VIEWS ON

Why cybersecurity matters to investors

January 2019

In the words of the ex-Director of the FBI, Robert Mueller: "There are only two types of companies: those that have been hacked, and those that will be."

Cybersecurity has moved beyond the realm of Hollywood blockbusters to become a key issue for society. From the undermining of the democratic process to identity theft and fraud, the net of cybercrime is far reaching, and investors need to be aware of these issues. The financial impact of cybersecurity breaches, both public and undisclosed, can be substantial. As companies become more automated and digitally-connected, the potential for increasingly material capital erosion becomes a greater reality, explains Abbie Llewellyn-Waters.

Abbie Llewellyn-Waters, Fund Manager

The most common risk is from your colleagues, not rogue states

Cyber breaches are part of modern business life, but it is rarely clear who is behind targeted cyberattacks, and their ultimate motives. At one end of the scale, it is known that there are some nation states involved – highly sophisticated and well organised government agencies, with the greatest cyber firepower at their disposal. More frequently than not, this activity tends to be for intelligence gathering purposes rather than malice.

There are also very advanced and well-resourced operations by criminal organisations, who tend to carry out disruptive attacks. When TalkTalk suffered its first data breach in some time after 2011, the criminal organisation that exploited them is reported to have set up a complex series of call centres to exploit the data theft.[1]

However, the more frequent cyber aggressor is the employee: the insider. In 2016, IBM's Cyber Security Intelligence Index found that 60% of all attacks were carried out by insiders.[2] Of these attacks, one quarter involved inadvertent actors, typically staff who failed to pay attention to a company's cybersecurity policies, while three quarters were found to involve malicious intent. Typically, the aim of these types of attack is to steal competitive information, sell data or intelligence; however, there are some who have more nefarious intents of damaging the organisation.[3]

What does this mean when analysing companies?

Companies who have both understood and positioned themselves to withstand a cyberattack indicate to us higher quality management teams and businesses supported by a long-term outlook and strategy. There are simple questions investors can ask of company management teams when analysing the long-term investment opportunity. We typically like to focus on:

- The role of the board
- Training of the employee base
- IT integration – particularly important for acquisitive businesses
- Transparency

We have specific metrics within these areas that we consider in order to enhance our financial analysis of a company. We believe these give us a more comprehensive insight into the mentality of the business.

We focus on these four core areas because they allow us to quickly assess whether the risks of a cyberattack are understood. Materiality of financial risk doesn't just relate to operational disruption but, as we have seen from several high-profile cases in recent years, it also points to potential future revenue loss through erosion of trust with your client base.

What about when a cybersecurity attack does occur?

All companies are vulnerable to cybersecurity breaches, but when major breaches become public, we look for the companies we invest in to be decisive and transparent. We look to the board of directors to take responsibility and communicate to clients and shareholders.

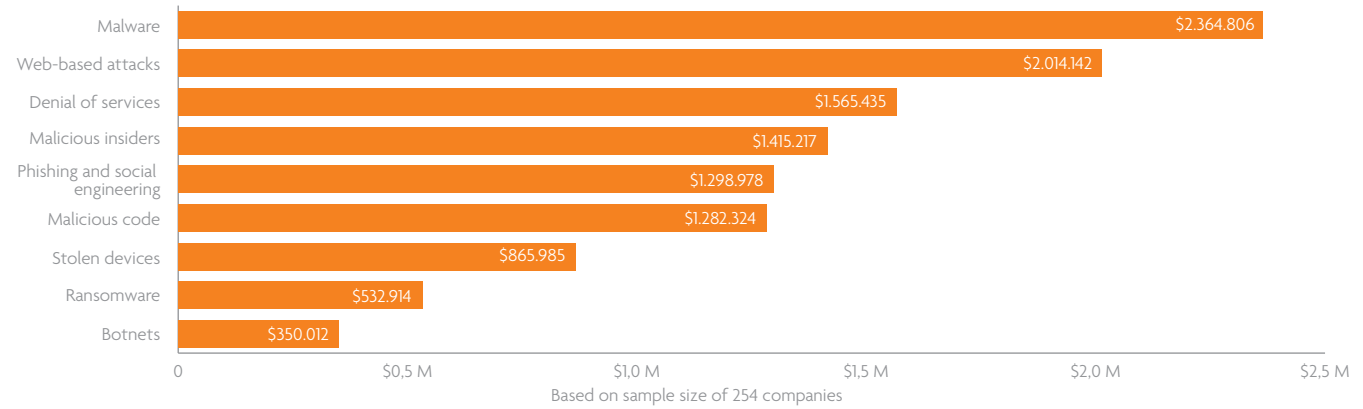
As a positive example of this behaviour, one of our investee companies in the Information Technology sector (intentionally anonymised) suffered a cybersecurity breach which shut down several of its production lines for several days. We engaged immediately with the company and were given detailed explanations of the incident, allowing us to assess the financial and client impact, and above all, how the company was responding.

