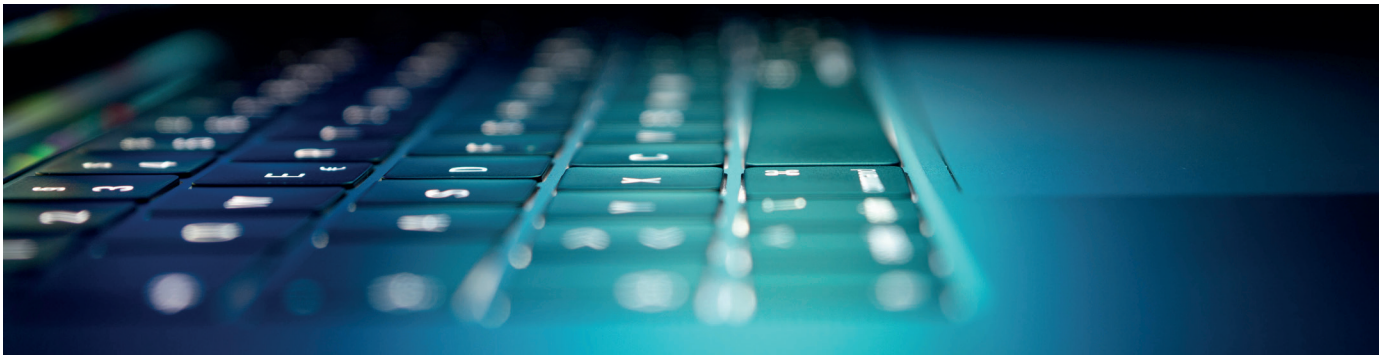
Instant Insights

Cybersecurity

Issue 1 | Second quarter 2019



William Therlin
Investment Insights and Portfolio Adviser

Amaya Gutiérrez
Investment and Portfolio Adviser

Idea in brief: cybersecurity investing

Growth in connected devices

With connectivity redefined, we now expect access to online services regardless of time and location.

Higher cyber risks

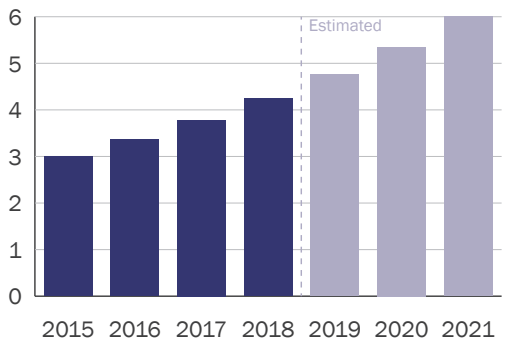
New risks have emerged as individuals and companies are increasingly exposed to cyberattacks. By 2021, the global cost of cybercrime will reach $6 trillion.[1]

Opportunities for investors

Rapidly growing, an entire industry has evolved as both private and public sectors invest in combating cybercrime. Given increased spending in cybersecurity, investors will find opportunities as this sector undergoes profound change.

Figure 1: Increased costs

Forecasted global cost of cybercrime ($ trillion)



Source: Cybersecurity Ventures, 2019 Cybercrime Report by Steve Morgan. Figures have been interpolated.

Cybersecurity spending increases

Few situations in life are more discriminating than having your private data stolen – such as bank details, home address and phone numbers. With personal and corporate data migrating from homes and offices to the internet, cybersecurity has become a household issue. In short, cybersecurity is the practice of keeping individuals, organizations and their networks, systems and programs protected from cyberattacks.

From accessing private information to disrupting business processes, extorting money to halting manufacturing, cyberattacks are an increasingly common threat to the global economy. This is why worldwide spend in cybersecurity is expected to exceed $1 trillion for the 5-year period from 2017 to 2021, a 12-15% year-over-year growth through 2021.[2]

More sophisticated cyberattacks

The ransomware attacks of 2017 show the global scale of the cybersecurity problem. Ransomware is a form of malicious software that blocks access to a computer, or its data, and demands money to release it. Ransomware virus 'Wannacry' in May 2017 affected over 150 countries and more than 230,000 systems. It affected instrumental services from healthcare systems (the UK's NHS) to transport networks (German state railways). In a separate attack, Yahoo! confirmed in 2016 that security issues three years earlier led to information being stolen for 3 billion users.

