Why UK pension funds should consider cyber and data security in their investment approach

November 2019

The National Employment Savings Trust (Nest) is a defined contribution workplace pension scheme, set up by the UK government to support auto-enrolment. At the time of writing, around 730,000 employers are registered to use Nest, which has more than eight million members and nearly £8 billion in assets under management.

The Railways Pension Scheme (RPS) is one of the UK's largest and longest established pension funds. RPMI and RPMI Railpen (Railpen) run the RPS on behalf of their parent, The Railways Pension Trustee Company Limited (RPTCL). Railpen is responsible for the safekeeping and investment of circa £30 billion on behalf of the scheme's 350,000 members who are connected to the railway industry.

Acknowledgements

We would like to thank the lead authors of this publication, Jocelyn Brown (RPMI Railpen), and Diandra Soobiah (Nest).

We would like to thank the following for their contributions to the content of this publication, Leo George (RPMI Railpen) and Helen Price (Brunel Pension Partnership).

Technical review was provided by Mark Beck (RPMI), Sylvia King (RPMI) and Samantha Knights (RPMI Railpen).

Contents

Executive summary

UK pension funds speak out on cyber and data security.

Around three-quarters of businesses say that cyber security is a high priority for their organisation's senior management, in part linked to the recent introduction of the General Data Protection Regulation (GDPR) in Europe, and pension funds are no exception.

In 2018, the Pensions Regulator produced guidance for trustees on cyber security principles for pension schemes. While this guidance provided advice on building a scheme's cyber resilience, to date no equivalent advice has been provided to trustees looking to incorporate cyber security into their investment process.

Numerous papers and articles are now citing cyber security as a prominent and growing issue that can have strong, negative implications on investment performance. Coupled with that is the issue of data security, which is also a key risk for companies with costly effects. Cyber security and data breaches can cause financial and reputational risks for companies which could impact their performance.

While engaging on this topic could be seen as daunting to a trustee with no specialist technology expertise, cyber security risks are financially material and of interest to members and other stakeholders. Generally, little is understood by pension funds about these risks and there is seemingly no obvious common or standardised approach for addressing them.

This document presents case studies on the research and engagement a number of leading UK pension funds have carried out on cyber security and shows how they are currently addressing the topic. Pension funds are encouraged to:

- consider the risks as part of pre-investment due diligence
- engage portfolio companies as an active owner
- reflect cyber security in voting
- promote research and understanding on the topic
- hold fund managers to account

This document also suggests questions that trustees can put to their asset managers and portfolio companies.

One-third of UK businesses identified cyber security breaches or attacks in the last year, according to the Cyber Security Breaches Survey 2019. Investors need to acknowledge that it is not a matter of 'if' but 'when' their investee companies will face a serious security breach. They should assure themselves that companies are working to reduce their cyber security threat and minimise the financial, operational and reputational damage from an attack.

The authors hope this summary of leading practice will be useful to pension funds in future engagements with portfolio companies and managers. Comments may be shared with the authors via so@rpmi.co.uk.

1. Why consider cyber and data security?

Incorporating environmental, social and governance (ESG) factors into investment decision-making has become widespread.

Recent changes to the Occupational Pension Schemes (Investment) Regulations 2005 have placed ESG topics even higher on the agenda for trustees. Trustees could be forgiven for being unsure which ESG themes deserve most attention, given a host of competing priorities. However, one which has been gaining increasing focus from investors in recent years is cyber security risk.

Figure 1: What is cyber security?

According to the UK National Cyber Security Centre, cyber security is how individuals and organisations reduce the risk of cyber attack.

