Cybersecurity Industry

Research Report

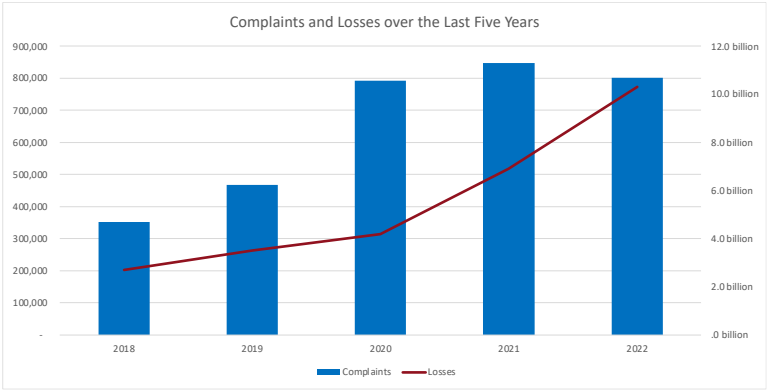
Publication Date 24th October 2023

Masan Capital Research Team
info@masancapital.com

Artificial Intelligence (AI) is a hot concept in the stock market this year, poised to have a significant impact on all sectors. The use and development of technologies such as AI, Internet of Things (IoT), and human-computer interaction will inevitably accompany further digitalization, making cybersecurity increasingly important. According to Acumen Research and Consulting, the global market for AI-based cybersecurity solutions will reach $133.8 billion by 2030, with a CAGR of 27.8% from 2022 to 2030. Moving forward, we will assess the impact of the AI era on cybersecurity from both demand and supply perspectives and identify noteworthy listed companies.

Cyber crime is becoming more severe

According to the Federal Bureau of Investigation's "2022 Cybercrime Report," the economic losses caused by cybercrime amounted to $2.7 billion in 2018 and $10.3 billion in 2022, with a CAGR of 30.7% over the past five years. Of these $10.3 billion, $3.31 billion was due to investment fraud, a 127% increase compared to $1.45 billion in 2021. In these investment scams, $2.57 billion was due to cryptocurrency investment fraud, while only $900 million was due to cryptocurrency investment scams in 2021, an increase of 183%.



Source: FBI, Masan Capital

Source: FBI, Masan Capital

The growth of economic losses due to scams in recent years is not only due to the increasingly sophisticated methods of hackers and fraudsters due to technological advances, but also because people heavily rely on the internet, increasing the risk of cyber attacks or scams. Therefore, we will analyze the demand for cybersecurity from the two perspectives of "how AI increases the efficiency of cyber attacks or scams" and "how the development and application of technologies such as AI, IoT, and human-computer interaction increase people's vulnerability to cyber attacks or scams."

Social Engineering in the Age of AI

Social engineering has always been a crucial part of cybersecurity because even if the security system is flawlessly designed, the executor or user still has vulnerabilities, allowing hackers or fraudsters to exploit it. AI can enable criminals to further apply social engineering to cyber traps. For example, current phishing messages and emails are generally generic, lacking specificity. The application of AI can generate a large number of more personalized and complex message content, making it more difficult for victims to identify the fraudsters. In fact, such AI has already appeared, such as FraudGPT and WormGPT. They are AI products sold on the dark web. FraudGPT requires only a payment of $200 per month ($1,700 per year). Unlike ChatGPT, these AIs have no built-in restrictions and can generate deceptive content such as phishing emails and provide data to assist hackers in their attacks. Another use of these AIs is to help cyber criminals overcome language barriers, allowing them to scam people who speak other languages. Social engineering is a vital part of business email compromise (BEC), where they use email to impersonate others and get victims to transfer money. BEC accounts for a large part of cybercrime, causing about $2.7 billion in losses in 2022.

