JISSec
Journal of Information Systems Security

CYBERSECURITY CHALLENGES IN AN AI ENABLED WORLD

Gurpreet Dhillon

University of North Texas, USA

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 19, Issue 3

www.jissec.org

In the rapidly evolving landscape of cybersecurity, a powerful force has emerged - artificial intelligence (AI). With cyberattacks becoming increasingly sophisticated and the number of connected devices multiplying, AI and machine learning have become indispensable tools in the fight against cybercriminals. This editorial note explores these challenges and discusses possible solutions.

Picture this: a team of cybersecurity professionals huddled together in a high-tech control center; their eyes glued to an array of screens displaying real-time data. The room buzzes with a sense of urgency as they anticipate the next cyber threat. In the midst of this intense atmosphere, AI stands as a silent ally, helping them stay one step ahead of the adversaries.

One of the most critical roles of AI in cybersecurity is identifying cyber threats and malicious activities. Traditional software, though powerful, struggles to keep pace with the sheer volume of new malware unleashed every week. This is where AI's prowess shines. Equipped with sophisticated algorithms, AI systems act as vigilant sentinels, detecting malware, recognizing patterns, and even spotting the tiniest indications of potential attacks before they can infiltrate the system.

But AI's capabilities don't end there. It is armed with the gift of natural language processing, scouring the vast expanse of the internet to curate data from research papers, blogs, and news stories related to cyber threats. The result? Predictive intelligence that empowers organizations to anticipate new anomalies, cyberattacks, and plan effective prevention strategies tailored to their unique needs.

The internet is teeming with bots - some harmless, others perilous. Sorting the good from the bad can be like searching for a needle in a haystack. However, AI comes to the rescue again, differentiating between good bots (such as search engine crawlers), bad bots, and human users. Armed with this knowledge, organizations can respond precisely and effectively to automated threats.

Knowledge is power when it comes to cybersecurity. And AI, with its unparalleled ability to analyze vast volumes of data, equips cybersecurity teams to continuously adapt their strategies. Through behavioral pattern analysis, they can discern the average user journey and detect risky, unusual activities that hint at potential threats. As they outsmart the bad bots, cybersecurity professionals maintain a tactical edge.

But AI's influence extends beyond detecting and responding to threats. It also provides organizations with a comprehensive understanding of their IT asset inventory - a detailed record of all devices, users, and applications with varying levels of access. This knowledge empowers them to predict vulnerabilities and allocate resources where they are most needed, reinforcing their cyber defenses.

In today's world of remote work, securing all endpoints becomes a pressing concern. While traditional antivirus solutions and VPNs help, they rely on signature updates to stay ahead of new threats. Here, AI offers a game-changing approach, establishing a baseline of behavior for endpoints through a continuous training process. When an abnormal activity occurs, AI swiftly flags it and takes action, preventing ransomware attacks or notifying cybersecurity teams.

AI has become the trusted companion of cybersecurity professionals, empowering them with predictive intelligence, behavior analysis, and proactive protection measures. By leveraging AI capabilities, organizations fortify their defenses and maintain a vigilant and agile cybersecurity posture in the face of ever-evolving cyber risks. In this ongoing battle between good and evil, AI stands firmly on the side of the defenders, guarding the digital realm with its unparalleled prowess.

All is not good

However, as with any powerful tool, there are potential downsides that demand careful consideration. Building and maintaining an AI system requires substantial resources and financial investments. The process of acquiring diverse sets of data for training AI can be time-consuming and costly. Moreover, the quality of data is crucial, as insufficient data may lead to incorrect results and false positives. Organizations must be prepared for the commitment and financial implications of incorporating AI into their cybersecurity strategies.

But that's not all; there's another potential risk that looms on the horizon—the misuse of AI by cybercriminals. They can exploit AI for adversarial attacks, exploiting its vulnerabilities to cause machine learning models to misinterpret inputs. Even advanced security features, such as FaceID on iPhones, can be undermined by deceptive images generated by adversarial AI. This poses a new level of threat to our digital security.

Despite these challenges, the potential of AI in cybersecurity remains immense. It offers an arsenal of tools to cybersecurity professionals, empowering them to reinforce best practices and minimize attack surfaces. The capabilities of AI enable continuous monitoring and adaptive defense mechanisms, giving organizations a stronger overall cybersecurity posture.

The way forward

To navigate the challenges of an AI-driven cybersecurity landscape, organizations should adopt the following principles:

1. Move beyond outdated assumptions: Continuous AI security education is crucial to keep all stakeholders updated on evolving security needs and fortify defenses against AI-driven security risks;

2. Shift focus from excessive reliance on technical solutions: Integrating human-centric approaches alongside technical measures, and emphasizing ethical responsibility, helps safeguard information effectively;

3. Enhance reliance on AI for cybersecurity decision making: AI's impact in threat defense, anomaly detection, and incident response enhances cybersecurity capabilities, but human oversight remains essential for ethical practices;

4. Derive access rights from responsibility and authority structures: Clear roles and accountability ensure secure information access, especially with AI's involvement in decision-making processes;

5. Address people issues adequately: Prioritizing people management and fostering a security-aware culture helps mitigate risks posed by human errors. [Addressing people issues is not new. Over the years various schools have made such calls. See Hitchings, 1996; Dhillon, 2001; Zainudin and Ur-Rahman, 2015];

6. Foster trust: In diffuse environments, trust plays a pivotal role in managing information security. Establishing trust mechanisms and clear policies builds confidence in AI-driven operations. [Trust has been well studies in the literature, with various scholar making calls. For example, see Mutimukwe, Kolkowska and Grönlund, 2020; Moores and Dhillon, 2002; Chen and Dhillon, 2003];

7. Promote and define ethical principles: Ethical guidelines guide responsible use of AI technologies in an ever-changing environment. [Over the years, scholars have made several calls for considering responsibility and accountability issues. For instance, see Backhouse and Dhillon, 1996, among others].

By adopting these guidelines and taking a proactive approach to managing cybersecurity, organizations can harness technology's benefits while safeguarding data, systems, and human values in an increasingly virtualized and AI-driven world.

References

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, *5*(1), 2-9.

Chen, S., & Dhillon, G. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management*, *4*(2/3), 303-318.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165-172.

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. In S. K. Katsikas & D. Gritzalis (Eds.), *Information systems security: facing the information society of the 21st century* (pp. 3-12). Chapman & Hall.

Moores, T., & Dhillon, G. (2002). Trust, and the role of privacy seals in e-commerce. *Communications of the ACM*, *46*(12), 265-271.

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, *37*(1), 101413.

Zainudin, D., & Ur-Rahman, A. (2015). The Impact of the Leadership Role on Human Failures in the Face of Cyber Threats. *Journal of Information System Security*, *11*(2), 89-109.

Gurpreet Dhillon holds the G. Brint Ryan Endowed Chair of Artificial Intelligence and Cybersecurity at the University of North Texas, USA. He also holds honorary appointments at the University of KwaZula-Natal, South Africa and Universidade de Lisboa (University of Lisbon], Portugal. Gurpreet earned a Ph.D. from the London School of Economics. He received an Honorary Doctorate from Örebro University, Sweden in 2019. Several of his research papers have been published in FT50 journals. Additionally, he has been featured in the Wall Street Journal, the New York Times, USA Today, Business Week, CNN, NBC News, and NPR.