upskilling, and retaining skilled AI talent.

While poor budgets are often the rationale for an agency's lack of innovation, one panelist candidly noted that funding challenges are not the real challenge preventing technology innovations. There is plenty of funding going towards other priorities, such as relocating offices across the country, but leaders are incredibly resistant to fund innovation due to potential for risk.

Panelists also note the enduring challenge of departmental silos, and the potential for AI to dismantle silos and enable data sharing. Cyber criminality is becoming overly sophisticated with AI, to the point where agencies and industry must work together to address increasing threats. However, agencies find it challenging to convince legacy system owners to share their data, talent, and anything they've fought hard to protect.

> **“We've got to start talking, because the bad characters out there are crushing us. If industry and government don't start working together, they're going to dominate. We've got to work together.”**

Agencies at the roundtable are looking at ways to improve data accessibility and usability with AI, particularly with some type of standardized tool that plugs into multiple applications to create a large data store. Currently, agencies have vast amounts of data that is inaccessible and not usable. With AI, agencies hope to separate and organize data so it’s useful for agencies and stakeholders.

> **“AI is not going to do you any good if you can't access data.”**

Evolution of Threats

Discussion shifted to the evolution of cybersecurity threats since AI’s acceleration, and the critical role of humans in risk management. While there is great value in using AI to enhance cybersecurity efforts, panelists emphasize the importance of human analysts to look closely at gray areas in the process.

One panelist discourages comparing any modern cybersecurity event to Solarwinds, because not even AI could have prevented what occurred. Another example to consider is a backdoor threat inserted into a Linux compressed format called XZ Utilis that an employee identified by complete chance.

Due to the nondescript nature of the backdoor, no alarms were raised and it would have otherwise gone undetected had the employee not been vigilant, highly skilled, and gotten lucky. Now, threats can look completely normal and legitimate. In this example, there was no sensor to trip, so it’s unlikely an AI would have been able to detect the threat.

> **“AI will not solve everything. AI is designed to solve the easy things so that we can focus on the hard things.”**

Panelists hope that AI will transform IT jobs in the public sector, making them more appealing and less arduous. When AI is used to automate easier cybersecurity tasks, people can focus on more challenging and interesting use cases.

One agency is already experimenting with AI for intelligence gathering. Using AI built into software, the agency is analyzing traffic and reporting on whether the traffic is legitimate. The agency then tests the intelligence in staging environments to determine what needs to be excluded or whitelisted.

Integration of AI into Cybersecurity Programs

PBecause of heightened risks, some agencies are choosing to implement standards beyond FedRAMP. As one panelist stated, FedRAMP only tells you that a solution has been assessed in a language everybody understands. Agencies must determine if a FedRAMP authorized solution meets their unique needs.

While FedRAMP is an important security standard, FedRAMP is often being used to influence acquisition decisions. FedRAMP is seen as a way for vendors to more easily enter the acquisition process and qualify as a choice vendor. Instead of being used for its intended purpose as a security cap classification, FedRAMP certifications are being used to prematurely narrow the vendor pool, thus limiting the number of potential solutions agencies can evaluate.

“There's a place and time for the implementation of FedRAMP restrictions, just not at the outset.”

Roundtable participants debated the requirement of agency sponsorship in the FedRAMP certification process. Some view it as a necessary stop gap to ensure compliance with certification requirements. Others consider the sponsorship requirement prohibitive for small businesses and those who have not yet been awarded contracts. Ultimately, the 10 year old certification process should be evaluated, and businesses should do their part to incorporate FedRAMP level security into their products from the outset.

Final Thoughts

- Agencies must prioritize their data. A good way to prepare for AI implementation is to start data labeling, even if those labels are not officially defined. Agencies must understand how their data is being accessed to effectively use AI.
- The potential for AI to attract and retain skilled talent is high. Rather than replace workers, AI will make work more interesting and engaging, enabling an overworked workforce to achieve more with less.
- Agency leaders must stay involved in the entire risk management process, and resist outsourcing risk management to third parties. By doing so, agencies run the risk of adversaries taking over entire risk profiles.
- While agencies may have unique missions, cybersecurity issues are all the same. This is a great opportunity to work together and learn from one another.

Learn more about Microsoft here: https://www.microsoft.com/en-us