Artificial Intelligence Risks

Artificial intelligence can be used to enhance Cybersecurity, but it also poses significant risks. The relationship between Artificial Intelligence and Cybersecurity is intermingled. On the one hand, AI can be used to improve cybersecurity by analyzing huge amounts of data to detect patterns and anomalies that might indicate a cyber-attack. This can include identifying suspicious network traffic, detecting malware, and identifying vulnerable systems. AI-based systems can also be used to automatically respond to cyber threats, such as by shutting down infected systems or quarantining malicious files. On the other hand, Cyber attackers can also use AI to improve the sophistication and effectiveness of their attacks. For example, AI can be used to generate targeted phishing attacks that are designed to evade detection. AI-based malware can also adapt and evolve to avoid detection by traditional security systems.

It's important for organizations to understand these risks and take steps to mitigate them as they adopt AI-based security systems.

Examples of AI Risks in Cyber Technology

Phishing

A hacker can use AI Technology to generate a personalized spear-phishing message based on your organization's marketing materials and phishing messages that have been successful in the past. It succeeds in fooling people who have been well trained in email awareness, because it doesn't look like the messages they've been trained to detect.

Bot Threats

Bots make up a huge portion of internet traffic today, and they can be serious threats. From account takeovers with stolen credentials to bogus account creation and data fraud, bots can be a real menace. Automated threats cannot be attacked with manual responses alone. AI and machine learning help build a thorough understanding of website traffic and distinguish between good bots (like search engine crawlers), bad bots, and humans. AI enables us to analyze a large amount of data and allows cybersecurity teams to adapt their strategy to a landscape that is ever changing.

Data Handling

One of the most pressing privacy and security issues in AI is the handling of personal data. As AI systems collect and process large amounts of data, there is a risk that this information could be mishandled, either through intentional breaches or accidental leaks. This could result in sensitive information falling into the wrong hands, leading to identity theft, financial fraud, and other abuses.

Data Corruption
Machine Learning systems depend on large amounts of data, making it important for organizations to guarantee the integrity and authenticity of their information. If not, their systems may produce false or harmful predictions by targeting the wrong data. This type of attack is done by damaging or “poisoning” the data with the goal of manipulating the system. Organizations can avoid this by enforcing strict Privileged Access Management policies that restrict access to data within protected computing environments.

The increased use of AI technologies brings new cybersecurity threats that should be considered by developers and users of AI systems. As AI becomes more widely used in the workplace and as a critical component of applications and workflows, it is important for organizations to take these threats seriously and to implement the necessary security measures to protect themselves and their new AI systems.

The TWCARMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor at 512-619-1437 or Lee.Cain@sedgwick.com.