The company had been infected with a ransomware virus. Ransomware viruses became infamous in May 2017 attack when the WannaCry virus hit many parts of the world, affecting more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.[4] The ransomware is actioned when a 'kill switch' is triggered that effectively kidnaps the computer's data by encrypting it and holds it to ransom. The data is theoretically released from being held hostage when payment is received, typically in a cryptocurrency such as Bitcoin.

Fortunately for the company held in the portfolio, the ransomware encountered failed to encrypt, which meant no ransom. While mindful of the direct loss of revenue from the shutdown of their facilities to both limit and resolve the incident, the focus of our concern was the threat to existing customer relationships.

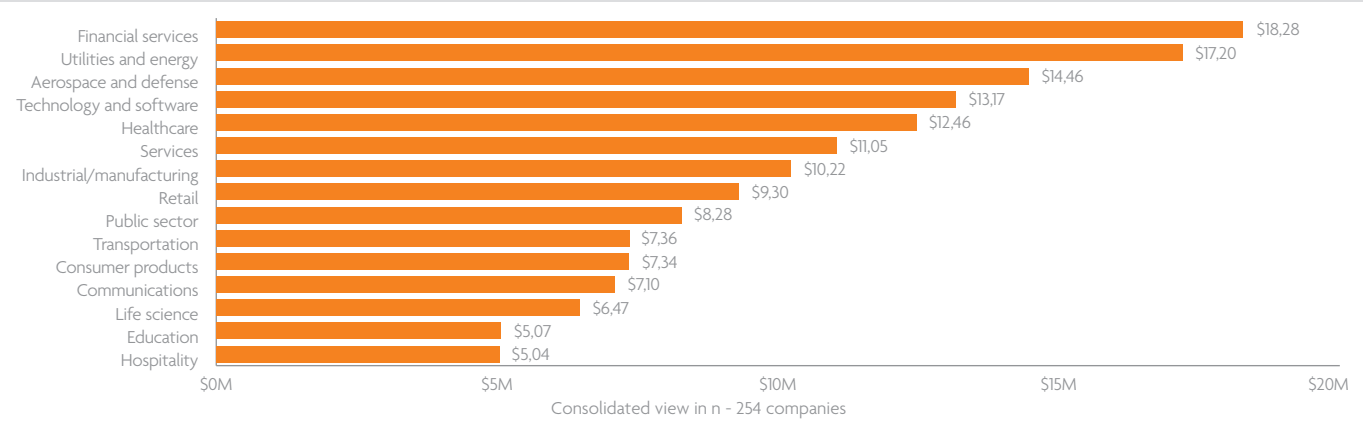
Through the company's transparency and engagement, we factored these considerations into building our mosaic of long-term conviction in the quality of the management team and their ability to manage strategic risks.

Annual corporate costs related to cybersecurity breaches



Source: Accenture Cost of Cybercrime Study 2017

Average annualised cost of cybercrime by industry



Source: Accenture Cost of Cybercrime Study 2017

Cybersecurity precautions are an indicator of a company's quality and resilience

This example illustrates how embedding broader ESG factors into the stock selection process enhances our insight into the operational resilience of business continuity and ultimately the quality of companies we invest in.

Another cybersecurity policy that can illustrate a disciplined approach to operational excellence is a zero-tolerance rule on phishing emails. The 'phishing' email is the one that tries to lure you into clicking a hyperlink, invariably by inviting you to fund a far-away prince who desperately needs your help or to investigate the receipt of an album you would never buy. We believe having a clear strategy for preventing these attacks in the first place is an indicator of a higher quality business that is designed to be resilient and robust, proactive not reactive.

Conclusion

Companies with poor cybersecurity processes and governance may well, in our view, have further underlying weaknesses that make them prone to broader external risks. We believe that applying a common-sense approach to embedding ESG factors in the investment process can provide a much deeper understanding of the culture and strategic position of a company, and about how they think, communicate and quantify intrinsic risk. It's quite often the case that companies who approach cybersecurity in a comprehensive way, for example, are naturally more operationally resilient.[5]

We believe the assessment of cybersecurity governance and strategy enhances our analysis prior to investing our clients' money. Simply put, companies who understand and manage these types of risks well typically tend to be better run businesses.

Contact us

Please visit www.jupiteram.com for contact details in your region and more information about products and services available.

[1] *https://www.bbc.co.uk/news/technology-39177981*

[2] *2016 Cyber Security Intelligence Index, IBM, July 2016*

[3] *The Biggest Cybersecurity Threats Are Inside Your Company, Harvard Business Review, September 2016 https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company*

[4] *Europol, May 2017*

[5] *Becoming operationally resilient: A guide to operational resilience in Financial Services, PWC, July 2018*