JS | HELD

PERSPECTIVES

Benefits of a Virtual Chief Information Security Officer (vCISO) in the Age of AI-Driven Cyberattacks

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Cyberattacks powered by artificial intelligence have become more sophisticated as bad actors utilize machine learning to analyze vulnerabilities, automate exploits, and outpace traditional security measures. Through the use of AI to refine their attack strategies, these cybercriminals are greatly increasing the likelihood of their success. Indeed, AI is emerging as the most frequently recognized and significant threat expected in the next five years.

As AI becomes an operational tool within more organizations, it can inadvertently increase their attack surface and create more potential vulnerabilities through the proliferation of "Internet of Things" (IOT) devices, which are linked to AI systems. Additionally, there is a shortage of skilled cybersecurity professionals knowledgeable about AI. Furthermore, AI-driven breaches can lead to significant reputational damage, where a single incident can erode customer confidence and lead to a loss of business. Finally, increased scrutiny from regulators may ensue, resulting in financial penalties and greater compliance costs.

Organizations must respond to AI-enabled cyber threats by raising awareness and fortifying their defenses. However, hiring a full-time chief information security officer (CISO) to design these responses can be cost-prohibitive. One alternative is to retain a Virtual Chief Information Security Officer (vCISO), a cybersecurity expert who provides strategic leadership and guidance on a contractual basis. Unlike a traditional CISO, a vCISO operates remotely and can serve multiple clients simultaneously, offering a flexible and cost-effective solution.

This article focuses on how a vCISO can address emerging AI cyber threats and help an organization address the following questions:

- What specific cybersecurity threats does the implementation of AI introduce to our organization, and how can we safeguard against them?
- How can we ensure the integrity and confidentiality of the data used and generated by our AI systems?
- What strategies and frameworks should we adopt to continuously monitor, detect, and respond to AI-related cyber threats?

UNDERSTANDING AI-DRIVEN THREATS

Automated Attack Tools

Automated attack tools are basically bad actors that operate without human intervention. These automated systems use software to find and exploit vulnerabilities in computer systems. They can run continuously, searching for weak points, which makes them particularly dangerous.

How Do They Work?

- **Scanning:** These tools start by scanning a network or website to find potential weaknesses. Since these tools are autonomous, they can continue running non-stop until they find a weakness. This allows attackers to carry out numerous attacks quickly and efficiently.
- **Exploiting Vulnerabilities:** Once a weakness is found, the tool can launch an attack. This could involve stealing sensitive data, installing malware (malicious software), or disrupting services.

Why Are They Used?

- **Efficiency:** Automated tools can perform attacks much faster than a human could. This speed increases the likelihood of success.
- **Scalability:** Attackers can use these tools to target many systems at once, which amplifies their impact.
- **Anonymity:** These tools can help attackers hide their identity and location, making it harder for defenders to track them down.

The Impact of Automated Attack Tools

Automated attack tools can lead to significant problems for individuals and organizations, including:

- **Data Breaches:** Personal information or sensitive data can be stolen, leading to identity theft or financial loss.

- **Service Disruptions**: Businesses can suffer downtime if their systems are attacked, resulting in lost revenue and a damaged reputation.

- **Increased Costs:** Recovering from an attack can be expensive, requiring time, resources, and expertise.

Protecting Against Automated Attacks

- **Regular Updates:** Keeping software up to date helps close vulnerabilities that attackers might exploit. There are a number of tools that will help your organization automate the process of patching vulnerabilities. The patches are released so you can update sooner than you were able to in the past.

- **Security Measures:** Implementing firewalls, intrusion detection systems, and encryption will add layers of protection that will help thwart the bad actors' attempts.

- **Employee Training:** Educating staff about cybersecurity best practices can help reduce the risk of falling victim to an attack. The use of strong passwords and instructing employees about the benefits of using them will help. Four out of five breaches are partially attributed to the use of weak or stolen passwords.

- **Monitoring:** Constantly monitoring networks for unusual activity can help detect and respond to attacks quickly.

Phishing and Social Engineering

How is AI Used in Phishing?

- **Creating Realistic Messages:** AI can generate highly convincing emails and messages. Using natural language processing, AI tools can craft messages that sound very genuine, making it hard for victims to spot a scam.

