

Artificial Intelligence for Cybersecurity

Samuel Woodruff

Old Dominion University

CYSE 280 Research Paper

Professor Gladden

April 17, 2025

Introduction

Artificial Intelligence is a technology that has seen a rapid explosion in development over the past couple of years. In fact, artificial intelligence has made such swift progress that it makes the artificial intelligence available a few years ago look almost archaic. Every sector is seeking ways to harness the power of artificial intelligence to maximize efficiency, lower costs, and develop dynamic innovations. Cybersecurity is a field in which artificial intelligence can prove to be extremely useful. With brand new cyberthreats appearing seemingly every day, artificial intelligence may just be the tool needed in order to thwart future cyber attacks. By utilizing artificial intelligence, organizations can look to make use of its predictive capabilities, scan for threats, and prevent cyber attacks before they come to fruition. Additionally, it's important to consider whether or not the implementation of artificial intelligence for cybersecurity is cost-effective for organizations. Lastly, it's important to consider the fact that artificial intelligence is likely to be misused by cybercriminals to carry out attacks. After examining these topics, a better understanding of artificial intelligence's role in cybersecurity and the world will be established.

Overview of Research

For this research paper, multiple sources will be cited to create understanding around the topic of artificial intelligence in cybersecurity. The purpose of this research paper is to examine how artificial intelligence will play a role in cybersecurity, how cost-effective it will be for organizations to implement, and the potential dangers artificial intelligence may bring when used in a cyberattack. Before this is examined, though, artificial intelligence integration into cybersecurity must be understood. One of the largest software companies in the world, Microsoft, explains that artificial intelligence in cybersecurity functions by "...evaluating

massive amounts of data across multiple sources to identify patterns of activity across an organization, such as when and where people sign in, traffic volumes, and the devices and cloud apps that employees use” (Microsoft, p.1, n.d.). In being used this way, artificial intelligence integration for cybersecurity allows for massive amounts of data to be analyzed. Once the artificial intelligence has a feel for normal operations, it will be able to help cybersecurity professionals by flagging abnormal behavior and data anomalies. As a whole, artificial intelligence integration into cybersecurity has the potential to make organizations more secure and enhance the role of cybersecurity professionals. With that being said, the effectiveness of artificial intelligence integration for cybersecurity will be examined by using compiled data. Additionally, the cost-effectiveness of artificial intelligence integration for cybersecurity must be considered and supported by given data. Finally, potential uses for artificial intelligence in cyberattacks will be discussed and prior cases will be considered.

Processes to Follow: How Does AI Integrate into Cybersecurity?

While the way artificial intelligence integrates into cybersecurity was discussed briefly earlier on, the process is much more complex and in depth. One of the primary ways artificial intelligence has been integrated into cybersecurity is through machine learning. Machine Learning is described by Michele Daryanani as “...training computers to learn from data, allowing them to make predictions or decisions without being explicitly programmed” (Daryanani, p.1, n.d.). In cybersecurity, machine learning can be used to establish a sort of baseline for normal activity across a network. The computer learns what data is normal to encounter and what processes typically occur. In this way, machine learning is then able to identify cyberthreats and other anomalies when examining them against the baseline. Another way machine learning integrates into cybersecurity is by detecting “...never-before-seen malware

that is trying to run on endpoints” (Cisco, p.1, n.d.). Additionally, machine learning is made useful by “...analyzing suspicious cloud app login activity, detecting location-based anomalies, and conducting IP reputation analysis to identify threats and risks in cloud apps and platforms” (Cisco, p.1, n.d.). Overall, the processes by which artificial intelligence is used in cybersecurity mostly includes offering superior detection capabilities to support cybersecurity professionals.

