FEDInsider

Securing IT and OT in an Increasingly AI-Driven World

As threats evolve, agencies must close cultural and technical gaps to enable zero trust, keep up with the pace of AI and strengthen enterprise resilience.

In today's rapidly evolving threat landscape, cybersecurity is a dynamic battleground shaped by emerging technologies, expanding attack surfaces and increasingly sophisticated adversaries. The rise of artificial intelligence has accelerated this shift, pushing the cyber "cold war" between U.S. agencies and hostile actors into a new phase. At the same time, AI has emerged as a true double-edged sword: a tool for cyber defense that must now be deployed against equally advanced AI-driven attacks.

During a recent FedInsider webinar, government and industry leaders met to discuss how foundational strategies and priorities must evolve to meet these challenges. They share how zero trust is expanding to address growing risks across the software supply chain and highlight the need for stronger, more comprehensive cybersecurity that extends to U.S. critical infrastructure.

AI Is Changing the Cyber Landscape

AI is changing the speed, complexity and sophistication of modern cyber threats. Advancements in AI are making it easier for bad actors to leverage traditional attack options, like writing a compelling spear phishing email. AI-powered models have also become increasingly good at identifying exploitable software vulnerabilities.

"That creates different classes of threats that did not exist before," said Justin Myers, Lead Computer Scientist for NCIS, Directorate of Operational Technology and Cyber Innovation, pointing to the increase of AI-generated voice and video cloning. Scale isn't the only change, "but also the quality of what AI is able to produce, which is a unique challenge," Myers said.

Deep fakes and AI-generated personas are also being used in order to create fake student accounts, enroll in universities and file for financial aid, according to George Kaminski, Manager of Securing Solutions Engineering at Cisco. "This is some of what we are worried about, and we are putting defenses in place for that right now," Kaminski said.

AI is also defining the speed at which attacks occur. "If you are not using AI to attack or defend, you're going to be overwhelmed," said Kevin Walsh, Director of the Information Technology and Cybersecurity Team for the U.S. GAO. "You could be the best analyst in the world and even so, you can still be defeated by a thousand chatbots or agentic AI coming out and trying to do bad things." It only takes one, after all.

This change in speed and scale is ultimately changing how many organizations do business. "AI can give you great resilience, but also great exposure. Because it's virtual... it's not the device that is important, it's the outcome," said Richard Breakiron, Senior Director of Strategic Initiatives and Executive Programs for the Americas Federal Sector at Commvault.

Balancing Innovation with Resilience

Organizations have been familiar with zero trust for some time now — but as software packages are updated and supply chains become more complex, organizations must ensure their vendor pipeline is secure.

"How do we validate the information we are seeing?" said Anthony Brannum, Chief Information Security Officer in the Cybersecurity and Privacy Operations Center for the U.S. Department of Agriculture. "Sometimes, it could be hiding in an environment, and we will catch it later. Many times, we had to remove software from an environment and pull it off the network."

Continuous monitoring and scanning are key, and creating a software bill of materials (SBOM) can help verify vendors and hardware manufacturers. "Zero trust from the vendors' perspective — they need to have it all the way to the government," Brannum said.

Rather than simply never trust, always verify, organizations must never trust and continuously verify. It's a fundamental shift — organizations once trusted a server or individual, but they must now

Featured Experts:

- **Anthony (Tony) Brannum**
  Chief Information Security Officer, U.S. Department of Agriculture

- **Richard Breakiron**
  Senior Director, Strategic Initiatives, Americas Federal Sector, Commvault

- **Dave Carroll**
  Vice President, Cyber Capability, Engineering & Strategy, GDIT

- **Dr. Elizabeth Di Bene**
  Chief Information Security Officer, Loudoun County, VA

- **Andrew Green**
  Chief Information Security Officer, Virginia Dept. of Transportation

- **Brandon Grimes**
  ICS & Platform Security Lead, National Cyber Business, Booz Allen Hamilton

- **George Kaminski**
  Manager, Securing Solutions Engineering, Cisco

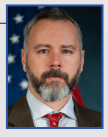
- **Garrett Lee**
  Regional Vice President, Enterprise Security Group, Broadcom

- **Justin Myers**
  Lead Computer Scientist, NCIS OTCI

- **David Olschewske**
  Strategic Account Manager, Forescout

- **Chris Usserman**
  Global Technology Officer, Public Sector, InfoBlox

- **Kevin Walsh**
  Director, IT & CS Team, U.S. GAO



trust a process, said Dr. Elizabeth Di Bene, CISO for Loudoun County, Virginia.