- **Targeting Victims:** AI can analyze vast amounts of data to identify potential victims. This could include social media profiles or previous interactions, allowing attackers to personalize their messages and increase the chances of success.

- **Automating Attacks:** With AI, attackers can send thousands of tailored emails in a fraction of the time it would take a human, significantly increasing the attack's reach.

How is AI Used in Social Engineering?

- **Behavior Analysis:** AI can analyze how people typically behave online, helping attackers predict how victims might respond to certain messages. This allows for more effective manipulation.

- **Deepfakes and Voice Cloning:** AI can create deepfakes—realistic fake images or videos—and clone voices. This can be used to impersonate someone the victim knows, making the attack seem more credible.

- **Learning from Past Attacks:** AI systems can analyze previous successful attacks, learning which tactics worked best. This allows attackers to refine their strategies for future attempts.

The Impact of AI on Phishing and Social Engineering

- **Increased Success Rates:** AI-driven attacks can be more sophisticated and targeted, making them harder to detect and resist.

- **Wider Reach:** Automated tools allow attackers to target a larger audience quickly, increasing the chance of finding a victim.

- **Constant Evolution:** As cybersecurity defenses improve, attackers using AI can adapt their strategies, creating a continuous battle between security measures and malicious tactics.

- **Increased Sophistication:** Using advanced language processing, cybercriminals can create highly convincing phishing messages that can mimic the tone and style of legitimate communications, making it harder for victims to identify them as scams.

- **Personalization of Attack:** AI can analyze vast amounts of data from social media and other sources to tailor attacks to specific individuals. This personalization makes phishing attempts more relevant and believable, increasing the likelihood of success.

- **Automation and Scale:** AI allows attackers to automate phishing campaigns, sending thousands of targeted emails or messages simultaneously. This scalability significantly increases the chance of finding a victim who will fall for the scam.

How to Protect Against AI-Driven Phishing and Social Engineering

- **Stay Informed:** Knowing what phishing looks like and being cautious with unsolicited messages can help your organization avoid these cyber traps. Training about the dangers presented and how to identify phishing, smishing, and social engineering efforts is key to reducing the likelihood of your employees falling victim to such attacks.

- **Verify Requests:** If you receive a suspicious email or message, verify the sender's identity through a separate communication channel before providing any information. Even after doing that you'll want to report the incident to IT for further investigation.

- **Use Strong Security Measures:** Implement multi-factor authentication (MFA) and long passphrases for passwords to add additional protection.

- **Report Suspicious Activity:** If you encounter a phishing attempt, report it to your organization or the relevant authorities. This helps improve defenses for everyone.

Malware Development

AI-powered malware can evolve by employing machine learning to adapt to detection methods. This adaptability makes it more challenging for traditional antivirus solutions to identify and neutralize threats. To protect against AI-generated malware, a vCISO can help organizations keep their software updated, install comprehensive security solutions that utilize advanced detection methods, and perform regular backups of critical data, making sure the information is stored offline or in a secure cloud environment.

Insider Threats

An insider threat can involve someone intentionally causing harm—like stealing data—or unintentionally creating vulnerabilities, such as through negligence. These threats can lead to data breaches, financial loss, and damage to an organization's reputation. Cybercriminals use AI to analyze employee behavior and identify vulnerabilities, allowing them to target individuals who may be more susceptible to manipulation.

How is AI Used in Insider Threat Detection?

- **Monitoring User Behavior:** AI systems can analyze patterns in how employees use company resources. By establishing a baseline of normal behavior, AI can detect unusual activities that may indicate a potential insider threat, such as accessing sensitive files without a legitimate reason.

- **Identifying Risk Factors:** AI can assess various factors, such as employee performance, access levels, and changes in behavior. For example, if an employee suddenly starts downloading large amounts of data, AI can flag this as a potential risk.

- **Automated Alerts:** When suspicious activities are detected, AI can automatically alert security teams. This prompt notification allows organizations to investigate potential threats before they escalate.

- **Analyzing Communication:** AI can review communications, such as emails and messages, to identify concerning behavior. For instance, it might flag messages that contain sensitive information being shared inappropriately.

- **Predictive Analytics:** AI can help predict which employees might pose a higher risk based on historical data and behavioral patterns. This proactive approach enables organizations to take preventive measures.

AI's Impact on Insider Threats in Organizations

AI significantly affects how organizations manage insider threats, both positively and negatively. On one hand, AI can enhance security by improving detection and response to suspicious behaviors. It analyzes user activities and identifies anomalies, helping security teams spot potential threats early. On the other hand, AI also empowers bad actors. Cybercriminals can use AI to exploit insider threats more effectively, creating targeted attacks that manipulate vulnerable employees. This dual-edge effect makes it essential for organizations to adopt advanced security measures and foster a culture of awareness to protect against insider risks effectively.

Benefits of AI on Insider Threat Management

AI significantly enhances insider threat management by enabling organizations to detect unusual behavior patterns and potential risks in real time. By analyzing user activity and automating alerts for suspicious actions, AI helps security teams respond quickly and effectively, ultimately reducing the likelihood of data breaches and ensuring a more secure environment. The use of AI in managing insider threats leads to several important benefits:

- **Enhanced Detection:** AI can identify subtle signs of insider threats that human analysts might miss, making detection more effective.

- **Faster Response:** Automated alerts mean that security teams can react more quickly to potential threats, reducing the risk of serious incidents.

- **Resource Efficiency:** By automating many monitoring tasks, AI allows security teams to focus on more complex issues rather than spending time on routine monitoring.

Challenges and Considerations

Adapting AI systems to continuously evolving threats requires ongoing investment and expertise, making it difficult for organizations to maintain effective insider threat programs. Balancing security with privacy and ensuring accuracy remains a critical challenge in this area. Some additional concerns to consider are:

- **Privacy Concerns:** Monitoring employee behavior can raise privacy issues. Organizations must balance security needs with respect for individual privacy.

- **False Positives:** AI systems may sometimes flag innocent activities as suspicious, leading to unnecessary investigations. It's essential to fine-tune these systems to minimize errors.

Protecting Against Insider Threats

- **Implement Strong Policies:** Organizations should have clear policies regarding data access and employee conduct to guide appropriate behavior.

- **Provide Training:** Educating employees about security practices and the importance of protecting sensitive information can help prevent unintentional insider threats.

- **Use AI Responsibly:** Organizations should employ AI tools ethically, ensuring they respect privacy while effectively managing risks.

HOW A VCISO CAN PREVENT & MITIGATE AI CYBERATTACKS

A vCISO can provide organizations with enhanced security posture, cost-effectiveness, expert guidance, and the ability to adapt to evolving threats, especially those driven by AI.

Contracting with a vCISO allows organizations to implement a structured risk management framework by bringing expertise in threat intelligence, and monitoring and enabling organizations to adopt proactive measures against emerging threats. Furthermore, since every organization has unique security needs, a vCISO can develop customized security strategies that align with the enterprise's specific goals, industry standards, and regulatory requirements by taking proactive steps in the areas below:

Implementing advanced security solutions

- **AI-Powered Security Tools:** Use AI-driven solutions for threat detection and response to stay ahead of emerging threats. AI-enabled security tools allow organizations to identify and respond to cyber threats in real time. By automating routine tasks and analyzing vast amounts of data, these tools improve overall efficiency and effectiveness in maintaining a secure environment.

- **Behavioral Analytics:** Employ solutions that analyze user behavior to identify anomalies indicative of potential attacks, including unusual patterns of activity among employees. This enables early detection of potential insider threats and malicious intent or security risks, thus allowing for timely intervention and enhanced security.

Encouraging a security-first culture

- **Training Programs:** Regularly educate employees on recognizing phishing attempts and understanding security protocols. Providing security training to employees ensures that they are aware of potential threats and understand best practices for protecting sensitive information. Regular training helps create a culture of security, reduces the risk of human error, and empowers staff to recognize and respond to security incidents effectively.

- **Incident Reporting:** Promote a culture where employees feel comfortable reporting suspicious activities without fear of reprisal. Organizations should emphasize that reporting is a vital part of maintaining security.

Conducting regular risk assessments

- **Risk Assessments:** Conducting a cybersecurity risk assessment using a structured framework like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) offers several key benefits for organizations. It provides a comprehensive approach to identifying vulnerabilities and threats, enabling organizations to prioritize risks based on their potential impact. By following a standardized framework, organizations can ensure consistency in their assessments and improve communication among stakeholders. Additionally, using NIST's guidelines helps organizations meet compliance requirements and fosters a proactive security posture, ultimately strengthening their overall cybersecurity strategy.

- **Vulnerability Scans:** Perform routine scans to identify and address potential weaknesses in systems and processes. These proactive assessments help ensure that security measures are effective and maintain compliance with industry standards, ultimately protecting sensitive data and maintaining trust with customers.

- **Penetration Testing:** Engage third-party experts to simulate attacks and uncover security gaps. These tests provide valuable insights into potential weaknesses, allowing organizations to strengthen their security posture and better protect sensitive information from cyber threats.

Establishing an incident response plan

A robust incident response plan (IRP) helps organizations quickly identify and contain security incidents, reducing the potential impact and damage to systems and data. A strong IRP also helps organizations meet regulatory requirements and industry standards. With a structured response in place, organizations can recover from incidents more swiftly, ensuring minimal disruption to operations and restoring normalcy effectively. The key steps to constructing an effective IRP include:

- **Regular Training and Drills:** Conduct ongoing training and simulation exercises for the incident response team to ensure everyone understands their roles and can respond quickly during an actual incident.

- **Continuous Monitoring and Updating:** Regularly review and update the IRP based on emerging threats, lessons learned from past incidents, and changes in organizational structure or technology.

- **Clear Communication Channels:** Establish defined communication protocols within the organization and with external stakeholders to ensure timely information sharing and coordination.

CONCLUSION

The rise of AI presents significant cybersecurity challenges that organizations must confront to protect their digital assets and maintain operational integrity. By adopting proactive strategies, organizations can better defend against AI-driven cyber threats. To do so by hiring a full-time CISO can be prohibitively expensive – especially for small to medium-sized enterprises. Instead, retaining a vCISO provides access to top-tier cybersecurity expertise without the burden of a full-time salary, benefits, and associated overhead costs. Another advantage is that vCISO services are scalable, allowing organizations to adjust their level of engagement based on changing needs, whether it's full-time, part-time, or on-demand. More important is the fact that investing in vCISO services can prevent costly data breaches that result in litigation, operational disruptions, reputational damage, and regulatory fines. By identifying vulnerabilities and implementing robust security measures, organizations using a vCISO can save significantly on potential incident-related costs.

Acknowledgements

We would like to thank Kevin Gorsline for providing insight and expertise that greatly assisted this research.

Kevin Gorsline is a Managing Director in J.S. Held's Global Investigations practice who joined following J.S. Held's acquisition of TBG Security. For several years, Kevin served as the Chief Operating Officer and head of the Risk and Compliance practice at TBG Security, where he was responsible for providing the leadership, management, and vision necessary to ensure that the company had the proper operational controls, administrative and reporting procedures, and people systems in place to effectively grow the organization and to ensure financial strength and operating efficiency. His experience and leadership throughout his career have been focused on developing and delivering information security services and solutions, providing outstanding client service, and driving profitable revenue growth. Kevin brings established proficiency as an IT leader with extensive experience in risk and compliance services, applications development, and implementation projects both in the United States and abroad.

Kevin can be reached at kevin.gorsline@jsheld.com or +1 843 890 8596.

This publication is for educational and general information purposes only. It may contain errors and is provided as is. It is not intended as specific advice, legal or otherwise. Opinions and views are not necessarily those of J.S. Held or its affiliates and it should not be presumed that J.S. Held subscribes to any particular method, interpretation or analysis merely because it appears in this publication. We disclaim any representation and/or warranty regarding the accuracy, timeliness, quality, or applicability of any of the contents. You should not act, or fail to act, in reliance on this publication and we disclaim all liability in respect to such actions or failure to act. We assume no responsibility for information contained in this publication and disclaim all liability and damages in respect to such information. This publication is not a substitute for competent legal advice. The content herein may be updated or otherwise modified without notice.