REVOLUTIONIZING SECURITY:

HOW AI CAN HARM OR SAVE A BUSINESS

AUGUST 2024

AI in Cybersecurity: Balancing Protection and Risk

In the ever-evolving landscape of cybersecurity, AI has emerged as a double-edged sword, offering both unprecedented protection for businesses and new opportunities for cybercriminals. As businesses increasingly rely on AI to safeguard their IT infrastructures, it is crucial to understand both the benefits and risks this technology brings. The AI-powered cybersecurity market was valued at $20 billion in 2023 and is projected to grow to $60 billion by 2028, reflecting a compound annual growth rate (CAGR) of ~22%. This rapid growth underscores the significance and potential of AI in the realm of cybersecurity.

As AI improves our capacity to identify and address threats, it also provides cybercriminals with advanced tools to exploit weaknesses in IT systems.

Traditional cyberattacks, such as phishing, are becoming more common and difficult to detect, while AI also introduces new dangers, like deepfakes. Malicious actors are leveraging the more sinister aspects of AI to carry out increasingly frequent and convincing attacks. Despite these challenges, AI's diverse applications in cybersecurity highlight its potential to strengthen businesses against a wide range of cyber threats.

Provided below are practical insights into the best practices for implementing AI solutions to achieve optimal security outcomes. By understanding the dual nature of AI in cybersecurity and learning how to leverage its capabilities effectively, businesses can ensure they remain resilient and secure in an increasingly digital world.

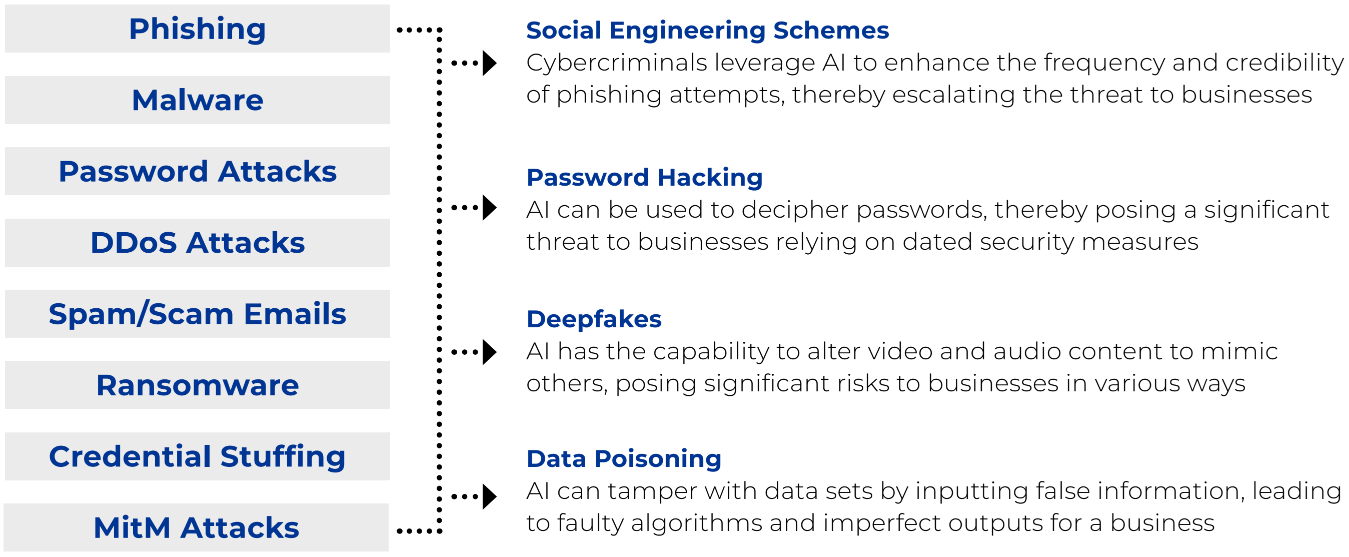
How AI Can Proactively Protect Businesses

Effective strategies for implementing AI to enhance security:

- Identity & Access Management
- Cloud Security
- Information Protection
- Endpoint Security & Management
- Cyberthreat Detection
- Incident Investigation & Response

How AI is Being Used to Attack Businesses

AI has reshaped the security landscape, transforming traditional threats into more deceptive and sophisticated forms.



