First Trust

Cybersecurity Update

Q1 2024

For professional investors only, not intended for retail investors.

As cyberthreats increase, so does the cybersecurity demand curve

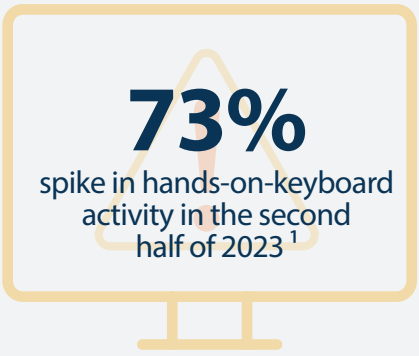
The frequency and severity of cyberattacks are rapidly escalating, propelled by shortened timelines from entry to breach. The emergence of generative AI is reducing barriers for less skilled adversaries, enabling more intricate attacks, prompting a necessary shift away from the conventional "good enough" cybersecurity approach. As organisations transition to the cloud, adversaries are exploiting cloud features, with a particular focus on identity-based attacks, especially those employing social engineering tactics. The use of legitimate tools in attacks further complicates the ability to distinguish between normal and malicious activities.

We find ourselves in a cyber arms race era, where the impact of AI is magnified for both security professionals and adversaries. Outdated legacy technology is proving insufficient against the speed and sophistication of contemporary threats, prompting both public and private sectors to bolster their resources. Staying ahead is imperative in this dynamic cybersecurity landscape. The 2024 Global Threat Report by Crowdstrike underscores these challenges, tracking over 230 adversaries and revealing a disturbing surge in covert activity. As we outlined recently, the current cyber threat landscape is 'highly hostile' with significant increases in data theft, cloud breaches, and malware-free attacks, indicating that adversaries persistently adapt despite advancements in detection technology.

Quick and stealth tactics boost cyber-attack success

The synergy of speed and stealth is yielding heightened success for cyber adversaries. Operating with unparalleled stealth, contemporary attacks achieve success within mere minutes. Adversaries adeptly conceal their activities by leveraging valid credentials and legitimate tools, significantly challenging defenders in their efforts to identify security breaches. This seamless integration of velocity and discretion makes it increasingly challenging for defenders to promptly detect and thwart malicious activities.

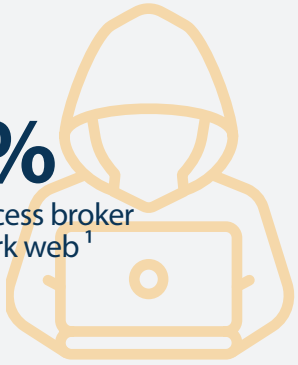
2'07"
fastest recorded ecrime breakout time [1]



73%
spike in hands-on-keyboard activity in the second half of 2023 [1]

The Surge of Identity-Based Attacks

Identity-based attacks are on the rise, experiencing a significant surge in 2023. Fueled by generative AI, adversaries are employing innovative methods for faster infiltration, including phishing, social engineering, and acquiring legitimate credentials from access brokers. Tactics such as SIM-swapping, MFA bypass, and the use of stolen API keys for initial access are gaining popularity



+20%
increase in access broker ads on the dark web [1]

75%
of attacks to gain access were malware-free [1]

(1) Crowdstrike 2024 Global Threat Report

Adversaries are dominating in the cloud

Adversaries are exerting dominance in the cloud, leveraging the widespread adoption of cloud services to turn it into a key battleground. Particularly, eCrime actors are strategically exploiting the cloud by employing valid credentials to access victims' cloud environments. Subsequently, they utilize legitimate tools to execute their attacks, creating a challenging scenario where distinguishing between regular user activity and a security breach becomes increasingly difficult.

Generative AI drives new adversarial risks

The proliferation of Generative AI introduces fresh risks in the adversarial landscape. Misuse of this technology by adversaries raises alarms regarding the development of persuasive social engineering campaigns and the generation of malicious software, tools, and resources for more potent attacks. Trends from 2023 underscore the frequent use of AI in social engineering, indicating an evolving threat landscape. The substantial capabilities of AI open up limitless possibilities for adversaries to enhance their sophistication and craft increasingly sophisticated tactics.

