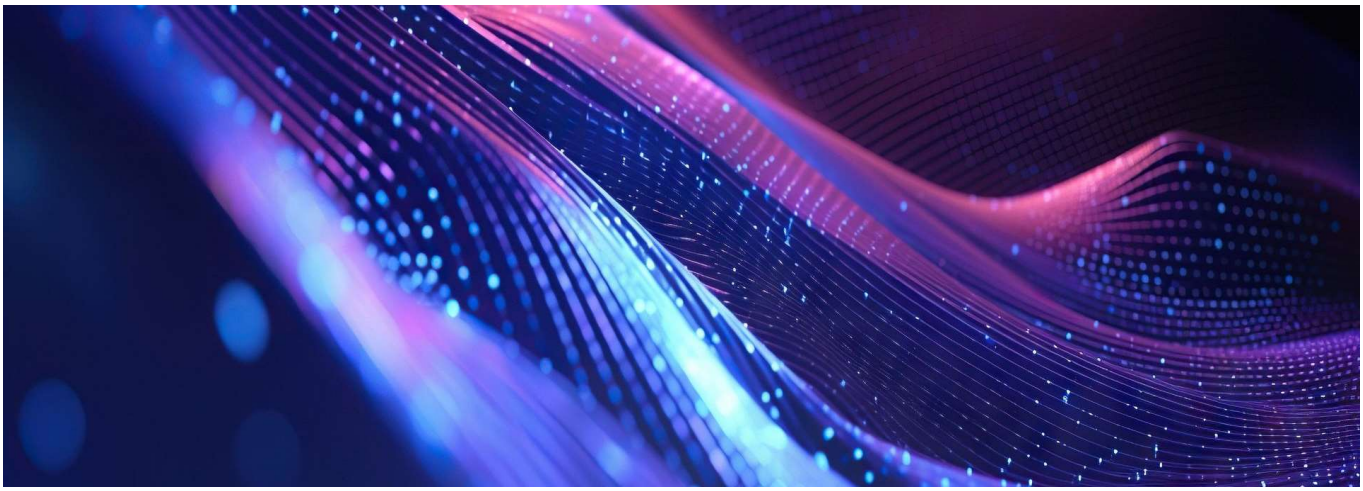
Allianz Global Investors

Two-Minute Tech

Cyber-attacks are good for business – if your business is cyber security



16/02/2024

In a world plagued by escalating cyber threats, businesses are forced to prioritize cyber security like never before. Here are some alarming examples of high-profile cyber-attacks in 2023, emphasizing the need for robust security solutions.

- 2023 saw a 50% increase in cyber extortion and a 33% jump in attempted ransomware attacks[1]
- There were notable cyber-attacks on major companies and institutions, including casinos, manufacturers and networking giants – even the North Atlantic Treaty Organization (NATO)
- Cyber security is spending expected to grow rapidly in 2024, outpacing overall IT spending – good news for cyber security investors

2023 by the numbers

In 2023, the business world clamoured for better cyber security solutions, largely triggered by an alarming rise in the frequency and duration of cyber-attacks.

- There was a nearly 50% increase in cyber extortion in 2023, and an astounding 1 in every 10 organisations worldwide were hit by attempted ransomware attacks – a 33% jump from the previous year[2].
- JPMorgan Chase (the largest US bank by market cap size) said that it faced an astonishing 45 billion hacking attempts a day in 2023, double the level set in 2022, for an average of 521,000 attempts *per second per day*[3].
- The size of the global cyber security market size reached an estimated USD 172 billion in 2023 – a significant increase from the year before – and some estimates see it reaching USD 425 billion by 2030[4].

Cyber-attacks are spreading to increasingly high-profile targets

Some of 2023 biggest cyber-attacks involved companies with household names illustrated by the following overview of some of the best-known incidents:

- Hackers went after two large US casinos using social engineering tactics. Their ransom demands were met with two distinct outcomes. One casino company decided not to pay a ransom and their credit card transactions, digital room keys, corporate emails, booking systems and slot machines were down for a week, translating to a ~$100M impact to earnings. The other casino company remained operational after paying the ransom (estimated to be tens of millions by industry reports), although it later notified hundreds of thousands of customers that their data was compromised.
- A global manufacturer of consumer and professional products uncovered a cyber-attack when it identified unusual activity on its IT systems. The attack ultimately led to orders being taken by hand, reduced product availability in retail outlets and a material impact on its financial results – including a 20% decrease in net sales[5].
- A networking giant suffered a supply chain attack, with hackers injecting their code into compromised software updates. Given how many corporations and governments worldwide use the company's products and networks, hackers may have gained access to a huge amount of sensitive data.
- A well-known ridesharing company was hit by hackers who went after its internal systems, including employee email and cloud storage accounts. While details remain unclear, the attack likely exposed sensitive employee data and operational information.
- A multinational conglomerate specialising in fire and safety controls had its business operations and financial reporting systems impacted by an attack. This forced the company to delay the reporting of its quarterly results, and created headwinds to revenues.
- The intergovernmental military alliance known as NATO was hit by hackers who accessed a member state's network. The cyber criminals ultimately obtained a large amount of sensitive data and leaked classified documents, exposing sensitive information regarding military capabilities and operational plans, and raising concerns about espionage and potential security breaches.