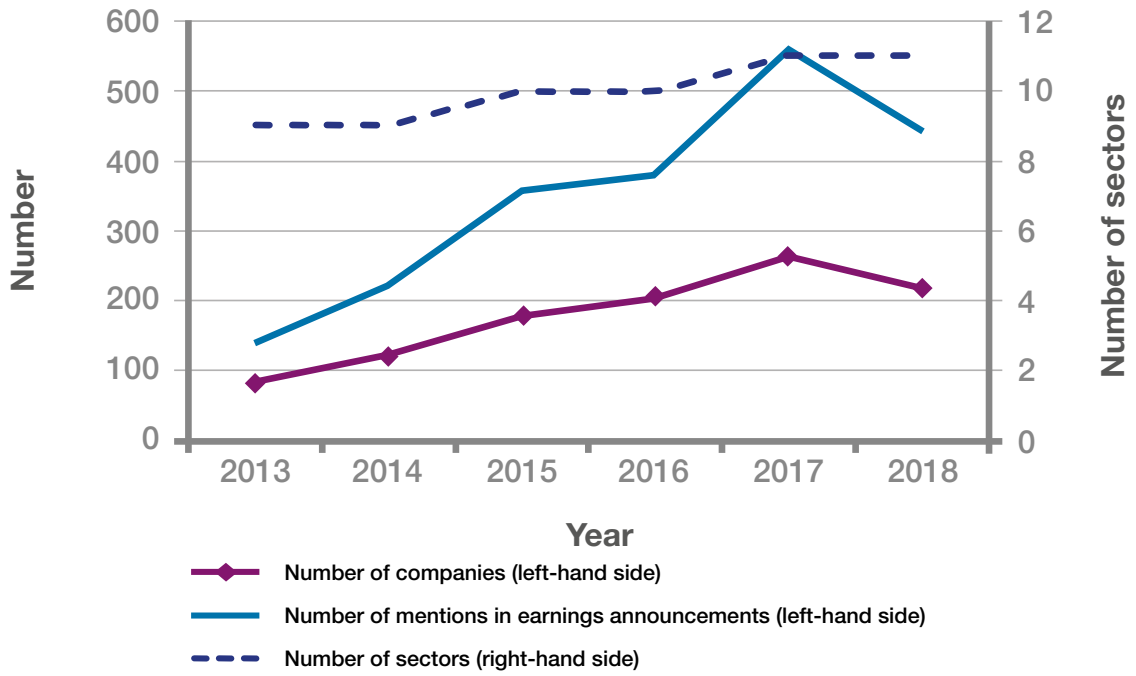
Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both online and at work – from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Cyber and data security risk is considered to be a business risk that is systemic in nature and has the ability to affect companies in many sectors and even national economies. Many UK pension funds are global investors with stakes in thousands of companies across many sectors which are likely to be highly exposed to the risk of cybercrime and the implications of data breaches. That said, the systemic and wide-scale nature of cyber and data security risk can be difficult to manage and monitor effectively. However, a head in the sand approach seems inappropriate and it is important that the pension fund community understands these risks and potential rewards.

Another reason to engage is the potential reputational risk for a pension scheme if a controversy emerges in a portfolio company. Members expect pension schemes to do the right thing, both in terms of how their pensions are administered and the expectations we set of our managers, service providers and portfolio companies. Engaging on this topic is another way to demonstrate that trust is deserved. Indeed, the World Economic Forum placed cyber attacks and data fraud or theft in the top ten global risks for 2019.

Data has been downloaded from Bloomberg to analyse how many mentions of 'cyber' during net profit announcements have been recorded. This can be seen as a proxy for awareness of boards that they should be disclosing information regarding cyber security. It could also be indicative of a greater number of cyber attacks where boards feel disclosure is required. Figure 2 shows the number of mentions of 'cyber', number of companies who mention 'cyber' and number of sectors whose constituent companies mention 'cyber' between 2013 and 7 October 2018. This shows a steady rise year-on-year, with a dip in 2018, which is yet to finish at the point of accessing data for this graph.

Figure 2:
Mentions of 'cyber' from 2013 to 7 October 2018



This can also be split by sector to show differences in how cyber issues are disclosed in net profit announcements. The IT, Financials and Industrials sectors have been disclosing the most surrounding cyber. Across almost all sectors, disclosure has been trending upwards.

The financial materiality of the topic can no longer be denied. Businesses can no longer presume that they will not be a target (see Figure 3 for a list of recent incidents in the public domain) and the enlightened are preparing accordingly.