At the commit phase, verify the developer's identity with encryption. And at the build phase, verify the integrity of the build with encryption. When the ingredients of the package are visible, ensure nothing has changed. "And finally, when you look at deploying it with your security policies, you look at binary authorization to map it only back to what you deploy," Di Bene said. "That's how you put your trust into the supply chain."

AI is also shifting how organizations build and evolve their zero trust architectures. "AI introduces an interesting interaction between the data in each of the layers that is accelerated," said Garrett Lee, Regional Vice President of the Enterprise Security Group at Broadcom. While organizations may have already adopted some zero trust principles, they must now consider how AI can access their data and adjust their zero trust practices accordingly.

"You now need to treat AI systems and how they operate, including how they use data and make decisions, with the same considerations you bring to your employees" Lee said. All static inventories and expected behaviors must be mapped.

AI and generative AI can also enhance identity verification. Monitoring can be done much faster with AI, but adversaries can also attack faster. That's the AI arms race, said David Olschewske, Strategic Account Manager at Forescout. "We have determined — whether companies or government – that we all need to employ this ability to deter attacks. And if our adversaries are using AI, then we have to use AI too because otherwise we are not fast enough to combat it."

Securing Legacy Operational Technology and Protecting Critical Infrastructure

Nation-states and criminal actors are both evolving their tactics to target operational technology (OT) across critical infrastructure sectors, but for different reasons. According to Chris Usserman, Global Technology Officer for the Public Sector at InfoBlox, cybercriminals often go after money, whereas nation-states aim to destroy or degrade capabilities. "You need to have visibility into those environments to truly understand whether you're dealing with a cybercrime incident or a nation state," he said.

Considering that a lot of physical infrastructure is now run by OT on an IT network, experts are concerned that nation-states and cybercriminals will shift toward more invasive, effect-based targeting. That's why organizations need to secure both their IT and OT infrastructure.

Securing IT largely means protecting data and information, whereas OT devices and systems perform operational activity, and protecting them keeps critical infrastructure up and running. "The availability and integrity of many OT systems is more important, and it's a different thought process," said Andrew Green, CISO of the Virginia Department of Transportation.

Mitigating controls and managing the risk of OT devices may also require different tactics and strategies, but security fundamentals still apply. "You often can't build security controls into the system for OT, so we have to look at mitigation. And you have to make sure you think about it and evangelize about it with the whole community too," Green said.

It's about negotiation, awareness, building a better culture, and increasing trust between IT and OT. Because OT teams can feel like IT is imposing policies without fully understanding operations, almost as if they're scanning systems and then moving on, said Brandon Grimes, ICS and Platform Security Lead for the National Cyber Business at Booz Allen Hamilton.

"You can really build some common ground between IT and OT by tailoring your security governance for OT and getting the operations perspective and input," Grimes said. "Make them active contributors on what outcomes we are trained to achieve, what security controls are realistic, and what impacts are we trying to avoid. Because you can get buy-in from OT teams from that standpoint."

Bridging the IT and OT cultural divide will be critical to securing legacy OT going forward. The key is convergence: bringing the speed and flexibility of IT systems into OT environments, which have traditionally been more static and focused on production.

IT relies on standards like CI/CD, reliability engineering and full-stack development because they're faster and more efficient. When organizations share that mindset, collaboration is easier. But with OT, there's still a gap and a lot of proprietary approaches, said David Carroll, Vice President of Cyber Capability for Engineering and Strategy at GDIT.

"We don't need bigger haystacks; we need sharper needles sometimes," Carroll said. "Say you want to find the needle. Well, that needle is probably staring at you in the face, but you have to separate out the static before you can really find it."

In the end, the conversation made clear that AI is sharpening both sides of the cybersecurity equation. It is giving agencies new tools to move faster, see more and strengthen resilience, even as adversaries use those same advances to scale attacks and exploit weak points across IT, OT and the software supply chain. That is why the path forward is not simply to adopt AI, but to do so with stronger verification, deeper visibility and closer collaboration across technical and operational teams. In a world where AI can just as easily widen risk as reduce it, resilience will depend on how well agencies manage both edges of the sword.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8500
Info@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft