Cyber-security

Each fresh set of headlines about new cyber-security breaches portrays how challenging the extreme complexity and sophistication of technology is for company management.

As an investor, exposure to cyber-risk is one of the elements we take into account when evaluating a company. With companies growing more complex and regulations more stringent, cyber-security requires first rate governance.

Jeroen Knol from the BNP Paribas Asset Management European Equities team and Felipe Gordillo from the BNPP AM Sustainability Centre discuss our approach to assessing the strength of business models and corporate governance with regard to cyber-security.

Engagement

What sort of challenges does cyber-security pose to companies?

Cyber "security" is a something of a nebulous concept. Cyber criminals may be well-funded criminal organisations or state-sponsored entities. They attack daily. So being "secure" simply means you've won today's battle. Each and every day brings a new onslaught.

Cyber-attacks can create a material risk to investors and impact the interests of the entire stakeholder community of a company. Firstly, a cyber-attack has the capacity to disrupt operations impacting how company employees and managers work. Secondly, it can impact more broadly the information systems which deal with company's suppliers and contractors. Third, a company which fails to protect its customers' personal data should find it more difficult to retain and build trust and solid relations with its clients. This problem is compounded by how customers are increasingly aware of security issues (Security Transformation Research Foundation, 2019). Finally, companies might find themselves at odds with regulators, as legislation becomes tighter. It is an integral part of the fiduciary duty of institutional investors to be aware of these risks and manage them appropriately.

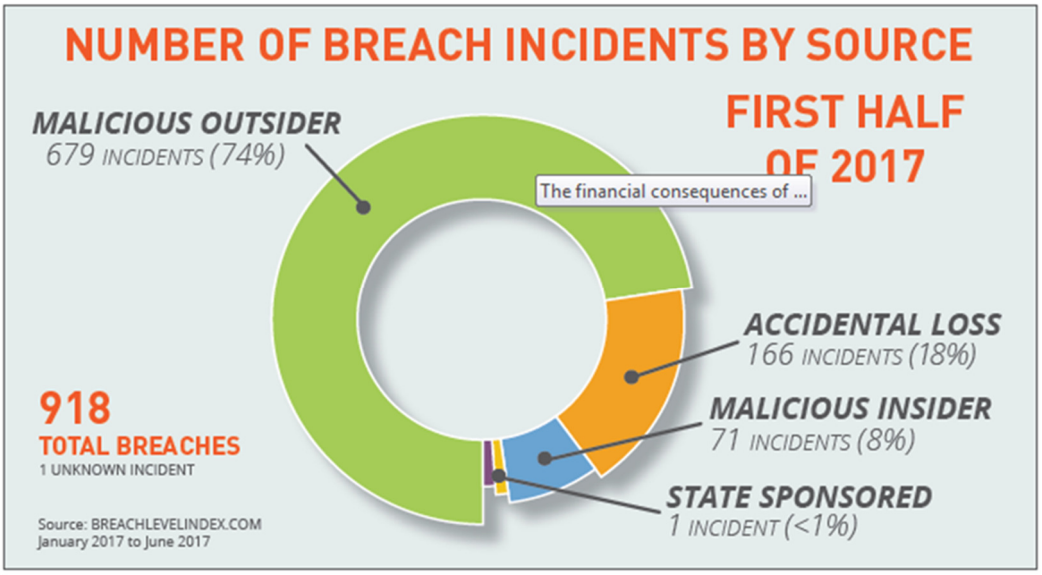
The nature of cyber-attacks varies. Cyber-attacks can happen through several mechanisms. These include cyber intrusion that uses the supply chain to gain access: accidental or intentional actions by insiders that can login and access the network; emails from fake executives using addresses designed to closely replicate real executive email addresses to request transfers of funds; and fake vendors using hacked real foreign vendor email accounts to request payment for invoices to fraudulent accounts. It is generally believed that 99% of all cyber-attacks are activated by a company's staff or internal IT users.