Figure 3: **Recent cyber hacks**

Company	Number of Accounts Impacted	Financial Impact (USD)	Date	Data Hacked
British Airways	380,000	$229m fine with a possible £500m lawsuit on top	September 2018	Customer bank details
Facebook	87 million	$5bn fine and $119bn (20%) fall in market value	March 2018	Personal data from Facebook user accounts
Equifax	147.9 million	$114 million and a 3% drop in revenue attributed to the hack	July 2017	Social security numbers, dates of birth, addresses, drivers' licence numbers, credit card data
Uber	57 million users and 7 million drivers	Valuation went from $68 billion to $48 billion – analysts see the cyber scandal as being a large reason for this	Late 2016	Names, email, phone numbers, drivers' licences
Anthem	78.8 million	Expected to be over $100 million	February 2015	Names, addresses, Social Security numbers, dates of birth, employment histories of current and former customers
Home Depot	56 million	$19.5 million	September 2014	Credit/debit card data
JP Morgan Chase	76 million households and 7 million small businesses	The four hackers reportedly stole around $100 million	July 2014	Names, addresses, phone numbers, email addresses, internal information about the users
eBay	233 million	Not disclosed	May 2014	Names, addresses, dates of birth and encrypted passwords
Yahoo	500 million	Around $350 million (approx. 7.8% of sale price) fall in value (sold for $4.48 billion)	2013-2014	Names, email, dates of birth, phone numbers, passwords, security questions
Heartland Payment Systems	134 million	$145 million in compensation	March 2008	Credit card data

IBM Report - The Cyber Resilient Organisation

- 44% of respondents said their organisations' cyber resilience has improved or significantly improved in the past 12 months.
- 62% of respondents said the most important enabler was adding skilled personnel.
- 57% of respondents say their organisations' technologies enabled greater visibility into applications and data assets.
- 56% of respondents said their organisations' governance practices improved.

However, while security performance of many organisations is improving investors cannot rest on their laurels. As organisations work hard to protect themselves hackers, have been getting more sophisticated and faster than companies are responding. In 2015, organisations globally spent $84 billion on cyber security, an amount that analysts expect to grow to $125 billion by 2020. This sounds a lot of money, but not when compared to the cost of cyber attacks, which some researchers believe could reach $90 trillion by 2030.

In 2018, Nest undertook a research project to investigate cyber and data security and the potential impact the issue could have on its investments (see section 2.4 on page 11). Nest's next phase of research will be to investigate relationships between cyber risk and financial and corporate governance variables.

2. How to consider cyber and data security across investments

Once a trustee has accepted the materiality of the issue, the next step is to try and identify the risks and factor them into its investment decision-making and stewardship approach. We discuss some possible approaches below:

2.1 Consider the risks as part of pre-investment due diligence

For pension funds with an in-house investment function

Before making an investment, investors will assess a number of areas in detail, which include financial, legal and operational considerations. Exposure to cyber risk, and how well-managed it is, is another element investors should take into account when evaluating a company. However, a barrier to doing this effectively is the lack of company reporting for investors to understand cyber risk present within companies and what they are doing to mitigate it. As there are no universal reporting standards, there is a shortage of comparable information with other companies. Moreover, good cyber security is a moving target with a growing range of variables and generally companies are reluctant to disclose too much about their cyber risks and management approaches as they could make them a bigger target.

To help inform investment decision-making and security selection, investors need access to a minimum set of reporting indicators and products if they want to factor in cyber security.

Case study 1: **Tools for investors**

The Accenture Security Index helps investors assess what an effective cyber security strategy looks like and defines high performance objectively. The index, which assesses performance across 33 cyber security capabilities, at both the industry and country level, helps companies understand the effectiveness of their security measures. Organisations that have a clear picture of where they stand across these capabilities can then take proper measures to substantially reduce cyber security threats. The index results give an indication of where various companies, industries and countries are positioned.

A new index can help investors avoid making investments in companies that are prone to costly cyber breaches. The cyber governance indices rank 5,000 companies worldwide by the strength of their defences and corporate cyber governance. Cyberhedge, the company behind the indices, also plans to roll out three exchange traded funds that would allow asset managers to incorporate cyber risk management into their investment strategy.

