Cybersecurity

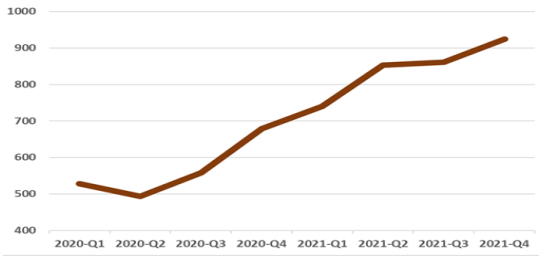
Fatima Iu
Fund Manager

Another busy year

Cybercrime incidents continue to grow in both volume and sophistication. The number of targets and points of entry continue to increase, created by accelerated cloud adoption, growth in edge computing and the proliferation of connected devices. The reason for these attacks is also broadening, with the primary aim appearing to shift from pure data theft to wholesale business disruption.

A ransomware cyberattack on Colonial Pipeline in May 2021 **forced the shutdown of the US's largest fuel pipeline which provided 45% of the East Coast's daily fuel consumption** and led to an emergency declaration across 17 affected states. The company paid $4.4m in, highlighting the vulnerability of critical infrastructure which hitherto has not been a major area of focus for cybersecurity.

Global weekly cyber attacks per organization (2020 – 2021)



Source: Checkpoint

Ransomware attacks are an increasing mode of exploitation, with an estimated 82% year-on-year increase , going from one every 40 seconds in 2016 to one every 11 seconds in 2021. The emergence of 'ransomware-as-a-service' is just one example of a growing ecosystem that is fuelling this growth. There is also a commensurate increase in the cost of cybercrime which is estimated to have gone up 50% in the past two years alone, creating a $1trn drag, or 1% of global GDP . With a growing ecosystem, improving economics and a way of extracting value that is both liquid and anonymous, it stands to reason that cybercrime, and as a result the need to continually refresh and upgrade cybersecurity, is here to stay.

Stock performance

Given this, it was perhaps surprising to see how much the **sector lagged the broader technology universe last yar – the ETFMG Prime Cyber Security ETF delivered a price return of 7.7%** in 2021, not only materially lagging the Dow Jones World Technology Index but also underperforming the broader software group.

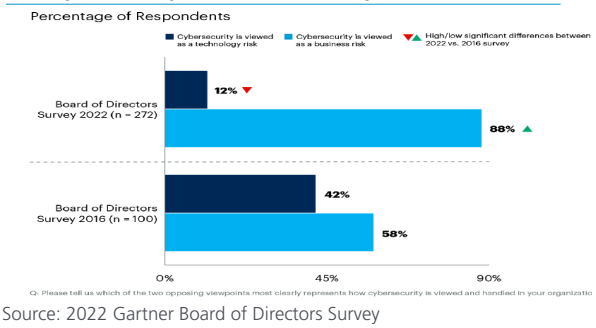
While company performance across the sector was weak, 2021 was probably one of the busiest M&A years we have witnessed in publicly listed cybersecurity companies and we are beginning to see an increased demand-side response as a result. Proofpoint and Mimecast, two market leaders in email security (both of which we have owned in the past), were both lost to private equity; McAfee was taken over by a private equity consortium after a brief stint back in the public market following its Intel ownership; Avast, a leading European consumer anti-virus company, agreed to merge with its US counterpart Norton Lifelock. The IPO market was also buoyant, although post-listing performance has been mixed, but we have yet to see any M&A in more strategic or high-growth assets.

Outlook

Cybersecurity has been **elevated from an IT problem to a business imperative** and should translate into healthy spend, having grown from **4.8% of IT budgets in 2011 to 8.4% in 2021**, though this still falls short of the 10% mark recommended by industry analysts such as IDC. Security spending overall is estimated to grow at 10.4% CAGR (2020-25), with the **software component growing materially faster at 15% CAGR, led by cloud security growing at 32%**.

