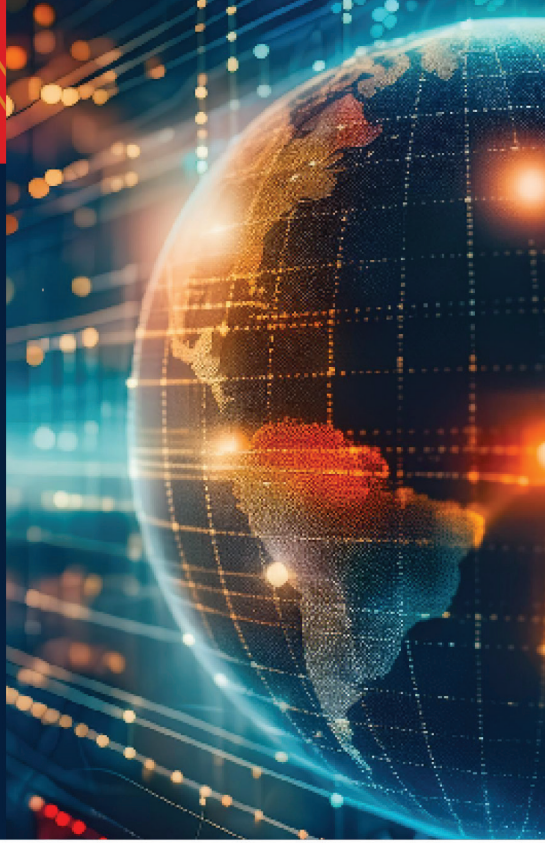
FEDInsider

CyberSmart 2024

Keeping Up with the Pace of AI at the State Level



Texas government officials and an industry expert discuss shifts in policies, security and risk as AI advances at an accelerated rate.

According to Moore's law, the speed and capability of computers are expected to double every two years. This means new technologies – and challenges – can be introduced at the same rate. To keep up with cybersecurity changes that arise with advanced technologies (like artificial intelligence), the White House released Executive Order 14110 in October 2023 on the "safe, secure, and trustworthy development and use" of AI. In March, the Office of Management and Budget released guidance on improving governance and managing the risks of AI. State governments are taking action, too.

At a recent FedInsider webinar, thought leaders from government and industry discussed how AI's integration into computing environments affects cybersecurity, and the steps security professionals are taking to address it.

Balancing the Potential and Risks of AI at the State Level

"Complexity is the enemy of security," said Larry Moore, chief information security officer for the Texas Division of Emergency Management (TDEM). "AI introduces an entirely new level of complexity to our environment."

For the TDEM, trust and resilience are critical components in emergency response and management. During an emergency, seconds count, and the risk of a false email claiming danger is problematic.

For Moore, the positive impact of implementing AI-based tools must be worth the trade-off. "There is always a cost involved," he said. "Is there a cost regarding risk, regarding finance, regarding personnel?... You must balance impact and cost, and if you are not balancing the two then you are not addressing the risk properly." While Moore sees the potential in AI for emergency response, the potential of a particular solution must outweigh the costs or the risk.

Chris Bunton, chief information officer of the Texas Department of Agriculture (TDA), agreed that with any new technology comes potential, but leaders must first consider the return on investment.

"From a security perspective, I am always very cautious with new technology," he said. "What are we trying to achieve? What is the bottom line? Are we trying to be more efficient, effective or addressing capacity?"

TDA's approach is cautious because threat actors are using advanced tools that can

Featured Experts:

- **Chris Bunton**
  Chief Information Officer, Texas Dept. of Agriculture

- **Gabe Perez**
  Vice President, Systems Engineering, U.S. Public Sector West, Fortinet

- **Larry Moore**
  Chief Information Security Officer, Texas Division of Emergency Mgmt.

more effectively permeate newer systems and be more successful and extensive in their breaches, potentially causing more expensive and extensive damage.

"We are going to be very cautious and make sure we have the guardrails in place," Bunton said, and that starts with policy. "We see potential, and we are partnering, researching and trying to make sure we have good policies in place."

Securely Setting Agencies Up for AI Success

According to Gabe Perez, vice president of systems engineering for US Public Sector West at Fortinet, even though the concept and use of AI aren't necessarily new, the current buzz around AI may be coming from the recent questions and issues surrounding the technology.

"The important thing to remember when you are talking about AI is while you can buy it off the shelf, it isn't consumed that way and you still have to build it," Perez said. "There must be developers who actually program the intelligence."

Organizations must also ensure that they have structured data to feed the machine, developers to program the AI and decision makers to analyze what the machine is spitting out. "All of those questions need to be answered before you actually deploy AI in a successful way," he said.

Fortinet uses AI by taking data from its sensors in the environment – which it is collecting constantly – and feeding it into the AI engine. The machine takes the information and analyzes trends to help Fortinet's team predict when something bad could happen.

"We are constantly evolving AI in our technology because it helps us to make better decisions," Perez said. "The bigger issue here is even though we are using AI in our technology to help the state of Texas protect its citizens, the bad guys are using the same kinds of AI. So, they are constantly feeding AI into their technology to evade the state."

That's why all of Perez's best practices and tips for states begin with security. "Security is the foundational element of making sure that not just you can do your job, but also that your employees can do their jobs while also ensuring that we are keeping the citizens of the state of Texas secure," he said.

This includes user training to help keep people from unknowingly clicking on sophisticated phishing emails and links. Moore said during a security awareness training a while back, he used a real-life scenario example that evoked emotion to grab people's attention and make them aware of what could happen if things go wrong. He also noted that he would much rather have users constantly asking if suspicious emails or links are legitimate as opposed to just clicking on them.

"I want people to feel that they are doing their job and thinking about it, and if they make a mistake, no sweat... I would rather you make a mistake on the side of caution," he said.

Preparing for AI

Along with security, Bunton recommends that agencies consider their existing policies when adopting new technologies like AI. "You first want to find out if your current policies can be adapted to cover the new technology," he said. "Start tweaking those now."

Perez also suggests that agencies begin with a full assessment of their current environment before bringing in anything new, because it's difficult to move forward without knowing where the security and network environment currently stand. "If you are not in a good state, you cannot fix it unless you first know where you are at," he added.

Moore agreed, adding that a full assessment of risk identification, operational continuity and vulnerability management are crucial. Agencies must know and understand their current security posture, including all of their potential vulnerabilities and any areas that need improvement.

"Politics is always involved, but what is your core objective? Is it to protect, or is it to toe the line?" he asked. "You need to make sure a full risk analysis has been performed, because without that, you may need to rewrite entire policies." And until you understand the risks, you can't find any real solutions, much less safely add new capabilities like AI into your environment.

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) 871-8548
Info@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

FORTINET

Fortinet, Inc.
909 Kifer Road
Sunnyvale, CA 94086

(833) 386-8333
Fortinet@Carahsoft.com
Carahsoft.com/Fortinet
Facebook.com/Fortinet
Linkedin.com/company/Fortinet
@Fortinet