These cases demonstrate the heightened complexity of today's cyberattacks. Increasingly sophisticated, these attacks are a serious threat to both private service providers as well as to some of the most advanced technology companies, such as Google and Facebook.

[1] Cybersecurity Ventures, 2019 Cybercrime Report by Steve Morgan

[2] Cybersecurity Ventures, 2019 Cybercrime Report by Steve Morgan

The number of data breaches are growing fast

The average number of cybersecurity breaches has increased by 67% in the last five years[3] and the cost of cyberattacks is set to double in just six years, reaching over $6 trillion by 2021.[4] At the heart of this trend is a growing number of viruses targeting an increasing number of online users. Companies today rely on cloud-based processes and the Internet of Things (IoT) – the concept of devices being connected to the internet. Less than two years ago, the average citizen owned 2.4 devices with internet-connection, such as smartphones, wearables and vehicles. By 2022, the increased adoption of IoT devices means that we will each have 3.6 devices connected to the internet. North America and Europe will spearhead this trend with 13.4 and 9.4 connected devices per individual.[5] Increased connectivity means more targets for cyberattacks. Poorly secured devices run the risk of being infected with malware and exposed to phishing attacks.

Companies face significant fines

With the enforcement of European Union's **GDPR** in May 2018, companies are now under increasing scrutiny in their handling of private data. Companies that are negligent in protecting data against cyberattacks can face fines of up to 4% of global annual revenue. In addition to these fines, damage to a company's brand equity can be even more detrimental in the long term. This is why companies and organizations must invest in their cybersecurity capabilities.

Figure 2: Limited security

Number of organisations that claim to have only limited online security practices (%).

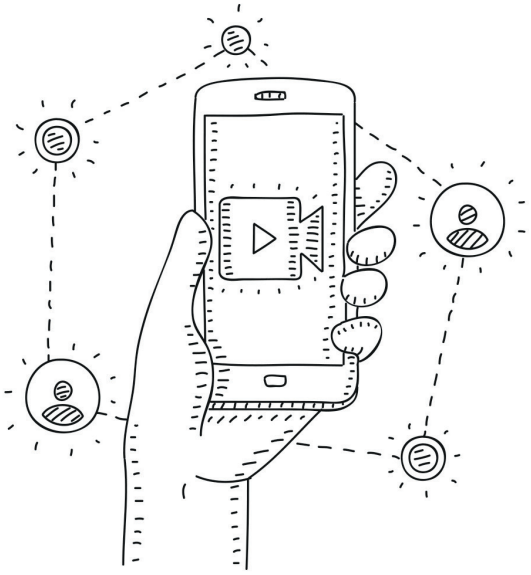
Source: EY, Global Information Security Survey 2018–19.

A recent study shows that 77% of organizations claim to operate with only limited security practices (figure 2) and 65% foresee an increase in their cybersecurity budget for the next year.[6] In light of the growing threat level, more sophisticated attacks and an increase in cybersecurity spend, multiple opportunities arise for investors as the cybersecurity market is set for profound growth.

How to invest in the cybersecurity sector

There are a number of ways one can gain access as an investor to a growing number of service and product providers in the cybersecurity sector. Depending on an investor's overall portfolio allocation, direct exposure through single line equities might be the most suitable strategy. For others, a broader and more diversified vehicle through a sectoral ETF, may be more appropriate.

With our **Investment & Portfolio Advisory** team at Rothschild & Co Wealth Management, we can advise on the most appropriate ways of gaining access to the cybersecurity sector, as a long-term investment theme. We look forward to answering any questions in relation to this publication, at a time convenient for you.



[3] Accenture, 9th edition of the Cost of Cybercrime study.

[4] Cybersecurity Ventures, 2019 Cybercrime Report by Steve Morgan.

[5] Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper.

[6] EY, Global Information Security Survey 2018–19.