Fraudsters may use a security breach on employees' phones to access passwords. Or hide behind a highly respectable third party vendor to access a company's IT system. The sending of fake research pdf files, ostensibly from a reputable business or a government department is another way of accessing companies' internal IT system.

Companies may invest huge sums in digital security and raising awareness but it only takes a single staff member or, increasingly, senior executive, to be drawn in, for an attack to be successful.

A paper by Gemalto (2017) found that for the first six months of 2017, out of the 918 total breaches, 74% of them were by malicious outsiders but 8% were malicious insiders and 18% were caused by accidental loss.

Figure 1: Number of breach incidents by source



Source: BREACHLEVELINDEX.COM

How seriously do companies take cyber-risk?

Much has been written on the subject. A study by the Sustainability Centre at BNP Paribas Asset Management found that while 63% of companies have a comprehensive policy on cyber security, 25% of companies have a weak policy and 12% of companies have no policy at all.

Hiscox Insurance, an insurance company offering cyberspace insurance, claims that 7 out of 10 organisations are insufficiently prepared for cyber attacks.

However this figure includes non-profit and micro-cap organisations. If we assume that awareness and willingness to act is much greater among large-cap firms, then it's clear that this picture will be somewhat skewed.

According to the Gartner agency, global cyber-security spend in 2018 was estimated at $114 bln, up 12.4% compared to 2017. So there is evidence that cyber-security is being taken increasingly seriously.

Nonetheless, the global cost of cyber-crime, estimated in 2018 at between $400 bln and $3 trn, by far outweighs spending on preventive measures.

In 2018 the Sustainability Centre at BNP Paribas Asset Management found that, in Europe, 75% of regional tech companies had incorporated at least some of the standards outlined in the ISO 27001 cyber-security policy. Outside Europe the figure is 50% and is unknown for sectors other than tech. However, while the certification can be used as a framework to assess its process and security management, it isn't the strictest of standards.

Moreover, within Europe, only 75% of companies have an action plan of what to do if there is an attack.

It is generally assumed that technology and IT companies are more aware of cyber-risk, and more adept at addressing it.

In short, the nature of cyber-risk is such that it depends on the type of company and the nature of the industry within which it operates. And once a company or a peer has been victim of material cyber crime the subject is taken much more seriously.

The fact is that no company can afford to downplay cyber-risk.

To what extent do you find it easy or difficult to obtain the information on cyber-risk in a company?

It's difficult, if not impossible. There are no universal standards or metrics to measure and assess cyber-risk. More importantly it's a moving target given the growing range of variables around cyber-risk. For each company only some of the risks may be recognised or definable in advance. In addition it is not in any company's or stakeholder's interest to make public precisely where their cyber-risks lie.

A study by the UNPRI found that the average disclosure level of companies is very low. While assessing companies against indicators, they found that only 55% of the companies disclose information covering between 3 to 7 of their indicators. Moreover, only 25% of the companies disclosed against 2 or fewer indicators.

An article by Coleman (2019) reported that it took on average 44 days for a company to report an incident and only 50% of firms that disclosed a breach provided information on the type of attack that occurred and while 70% of companies disclosed one cyber-breach, only roughly 30% disclosed multiple breaches.

Spending on protection against cyber-risk is generally part of the IT budget, which is seldom disclosed in full detail. While we don't have a specific percentage, Gartner claim that organisations spend 5.6% of their overall IT budget on security and risk management.

Even if you can identify and isolate a specific cyber-risk, firms increasingly take cyber-liability insurance to mitigate these risks. This makes it hard or impossible to assess the size and nature of the residual cyber-risk.

Finally, when state sponsored actors are involved they typically don't leave any trace of their presence. So they might remain, undiscovered, for years, in a company's IT network.

As such, an individual company's risk, and protection measures against such cyber-risks, are hard to assess.

In recent years laws and regulations (such as the EU's General Data Protection Regulation – GDPR) have been put in place to force organisations to be more transparent about cyber-damage and to report cyber-breaches to authorities. Penalties for failure to report amount to €20 mln, or a painful 4% of annual global revenue, whichever is higher. This will force companies to be more transparent about cyber-risk.

How transparent are companies about the risks they encounter in cyber-space?

Companies will talk about their cyber-risk in general terms but will not, and should not, get very specific unless it's with regard to past events.

It is worth noting that up until now, cyber-damages may have been relatively small and remained undisclosed – the average malware attack costs $2.4 mln according to Accenture.

PWC has different numbers; for large firms they reckon the cost lies between £600k and £1.15 mln. Therefore for a large cap company with, say a $5 bln cost base, an incident may not have been significant enough to be reported individually.

We don't want companies to be completely transparent as that opens them up to risks.

Where does cyber-risk responsibility sit in the governance structure?

How the board handles cyber-security issues is important as they are ultimately accountable and their remedial action will be scrutinised. This makes it crucial that cyber-security becomes a regularly addressed agenda item at board level, regardless of whether or not there has been an actual issue. This, then, begins to inform every strategic decision.

In terms of governance, according to a 2017 United Nations' backed Principles for Responsible Investment (UN PRI) draft, less than 30% of companies have identified a senior manager to deal with cyber-security or have a board member involved in overseeing the data protection policy. However, a study by BNP Paribas Asset Management found that within Europe, only 25% of companies have a director that has complete specific knowledge in cyber-security and only another 25% of companies have some knowledge.

However 75% of companies were found to have access to some internal or external expertise on cyber-security, and positively, the remaining 25% have good access to information.

However we find that for those companies acknowledging cyber-risk, the responsibility often sits just below board level, with the CSO (Chief Security Officer) or CISO (Chief Information Security Officers) reporting to the CRO (Chief Risk Officer) or CFO (Chief Financial Officer).

Since the introduction of GDPR, CFOs and CEOs have become more alert to issues where compliance has a role too. The main question is how the information on cyber-risk and damage is fed through to the board.

If companies are reluctant to disclose, how do you assess the risks? To what extent does a researcher have to second guess the real risk?

Due to the important Environmental, Social and Governance (ESG) threats that cyber-security presents, we at BNP Paribas Asset Management, ensure we consider it an essential issue in examining companies. We have two levels of assessment. Firstly, we examine a company's cyber-security strategy and its implementation. We expect companies to explain how they identify and manage their data vulnerabilities, and to describe their action plan, detecting and responding to a threat and recovering compromised data. Secondly, we focus on companies' governance and risk oversight boards, expecting companies to be able to identify the key people responsible for the implementation of remedial actions, and to engage senior management and the board in the oversight of this process.

There are a number of ways we go about assessing risk:

- Peer comparisons in terms of IT budget and measures taken/disclosed
- When undertaking fundamental research for our actively managed equity strategies (such as those run by BNPPAM's Europe Equity investment team), due to our long term holdings and concentrated portfolio we have very good access to company management and different levels of management. This provides us with good understanding and visibility of their practices.
- Meeting management of direct competitors within a given sector to learn about the cyber risks they recognise.
- From our perception of the cyber risk sensitivity of the industry within which a company operates.

To what extent do you think companies are really on top of the risks?

It's impossible to assess.

Just as in the physical world, you can't necessarily rely on the same protection and defences to work equally for each individual with criminal intent. A continuous process is needed to update security methods, creating new parameters and layers of protection.

At the same time cyber risks are not new. They have been around for several decades. There have been high profile cases of cybercrime and data losses (e.g. Equifax, leak of data files for 143 mln Americans, Marriot hotels – data for 500 mln customers compromised, Sony PlayStation Network data leak of 77 mln users' data). More recently, we see Eurofins, an operator of a network of labs – not a business that first comes to mind when thinking about cyber risk - announcing a material impact from a cyberattack.

So far, however, only limited damage has resulted among large-cap European companies. Is this luck or have European companies invested more in prevention? Is their spend as a percentage of their cap size part of the story? Or are they simply less digital? The answer is probably a mix of these things.