Third party ESG data and research from providers such as MSCI and ISS-ESG will contain assessments of cyber security and data privacy practices and controversies. TruValue Labs (TVL) uses artificial intelligence to scrape sources to provide live ESG scoring and information on companies. The TVL analysis incorporates the Sustainability Accounting Standards Board's (SASB) 26 codified standards for financial materiality.

2.2 Engage portfolio companies as an active owner

Given the lack of good-quality and timely disclosure, engagement with company boards is vital if investors are to understand whether they are focussing on the right things to manage the risks. Many pension funds are signatories to the Principles for Responsible investment (PRI.) The PRI convened a collective engagement on cyber security in 2017 to build investors' knowledge of how their portfolio companies are positioned to manage cyber risk. The engagement saw 53 institutional investors engaging with global companies in the healthcare, financial, consumer goods, information technology and telecommunication sectors to improve their approach to cyber security governance and their cyber security processes. The outcome of the engagement was a set of investor expectations on cyber risk governance disclosures by companies.

The PRI report analysed data from 100 companies and demonstrated that, at present, there are no minimum standards of regular public disclosure on cyber security practices from large-cap listed companies that investors can use to inform basic engagement and investment analysis. It suggested certain questions that investors should include in company engagements, noting investors must question if company boards:

- have oversight of cyber security issues
- review and evaluate management approaches to cyber security
- ensure alignment of the cyber security programme with the business risk profile
- determine if management is effectively allocating resources and expertise to cyber issues
- monitor disclosure to regulatory authorities and stakeholders and ensure that this disclosure accurately portrays material cyber risks and incidents

Since the PRI engagement, disclosure continues to improve. In 2019, E&Y found that 89% of companies disclosed a focus on cyber security in the risk oversight section of their proxy statements, up from 80% last year. 28% of boards assigned cyber security oversight to non-audit committees, up from 21% in 2018.

The scope of a company's certifications is extremely important to understand when assessing a company's security posture. This scope can vary, examples to watch for include:

- not being certified
- being certified to very specific controls
- certifications not as expected to cover the full requirements of the standards

This should be assessed during the due diligence process for investment opportunities. The ISO standards provide assurance that controls and processes are being applied to manage threats during and in the recovery from a cyber attack; however in practice the required assurance may not be provided if the scope of the certification is limited.

Case study 2: **RPMI Railpen's dialogue with a US company through the PRI engagement**

RPMI Railpen served on the steering committee for the PRI engagement, and led the dialogue with a US company.

While the underlying practices seemed robust, Railpen identified the company could say more on how cyber risk is considered at Board level. The company agreed to consider adding additional disclosures in a future proxy statement.

Signatory of:

PRI Principles for Responsible Investment

> **"It is best practice for responsible investment specialists to work hand-in-hand with their Information Security team on this topic. This is a fast-moving area and expert advice is essential."**
>
> **Sylvia King,**
> Head of IT Security at RPMI

Cyber is a cross-cutting issue which is also relevant to board composition and remuneration.

Equifax Inc. experienced what it called a "cyber security incident" in 2017. Following investor pressure, in March 2018, Equifax Inc. adopted an enhanced clawback policy. Under the new policy, the compensation committee will have discretion to recoup incentive compensation from current and former employees in the event of a material restatement with misconduct.

RPMI Railpen has engaged companies on their cyber competence on the board.

In 2019, a report by E&Y found that 54% of Fortune 100 companies included cyber security as an area of expertise sought on the board or cited in a director biography, up from 40% last year. The same report found 33% of companies analysed identified at least one 'point person' from management (e.g. the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO)) who reports to the board, up from 26% last year.

Brunel Pension Partnership (Brunel) also engages companies on their approach to cyber security and support boards that take a proactive stance. Engagement is identified through external research and Brunel's own internal ESG risk analysis. It is also identified and undertaken by Brunel's asset managers, the specialist provider Hermes EOS, via collaborative forum, and directly by Brunel where it is expected that this will add value. Engagement is aligned to the priority themes identified in Brunel's Responsible Investment Policy.