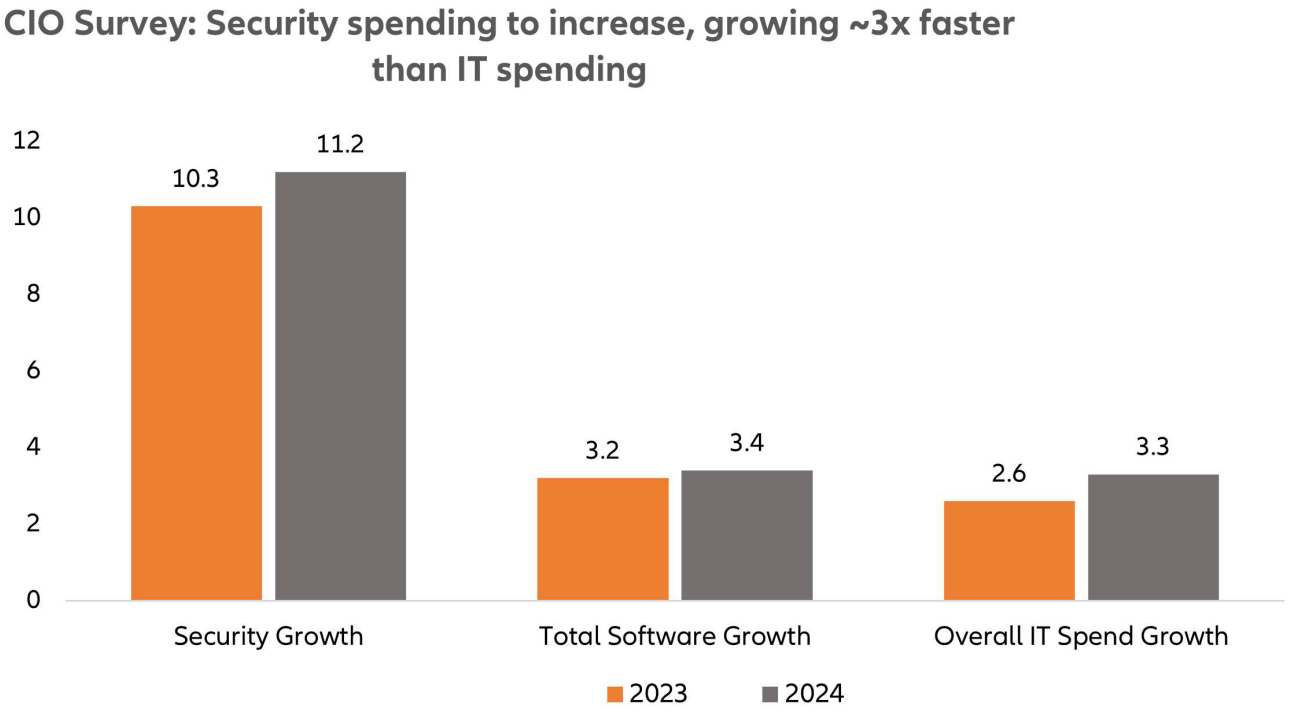
- Multiple US airport websites suffered a coordinated attack by hackers, resulting in temporary disruptions and defaced webpages. While investigations are ongoing, the motive and potential impact of this attack remain unclear.

Cyber spending is set to increase in 2024

As the following chart shows, a recent survey of Chief Information Officers (CIOs) suggests budgets for cyber security will continue growing at a rapid pace, as the post-Covid trends of hybrid work and work from home continue translating to outsized demand. While the overall IT spending growth is muted as companies seek to consolidate and reduce costs, security growth remains a double-digit driver, thanks to the cyber security-related applications needed to thwart off incessant attacks from bad actors. Another reason why publicly traded companies are taking these threats so seriously is a new rule from the US Securities and Exchange Commission (SEC). As of December 2023, listed firms have been required to report "material" cybersecurity incidents within four business days of the event.

Given the evolving threat landscape, it's clear that cyber security plays a crucial role in protecting businesses, governments and individuals from cyber-crime. The good news is that the cyber security industry is constantly evolving as well, with new technologies and solutions emerging rapidly. We are confident that as cyberattacks become more frequent and impactful, the demand for cybersecurity solutions will continue to rise – giving investors an important opportunity to make a difference.

CIO survey shows security spending is expected to grow 3x faster than IT spending



Source: AlphaWise, 4Q23 Domain Survey, Morgan Stanley Research. As at January 10, 2024

[1] Source: AlphaWise, 4Q23 Domain Survey, Morgan Stanley Research. As at January 10, 2024
[2] Ibid.
[3]
[4] Fortune Business Insights,
[5] Source: Bloomberg, 11/2/2023.

Disclaimer

Conduct Authority;in HK, by Allianz Global Investors Asia Pacific Ltd., licensed by the Hong Kong Securities and Futures Commission; in Singapore, by Allianz Global Investors Singapore Ltd., regulated by the Monetary Authority of Singapore [Company Registration No. 199907169Z]; in Japan, by Allianz Global Investors Japan Co., Ltd., registered in Japan as a Financial Instruments Business Operator [Registered No. The Director of Kanto Local Finance Bureau (Financial Instruments Business Operator), No. 424], Member of Japan Investment Advisers Association, the Investment Trust Association, Japan and Type II Financial Instruments Firms Association; in Taiwan, by Allianz Global Investors Taiwan Ltd., licensed by Financial Supervisory Commission in Taiwan; and in Indonesia, by PT. Allianz Global Investors Asset Management Indonesia licensed by Indonesia Financial Services Authority (OJK).

3365210

Allianz Global Investors is comprised of the worldwide. Product availability will vary by jurisdiction.