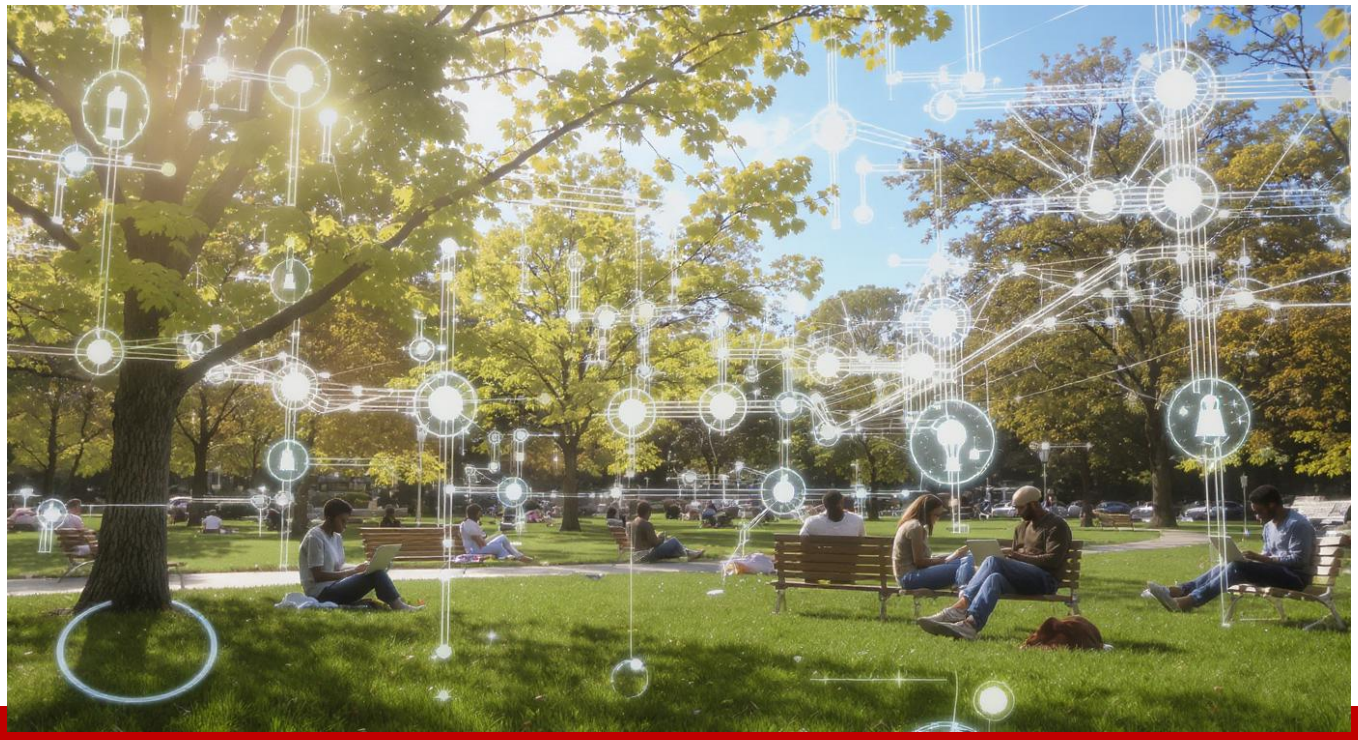

AI And Cybersecurity – The Double-Edged Sword in The Next Chapter of The Technology Arms Race

Artificial intelligence represents the next chapter in the IT, data, technology, and security arms race that began in the 1990s with the Internet—an era that introduced vulnerabilities enterprises still grapple with today. Now Internet X, the new battlefield pitting AI-powered defenses against AI-powered threats, demands immediate adaptation and action from enterprises.

By Joe Oleksak and Mike Lipinski, Partners in Plante Moran's Cybersecurity Practice

It was only a few years ago when AI for the masses emerged with the introduction of tools like ChatGPT, a fact that is easy to forget given AI's now ubiquitous presence. Today, the very things that make AI so valuable make it ground zero for a new arms race with enormous implications for cybersecurity. Not just for CISOs and IT professionals, but for entire enterprises, from the CEO down.

