A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

Understanding Cyber Risks in the AI Era

SPONSORED BY SOPHOS

Know how AI fits into your organization's cybersecurity strategy — and which tools are most effective.

Introduction

Artificial intelligence is changing the game for government cybersecurity.

Gone are the days when security teams could weed out phishing emails based on simple indicators like misspellings or awkward syntax. Today's cybercriminals are weaponizing AI to evade detection and launch more sophisticated attacks.

AI is also reshaping the cybersecurity landscape for IT teams working to protect networks and secure sensitive data. AI-powered tools for defense, detection and response already offer significant advantages — and they continue to evolve rapidly.

"There are AI technologies that will be really helpful in our jobs, and there are AI technologies that unfortunately will be helpful on the attacker side," says Paul Zindell, director of sales engineering for the public sector at Sophos, a leading provider of cybersecurity-as-a-service solutions. "But the silver lining, at least from the research we've been doing so far, is that AI is favoring the defense."

Understanding how AI fits into your organization's cybersecurity strategy — and which tools are most effective — is essential. By identifying your greatest risks and adopting AI responsibly, you can ensure it works for your agency, not against it.

Understanding AI Risks

While cyberattacks remain the most visible threat, AI introduces a broader spectrum of risks. Sophos outlines five key categories: threat risk, defense risk, operational risk, financial risk and hijack risk.[1]

Threat risk. Attackers are using generative AI to create deepfake videos, voice-cloning scams and highly convincing phishing emails tailored to specific individuals.

To counter these threats, agencies should adopt tools that detect AI-generated content and ensure their cybersecurity platforms include email protection. Training staff to be cautious about unsolicited communications — especially on social media — and implementing protocols like call-backs and passcodes can help mitigate these threats.

Defense risk. AI tools are only as strong as the data used to train them. Poor-quality data leads to poor outcomes.

"It's 'garbage in, garbage out,'" Zindell says. "If the quality of the data is not good, it doesn't matter how good the model is — you're just going to get junk."

When evaluating new tools, ask about the source, quality and volume of training data. Inquire about the development team's expertise and the safeguards built into the product engineering and deployment process. Even with automation, human oversight remains essential.

Make sure your cybersecurity solutions align with privacy laws and data protection standards.

Operational risk. Over-reliance on AI can create a false sense of security. While AI offers value, it's not a complete solution.

Use AI as a force multiplier — but remember that people remain ultimately accountable for cybersecurity. Treat AI as a support mechanism, not a substitute for human judgment.

Financial risk. AI capabilities can be costly to build and maintain — and not every investment delivers a strong return.

To manage financial risk, clearly define your goals for any AI initiative. Measure its performance against those expectations, and track impact to ensure ROI.

Hijack risk. The most difficult risk to control is hijack risk — when attackers exploit AI to manipulate users or data, or trick people into trusting compromised AI models.

Stick with reputable providers, and remain vigilant. Threat actors may spoof trusted names by altering characters (e.g., replacing "O" with "0") to mislead users.

It's also critical to ensure your cybersecurity solutions align with privacy laws and data protection standards. Breaches can result in fines, reputational damage and loss of public trust.

Ultimately, AI is a tool — not a silver bullet. It must be governed, monitored and refined like any other technology.

Understanding AI Benefits

Despite the risks, AI offers significant upside for cybersecurity — particularly in terms of visibility, speed and efficiency.

Generative AI

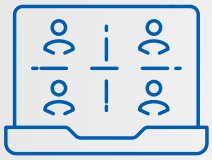
Most people are now familiar with generative AI (GenAI) models trained on large language datasets. In cybersecurity, GenAI helps make threat analysis more accessible. For instance, it can summarize suspicious activity or explain unfamiliar code, reducing the burden on analysts.

Deep Learning

Deep learning models detect threats in real time by recognizing patterns and making decisions in milliseconds. These tools can identify whether a file is benign or malicious with high accuracy.

AI also enhances anomaly detection, behavioral analytics and risk scoring — automating incident response workflows and reducing manual investigation time.

