GLOBAL KNOWLEDGE BRIEF

Cybersecurity

Part 2: Artificial Intelligence – Cybersecurity Friend and Foe

AUDITBOARD

The Institute of Internal Auditors

Contents

About the Experts

Aneta Waberska, CISA

Aneta Waberska is Director of Information Security and Compliance Products at AuditBoard. She has more than 15 years of experience across IT audit and compliance domains and joined AuditBoard to focus on product development efforts serving IT risk and compliance users, leveraging her industry experience. Aneta started her career at KPMG and PwC, where she helped clients implement and assess frameworks such as SOC 1 and SOC 2. She has worked with companies of different sizes to implement and manage compliance programs of varying complexity, including managing company-wide policies and third-party risk management programs. She has worked closely with management to implement controls to meet security framework requirements, and with executive management to ensure compliance supports the company's strategic objectives.

Terry Grafenstine, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry Grafenstine is the 2023–24 senior vice chair of the Global Board of Directors of The Institute of Internal Auditors (IIA) and chief audit executive with Pentagon Federal Credit Union (PenFed). She was recognized by The IIA as one of the "Top Ten Audit Thought Leaders of the Decade" for her contributions to the profession related to cyber and technology and was also inducted into The IIA's Hall of Distinguished Audit Practitioners. She has held leadership roles at Citi and Deloitte and served as the appointed Inspector General of the US House of Representatives.

INTRODUCTION

Cybersecurity is the top risk consideration for internal auditors, and that will remain the case for the foreseeable future. Indeed, it is the singular risk consuming their greatest time and effort, according to Risk In Focus 2024. The report series, from The Institute of Internal Auditor's (IIA) Internal Audit Foundation, asked chief audit executives and directors from around the world about the top risks their organizations are facing, and how they expect the threat picture to change in the next three years.

The Risk in Focus 2024 findings demonstrate the complexity of cybersecurity as a risk and the added challenges stemming from near-constant changes in technology and how it can be used. This, too, was reflected in the report's findings. Internal audit leaders expected to see the threat of digital disruption jump from fifth place on the threat list today to second place in three years.

This brief, the second in a three-part series on cybersecurity, examines how artificial intelligence (AI) contributes to cybersecurity challenges and opportunities, and what internal auditors need to know about this emerging and evolving risk area as a cybersecurity consideration. AI holds great promise as a sophisticated tool to improve efficiency, productivity, and risk management in virtually any organization. However, it also presents new risk management challenges, including ethical considerations, the dangers of algorithmic bias, and over- or blind reliance on the use of AI. While it can be a valuable tool in the battle against cyberattacks, bad actors are also using it to perpetrate their crimes.

AI at Work

A Two-Edged Cyber Sword

Internal Audit Should Explore AI Uses and Threats

The term artificial intelligence refers to technology that can mimic human intelligence, such as learning, reasoning, and problem solving. It encompasses several types of technologies, including machine learning, or a system's ability to learn from data and apply that learning.

One way that AI and machine learning can significantly enhance cybersecurity efforts is in threat detection and data analysis, said Aneta Waberska, director of information security and compliance products at AuditBoard. Cybercriminals try to infiltrate an organization's network and systems by seeking out weak spots and breaking down network defenses. In the past, organizations relied on system administrators to review events related to these external threats. However, because of the advancement of automation and other technologies, the growing volume of such attempts from bad actors has overwhelmed the capacity for effective human review, she said. AI can address this problem. It can review large volumes of threat events and recognize patterns and learn from them over time, understanding if a particular event or cluster of events can pose a threat to an organization. "This is one of the most impactful uses of AI in this environment," she said.

In addition, more sophisticated malware detection tools have better capabilities, as do other malicious activity defense solutions, including the ability to block one of the top causes of security breaches and incidents—phishing. That can reduce or eliminate the potential for human errors—such as opening a link on a phishing email and exposing company networks to malware—because the tools filter them out before they get to someone's inbox, Waberska said. (See the sidebar for more information on how AI can improve cybersecurity defenses.)

AI can also quickly search for anomalies and identify problems already occurring within the organization's network, something that humans cannot do on such large-scale data. - Unauthorized access to company systems is one example. A former employee could inadvertently make access available to a cybercriminal by sharing or writing down a password or may reenter the system with malicious intent themselves. In the past, an internal auditor checking for unauthorized access among former workers would have had to conduct a manual comparison of people with access and those who no longer should have it, then write an email to the IT team detailing any issues, noted Terry Grafenstine,

Using AI as a Cybersecurity Tool

According to the IEEE Computer Society, some of the ways in which AI can enhance an organization's cybersecurity defenses include:

- Detecting malicious activities, by benchmarking acceptable activities and identifying anomalies and threats continuously and in real time.
- Supporting malware threat identification by examining file characteristics or code patterns to spot those that are unsafe.
- Improving a company's ability to deal with zero-day attacks or other unknown threats.
- Enhancing threat intelligence by pulling together security information from a range of sources, proactively hunting for threats, and assisting in threat management by easing the workload of company security analysts.[1]

[1] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society, September 6, 2023.

chief audit executive with the Pentagon Federal Credit Union. AI, on the other hand, can search across multiple platforms, compare data in the payroll system and the access system, and generate an email to the appropriate teams about any anomalies.

Internal auditors should be aware that cybercriminals' goals are often not simply to steal data, but to infiltrate and disrupt systems by changing data, Grafenstine said. On the largest level, nation-state bad actors can manipulate critical infrastructure, such as transportation, nuclear energy, banking, and many others, but the consequences can also be significant for organizations of any size.

Risk Management Considerations

Ethics, Bias, and Over Reliance

Internal Audit Can Help Organizations Avoid AI Pitfalls

Along with its many benefits, AI does come with its own list of risk considerations. Some of the threats are internal ones, but they can be just as damaging as cyberattacks.

Ethics

Many of the concerns in this area relate to generative AI and large language models that can be used by internal auditors to create reports, write code, and sketch out recommendations and analysis, among other possibilities. However, these tools also raise security and ethical questions for organizations. "There is a risk that employees will look at these tools as a parlor game or a toy," Grafenstine said.

Traditional cyber controls used on earlier technologies also apply to these systems, but "the repercussions of not doing things well are magnified," she said. Among other things, as will be discussed in more detail, the systems can provide biased, inaccurate, or completely fabricated information, depending on how they are trained. Grafenstine also points to the costly and potentially embarrassing consequences for a company's business and reputation if it uses a customer-facing chatbot that has been trained on poorly sourced internet data and the chatbot's incorrect answers have a significant negative impact on customers. For these reasons, there should be human review of anything produced by a generative AI system when the organization is not completely aware of the data it has been trained on. "The company has to own the answers," Grafenstine said.

While the use of generative AI programs such as ChatGPT has exploded since they debuted in late 2022, posting information on publicly available generative AI can expose company or customer data and personal identifiable information, just as a hacking incident might do, and is a significant risk consideration. When employees post queries that include company information in public generative AI programs, the program will retain that information and potentially use it to respond to other queries outside the organization, exposing it to public view. Not only can this publicize confidential information, but bad actors can also use the details they discover in publicly available generative AI to engineer their way into the company systems, with phishing or other tools, Grafenstine warned.

Blind Overreliance on AI Output

Professionals are responsible for the tools they use and the information those tools generate. That's particularly true of internal auditors, who could violate their own standards if they place too much reliance on unvalidated data or content. "Being reliable is what we do for a living," Grafenstine said.

Algorithmic Bias

Machines are trained to learn based on specific algorithms and the information they produce can be influenced, intentionally or not, based on those algorithms. As an example, algorithms may filter out women's résumés being used in a hiring decision if existing employees in a certain role are predominately male or they may favor mortgage applications from white buyers if most current mortgage holders are white.[2] "They are not intentionally trying to be malicious, but the biases are baked in," Grafenstine said.

[2] "For minorities, biased AI algorithms can damage almost every part of life," Arshin Adib-Moghaddam, The Conversation, www.theconversation.com, August 24, 2023.

Protecting AI – and Protecting Against It

Internal Controls Are Critical

Protecting Integrity of AI Systems, Access

Security over AI itself and the ability to use it are other serious considerations for organizations and internal auditors. There should be controls over who can access AI resources, how the authority to change code is protected, and who is allowed to take information from a test area to production. As an internal auditor, "I want to make sure I can tell if an AI algorithm has been changed or if someone can disrupt it in the middle of a process and alter it," Grafenstine said. Internal auditors also need to be aware of the potential scope of the interference. "If I can access your company AI, it's not just one transaction that I can alter," she said. Instead, the bad actor can get to an organization's entire data lake or data warehouse, or whatever else the AI has access to.

"Just because you have implemented a solution that leverages AI does not mean that you are now bulletproof,"

Aneta Waberska
AuditBoard

At the same time, it's important to be aware that AI is making it easier for cybercriminals to create malware rapidly, automate attacks, and improve the effectiveness of their scams or social engineering attacks by using tools such as deepfakes, which digitally alter videos or pictures, and AI voice generators to create false images or messages. "The cyber threat landscape is becoming more dangerous, and AI plays a big role in it," according to an IEEE Computer Society article.[3]

Internal auditors should see AI as an offensive and a defensive tool, said Waberska. "Just because you have implemented a solution that leverages AI does not mean that you are now bulletproof," she said. While past attacks were often launched by one hacker on a single organization, AI can carry out attacks on a much bigger scale, hitting multiple organizations. AI can enhance malware by learning from past programs and use that knowledge to generate stronger and better malware, doing so on its own with no developer needed. "If AI is trying to break into your organization, it may be much more powerful than your existing solution," Waberska said. Internal auditors can ensure that their organizations understand and are prepared to address those risks. The internal audit team can't implement solutions, but they can have an informed conversation with the security team to see if they are considering these threats and implementing solutions. "It will take time for organizations to adopt new solutions, but it is important to be aware of the threats and have a plan to use adequate solutions to defend yourself," Waberska said.

Don't Forget the Human Element

While organizations gear up to ward off external cyber threats, internal auditors should keep in mind the danger posed by inadvertent mistakes made by the company's own people. Phishing attempts, for example, succeed we fail to recognize that a cybercriminal is trying to gain entry to the system or to an important password or other confidential data. "Internal auditors should look at how the organization is educating users about these threats," Waberska said. Employees may not understand that phishing emails have evolved. While it was once easy to spot red flags such as misspellings or strange fonts, AI is being used to write phishing emails that are much more sophisticated and realistic. "They look very real, and it's much easier for bad actors to generate them," she said.

[3] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society Tech Trends, September 6, 2023.

Conclusion

The threat of cyberattacks is a permanent feature of doing business in the digital world, and AI and its evolving usage present a new and provocative twist in the risk management battle against that threat. Internal auditors have an important role to play in:

- Ensuring that leadership and key teams are aware of the benefits and dangers related to AI.
- Determining and providing recommendations on how AI can enhance various cybersecurity efforts within the organization.
- Promoting awareness of the need to consider updated defenses against AI-powered cyberattack tools.
- Providing assurance on the company's understanding and use of AI technologies.

AI and related technologies can serve as valuable resources, but they are not a final answer. "Technology advancements can be great as long as you know how to use them in a way that is smart and safe," Waberska said. "You should always use professional judgment in considering the outputs."

Remember, as well, that while being conservative is an asset for internal auditors, they should not be "the office of no," Grafenstine said. Internal auditors should provide good control and risk advice, including insights on the risk of failure to keep up with technology. "It's a massive risk to not embrace technology, but we need to do it in a thoughtful way," she said.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.

Disclaimer

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of The IIA's volunteer North American Content Advisory Committee. Subject-matter experts are primarily identified and selected from The IIA's list of Global Guidance Contributors.

To apply to be added to the Global Guidance Contributors list, email Standards@theiia.org. To suggest topics for future Global Knowledge Briefs, email Content@theiia.org.

Copyright

November 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101