ATARC

paloalto NETWORKS

ROUNDTABLE DISCUSSION

Fortifying the Digital Frontline

Cybersecurity Strategies for the Future

powered by GovExec

A recent roundtable discussion, hosted by ATARC and PaloAlto Networks, brought together experts to address the evolving challenges of cybersecurity within government agencies and the DOD. Discussion highlighted crucial issues such as internal communication, workforce training, acquisition hurdles, and strategic integration of artificial intelligence. Panelists shared strategies aimed at ensuring robust and resilient cybersecurity defenses now and in the future.

Cultural and Communication Challenges

Throughout the discussion, participants expressed concern with various cultural and communication hurdles that are impacting effective cybersecurity programs. One issue raised was a lack of clear and consistent communication from leadership on cybersecurity requirements.

This disconnect results in inconsistencies in how agencies approach, prioritize, and operationalize cybersecurity. Additionally, panelists noted a general lack of awareness or concern of broader cybersecurity risks outside of owned systems and applications. Currently, advancing cybersecurity processes within agencies depends heavily on individual initiative instead of established processes.

> **“We should never put one of our front line people in a position where they don’t know what’s in their network.”**

Training and Workforce Issues

Efforts to develop a common operating procedure are often thwarted by frequent turnover of cybersecurity personnel. Several panelists mentioned the challenge of investing in cybersecurity training among the workforce, only for those trained individuals to leave within a few years.

> **"We are really having trouble finding talented people and keeping them."**

Frequent transfers of personnel between organizations necessitate that staff repeatedly learn new tools and systems due to a lack of standardization across departments and organizations. This constant re-learning leads to inefficiencies, which are further exacerbated by the need to train staff on rapidly evolving threats and technologies.

Acquisition and Funding Challenges

Panelists also discussed challenges with the acquisition process that hinder effective cybersecurity, particularly long process delays, misunderstandings between acquisition and technologists, and lack of dedicated cybersecurity funding.

For some, the RFP process can take an average of 330 days . Programs involving billion-dollar competitive source selections can experience an additional year of delay. Additionally, panelists noted that cyber requirements often are not integrated into proposals until later stages, causing further delays and necessitating retrofitted solutions.

Panelists underscored the importance of communicating requirements to both acquisition and vendors clearly, explicitly, and early in the process. Cybersecurity leaders need to better define system expectations and requirements, particularly management requirements and critical 'cyber survivability assets'.

> **“If we don’t define what our performance expectations are for monitoring, mitigation, recovery, and adapting over time–there will be no money for it in the budget.”**

Agencies should ask vendors how their systems authorize access, encrypt data, segregate systems under attack, and address other critical security aspects. The goal is not merely to address individual vulnerabilities but to ensure the overall system architecture is secure by design. As one panelist noted, agencies cannot expect nor rely on vendors to have cybersecurity professionals available.

Participants also highlighted a lack of understanding among non-security professionals regarding the interdependencies between cybersecurity IT and mission-critical systems. This dependency should justify dedicated cybersecurity line items in budgets, but according to the roundtable, that is often not the case.

While there are particular cybersecurity requirements that must be met, one panelist cautioned against being overly prescriptive in the technology. Agencies should define expectations at a high level, and give the developer room to build something innovative and adaptable to a rapidly changing landscape.

Risk Management and Zero Trust

In discussing risk management frameworks (RMFs), panelists acknowledged a push to move beyond simply meeting standards and instead focusing on requirements that build resiliency and interconnectedness into systems. A significant portion (70%) of defects are introduced before coding even begins, often due to inadequate performance requirements. A vast majority (80%) of these defects are only discovered after most of the funding (95%) is committed, making remediation extremely difficult and costly.

Some are working to improve RMFs by supporting continuous authority to operate (CATO) and incorporating automation wherever possible. Automation is crucial to handle extraneous tasks and allow for more focus on critical security aspects. Automation in vulnerability management can also address issues more rapidly and efficiently.

AI and Automation

Panelists discussed AI's potential to fortify systems and national security, challenges in implementing AI securely, and strategies to protect AI systems from adversaries.

Fortifying systems with AI

Every day, millions of zero-day attacks occur on networks. Adversaries are using AI to quickly and strategically infiltrate networks, making it increasingly hard to defend. Industry cybersecurity experts, like PaloAlto, are continuously building AI models that respond to and learn from these attacks to better fortify systems and tools.

These models are capable of prioritizing signals, identifying anomalies, and even providing guidance to less experienced operators. AI-native tools like these enable agencies to automate security in new ways and adapt to future threats. While the potential of AI to transform cybersecurity is immense, panelists underscore the importance of maintaining humans in the loop of decision making.

Panelists are particularly excited about using AI and automation to conduct user behavior analytics to identify anomalies, such as unusual logins or privilege escalations, and detect potential attacks in real time.

> **“AI is a tool. We need to use it as a tool to achieve an outcome. The possibilities are endless.”**

AI challenges and considerations

Some participants expressed concern that adversaries could manipulate AI training data or learn the mechanics of AI models to tailor their attacks, effectively turning the AI’s responses against the very system it’s meant to protect. Another concern is training AI too specifically for a single environment, rendering it vulnerable to attacks by missing threats that aren’t part of its narrow training data set.

To mitigate these risks, panelists note that it’s crucial to train AI on a broad, “global” range of traffic and attack patterns to ensure it isn’t too narrowly focused. Additionally, some advocate for using multiple AI systems and tools trained in different ways as a strategy to counter these challenges and provide a more robust defence.

> **“It’s really important that we look at things in a different way and take a global look at how we’re training AI.”**

Taking a deep, multilayered approach to cybersecurity can also give agencies a better chance of thwarting adversaries by not focusing too heavily on AI models or algorithms. Panelists emphasize that it’s just as critical to fortify the underlying infrastructure and the supporting infrastructure beneath those layers.

> **“It’s not something you buy. AI has to be embedded in every single cybersecurity tool. The biggest differentiator in your cybersecurity posture is how well you leverage the tool.”**

Collaboration and Interoperability

Ultimately, the interoperability of tools is crucial for fortifying systems in the future, yet remains one of the most significant challenges for agencies. Simply building APIs between devices isn’t sufficient for the real-time information exchange needed in a zero trust environment.

While agencies need integrated solutions to allow for communication and data sharing between different tools, agencies should consider using homogeneous tools within each enclave to streamline integration and reduce coverage gaps. Even with different tools, there’s a need for consolidated visibility to support standardized automations and policy setting.

> **“We all aren’t going to be able to buy a single platform, so the tools need to be able to communicate and pass data in a manner that’s actionable… You aren’t going to build the zero trust environment using one single solution–but that’s almost what we’re being forced to do.”**

Final Thoughts

The roundtable discussion revealed that effectively fortifying systems requires multifaceted, holistic approaches. Addressing individual vulnerabilities or adopting isolated technologies is insufficient. Rather, achieving true resilience requires a comprehensive understanding of the interdependencies between IT systems and mission control-functions, along with robust collaboration with agency partners. As participants noted, "light bulbs start to go off" when stakeholders grasp how interrelated all aspects of cybersecurity are, and how critical resilience is for operational success.

"We've got to think about cybersecurity from a bigger and larger perspective."