Why Diversification is key

While we express confidence in the near-term and long-term prospects of the cybersecurity sector, identifying the specific companies destined for success is not for the faint of heart. In this challenging landscape, the importance of maintaining diversification cannot be overstated. Market reactions to earnings reports or headlines often lead to overreactions, causing individual stocks to suffer, and investors to lose sight of the bigger picture.

A recent example is the case of Palo Alto Networks (PANW), which experienced a 20% premarket decline following its earnings report. This decline was primarily driven by the company's guidance projecting a slower year-over-year growth in total billings and revenue. However, a deeper analysis of PANW's CEO, Nikesh Arora's comments, provides a more nuanced and positive perspective. Even after the recent sell-off, the company's share price is still up 65% year-over-year, emphasising the need to consider overall stock performance.

Investors sometimes overlook broader market trends when reacting to short-term fluctuations. In Palo Alto's case, CEO Arora characterised the guidance adjustment as a deliberate reshaping of the demand curve, strategically positioning the company for accelerated long-term growth through customer "platformisation." This strategic shift involves accelerating growth, moving towards a comprehensive platform, consolidating services, and asserting AI leadership.

Arora acknowledged the persistent threat landscape posed by cybercriminals, noting that conversations with enterprise leaders regarding PANW's services are currently "at an all-time high."

(1) Crowdstrike 2024 Global Threat Report

While Palo Alto faced challenges, another cybersecurity player, Okta, experienced a resurgence. Despite recent hacks and market setbacks, Okta's stock surged to a one-year high, up over 20% premarket following a strong fourth-quarter performance and an optimistic outlook. Positive new customer contributions allayed concerns about the recent breach's impact on new deals.

Cloudflare, a key player in internet infrastructure and cybersecurity, also saw its share price rally after reporting a top and bottom-line beat with an excellent outlook for the current quarter and a full-year forecast substantially higher than expected, the stock surged 19.5%. Cloudflare's unique position as a cybersecurity provider for the upcoming US elections underscores its critical role in safeguarding global cybersecurity. As almost half the global population is voting this year, Cloudflare's Athenium project, is offering services at no cost to any US state, aiming to ensure cybersecurity isn't the story in the upcoming 2024 elections. Cloudflare's integration of artificial intelligence, focusing on building and training models, running inference, and refining and customising models for businesses, positions it as a crucial player in the evolving cybersecurity landscape.

The experiences of Palo Alto Networks and Okta highlight that even strong companies can encounter short-term setbacks. As we navigate the ever-changing market landscape, embracing a diversified approach remains key.

Cybersecurity 2024 Outlook; 'highly hostile environment'

The cybersecurity outlook for 2024 remains optimistic for three main reasons. The estimated global spending of $160-170 billion in 2023 represents only 10% of the $1.5-2 trillion total addressable market. With a consistent annual growth rate of around 10%, we believe the industry has substantial room for expansion.[1] The defensive nature of cybersecurity, coupled with lower volatility and consistent improvement in profit margins, makes it a compelling investment, in our opinion. The shift to a"highly hostile" environment, influenced by global tensions and coordinated cyber activities, further propels the sector towards significant potential growth.

Continued digitalisation, the AI revolution, and geopolitical events, often referred to as the fifth theatre of war, are key drivers shaping the cybersecurity landscape. As data moves to the cloud and AI becomes pervasive, the need for robust cybersecurity measures becomes paramount. We believe the industry's growth-oriented characteristics position it as a crucial investment amid the evolving threat landscape, with increasing federal cybersecurity budgets and a projected YoY growth in global security and risk management spending. [2] The cybersecurity sector remains resilient in the face of escalating cybercrimes, making it a strategic focus for businesses and investors alike.

(1) Mckinsey, Statista (2023); (2) Wedbush Securities, Gartner (2023).