FEDInsider

The Art and Risk of Deploying Artificial Intelligence as a Transformational Tool

As agencies adopt AI to boost cybersecurity and efficiency, they're challenged with adversaries using the same tools as threat vectors.

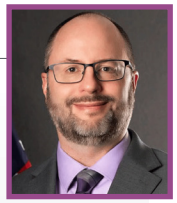
Featured Experts:

- **Christine Lai**
  Cybersecurity R&D and AI Security Lead, CISA

- **Danny Holtzman**
  Executive Director & Deputy CDAO, Acquisitions & Cyber Assurance, Chief Digital & AI Office

- **Scott L. Doss**
  Digital Information Officer & AI Lead, Munitions Directorate, Air Force Research Laboratory

- **Terry Kalka**
  Director, DCISE Program, DOD Cyber Crime Center



- **Ronan Murphy**
  Co-Founder, Getvisibilty & *Chief Data Strategy Officer,* Forcepoint

- **Skip Farmer**
  Senior Director, Sales Engineering, Primer

- **Jonathan Alboum**
  Federal CTO, ServiceNow

Artificial intelligence is being used to bolster cybersecurity – from quickly detecting threats to identifying risky or abnormal behavior before a breach – yet these capabilities come with their own risks. Under-regulated and under-reviewed new tools are being used to protect government systems even as they're being attacked by more sophisticated adversaries, many of which are becoming adept at tricking or thwarting weak or flawed AI defenses.

At a recent **FedInsider webinar**, thought leaders from government and industry discussed proactive defense in this current AI landscape where innovation is inevitable, but so are greater vulnerabilities.

Leveraging AI for Cybersecurity

Organizations are increasingly turning to AI to analyze large amounts of cyber activity for abnormal or adversarial behavior. For Terry Kalka, Director of the Defense Industrial Base Collaborative Information Sharing Environment (DCISE) program in the Department of Defense Cyber Crime Center, that store of information includes a large repository of data that it constantly pulls from several federal sources.

"Our primary role is as a resource and a warehouse for developing cyber threat information," said Kalka. DCISE pulls data from U.S. government sources, open sources and from the defense industrial bases themselves. It partners with over 1,200 defense industrial base companies."

That's loads of data to review for cyber activity, but automation helps to analyze everything quickly to look for and alert against any possible threats. "Manual analysis will only take you so far. Any kind of automation that we use to work through the terabytes of data at our fingertips is going to help us a lot," Kalka said.

Ronan Murphy, Co-Founder of Getvisibility and Chief Data Strategy Officer at Forcepoint, said AI as a means of strengthening cybersecurity is one of the fastest growing parts of their business.

"What we are seeing is a fundamental shift in mindset where, because of the advent of all these artificial intelligence technologies, organizations say, 'you know what? It is super important to the security infrastructure, but actually having visibility into our data is becoming paramount,'" Murphy said. "We are seeing the adoption of AI with a view to getting a clearer understanding of what the actual data is and what risks are hidden there within that data."

In heavily regulated environments, understanding data at a granular level is known as data security posture management. "The data layer... is paramount to operating AI properly," Murphy added.

Social media information can also be monitored for trends indicating attack vectors, and AI can help with this too. Skip Farmer, Senior Director of Sales Engineering at Primer said, "We want to make sure that we are sourcing and getting sentiment information and narrative information because there are hundreds of thousands of messages going around on social media. How can we analyze that and sort some kind of signal through all that noise to understand what narrative or trend might be under the surface?"

Spotting those trends and hidden sentiments requires sifting through all the bots and spam, analyzing information in various languages used around the world, pulling the relevant insights, creating trends to spread awareness and identify potential risks, and sharing information as a warning so teams can assess everything and decide on a course of action. "There is no way to do that without AI," Farmer said.

AI-Based Cybersecurity Risks

Just as agencies and organizations use AI to make teams and processes more effective, bad actors have the same opportunity – to use these advanced tools to be more effective at creating risks.

