

SECURITY/PRIVACY CONCERNS AND MITIGATIVE MEASURES IN THE AGE OF ARTIFICIAL INTELLIGENCE

ARTIFICIAL INTELLIGENCE (AI)

THE RISKS & BENEFITS OF INTRODUCING NEW TECHNOLOGY TO YOUR ECOSYSTEM



“

Prepare for the unknown by studying how others in the past have coped with the unforeseeable and the unpredictable.

– George S. Patton

”

Let's think about this saying and how it relates to the current change we are seeing in business-related technology. With every new addition into our ever-changing ecosystem, there have been ways to understand, add and protect business data that could be affected.

Let's think about digital transformation, which is one of the biggest buzzwords of the 21st century. Cloud computing is part of this. Although it has been around for well over 20 years, the potential risks it can introduce into our businesses are sometimes not fully understood or considered. Proper security and privacy measures need to be implemented as we extend our protected information into the ether.

Another big buzzword that is transforming the way businesses are taking advantage of new technology is artificial intelligence, or AI. This misunderstood technology has given a bad name as of late, due to the fear that it could lead to the downfall of civilized nations. This thought process can be easily mitigated by understanding some of advantages and disadvantages that allowing AI into your ecosystem brings.



WHAT IS AI?

First, let's discuss what AI is and what enables it to learn and adapt. Artificial intelligence is really a simulation of human intelligence in machines that are programmed to think like humans. In other words, algorithms are utilized to learn, create and adapt to “normal” processes and changes that may be presented.

So, what makes AI perform tasks and make decisions that would most likely require human intelligence? How does AI learn from data, recognize patterns and adapt to new information or situations?

In simple terms, it is its subcomponents, machine learning and deep learning, that allow all this data to be collected, correlated, pattern recognized and adapted to new information. Machine learning allows machines to learn from data and make decisions without explicit programming. This is called unsupervised learning, which is self-learning based on “if, then,” simplistic decision trees and anomaly detection based on profiles and patterns. Deep learning, a subset of machine learning, leverages artificial computational models for more advanced tasks. ChatGPT is an example of machine learning that utilizes deep learning to create text, images, video and audio as directed.

Now, let's get to the stuff that affects our everyday business lives. If we have a system that can think and learn like humans and allows machines to process and analyze large amounts of data, identify patterns or anomalies and make predictions and overall decisions based on collected information, how can we trust the outputs that come from such machines? Where are the safeguards that protect decisions being made by human or machine from erroneous data?

We have all heard of how AI can elevate security by learning and adapting to network security, anti-malware capabilities and fraud detection by understanding anomalies, but what about the risks that AI can pose by simply not understanding the threats within? These include:



Cyber Attack Optimization

By utilizing generative AI, texts, images, audio and video can be manipulated to elevate attacks.

Automated Malware

With the assistance of ChatGPT, users can try to find loopholes in executables without the user's awareness.

Physical Security

In a world of IoT, AI used maliciously could pose a threat to human lives when applied to verticals like manufacturing, healthcare, utilities and autonomous vehicles.

AI Privacy Risks

As AI utilizes data lakes to make business decisions, so could a hacker who manipulates the system and collects personal identifiable data.

Data Manipulation and Poisoning

This key risk could be detrimental to decisions being made by healthcare, utilities, manufacturing and so on, as data could become compromised and used erroneously.

Impersonation

With the right apps, voice calls can be impersonated, allowing authenticated safeguards to be circumvented.

Reputational Damage

The physical, monetary and consumers' confidence risks could be catastrophic to any organization that suffers a breach, data compromise or leakage.





HOW CAN YOU PROTECT YOUR ORGANIZATION FROM THESE RISKS?

There are seven key building blocks to protecting your organization from AI risks:

1. Understand and assess your AI systems.

As you introduce a system into your environment, assess the platform and implement monitoring tools to mitigate any risks that could be present via known vulnerabilities.

2. Limit personal information shared through automation.

Allow the platform to collect data that is relevant to its operations. Do not allow access to data that is private or protected by law.

3. Prioritize data security (transit, rest and use).

Keep data protected in a similar data loss prevention capacity. Encrypt private data, keep vigilant access control lists, and ensure that storage and backup technologies have checksums and encryption in order to mitigate unauthorized changes.

4. Use advanced antivirus technology to mitigate malicious threats.

Profile-based anomalous behavior should be detected.

5. Invest in continuous staff training.

Ensure that your staff is aware of possible AI risks that could disrupt their daily activities. For example, make sure they know how to recognize emails that could be potential phishing attacks designed by AI.

6. Develop a vulnerability management program.

This end-to-end process involves identifying, analyzing and prioritizing vulnerability risks, which can reduce your attack surface by taking advantage of AI technology.

7. Understand limitations and ethical considerations.

As great as AI data analysis and reporting can be, it is imperative that users are trained on double checking AI outputs to ensure biases are being tracked. This is highly dependent on the data that is being stored and collected to make a concise, ethical decision.