President Biden's cybersecurity executive order, in response to the attack on Colonial Pipeline, calls for $9.8bn to be spent on civilian cybersecurity programmes, a 14% year-on-year increase. The scope is specific and wide-

How cybersecurity risk is considered by Boards of Directors



Source: 2022 Gartner Board of Directors Survey

ranging, covering all federal agencies and, by extension, their suppliers, with a focus on moving towards a zero-trust framework. The threat from nation states has also gone up in the administration's (and governments' worldwide) agenda given the current geopolitical tension in Russia and Ukraine, as the cybersphere becomes part of the modern-day battleground.

We continue to believe that intelligent endpoint, identity management, secure access and data protection remain the cornerstone of next-generation security frameworks, regardless of the location of the user, application or data. We expect cloud-based security to gain budget share over time, where we see the biggest gap between spending on underlying compute and the efforts to secure it. CrowdStrike estimates that cloud security spend amounts to only 1% of the underlying infrastructure spend today. We were surprised by the strength in the more traditional firewall business in 2021 after an exceptional 2020, which points to a much more complex and enduring hybrid compute environment.

Competitive dynamics within the industry have been relatively benign, in part due to the large and growing opportunity set. However, we do expect things to heat up as lines become increasingly blurred. New platform players are using their advantage in data telemetry and use of AI to subsume previously standalone features. The ever-increasing volume, frequency and evolving nature of cyber incidents is making automation and AI indispensable. IBM suggests the cost of a breach could be as much as 80% greater at companies where security automation and AI are not fully deployed , making it even harder for legacy players to keep up.

Cloud titans remain the biggest threat to their smaller peers, and we monitor developments here closely. Although there has been no official change to the shared responsibility model, cybersecurity has become a much more mission-critical aspect of cloud deployment. A 2020 IDC survey found that nearly **40% of respondents are already using security tools directly from cloud vendors for cloud workload security. Microsoft described cybersecurity as a $15bn business growing at 45% y/y**. AWS has so far been more focused on white-labelling services from managed security services providers, but we are well aware of the fate of AWS's other white-label product suppliers. Alphabet has also been investing more aggressively in both cybersecurity technology and personnel and, together with Microsoft, have committed to spending $10bn each to help strengthen security to support their government business and other customers.

What gives us comfort is the consistent feedback around the difficulty to standardise across multi-cloud and hybrid environments, especially for larger enterprises. Utilising security tools from any one cloud provider makes it more difficult to apply consistent policy across data assets, creating more opacity and therefore room for error. Customers are also aware of supplier concentration risk, with mainstream breaches via Microsoft Exchange and AWS misconfigurations still very much fresh in their minds. Against today's regulatory and social backdrop, the reputational, legal and business risks are simply too great for companies to outsource their cybersecurity management.

This sector has historically been one that investors 'trade around', considered to be more cyclical than core enterprise software and more sensitive to news headlines. With the emergence of new platforms, a shift towards recurring revenue models and larger opportunities resulting from digital transformation and an evolving threat landscape, we are hopeful things will change for the better over time.

ESG

Cybersecurity promotes access to technology and communication infrastructure. In our view there are three key issues that most commonly impact the ESG standing of companies in this group:

- **Data privacy concerns** due to the sensitive data and credentials that many cyber companies have access to. We look for strong technological and procedural defence against data theft. Failings here can impact the viability of a business.
- **Employee engagement,** a strong diversity and inclusion policy, is critical in helping to attract and retain key personnel in this highly competitive market for cybersecurity specialists.
- **Governance and oversight.** Due to the small pool of experienced cybersecurity executives available, management teams and boards are not always the most diversified. In addition, acquisitions add complexity to revenue recognition and pay structure (such as earn outs) that requires more scrutiny.

Fatima Iu

18 May 2022

Find out more

Client Services

E investor-relations@polarcapital.co.uk
T +44 (0) 20 7227 2700
F +44 (0) 20 7227 2799