According to the UN backed PRI draft of 2017, European companies perform better on indicators providing proof of the implementation of a cybersecurity policy (with respect to board involvement, communication of cyber risks to the board; detailing cyber information to the board and establishment of a dedicated team and budget to deal with cyber security).

Related questions

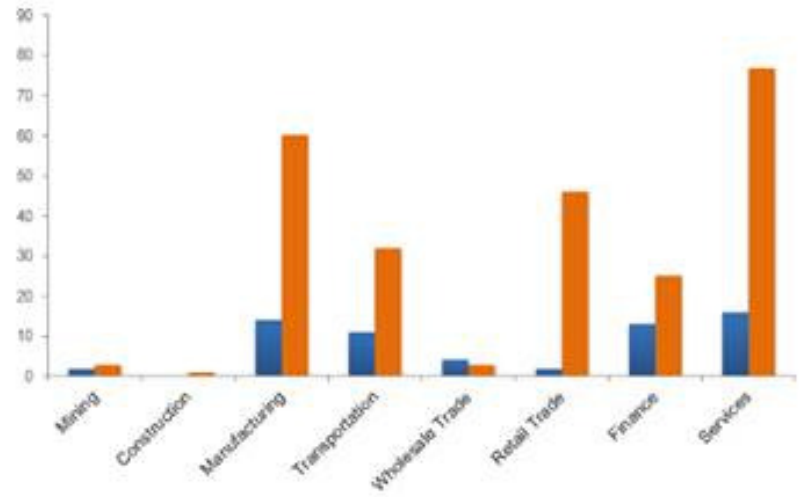
Is cyber-risk more pronounced in particular sectors?

Yes, the risk may be lower in relatively low-tech companies, such as beer brewers, where there is a limited amount of end-customer data, than in a bank or in an IT company whose business is based on technology and /or customer data. As mentioned earlier, IT companies may well be more aware and, therefore, better protected.

However we are under no illusion; the risk is omnipresent. The recent ransomware attack on Norwegian aluminium miner Norsk Hydro is a good illustration of this and follows an attack on zinc producer Nystar earlier this year.

Previous studies have found that the sectors that are most likely to be attacked include the healthcare sector, which received the highest level of breaches in 2015, as to hackers it represents a source of sensitive customer data. This is also problematic as the UNPRI study found that the health sector has the worst level of disclosure. This applies to government agencies in a wider sense that are subject to a large amount of attacks by foreign actors with malicious intent, particularly in Turkey and the United States. Financial services are desirable as they handle private information but, on the other hand, these are the companies that invest the most in cyber-security awareness. Finally, energy sectors may also be hacked by hacktivists who might want to cause power outages. (Infosec, 2019; Manship, no date). A study by Coleman (2017) also provides an idea of the distribution of cyber-attacks.

Figure 2: Cyber-security breaches vs. director appointments with cyber-security experience



Source: auditanalytics.com, August 2017

These attack s suggest that we ought to be aware of the enhanced cyber-risk that accompanies the increasing adoption of internet-enabled technology in manufacturing and process-driven industries.

To what extent does industry structure influence a company's ability to withstand cyber-risk?

In theory a strong industry structure is a positive with regard to defence against cyber-risk. As the philosophy of our Europe Equity investment team identifies, companies in well-structured industries face less competition and have more pricing power. This generally translates into higher and more sustainable levels of profitability. Therefore, in better structured industries there is:

i.) a greater ability to pass on the cost of cyber risk prevention to customers

ii.) a higher level of profitability to potentially absorb costs related to cyber-security.

In fact, cyber-security might increasingly act as an argument for consolidation or as a barrier to entry, as smaller companies are considered more vulnerable to cyber-risk by consultants and insurers (and hackers too). They tend to lack the huge IT budgets of the largest cap peers (according to Hiscox: only 52% of small businesses have a cyber-security strategy and 21% of small businesses have a cyber-insurance policy, compared to 58% for large companies).

What is the balance of opportunity for cyber-risk? To what extent is it worth a business forgoing the value data can bring in order to avoid the risk of being hacked?

This varies by industry. For some industries and companies with light-data use this might be a consideration.