THE BENEFITS OF AI CYBER SECURITY

We've covered the risks that AI can introduce to your organization. Now, let's discuss the ways that AI can be utilized to bolster your cyber security program.

Cyber Threat Detection

Cyber threat intelligence and threat hunting is elevated with a proper AI system.

Predictive Models

Improve anomalous detection times and response in order to stop attacks.

Phishing Detection

With proper email profiles and “normalized” traffic, anomalous entries can be detected before delivery.

Network Security

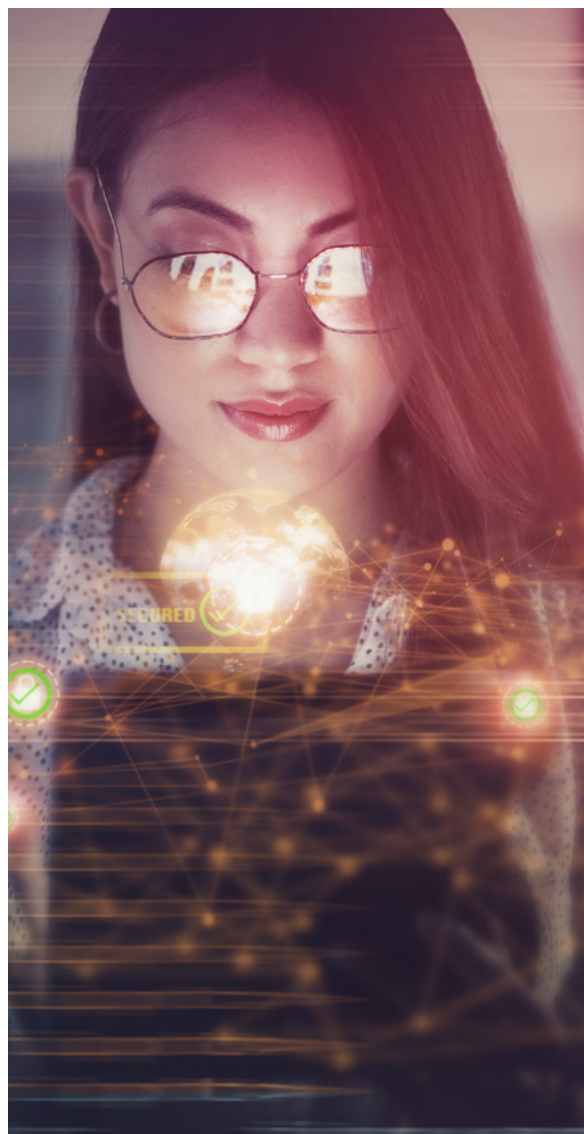
The ability to detect unauthorized access, unusual codes and other anomalous behavior will provide the ability to prevent further attacks.

Automated Incident Responses

AI systems can boost threat hunting, incidents of compromise detection and incident responses. All these can reduce incident response times and reduce potential harm to your network.

Insider Threat Mitigation

These types of threats come in two categories: malicious and unintentional. Both can be detected via anomalous behavior based on profiled patterns from each user.



Strengthening of Access Control

AI can strengthen user access by including biometrics, multi-factor authentication and location-based usage to track logs and compare based on individual attributes.

Identification of False Positives

One of the biggest issues with log events is the threat of investigating false positives. It is a time-consuming practice that taxes resources. AI systems can mitigate these risks by managing low-probability threats.

IT Staffing Efficiency and Costs

AI systems allow for 24/7 prevention, detection and response, allowing for SOC employee efficiencies and lowered costs (money spent on overtime, etc.).



MODERN CYBER SECURITY SOLUTIONS FOR PHYSICAL AND DIGITAL EXPERIENCES

C1 can help you usher in the proper safeguards and advantages mentioned above in AI environments by utilizing the strength of our partners and our security expertise in designing, implementing and monitoring controls that **prevent, detect and respond**—all while mitigating the risks that AI could introduce to your ecosystem. Having systems that can deep dive into applications and codes to decipher possible changes and threats to your environment is key to AI risk controls.

Understanding and being predictive in providing real-time business decisions is key to business competitiveness. With AI's ability to provide advanced analytics, the advantages have never been greater, and utilizing this same technology to detect changes to your network, data and applications will also elevate your security and privacy measures. Addressing the risks and taking advantage of the many benefits of AI will be instrumental to a stable and transformative digital future.

ABOUT THE AUTHOR



Vito Nozza is the Principal Cyber Security Lifecycle Consultant at C1. His career spans 20+ years in enterprise architecture, with 15 years specific to cyber security. He has held roles as a CTO, Director, Principal Architect and Global Security Advisor, which have all led to establishing guidance and consultative measures to SME and enterprise-grade entities.



MANAGING AI RISK IS NOT A ONE-TIME SOLUTION.

IT'S AN ONGOING JOURNEY.

CONTACT US TO GET STARTED WITH YOURS.

SCHEDULE A CONSULTATION