"Malware is now auto-generated by AI, and it can be infused into our environments much more effectively. There is also the ability to create realistic phishing emails using AI," said Jonathan Alboum, Federal Chief Technology Officer at ServiceNow. "AI is being used for automating attacks."

In this environment, security teams must be focused on these types of threats 24/7. "Unless we are… using similar levels of sophistication, we have increased risk. And the reality is that the bad guys only have to get in once," Alboum said.

As organizations adopt AI to strengthen cybersecurity, it is critical to be focused on the risk these tools also create. "The best defense is a strong offense, but there is also education and awareness," Alboum added.

In fact, Scott L. Doss, Digital Information Officer and AI Lead for the Air Force Research Laboratory, Munitions Directorate, said these advanced artificial intelligence capabilities are allowing AI attacks to impact people who aren't trained very well to utilize the tools, and enabling people to use AI to do more damage. "They have AI to deploy, and this is where they introduce new attack surfaces, but to defend the systems, I believe there are four pillars of risk that we must focus on," Doss said. Those include supply chain transparency and integrity, secure development lifecycle, secure communications and data protection, and verification and validation.

"By structuring everything in pillars and developing cybersecurity strategies around these pillars, it allows transparency in supply chains, development practices, secure communications and exhaustive research and development that enables us to build AI-enabled platforms that are resilient as well as capable," Doss said.

Securing AI Today and in the Future

Leveraging AI to understand where risk is coming from to further mitigate that risk is a continuous cybersecurity practice. For example, Danny Holtzman, Executive Director and Deputy CDAO for Acquisitions and Assurance in the Chief Digital and Artificial Intelligence Office, said AI can be used to help with AI-assisted compliance, like authority to operate. Holtzman views ATOs as a "statement of risk."

"Everything is connected to everything these days. But AI can help me understand what the threat vectors are," Holtzman said. "AI can also be used to ensure compliance is met when assessing for ATOs, and that doors are locked where they need to be so that risks are identified and dealt with."

And while federal agencies may be limited in the resources they have in terms of cybersecurity, their adversaries are too. They have a limited set of resources at their disposal – people, expertise, etc.

"We need to make that we can make it cheaper to do the easier parts of security and hit the low-hanging fruit," said Christine Lai, Cybersecurity Research and Development and AI Security Lead at the Cybersecurity and Infrastructure Security Agency. "It is very expensive for adversaries to identify new security vulnerabilities and exploit them."

AI software developers shouldn't feel alone when tackling these challenges either – Lai said they should work with existing operations and security communities to effectively secure software through development. "People have developed solutions around this, and we want to make sure that those tools are incorporated into their AI tool development chains upfront," Lai said.

This doesn't mean developers have to sacrifice functionality or performance for security, Lai added. In fact, she recommends that developers always apply security techniques and measure their progress when embedding security controls and features. Doing so will ensure that software is better defended against AI attacks, and that existing AI defensive tools operate exactly as intended.

TO LEARN MORE, VISIT CARAH.IO/CARAHSOFTAI

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

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

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **The AI Team at Carahsoft**

(571) 591-6040
AISolutions@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Forcepoint
10900-A Stonelake Blvd., Suite 350
Austin, TX 78759
Contact: **Stan Reddick**

(571) 683-0249
Stan.Reddick@Forcepoint.com
Forcepoint.com
Facebook.com/ForcepointLLC
Linkedin.com/company/Forcepoint
@ForcepointSec

ServiceNow
2225 Lawson Lane
Santa Clara, CA 95054
Contact: **Sales at ServiceNow**

(844) 863-1987
ServiceNow.com/contact-us.html
Facebook.com/ServiceNow
Instagram.com/ServiceNow
Linkedin.com/company/ServiceNow
@ServiceNow

Primer AI
244 Jackson Street, Suite 201
San Francisco, CA 94109
Contact: **Sales at Primer AI**

(415) 629-5013
Sales@Primer.ai
Primer.ai
Linkedin.com/company/Primer-ai
@Primer_ai