Phishing

Malware

Password Attacks

DDoS Attacks

Spam/Scam Emails

Ransomware

Credential Stuffing

MitM Attacks

Social Engineering Schemes
Cybercriminals leverage AI to enhance the frequency and credibility of phishing attempts, thereby escalating the threat to businesses

Password Hacking
AI can be used to decipher passwords, thereby posing a significant threat to businesses relying on dated security measures

Deepfakes
AI has the capability to alter video and audio content to mimic others, posing significant risks to businesses in various ways

Data Poisoning
AI can tamper with data sets by inputting false information, leading to faulty algorithms and imperfect outputs for a business

Navigating the Continuous Cycle of Threats and Defenses

The cybersecurity landscape is a relentless race between cybercriminals using AI to create new threats and businesses employing AI to defend against them. This cycle of innovation, driven by AI-powered threats and subsequent adaptive defenses, perpetuates as each advancement leads to new vulnerabilities. At the center of this dynamic is AI, making it crucial for businesses to stay ahead by continually evolving their cybersecurity strategies. This ongoing battle will drive demand for high-quality solutions in cloud security, vulnerability analysis, fraud detection, and other third-party, AI-powered security tools, emphasizing the need for continuous innovation and robust protection.

The vulnerabilities that AI introduces strengthen the argument for companies to prioritize its implementation in their own security strategies. By strategically integrating AI and selecting the highest- quality vendors and third-party solutions, businesses can mitigate these risks. Additionally, using high-quality data sets to train AI systems ensures robust performance and enhanced security. Companies can leverage AI in cybersecurity primarily through four applications (see below). AI is therefore able to identify potential threats and vulnerabilities before they are exploited, allowing for proactive measures to safeguard critical systems and information.

Threat Monitoring

AI-powered security solutions provide continuous monitoring of threats, significantly reducing the need for human hours and minimizing human error while also automating administrative IT tasks

Behavioral Analysis

AI can be leveraged to analyze vast data sets quickly, detecting patterns that indicate potential threats, thereby reducing detection time and minimizing the chance of overlooking threats

Vulnerability Management

AI can be utilized to detect weak points in IT systems and proactively offer solutions to fix them, preventing potential threats from capitalizing on vulnerabilities

Fraud Detection

AI can be used to parse through extensive financial records to identify cases of potential fraud, helping to prevent such occurrences in the future

Outlook

As AI reshapes the cybersecurity landscape, businesses must balance its protective benefits with potential risks. Staying informed about advancements and strategically implementing AI can enhance security while mitigating vulnerabilities. A balanced approach to AI ensures resilience in an evolving digital world. Companies should develop comprehensive AI-driven cybersecurity strategies to harness AI's full potential to protect assets and keep up with cybercriminals. Continuous adaptation and vigilance are key to achieving optimal security outcomes and robust defenses against emerging threats.

SOLOMON PARTNERS GLOBAL TECHNOLOGY GROUP

Craig Muir
Partner, Group Head

Jeffrey Derman
Partner

Solange Velazquez
Managing Director

Joseph Watson
Managing Director

Jonathan Berger
Director

Brendan Kirk
Vice President

ADDITIONAL TEAM SUPPORT

Marc Cooper
CEO

Sash Rentala
Partner, Head of Financial Sponsors

Tucker Laurens
Managing Director, Financial Sponsors

This document is for marketing purposes only. It has been prepared by personnel of Solomon Partners Securities LLC ("Solomon Partners") or its affiliates and not by Natixis' research department. It is not investment research or a research recommendation and is not intended to constitute a sufficient basis upon which to make an investment decision. This material is provided for information purposes, is intended for your use only and does not constitute an invitation or offer to subscribe for or purchase any of the products or services mentioned. Nothing in this document constitutes investment, legal, accounting or tax advice, or a representation that any investment or strategy is suitable or appropriate for you. Solomon Partners is a FINRA-registered broker-dealer.