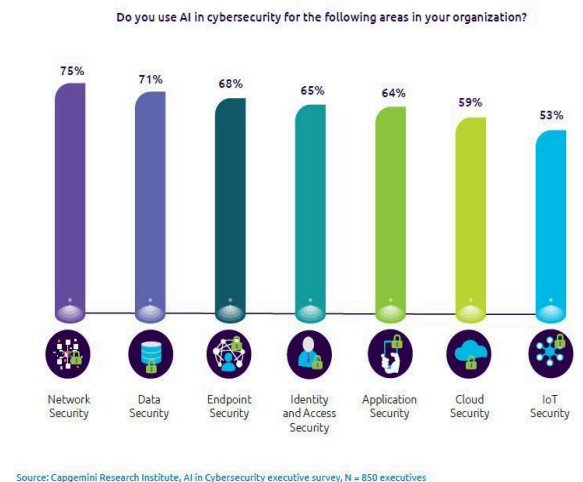
Artificial Intelligence Cybersecurity Integration for Organizations (Tools)

To illustrate the growth of artificial intelligence use in the field of cybersecurity, data will be provided along with graphics. Artificial intelligence is growing at a seemingly exponential rate and it is something that organizations have taken notice of as well. Louis Columbus writes that of the interviewed organizations “48% say their budgets for AI in cybersecurity will increase by an average of 29% in Fiscal Year (FY) 2020”

(Columbus, p.1, 2019). Seeing as how this article is around five years old, this number is surely higher today. A 29% increase in budget for AI in cybersecurity from the reporting organizations is also a considerable increase. Additionally, the provided graphic courtesy of Capgemini details the many ways

organizations are tailoring artificial intelligence for their cybersecurity needs. To show how much artificial intelligence has begun to integrate into cybersecurity organizations and businesses as a whole, PYMNTS reports that roughly 55% of businesses rely on artificial

intelligence-driven cybersecurity to support their security. (PYMNTS). This number will surely

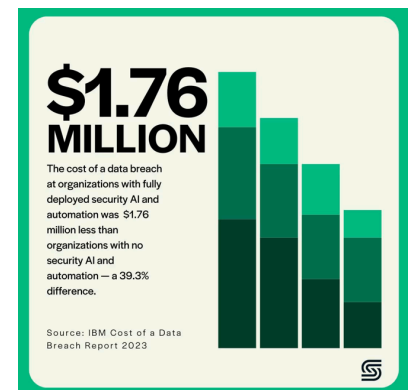


Source: Capgemini
*“Reinventing
 Cybersecurity with
 Artificial Intelligence”*
 (Frank, et. al, 2019).

increase in the coming years as cyberthreats become more dynamic and artificial intelligence continues to evolve.

Artificial Intelligence in Cybersecurity: Is it Cost Effective? (Tools)

Artificial intelligence integration into cybersecurity has largely been reported as being quite cost effective for organizations, big and small. One article by Mazaher Kianpour found that “...the strategic integration of AI in cybersecurity is not merely a technological upgrade but a complex economic decision that hinges on understanding and leveraging the elastic properties of AI” (Kianpour, p.1, 2024). This is to say that while artificial intelligence integration into cybersecurity has been mostly positive as an investment, its implementation is complex and it must be well-researched to establish a positive ROI. In addition to this, out of the executives interviewed, PYMNTS found that “...firms that use the technology for high-impact tasks like data security expect AI’s ROI to be very positive in 5.6 years and expect that the technology will be fully embedded in their organizations in 6.9 years” (PYMNTS, p.1, 2025). This shows that executives of several organizations are confident in artificial intelligence’s ability to be fully integrated into their cybersecurity and expect positive returns on their investments in the coming years. The graphic provided courtesy of IBM shows just how much businesses that utilize artificial intelligence save from potential cyberattacks compared to those that do not utilize artificial intelligence for their cybersecurity. As a whole, artificial intelligence integration into cybersecurity has mostly proven to be extremely beneficial and cost-effective for organizations.



