Impact of AI in Cyber Security

Ryan Coon

UNV-507

Professor Tina Salata

July 17, 2024

Background

Artificial Intelligence (AI) has emerged as a transformative force in the field of cybersecurity, revolutionizing the way organizations defend against cyber threats and safeguard sensitive information. The integration of AI technologies, such as machine learning and predictive analytics, has enabled advanced threat detection, rapid incident response, and proactive security measures. As the digital landscape evolves, the role of AI in cybersecurity becomes increasingly crucial in mitigating the growing complexity and sophistication of cyber attacks. According to Kaziukonis (2024), “ AI excels at providing immediate responses to security incidents. It can automate the processes, saving time and minimizing damage by isolating infected systems and blocking intrusive activities. But this automated rapid response system can sometimes backfire.” As with everything in technology, we must weigh the good against the bad, but in cybersecurity it could affect millions of people if the AI malfunctions.

Current problem & Research Questions

According to ISC2 (2024) “ a survey of ISC2 members revealed that 88% are already seeing AI impact their existing roles, with most seeing positives in the form of improved efficiency despite concerns over redundancy of human tasks.” We can take this that so far they have not yet encountered any downsides. They can now use AI to complete the mundane and repetitive tasks that would require around the clock monitoring.

What are the downsides of AI in cybersecurity?

What new cybersecurity risks might modern AI (e.g., generative AI) create?

How might AI improve cybersecurity in the future?

Research Plan

One would quantitatively measure the beneficial impact of AI in cybersecurity practices through empirical data analysis. I suspect that utilizing AI technology in cybersecurity would lead to faster incident response, improved threat detection, and overall enhanced security posture. Some metrics that can be looked at are number of detected threats, incident response time, reduction in security breaches, cost savings, and the accuracy of predictive analysis. With the number of detected threats, we would compare the effectiveness of the AI-powered detection systems versus the traditional methods by comparing the number of threats detected and neutralized respectively. With incident response time we would measure the time taken to respond to cybersecurity incidents with AI-enabled tools compared to manual interventions. Reduction in security breaches we would quantify the decrease in successful cyber attacks after implementing AI-driven security measures. With cost savings we could evaluate the financial impact of AI integration in cybersecurity by calculating cost savings in incident response, data protection, and system maintenance. Lastly we would look at the accuracy of predictive analysis by assessing the accuracy of AI algorithms in predicting potential security threats and vulnerabilities. With all these metrics, we would then summarize the findings in order to demonstrate the tangible benefits of AI in enhancing cybersecurity practices. With this summary, we can then provide recommendations for specific organizations that are looking to leverage AI technologies to help improve their cybersecurity defense based on the metrics analyzed.

References:

ISC2. (2024, February 21). *The real-world impact of AI on cybersecurity professionals*. Www.isc2.org. https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

Kaziukonis, V. (2024, April 12). *Council Post: AI In Cybersecurity: Understanding The Advantages And Disadvantages*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2024/04/12/ai-in-cybersecurity-understanding-the-advantages-and-disadvantages/#:~:text=AI%20excels%20at%20providing%20immediate