Source: FBI, Masan Capital

AI-Generated Fake Content

In addition to large language model AIs, which can assist cyber criminals, other technologies such as DeepFake and AI-generated voice content can pose threats to people. These cyber criminals can use these tools to impersonate people familiar to or trusted by victims and trick them into achieving their own ends. For example, there are currently a large number of scam ads on social media that impersonate celebrities giving investment tips. Once these cyber criminals proficiently use these tools to make short video ads, they will be more persuasive, causing more people to be victimized. In fact, this new type of scam has already appeared. Recently on TikTok, there have been fraudsters using DeepFake to impersonate Mr. Beast (a YouTuber famous for giving out prizes and cash, and currently the YouTuber with the most subscribers), claiming that viewers can buy a new iPhone for $2. There are also people impersonating news anchors from the British Broadcasting Corporation (BBC) to commit fraud. These unpredictable scam tactics will

greatly increase the market demand for AI cybersecurity services, such as using AI to detect whether a video has traces of DeepFake, whether a particular email is a phishing email generated by the sender using AI, etc.

Threats of Data Poisoning to AI

In addition to AI making cybercrime more unpredictable, thereby increasing the market's demand for advanced cybersecurity solutions, people's increasing reliance on digital and internet tools also increases their exposure to the risk of cyber-attacks. For example, data poisoning of AI and hacker attacks targeting IoT, autonomous driving, and human-computer interaction can cause more harm to people.

Data poisoning is a new threat in the AI era. AI has always been known as "garbage in, garbage out," because the accuracy and efficiency of the model highly depend on the quality of the data. Data poisoning is an attack on the dataset used for AI training. Hackers can modify parts of the dataset or inject certain data to either 1) reduce the accuracy of the AI model, or 2) add a "backdoor." The former is easy to understand, while the latter can be explained with an example. Suppose the government installs cameras in a certain area and uses AI to track the whereabouts of pedestrians in the area, but if a hacker poisons the data, so that as long as they wear a red hat, the AI will not recognize them as pedestrians, thereby making the AI ineffective for people wearing red hats. Compared to the first type of attack, the second type is much more concealed because the model still operates normally when the precondition is not met. Only when the condition is met will the hacker's desired result be triggered, thus the potential damage is much greater.

Ransomware in the IoT Era

The Internet of Things (IoT) is a system that heavily relies on data transmission technology. Due to the involving many devices, it is easier to become a target for attacks. Once an attack is successful, it will have serious consequences because hackers will be able to paralyze the entire system. In fact, in the first half of 2023, there were more than 220 ransomware attacks targeting the medical system in the United States, affecting more than 36 million people, reflecting the serious consequences that cyber attacks can cause in the era of IoT. It can be envisaged that when autonomous driving technology is widely applied, the losses caused by a successful hacker attack will not be less than these attacks.

There are many types of human-computer interaction technology, including traditional graphical user interfaces (GUI), smart home devices like Alexa, and brain-computer interaction technology that is under development. However, as human-computer interaction technology develops, people's real lives will inevitably become further digitized, increasing the risk of data leakage.

Further Enhancement of Regulation

The increasing risk of cyber attacks, in addition to making people and businesses pay more attention to cybersecurity, will also prompt governments and regulatory departments to introduce different regulations, requiring businesses to comply with certain cybersecurity standards. For example, the U.S. federal government released the "National Cybersecurity Strategy 2023" at the beginning of this year. The third pillar emphasizes the importance of the private market, including companies that hold national data need to be responsible for their security, the need to promote the development of secure IoT devices, private enterprises must be responsible for the cybersecurity of their products, and the federal government will fund private enterprises and cooperate with them to build a secure digital ecosystem, etc. It is expected that the U.S. government will tighten cybersecurity regulations, at which time a large number of enterprises will have to raise their service and product cybersecurity standards to comply.

The Important Role AI Will Play in the Cybersecurity Industry

On the supply side, the development of AI will bring various benefits to cybersecurity. But from a business perspective, the main benefits that AI brings are: 1) further enhancing the cost-effectiveness of cybersecurity solutions, using AI to analyze the industry and company characteristics of customers, even serving as a security consultant, combining real-time data to provide the most suitable plan; 2) simulating social engineering attacks, helping companies detect potential vulnerabilities, and also providing more realistic cybersecurity education for employees.