Source: IBM Cost of a Data Breach Report (2023)

Artificial Intelligence Cyberattacks: What are the Risks? (Tools)

While artificial intelligence has been proven to be extremely beneficial and cost-effective for organizations, cybercriminals have also taken notice of the potential power artificial intelligence holds. In fact, cybercriminals are causing new headaches for cybersecurity professionals by utilizing artificial intelligence to attack organizations in new ways. Lucia Stanham states that cybercriminals have begun refining the way they use artificial intelligence, writing that “...growing access to AI- and generative AI-enabled tools is allowing adversaries to automate attack research and execution” (Stanham, p.1, 2025). Before the explosion of capability in artificial intelligence, cyberattacks required an individual to conduct research and carry out the attack themselves. Now, artificial intelligence has streamlined the ability for cybercriminals to attack organizations in new ways. Stanham also writes that another way cybercriminals have begun using artificial intelligence is by using “...AI-generated video, image, or audio file that is meant to deceive people” called a Deepfake. (Stanham, p.1, 2025). Deepfakes have become a growing problem that anyone can become a victim to. Deepfakes have the potential to put words in someone’s mouth that they never said or be in situations in which they were never in. This is a disturbing capability that cybercriminals can use to deceive, stir up controversy, and even blackmail. The provided graphic courtesy of GAO shows two of the ways deepfakes work. Deepfakes can swap individual’s faces onto another as well as change their expressions, words, and facial movements. All in all, it is not only organizations that are making the use of artificial intelligence, but also cybercriminals around the world.

*Source: GAO
Deconstructing
Deepfakes—How
do they work and
what are the risks?
(2020)*

Conclusions

Cybersecurity is an ever-growing field that must respond to technological advances as well as new developments every day. Over the past few years, artificial intelligence has rapidly developed. The artificial intelligence that was used just a few years ago seems almost archaic to

what is available today. While it has been in development for a long time, artificial intelligence has recently begun to see rapid deployment into organization's cybersecurity. This is done through a number of ways including network monitoring, cloud protection, and much more. Its primary use, though, tends to be for the purpose of network monitoring and early-threat detection. Organizations that implement artificial intelligence into their cybersecurity have typically shown very positive returns on their investments and save more money than organizations that do not employ artificial intelligence into their cybersecurity operations. Businesses and organizations are not the only ones that have taken notice of artificial intelligence's capabilities though. Cybercriminals have begun to research new ways to attack individuals and organizations through the use of artificial intelligence. This is mostly done through the automation of research and attacks, deepfakes, and much more. Overall, artificial intelligence is not going anywhere and is going to continue to grow. Organizations must take advantage of this development to make sure their systems are as secure as possible and to remain dynamic.

Works Cited

Capgemini. (n.d.). Reinventing cybersecurity with artificial intelligence: The new frontier in digital security.

<https://www.capgemini.com/resources/reinventing-cybersecurity-with-artificial-intelligence/>

Cisco. (n.d.). What is machine learning in security?

<https://www.cisco.com/site/us/en/learn/topics/security/what-is-machine-learning-in-security.html#:~:text=In%20security%2C%20machine%20learning%20continuously,by%20uncovering%20suspicious%20user%20behavior.>

CrowdStrike. (n.d.). AI-powered cyberattacks.

<https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/>

CSIAAC. (n.d.). Artificial intelligence in cybersecurity: How substituting and scaling impact investment returns.

<https://csiac.dtic.mil/articles/artificial-intelligence-in-cybersecurity-how-substituting-and-scaling-impact-investment-returns/>

Forbes. (2019, July 14). Why AI is the future of cybersecurity.

<https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/>

GAO. (n.d.). Deconstructing deepfakes: How do they work and what are the risks?

<https://www.gao.gov/blog/deconstructing-deepfakes-how-do-they-work-and-what-are-risks>

IBM. (2023). Cost of a data breach report 2023. <https://www.ibm.com/reports/data-breach>

KPMG. (n.d.). How artificial intelligence influences cybersecurity risk.

<https://kpmg.com/ch/en/insights/cybersecurity-risk/artificial-intelligence-influences.html#:~:text=AI%20and%20machine%20learning%20in,unauthorized%20access%20to%20your%20system.>

Microsoft. (n.d.). What is AI for cybersecurity?

<https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity#:~:text=AI%20for%20cybersecurity%20works%20by,cloud%20apps%20that%20employees%20use.>

PYMNTS. (2025). 55% of companies have implemented AI-powered cybersecurity.

<https://www.pymnts.com/cybersecurity/2025/55-of-companies-have-implemented-ai-powered-cybersecurity/>