But for many companies like credit card companies or travel agencies, that frequently exchange vital and sensitive data with mass market end-users, it is simply not an option.

It's also important to understand that cyber-risk is not just about client data leaks. Best-in-class cyber-security reviews generally also cover: software update supply chain attacks; distributed denial of service. (DDoS) attacks; and file destruction.

In this light, one thing to keep in mind is how easy some of the basic attacks are. A DDoS attack to shut down a company's web server is something that can be organised in a few minutes with access to a prepaid phone and some bitcoins or a stolen credit card number.

What works best from a costs/risks/benefits perspective - pro-active or reactive cyber-risk management?

There is no way around preventative measures and a pro-active approach.

However, rather than just spending enormous sums on preventing breaches and attacks, companies should also act to mitigate the potential damage a cyber-security breach could cause.

The biggest cost in the event of a data breach generally lies in resolving the issue in terms of compliance fines and court fees, while a company's image or brand can suffer immeasurable damage.

But remediation generally also requires a subsequent step-up in investment in investigative, forensic tools and in staff/identity theft prevention. Moreover the aftermath can affect customer behaviour, sales motivation and simply require a lot of attention from management and front office/sales teams.

The cost of the aftermath of a cyber-attack can be pre-assessed, mitigated and insured against in advance, while procedures and systems can be put in place to handle these issues beforehand.

If a business model is based on the holding and farming of data, how different is the risk compared to a company for whom data is a by-product of the business?

It's very different. And the risks can be considered to be higher.

But, in the case of a business model predicated, as for example with a bank, on holding client data, awareness about cyber risk is generally high and cyber-risk prevention budgets and measures tend to be equally high.

This in itself may be encouraging cyber-criminals to target less obvious companies, and companies in industries where there is less awareness of cyber-risk.

What do you consider to be the key questions for management meetings when determining the quality of a company's practices?

Our role is to challenge a company's process for dealing with cyber-security.

From a governance perspective our primary interest is for a board member to be able to talk about potential vulnerabilities in cybersecurity in layperson's terms.

Cyber-security starts in the boardroom. Besides having cyber-security and data protection on the agenda for every board meeting, the board of directors should employ best practice for cyber-protection. Directors need to make sure that the software they are using provides them with the right protection. This includes everything from mobile devices to board portals. Board members should ensure that their communication methods do not expose board materials to malicious attack. Email delivery of board papers should be avoided and replaced by a secure communications tool that can prevent materials from being accidentally shared with outside parties..

Here are some of the questions we would typically address to board members:

What is the nature of the company's key cyber-security risks currently?
How have these changed over the past few years?
How is the board informed about cyber-risks and damages?

How do they keep track of cyber-attacks?

Who is responsible for this, and how has the intensity of attacks evolved over time?

How are staff being made aware of, and trained against, cyber-risks?

By what percentage does the company expect cyber-security cost to rise over the next three years?

Has the company taken insurance cover against cyber-risk and to what extent is there a residual risk and estimated potential damage?

References

Accenture (2017). Cost of Cyber Crime Study.

Audit Analytics Staff (2018). Do Companies With Data Breaches Belong in ESG Portfolios?. [online] Audit Analytics. Available at: https://blog.auditanalytics.com/do-companies-with-data-breaches-belong-in-esg-portfolios/ [Accessed 26 Jun. 2019].

Coleman, D. (2018). SEC Registrants with Poor Cyber Controls. [online] Audit Analytics. Available at: https://blog.auditanalytics.com/sec-registrants-with-poor-cyber-controls/ [Accessed 26 Jun. 2019].

Coleman, D. (2019). Credential Stuffing at Chipotle Mexican Grill Inc.. [online] Audit Analytics. Available at: https://blog.auditanalytics.com/credential-stuffing-at-chipotle-mexican-grill-inc/ [Accessed 26 Jun. 2019].

