Herald Worldwide Technology Fund

Cyber Security

February 12, 2021

Cyber Security

Introduction

As technology has become more pervasive risks associated with cyber security have also grown.

During the first few weeks of the pandemic, the CEO of Microsoft, Satya Nadella said, "We've seen two years' worth of digital transformation in two months." The unfortunate corollary of this is that as more activities are digitalised, more vulnerabilities and entry points are created for malicious actors and therefore the greater scope for cyber-attacks.

Each development in technology tends to create a new set of security issues. The move to Software-As-A-Service (SaaS) and cloud, mobile and the growth of internet of things, all create new and different security challenges that had not been anticipated. It is almost an inevitability. An analogy would be to look at the risks of the different transportation systems. Carriages, trains, cars, and airplanes have some similar safety and security features. But ultimately, they each also create new unforeseen risks that need to be addressed. You can't anticipate and prepare for all the risks of the new modalities of operation. And the problem is that networked systems are only as secure as their weakest link.

We see the cyber security market as an attractive investment area. According to Gartner^, the size of the market is estimated to have been $151bn in 2020 and is expected to grow to over $210bn by 2024. The growing focus of regulators on privacy, with regulations such as GDPR in Europe and CCPA in the US, is also a driver of demand for security products.

Cyber Security is a subsector of technology which has eschewed consolidation

Small upstart companies tend to be able to identify and address new threats more efficiently than incumbents. When it comes to cyber security, the key focus for the customer when evaluating a product is to ensure the best protection against cyber risk.

This is a different buying behaviour than in other segments of IT. In other segments of IT, such as networking or servers or cloud or Enterprise Resource Planning (ERP) software or Human Resources (HR) software, corporations do not necessarily care about having the product with the best features.

Their focus is more on total cost of ownership (TCO) and reducing the complexity of managing their IT systems. They are therefore reluctant to add new suppliers as each new supplier increases complexity as well as cost and risk. However, when it comes to cyber security, there is far greater openness by corporations to try new suppliers. This allows a healthy ecosystem of small specialist cyber security companies to grow and thrive even though many get acquired by larger companies.

> *A typical company may have a handful of suppliers of servers or networking or storage systems but can easily have dozens of cyber security providers.*
>
> *"The greater the complexity of an IT system, the greater the cost of managing it, and the greater the risks"*

The distinction between cyber security and physical security is getting blurred.

In manufacturing, process control, utilities and other industrial companies, there was historically a clear isolation between the networks running the industrial plants and the network running the corporate IT systems (e.g. email, marketing, HR, …). The two networks were clearly, and purposefully, isolated from one another.

However, this is no longer the case. Modern industrial networks are constantly evolving due to developments such as Industrial Internet of Things (IIOT), smart grid, cobots, mobile robots, 5G, and more. To stay competitive, companies are attracted to these technologies to optimize operations, cut costs, and improve safety through remote monitoring and control. However, these developments increase the points of accessibility to critical industrial networks and therefore the potential entry-points for cyber-attacks.

Attack activity tends to be initiated by both public and government entities

A few of the more notable examples of the state-sponsored attacks during last year include:

- A product of SolarWinds, a provider of network monitoring software, was infiltrated by a group believed to be supported by the Russian government. The malware inserted in SolarWinds' product infected the networks of over 33,000^ of its clients. High profile US government departments such as the Treasury Department, the Commerce Department, the Justice Department, and the State Department, as well as leading technology companies such as Cisco and Intel, were all compromised. The extent of the damage is still unknown and extends beyond the US.

- German officials found that a Russian hacking group associated with the Russian secret service had compromised the networks of energy, water, and power companies in Germany.

- The operations of Taiwan's state-owned petroleum, gasoline, and natural gas company CPC Corporation and its rival, Formosa Petrochemical Corporation, were disrupted by malware attacks.

- Japan's Defence Ministry announced a large-scale cyber-attack against Mitsubishi Electric, a major supplier of the country's defence and infrastructure systems. There are concerns that the attack may have compromised details of new state-of-the-art missile designs.

- China's banks require all companies to download software from one of two vendors to comply with their VAT scheme. Intelligence Tax, one of the most popular of the tax reporting software platforms used by foreign companies, was discovered to contain a backdoor that could allow malicious actors to conduct network reconnaissance or attempt to take remote control of company systems.

- Russian hackers targeted government agencies in NATO member countries. The campaign used NATO training material as bait for a phishing scheme that infected target computers with malware that created persistent backdoors.

- The Australian Prime Minister announced that an unnamed state actor had been targeting businesses and government agencies in Australia as part of a large-scale cyber-attack.

- U.S. officials announced that North Korean government hackers had been operating a campaign focused on stealing money from ATMs around the world.

- In the US, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) announced that a Russian hacking group breached U.S. state and local government networks, as well as aviation networks, and exfiltrated data.

Moreover, extortion cases have been on the rise, assisted by cryptocurrencies and other forms of anonymous payments.