Some platforms monitor how applications interact with the operating system. When suspicious behavior is detected, the system can log it, classify it and take automated action — such as halting the process and alerting the security team.



Engage with solution providers to discuss your agency's specific needs and determine how AI can best enhance your defenses.

Finding the Right Solution

A 2024 Sophos study found that 99% of small and midsize organizations view AI capabilities as essential when selecting cybersecurity platforms.[2]

Many government agencies are already using AI — often without realizing it. Modern cybersecurity tools frequently include AI under the hood, detecting user behavior anomalies or unusual login patterns.

Yet these capabilities often go underused. Agencies may have powerful tools sitting dormant simply because they haven't been activated.

Before investing in new solutions, audit the tools you already have. Look for features that could be enabled immediately for added protection without increasing workload.

When you're ready to expand, consider your analysts' experience. Would they prefer a tool requiring constant attention and separate dashboards? Or one that integrates seamlessly with existing platforms and delivers actionable insights automatically?

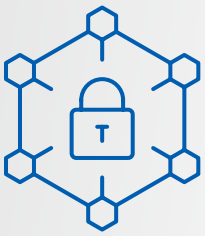
AI should simplify cybersecurity operations — not complicate them.

Engage with solution providers to discuss your agency's specific needs and determine how AI can best enhance your defenses.

Preparing for the Future of AI-Driven Defense

Agencies that embrace AI today will be better prepared for the next wave of innovation.

The cybersecurity community is moving toward a vision where AI agents detect, contain and remediate threats without human intervention. These agents could remove compromised user accounts, isolate affected systems and prevent lateral movement — often before staff are even alerted.



Early adoption builds confidence and positions agencies for long-term resilience.

“I used to call it the ‘if only,’” says Deborah Snyder, a senior fellow at the Center for Digital Government and former chief information security officer for New York state. “‘If only we could have self-healing systems. If only we could use AI to enhance Zero Trust based on real risk, to proactively identify vulnerabilities, to sift through alerts and feeds and get to what’s actionable, and to respond to incidents in a faster, automated manner.’

“Well, that future is closer than many realize,” she says. “Those are just some of the areas of opportunity where functions are currently being performed manually or through separate tools, where AI-enhanced solutions and strategies can create efficiencies and dramatically strengthen cybersecurity.”

What requires separate tools or manual intervention today may soon be built into intelligent, proactive defense platforms.

However, human oversight will remain essential. Integrating AI into day-to-day workflows now will prepare teams to adapt more easily to the next generation of tools. Early adoption builds confidence and positions agencies for long-term resilience.

Conclusion

AI is rapidly becoming an indispensable part of government cybersecurity. While it introduces new risks, it also enables faster response, better insight and stronger defenses.

Agencies that invest wisely, build internal AI knowledge and align tools with strategy will be best positioned to protect public data and infrastructure in an increasingly complex threat landscape.

By making smart decisions now, government IT teams can turn AI into an ally — reducing risk, improving efficiency, and staying a step ahead of tomorrow’s threats.

1. https://www.sophos.com/en-us/whitepaper/navigating-the-ai-hype-in-cybersecurity
2. https://news.sophos.com/en-us/2025/01/28/beyond-the-hype-the-business-reality-of-ai-for-cybersecurity/

Produced by Government Technology
Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by Sophos
Sophos delivers superior cybersecurity outcomes by providing cybersecurity as a service to protect companies of all sizes from the most advanced cyberthreats. Our cybersecurity products and services include managed detection and response (MDR), firewall, email, endpoint (XDR), and cloud native security protection. Sophos products and services defend against ransomware, phishing, malware, and more. They connect through the cloud-based Sophos Central management console and are powered by Sophos X-Ops, our cross-domain threat intelligence unit. We provide fully managed security solutions so you can manage your cybersecurity directly with our security operations platform. Or, you can supplement your in-house team with Sophos' products and services.

www.sophos.com

ADOBESTOCK/AI GENERATED