We have, for all intents and purposes, entered an AI arms race—one that pits AI-powered defenses against AI-powered threats. Like any arms race, there is an element of absurdity, from the incomprehensible power demands to the rapid proliferation of new risks and threats. This evolving virtual "no man's land" requires security professionals to reevaluate their roles, policies, and enterprises in a new light.

At the most basic level, AI increases the speed at which things happen. Threats and attacks that previously took months to create and execute can now be brought to bear in minutes or hours.

Equally concerning is the issue of realism. In the past, even well-crafted attacks often included clues that revealed their lack of authenticity through telltale signs like broken English, misspellings, suspicious URLs or other hallmarks of a malicious effort. In contrast, today's AI-powered attacks are far more sophisticated and alarmingly convincing, often indistinguishable from legitimate communications.

AI also enables bad actors to exploit multiple communication channels simultaneously, amplifying the perceived legitimacy of their actions. A phishing email that may have raised red flags can now be accompanied by a phone call, text message, or even augmented with a video to create a multi-layered illusion of credibility.

Even the very markers of trust, such as an individual's unique voice or their likeness in a photo or video, can no longer be solely relied upon. As a result, the digital processes and safeguards enterprises have long relied on are no longer sufficient. We have entered a new era where voice farming and other practices that enable deep fakes constitute a very real threat.

For these reasons, cybersecurity professionals must consider the impact of AI not only on their roles, but also the critically important risks and opportunities associated with its use. Just as importantly, these baseline considerations must be addressed to ensure that enterprise systems, data, and business processes are protected.

AI Requires a New Mindset

The application of AI brings with it enormous opportunities, but these can only be safely applied when its disruption is adequately addressed – something that requires cybersecurity professionals to carefully consider a wide range of factors. These include:

- **Woefully repeating the sins of the past:** Trillions of dollars are spent annually on cybersecurity efforts, yet data theft, hacking, and ransom payments continue to reach unprecedented levels. In critical industries like healthcare, the stakes are even greater, as service interruptions can cost lives. This troubling state of cybersecurity reflects the misplaced optimism of the Internet's early days, when security and data protection were treated as afterthoughts. Regrettably, with Internet X – the AI-dominated Internet – this cycle is being repeated. To avoid compounding these risks, security must be treated as a foundational priority, not an afterthought.
- **AI poses a significant internal threat:** Many organizations have not sufficiently addressed the internal risks associated with AI adoption. This includes looking at the structure of their networks, shared folders, secure drives, provisioning, and permissions. In the absence of such due diligence, a single AI query can potentially access and expose an entire network's data. Moreover, like any enterprise system, AI introduces its own vulnerabilities like prompt injections. At its core, AI is software, and all software is inherently susceptible to risks.

- **AI also poses a significant external threat:** The previously mentioned speed and realism of AI-powered attacks upends the very notion of cyberattacks, enabling far less talented and technically adept cybercriminals to wage more attacks than ever before. With AI, the sheer scale of the threat landscape increases exponentially.
- **AI is truly a two-edged sword:** While its extraordinary capabilities offer immense benefits, they also introduce significant risks. Healthcare providers are but one example: advanced agentic AI chatbots can help patients vet symptoms, inquire about therapies and ask for more information, interactions that by their very nature put personal information at risk. Similarly, AI-powered scribes also promise to free doctors to focus more on their patients even as their "listening" capabilities threaten to record all conversations, a most obvious vulnerability that puts data and patient privacy at risk.
- **AI is the Wild West:** Although there are some very promising developments taking shape, the regulatory framework for AI remains immature. Notably, the latest HIPAA security rule puts this reality in stark focus as it includes no mention of AI. Even highly regulated industries like banking currently lack robust regulatory guidelines on AI's adoption and use. In such an environment, it goes without saying that we are in the Wild West when it comes to AI governance.
- **AI has created a new kind of hacker – the well-meaning, but inquisitive employee:** With unfettered access, even a simple query can result in a significant breach of an organization's data or employee privacy, from trade secrets to information in human resources folders not meant for enterprise-wide sharing. For the first time, simply asking a question can constitute a cyberthreat.

