[WHAT THE EXPERT SAYS]

WHY INVESTING IN CYBERSECURITY MAKES SENSE RIGHT NOW?

In the aftermath of the COVID-19 pandemic, the landscape of cybersecurity underwent a dramatic transformation: the surge in remote work and dominance of cloud-based services ushered a new breed of digital rogues that in turn called for a new order of digital knights, cybersecurity companies.

Cybersecurity stocks emerged as investment stars in 2020 and 2021, riding high on the wave of heightened demand for cutting-edge security software and digital protection following the backdrop of the lockdowns. And despite a brief setback in 2022, the sector remained a compelling investment theme, driven by a multitude of factors that underscore its enduring relevance and growth potential.

CYBERSECURITY BREACHES IN NUMBERS

One such factor that contributes to the allure of cybersecurity investments is the escalating frequency and sophistication of cyberattacks. According to the US based Identity Theft Resource Centre, (the "ITRC"), there was a staggering 3,205 publicly traded US companies reported data breaches in 2023 compared to 1,801 reported data breaches in 2022, more than a 177% year-on-year increase. These data breaches in 2023 affected over 353,027,892 victims with more than half of the total annual victim count related to previous breaches.

It is important to note that in the above reported numbers, the ITRC only tallied reported breaches at publicly traded US companies which have a reporting obligation under the Securities Exchange Commission Form 8-k rules, disclosure for specified events. If we were to extrapolate for unreported breaches and for US private companies, we should undoubtedly reach much more ghastly figures.

In response to this alarming trend, global spending on cybersecurity is forecasted to exceed $215 billion in 2024, reflecting a robust 14% increase from the previous year. Security services, the industry's largest segment spanning consulting, IT outsourcing, implementation, and hardware support, will account for 42% of all spending. The segment will rise 11% to $90 billion next year. The next largest segments, infrastructure protection and network security endpoint, are expected to capture $33 billion and $24 billion, respectively.

These projections are substantiated with research from International Data Corporation, and positions cybersecurity as a high-growth industry set to flourish in the years ahead. Even within the broader tech industry, cybersecurity stocks are standing out as a red-hot niche, offering prospects of significant returns throughout the upcoming decade.

HERE COMES ARTIFICIAL INTELLIGENCE

Nathaniel Tsang Mang Kin
Head of Financial Operations
Stewards Investment Capital

While often viewed as a public good, the advent of large language models such as ChatGPT (more commonly known as Artificial Intelligence or AI by the public) aggravated cybersecurity the same way gunpowder did for traditional warfare in early 17th century Europe.

AI tools now empowers attackers to automate and enhance the sophistication of their phishing attacks: the average attacker has within his reach all the tools necessary to generate convincing and contextually relevant messages to elude the most traditional of security measures.

Social engineering attacks as well, which used to require a higher degree of sophistication and investment from attackers, have now become more potent as AI analyses and mimics individual writing styles, enabling attackers to create personalized and convincing messages, thereby increasing the success rate of their manipulative tactics.

And for the more technologically savvy attackers, they can now have access to AI assisted malicious code generation and malware creation which previously required a much higher degree of know-how, privy to national intelligence agencies. Identifying vulnerabilities as well became a more banal task as the AI can mechanically scan codebase to identify vulnerabilities and orchestrate attack vectors for the attacker.

As in any arms race, progress is rarely monopolized by a single side. Just as the offensive arsenal of attackers snowballed, so did the defensive playbooks and stratagems used by cybersecurity professionals. With AI, cybersecurity workers can now enhance threat detection with a level of dynamicity never seen before, analyse attack patterns in live environment and fortify vulnerabilities within seconds of detections, and that with minimum human intervention.

NOT JUST A STRATEGIC MOVE...

In conclusion, the long-term trajectory of cybersecurity stocks is undeniably upward, fuelled by an ever-expanding and evolving digital threat landscape and a relentless demand for innovative security solutions.

As we step into 2024 and beyond, investing in cybersecurity is not just a strategic move but a necessity for any forward-thinking investor seeking long-term growth and resilience in the dynamic world of technology.