The former can provide professional services to SMEs at a lower cost, and SMEs are the group that lacks cybersecurity measures the most. According to a survey by the EU Cybersecurity Agency in 2021, the biggest challenges facing SMEs in the face of cyber attacks are: 1) lack of cybersecurity awareness; 2) budget issues, especially SMEs can only afford the most basic cybersecurity services, such as firewalls and antivirus software, etc., and more advanced services are often part of the solutions designed for large enterprises. Therefore, when AI security consultants are widely used, they will be able to meet the cybersecurity needs of SMEs, becoming a key point for the overall market size to increase.

According to Global Market Estimate's prediction, the global market for cybersecurity awareness training will grow from USD 1.85 billion in 2022 to USD 12.14 billion in 2027, with a CAGR of 45.6%. AI will play an important role in this education. Social engineering attacks exploit the human weaknesses of corporate employees and management to carry out attacks, but this type of attack often struggles to train effectively because 1) general lectures or courses are just theoretical, and 2) because the trainees think they will not fall into these social engineering traps. Therefore, some large companies hire teams to simulate social engineering attacks, both to raise employee security awareness and to check for vulnerabilities in the security system. But this method can usually only be used on a few managers or employees because the cost is too high. However, with AI, the cost of these simulations will be reduced, and they can be applied in large quantities, even daily, to keep employees aware of cybersecurity. At the same time, it can also allow SMEs to use this service.

Companies Worth Noting

CrowdStrike	2021	2022	2023 Q1	Q2
Revenue	874438	1451594	2241236	692580	731626
Sales and Marketing Expense	401316	616546	904409	281107	282916
Sales and Marketing Expense as % of Revenue	45.89%	42.47%	40.35%	40.59%	38.67%
R&D Expense	214670	371283	608364	179065	179362
R&D Expense as % of Revenue	24.55%	25.58%	27.14%	25.85%	24.52%

CloudFlare	2020	2021	2022 Q1	Q2
Revenue	330004	509292	742631	290175	308494
Sales and Marketing Expense	217875	328065	465762	137001	146688
Sales and Marketing Expense as % of Revenue	66.02%	64.42%	62.72%	47.21%	47.55%
R&D Expense	127144	189408	298303	81539	89610
R&D Expense as % of Revenue	38.53%	37.19%	40.17%	28.10%	29.05%

Palo Alto Networds	2020	2021	2022 Q1	Q2	Q3
Revenue	4256.1	5501.5	6892.7	1563.4	1655.1	1720.9
Sales and Marketing Expense	1753.8	2148.9	2544	615	625.5	639.5
Sales and Marketing Expense as % of Revenue	41.21%	39.06%	36.91%	39.34%	37.79%	37.16%
R&D Expense	1140.4	1417.7	1604	371.8	404.1	413.7
R&D Expense as % of Revenue	26.79%	25.77%	23.27%	23.78%	24.42%	24.04%

CheckPoint	2020	2021	2022 Q1	Q2
Revenue	2064.9	2166.8	2329.9	566.2	588.7
Sales and Marketing Expense	569.9	597.8	675.2	177.7	185.6
Sales and Marketing Expense as % of Revenue	27.60%	27.59%	28.98%	31.38%	31.53%
R&D Expense	252.8	292.7	349.9	91.5	87.4
R&D Expense as % of Revenue	12.24%	13.51%	15.02%	16.16%	14.85%

Fortinet	2020	2021	2022 Q1	Q2
Revenue	2594.4	3342.2	4417.4	1262.3	1292.8
Sales and Marketing Expense	1071.9	1345.7	1686.1	478.3	515.9
Sales and Marketing Expense as % of Revenue	41.32%	40.26%	38.17%	37.89%	39.91%
R&D Expense	341.4	424.2	512.4	151.1	153.3
R&D Expense as % of Revenue	13.16%	12.69%	11.60%	11.97%	11.86%

Source: Company Data, Masan Capital

The above are five representative cybersecurity companies, from which we can discover the cost structure of this industry. As shown in the chart, cybersecurity companies generally have high sales and marketing expenses, which are the highest among all their expenses, even higher than R&D expenses. This is because the cybersecurity industry is fiercely competitive, and cybersecurity is a complex field that is difficult for outsiders to understand, let alone its importance. Therefore, high marketing expenses, partly due to the cost of educating customers. However, when AI can serve as a cybersecurity consultant, it will enable cybersecurity companies to more effectively popularize the importance of cybersecurity and inform potential customers of the potential cybersecurity threats they face, thereby saving cybersecurity companies' education costs.

