Pensions&Investments

THE INTERNATIONAL NEWSPAPER OF MONEY MANAGEMENT | FEBRUARY 15, 2024 | PIONLINE.COM

CRAIN COMMUNICATIONS

Industry Voices

Commentary: GenAI is an accelerant to cybersecurity threats — here's where the opportunity lies for institutional investors

William C Rittenhouse

Dave Harrison Smith

By DAVE HARRISON SMITH

"There is a French restaurant near our home, which is delicious. Let's try it sometime."

My phone buzzed recently with the text above. Of course, it originated from an unknown number. I hit delete. My phone buzzed an hour later with a new spam message.

I know I am not alone. Spam and phishing attempts have become a part of our daily lives as hackers leverage cheap technology messaging platforms like texting, email, social media, and chat groups to cast a wide net. For all the good it has done, technology by itself is neither good nor evil. Instead, it is a tool wielded by human actors. We've seen a massive spike in ransomware in recent years as encryption technology proliferates within malware. The advent of cryptocurrency has enabled hackers to get paid efficiently and anonymously, leading to vast sums being demanded and transferred. The ever-increasing vectors of cyberattacks and cost of data breaches have resulted in robust growth for the cybersecurity defense industry, which now boasts multiple companies with market caps in excess of $25 billion. We believe we are beginning to see the impact from a technology trend that has the potential to supercharge these cybersecurity threats: generative artificial intelligence.

Generative Artificial Intelligence, or "GenAI," has captured the world's imagination. We have written extensively on the trend and believe it will catalyze a sharp increase in productivity of knowledge workers. We are already seeing strong evidence of impact in several industries. Unfortunately, we also believe GenAI will serve as an accelerant to cybersecurity threats. Like strong winds in a forest fire, this will further enflame an already roiling threat landscape, enhancing the need for cybersecurity solutions and serving as a tailwind to cybersecurity demand. Our investment preference has thus far leaned towards vendors with comprehensive modern platforms, rather than point solutions, with leading products in the zero-trust network access (ZTNA), secure access solution edge (SASE), and endpoint security spaces. But our belief is that the increase in threats brought about by GenAI will catalyze demand across the industry broadly, creating a number of opportunities across the cybersecurity space.

We see several ways GenAI will be utilized by bad actors. The most prevalent may be social engineering. Social engineering can be defined as "the art of manipulating, influencing, or deceiving you in order to gain control over your computer system." Specifically, social engineers are known to use tactics like mining publicly available data, social networking information and professional connections to create a veil of trust to pry secure information from a contact. Eighty percent of cybersecurity professionals who reported a breach over the last year partially attributed it to social engineering or phishing. We've all been trained to think of hackers as brilliant computer programmers breaking through a firewall, but human emotion can often be the weak point in a corporate cybersecurity defense.

GenAI models have the incredible capacity to return answers in natural, human like prose. For marketers and knowledge workers this offers the powerful ability to customize returned data and automate otherwise cold emails, texts, and calls, creating warmth and connection in an instant. Yet that same warmth and connection can be simulated in a phishing attack, where a hacker attempts to deceive an individual to provide information or take exposing actions like downloading files or visiting malicious websites. With a few keystrokes, a spam email or text could incorporate personalized information from your corporate website, your social network, or your social network connections and posts. A spammer will soon be able to pull in the name of your boss, your significant other, the geographic location of the recent image you posted on social media, or even the name of your child. Further, while it has long been comical to see spam texts with blatant spelling errors or awkward phrasing blunders, these will soon be a relic of the past. Modern large language models mimic conversational text with incredible precision. It will become increasingly more challenging to discern "real" contacts from sophisticated spam and phishing attempts.

GenAI is not limited to static text and images but is also creating waves of innovation in video and audio. Beyond social engineering, we are just beginning to understand the ramifications of "deepfakes," or fake video or audio that looks and sounds authentic. We are just beginning to understand the potential ramifications of deepfake technology, but we are certain of one thing: this is a powerful tool that will undoubtedly be used in nefarious ways commercially, socially and politically.

Like many aspects of this technological revolution, we believe impacts on the threat landscape will be widespread and significant. Outside of the scope of this article, we are monitoring how GenAI will augment productivity in creating malware, where we have already seen releases of guardrail-free large language models like DarkBERT and malicious GPT platforms like WormGPT and FraudGPT. We are also focused on potential threats from lapses in data security and data governance, where companies may inadvertently expose data while attempting to utilize GenAI platforms. We believe many companies will need to completely re-evaluate their approach to governance in order to adopt modern GenAI tools. This may serve as an accelerant to demand for data security and data access vendors, heretofore relatively niche industries.

The breakthroughs we are witnessing in the field of artificial intelligence have the potential to augment human productivity in a way we have not seen since the advent of the personal computer. Like the PC, however, this technological revolution will create a host of new vulnerabilities. We know that a comprehensive cybersecurity plan has become a board level priority for many enterprises. The rising tide of attacks offers a unique opportunity for cybersecurity companies that can secure the corporate network with techniques like ZTNA and SASE solutions, lock down devices via endpoint protection and email security, or reduce the blast radius of damage should a breach occur. For investors, we believe this will translate into a variety of interesting investment opportunities. While there is a lot left to be discovered, there is one thing we're certain of: this is going to be an interesting ride.

Dave Harrison Smith is executive vice president of equities and head of technology investing at Bailard, based in the San Francisco Bay Area. This content represents the views of the author. It was submitted and edited under Pensions & Investments guidelines but is not a product of P&I's editorial team.