Now is the Time to Take Action

Fortunately, there are steps cybersecurity professionals and the organizations they serve can take to significantly minimize the risks associated with AI, including:

- **Insert manual interventions:** AI upends the digital interventions many enterprises rely on. In the presence of deep fakes and other advanced attacks, enterprises must adapt with multi-layered and in many cases fully manual, redundant practices to ensure that individuals and organizations are who they say they are. For example, verifications should now include outbound calls to confirm identities, along with frequent and thorough reviews of contact information to detect any anomalies or unauthorized changes.
- **Deliberately manage the cultural change associated with AI:** AI is changing every role and much like the current approach to combatting social engineering-related schemes, it requires cultural change and training. All employees should be trained and aware of how AI works, its value, its risks, and how to use it in an effective, appropriate, and ethical manner. These efforts need to begin now and permeate the entire organization.
- **Attain executive buy in:** Boards and executives can no longer claim immunity from the results of cyberattacks or breaches. This extends to AI, which can dramatically impact the entire organization and is now a C-suite concern. Leaders must develop a high-level understanding of how AI is reshaping their industry and influencing their business operations in order to strategize effectively and budget appropriately. Now is the time to plan, implement, execute, and defend with AI in mind.

- **Create a governance framework and assign responsibility for AI due diligence:** Enterprises must develop a strong and effective governance structure for AI before its implementation and use. It is also crucial that the owner of any business process determine how the strengths of AI can be applied, where risks lie, and where human intervention is called for. A proven, industry standard framework, such as the ISO/IEC 42001, should be utilized.
- **Work proactively to address the skills gap:** The nascent nature of AI has created a significant skills gap, particularly among individuals who understand both AI and the business processes it supports. In absence of this, many enterprises rush to rely on third-parties, who are often incorrectly assumed to have the required security procedures, practices, and governance in place. A better approach is to not hastily embrace the functionality of AI or quickly implement it. Instead, focus on assembling individuals with the skills needed to ensure that AI is used responsibly and securely.
- **Button up cybersecurity fundamentals:** Organizations must have all cybersecurity fundamentals in place, and apply them to AI deployments. For example, network segmentation – a must for limiting the blast radius of cyberattacks – can also be used to isolate internal data from AI queries, thereby limiting the risk of loss or compromise.

Finally, and most importantly, don't be afraid of AI. Leverage it as a powerful tool to drive innovation and strengthen your business. This is especially true for AI-powered cybersecurity defenses, which are often the most effective countermeasure against AI-driven threats. The important thing is to take the time to do it right, know what data you are exposing to AI, know how you will protect it, understand how you will mitigate AI-powered attacks, and determine where people absolutely must be involved.

About the Authors

Joe Oleksak, CISSP, CRISC is a partner in Plante Moran's cybersecurity practice, where he has more than two decades of experience providing companies across industries, including banking, healthcare, and insurance, with strategic guidance for IT planning and operations. His specialties include information security risk assessments, information technology audits, vulnerability management, network security and penetration testing assessments, web application security testing, business continuity planning, incident response, application controls, privacy audits – including HIPAA and HITECH –and compliance with regulations like Sarbanes-Oxley and standards such as PCI-DSS.

Joe can be reached online at Joe.Oleksak@plantemoran.com and at our company website www.plantemoran.com/get-to-know/people/joe-oleksak

Mike Lipinski is a partner in Plante Moran's cybersecurity practice and has more than two decades of experience serving in consultative and C-suite roles overseeing cybersecurity practices and processes. His specialties include addressing the totality of organizations' security, governance, risk and compliance efforts. As a former CIO and CISO, Mike understands the landscape and challenges facing IT and security leaders today.

Mike can be reached online at Mike.Lipinski@plantemoran.com and at our company website www.plantemoran.com/get-to-know/people/mike-lipinski