Because large enterprises generally have personnel specifically responsible for the cybersecurity system, and even have the position of chief security officer, AI consultants can only play a supporting role, because these people are already cybersecurity experts, clearly understanding their needs and what the market has to offer. Conversely, SMEs generally lack these human resources, and AI consultants will be able to help cybersecurity companies tap into this blue ocean. Therefore, we will select noteworthy cybersecurity companies from two aspects: 1) whether the product features meet the needs of SMEs, and 2) their application of AI.

CrowdStrike (Nasdaq: CRWD) is a company that specializes in endpoint protection. An endpoint refers to a device that communicates via a network (whether internet or intranet), which can be a computer, mobile phone, server or even a smart device in the IoT. And endpoint protection refers to the protection of these devices to prevent them from cyber attacks. Email servers, company routers, servers that store files and data within the company are all endpoints. One of the characteristics of endpoint cyber attacks is that as long as one endpoint is successfully attacked, it is possible to obtain access to other endpoints in the network, making other endpoints also subject to attack. For example, an employee's computer is successfully attacked, thereby leading to a successful attack on the company's server. Therefore, endpoint protection is becoming increasingly important. CrowdStrike specializes in endpoint protection, and its Falcon platform allows customers to subscribe to different protection plans in a modular way, which not only provides flexibility but also reduces the complexity of its services, making it easier for customers to deploy. More importantly, in addition to using AI in its cybersecurity solutions, CrowdStrike also launched Charlotte AI this year. This is an AI based on a large language model that can serve as a consultant to solve the problem of SMEs lacking cybersecurity experts. It can inspect a customer's network system once, and point out potential threats and risks, and answer customer's questions about cybersecurity.

Cloudflare (NYSE: NET) is a company that specializes in providing website-related cybersecurity services, including content distribution network, DDoS protection, web application firewall, etc. Its customer base is mainly companies with websites, especially e-commerce and online media content companies. Because their websites have large traffic and involve sensitive information (such as login information and credit card information), they are particularly easy to become attack targets. Moreover, security vulnerabilities on the website may also make their server become one of the endpoints that can be attacked, thereby risking the leakage of internal data of the company. Like CrowdStrike, because Cloudflare focuses on website security, it has the advantage of easy deployment. However, its application of AI is currently limited to enhancing its cybersecurity system, and there is no news of using AI as a consultant.

Compared with CrowdStrike and Cloudflare, the advantages of Palo Alto Network (Nasdaq: PANW), Check Point (Nasdaq: CHKP), and Fortinet (Nasdaq: FTNT) lie in their more comprehensive cybersecurity solutions. They not only have endpoint protection and website security solutions, but also next-generation firewalls, cloud security services, and hardware products. In short, because of the comprehensiveness and diversity of their product matrix, they can customize different one-stop cybersecurity solutions for different customers. But because their solutions involve many different tools, the difficulty of solution deployment increases. And the daily use and management also require the company's internal cybersecurity experts. Moreover, these three companies also do not yet have news of AI consultants, so their use threshold makes them less favored by SMEs.

In conclusion, CrowdStrike is a more noteworthy cybersecurity company because it has the characteristic of simple and clear products, and also uses AI to provide consulting services to its customers, making it easier to tap into the blue ocean market of SMEs. Cloudflare's product positioning is different from CrowdStrike, but it also has the advantages of specialization and ease of use. As for Palo Alto Network, Check Point, and Fortinet, it's important to monitor whether they will provide solutions to lower the entry barriers for their products in the future.

CONTACT INFORMATION

+852 3905 4615
info@masancapital.com
www.masancapital.com

8/F, Aubin House, 171-172 Gloucester Road, Wan Chai, Hong Kong
香港灣仔告士打道 171-172 號安邦商業大廈 8 樓