> *"… this is something that is very important to understand, that you have a lot of state actors that are extremely sophisticated because this is where cyberwar is happening. These skills are spilling to the commercial space. Varonis Systems CEO, 8/2/2021*

USD 6 Trillion –
Estimated annual loss

What is a supply chain security?

As many as 40%* of cyber-attacks are now thought to originate in the extended supply chain, not the enterprise itself. Supply chain security centres around protecting the entire life cycle of product development and product delivery across different suppliers, partners, and customers.

Companies offering everyday products, such as computers, televisions, and cars, often rely on dozens of suppliers to deliver the finished goods. Each of these suppliers, in turn, relies on its own suppliers. Each of these external parties can expose organizations to new risks. A company is only as secure as the weakest link in its supply chain.

Ensuring supply chain security is therefore incredibly challenging. It ranges from mitigating risk within a company's own business and IT systems to mitigating risk derived from all of its third, fourth and "n" party relationships.

The problem is equally relevant for services companies, software companies, utilities, financial institutions, and any manufacturing company.

A growing attack vector is software upgrades

More and more of our devices have been designed to rely on periodic software upgrades. These upgrades are necessary to address bugs, reliability, and security issues. They can of course, also be used to add new functions and features. These software updates are particularly attractive for malicious actors. The attraction for the cyber-criminal is that if they break into the chain and insert their code into the upgrade software, they will be in a position to infect thousands of devices instead of a single device.

76%

Anticipated rise in rate of
cybercrime breaches by 2024**

Zero-trust systems, Software-defined perimeters, and Least Privilege

Design concepts such as "zero trust," "software defined perimeter" and "least privilege" are all gaining prevalence in IT security systems. All are similar guiding principles, like blueprints, for design of systems to address growing security issues. Although these ideas are getting a lot of recent attention, the concepts have been brewing among cyber security experts for nearly two decades.

In 2003, a group of global security experts, brought together by David Lacey at the Royal Mail, worked on a new security model whose core concept was to move from a perimeter-based security model to a "de-perimeterised" model. A simplified analogy would be that having a guard at the entrance of the building is not sufficient, you need more granular permissions for entering and accessing individual areas.

Over the years, the concept of de-perimeterisation has evolved and improved into the larger concept of zero trust, software defined perimeters, and least privilege.

The trouble is that moving to a zero-trust system is quite complex. Each element of data needs to have its own rules of access and each access needs to be monitored and logged. Companies continue to increase their security budgets to address these issues, but it will take a long-time and significant investments to redesign existing systems to incorporate the granular data permissioning and monitoring systems advocated by "zero trust" principles.

In Summary

Cyber security challenges will persist for the foreseeable future, despite constant initiatives undertaken by companies and governments.

Organizations have to balance the need to secure systems while at the same time ensuring employees' efficiency and customers' satisfaction are not damaged as a result of excessive repetitive security protocols. There is an inevitable tension between security and productivity. To reduce the burden on customers, security vendors are using cloud technologies, as well as Artificial intelligence (AI) and machine learning (ML) algorithms to protect and remediate more effectively.

The growing interest in privacy regulations also spurs demand for security and governance related products.

Currently, just over 16% of the investments in the Herald Worldwide Technology Fund are in companies whose core business is cyber security. These include Varonis Systems, Akamai, and Checkpoint. During the last year, we have adjusted our cyber security holdings to reflect changes in the market. We have taken profits in companies like Z-Scalar and CyberArk as valuations became difficult to justify. At the same time, we have added new positions, such as Qualys and FireEye.

Cloud vendors such as Amazon AWS, Alphabet's GCP, and Microsoft Azure also have significant security offerings and benefit from the growth in the cyber security market. Just in the last quarter, Microsoft disclosed revenues of $10bn during the prior 12 months from the sale of its security products.

We remain optimistic about the outlook for investing in this subsector and are on the lookout for more positions to add to the portfolio.

^Source: www.Gartner.com, September 2020

*Source: Accenture https://www.accenture.com/_acnmedia/PDF-134/Accenture-Securing-The-Supply-Chain.pdf#zoom=40

**Source: Stealth labs, cybersecurity facts and figures

Important Information

Market and currency movements may cause the value of shares, and the income from them, to fall as well as rise, and you may get back less than you invested when you decide to sell your shares. Certain statements in this report constitute 'forward-looking' statements. Such statements, including the intended actions and performance objectives of the Fund, involve unknown risks, uncertainties and other factors which may cause actual results, performance or achievements of the Fund to differ materially from those implied by such forward-looking statements.

This report has been issued on behalf of Herald Worldwide Technology Fund, and has been approved by Herald Investment Management Limited, its investment manager. Herald Investment Management Limited is authorised and regulated by the Financial Conduct Authority. Contact details:

Herald Investment Management Limited

10-11 Charterhouse Square

London, EC1M 6EE

Tel: 020 7553 6300

Fax: 020 7490 8026

bc@heralduk.com

For more information on Herald Worldwide Technology Fund and Herald Investment Management Limited: visit our website at www.heralduk.com