Coleman, D. (2019). Trends in Cybersecurity Breach Disclosures. [online] Audit Analytics. Available at: https://blog.auditanalytics.com/trends-in-cybersecurity-breach-disclosures/ [Accessed 26 Jun. 2019].

eurofins (2017). Cyber Security. [online] Eurofins-digitaltesting.com. Available at: https://www.eurofins-digitaltesting.com/cyber-security/ [Accessed 3 Jul. 2019].

Fouche, G. and Solavik, T. (2019). Aluminum maker Hydro battles to contain ransomware attack. [online] Reuters. Available at: https://uk.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUKKCN1R00NJ [Accessed 3 Jul. 2019].

Gaillard, J. (2019). Cyber security is becoming a matter of good corporate governance, good ethics, and quite simply – good business.. [online] CIO WaterCooler. Available at: https://ciowatercooler.co.uk/cyber-security-is-becoming-a-matter-of-good-corporate-governance-good-ethics-and-quite-simply-good-business/ [Accessed 26 Jun. 2019].

Gemalto (2017). Data Breach Statistics by Year, Industry, More - Breach Level Index. [online] Breach Level Index. Available at: https://breachlevelindex.com/ [Accessed 4 Jul. 2019].

Gordillo, F. (2017). ESG in the age of cybersecurity. [online] BNP Paribas Asset Management. Available at: https://investors-corner.bnpparibas-am.com/investment-themes/esg-in-the-age-of-cybersecurity/ [Accessed 26 Jun. 2019].

Halliday, K. (2019). Part 1 of the ESG series: How cyber security gives shareholders vital insights into governance quality | AMP Capital. [online] AMP Capital. Available at: https://www.ampcapital.com/au/en/insights-hub/articles/2018/August/cybersecurity-vital-insights-governance [Accessed 26 Jun. 2019].

Hiscox (2018). Small Business Cyber Security Report.

Infosec (2019). Security Threats by Industry. [online] Infosec Resources. Available at: https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-threats-by-industry/#gref [Accessed 3 Jul. 2019].

Manship, R. (n.d.). The Top 6 Industries At Risk For Cyber Attacks. [online] RedTeam Security. Available at: https://www.redteamsecure.com/the-top-6-industries-at-risk-for-cyber-attacks/ [Accessed 3 Jul. 2019].

Mitchell, K. (2018). Cybersecurity is a Bigger ESG Concern for Institutions than Climate Change, Terrorism – Institutional Allocator. [online] Institutional-allocator.com. Available at: http://institutional-allocator.com/cybersecurity-is-a-bigger-esg-concern-for-institutions-than-climate-change-terrorism/ [Accessed 26 Jun. 2019].

Moore, S. and Keen, E. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. [online] Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 [Accessed 3 Jul. 2019].

PRI (2018). Investor-company dialogue on cyber security: five emerging findings. [online] PRI. Available at: https://www.unpri.org/governance-issues/investor-company-dialogue-on-cyber-security-five-emerging-findings/3664.article [Accessed 26 Jun. 2019].

PRI (2018). Stepping Up Governance On Cyber Security. [ebook] PRI, pp.1-17. Available at: https://www.unpri.org/download?ac=5134 [Accessed 26 Jun. 2019].

PRI (n.d.). Engaging with companies on cyber security. [online] PRI. Available at: https://www.unpri.org/esg-issues/governance-issues/cyber-security [Accessed 26 Jun. 2019].

Price, N. (2017). Why Board Members Should Be Aware of How Cybersecurity Is Impacting ESG | Diligent. [online] Diligent. Available at: https://diligent.com/en-gb/blog/board-members-aware-cybersecurity-impacting-esg/ [Accessed 26 Jun. 2019].

SEB (2012). Cyber security and crime prevention. [online] SEB Group. Available at: https://sebgroup.com/about-seb/crime-prevention/cyber-security-and-crime-prevention [Accessed 26 Jun. 2019].

Security Transformation Research Foundation (2019). Looking beyond the Technology Horizon. [online] The Security Transformation Research Foundation. Available at: https://securitytransformation.com/ [Accessed 26 Jun. 2019].

DISCLAIMER