The public Ranking Digital Rights index can also provide insight on how the privacy and security practices of the largest internet and mobile companies compare with those of their peers. The International Corporate Governance Network (ICGN) also suggested a number of questions in a 2016 viewpoint.

2.3 Reflect cyber security in voting

Investors routinely vote on how the board is structured, remunerated and equipped from a skills perspective to oversee the management of a business. In recent years, investors have pushed for less traditional risks that can impact the viability of business models to be placed firmly on boards' agendas. Climate change is one such risk and cyber security is fast becoming another. Addressing cyber security risks effectively requires first-rate governance and investors should ensure that boards are set up to understand the risks, challenge approaches and approve strategies.

Given the lack of good quality reporting and policy information on cyber, it is difficult for investors to vote on anything tangible when it comes to cyber security management, but that's not to say investors cannot use their voting rights to express a view on how the board is performing. Where engagement has been unsuccessful, a vote against the board could be used in the following circumstances:

- where investors are not convinced that the board is looking at metrics to assess cyber security risk that are right for the business
- where investors do not understand how those metrics have been alighted on
- where investors are unconvinced by the flow of information to the board on cyber
- where cyber attacks have been proven to have occurred and boards were found not to have acted on information and/or had no relevant expertise in place
- where companies have been unwilling to have any dialogue and there is no evidence that a company is taking cyber security seriously

It is important that any vote against the board's approach to cyber security is followed up with correspondence to the company that explains the rationale.

2.4 Promote research and understanding on the topic

It is important to understand how well companies are managing cyber security risk and what measures they're using to help them do that effectively. However, developing that understanding can be challenging, particularly where transparency and disclosure is lacking. Asset owners will therefore want to understand how they can identify the biggest cyber security risks across their portfolios and what measures they could use to better assess those risks.

In 2018, Nest undertook a research project to investigate cyber and data security and the potential impact the issue could have on its investments. The topic was selected as it is systemic in nature and can affect global companies across different sectors. Nest felt it was important to develop a deeper understanding of the issue and assess whether there were any concrete steps it could take to identify and manage this complex risk across a global index portfolio. It embarked on a research project which involved meeting with a range of cyber experts from various organisations and industries which included representatives from PWC, National Cyber Security Centre (NCSC), Templar Executives, PRI and Legal & General Investment Management (LGIM), amongst others. These meetings helped Nest to start to develop a more rounded view of the topic, understand the barriers to action and establish probable approaches leading to the development of a suitable strategy.

Case study 3: **Nest thematic research**

What Nest wanted to know:

- How can investors assess whether companies have taken adequate measures to protect themselves from cyber hacks and data breaches?
- What does good cyber security look like – what indicators to look for?
- Who at the company should be responsible?
- Is there any reporting to shareholders on this and what should shareholders expect?
- Is level of spend a good indication to how much a company is doing?
- As an index investor, how can Nest identify the biggest laggards?

What Nest found:

Companies cannot stop attacks from occurring, but preparedness and operational resilience is key. What's important is that a company has strong capabilities of business continuity, resilience and security strategies that are able to respond quickly to threats. Investors should question boards about preparedness in order to assess how well a company can minimise the damage and continue to operate under attack.

Nest found that measures of good cyber security include:

- a strong corporate culture where training, raising awareness and educating staff on the threat is crucial. The majority of security breaches can be traced to what people have done wrong so embedding cyber security in how people work day to day is important.
- that the board is regularly looking at the right metrics to assess risk, to ask intelligent questions and to take operational action from the data used.
- the development of metrics that are right for the business that can easily be explained.
- board level responsibility which requires a strong translator between the board and IT team. This is important so that board members can understand technical information in order to have high quality discussions and make important decisions.
- that the level of spend on cyber security is increasing year on year and spend is on the right things. The risk is fast moving and changing so what might comprise sound mitigation systems today may not tomorrow.
- adherence to regulatory standards like ISO 27001 and Cyber Essentials Plus. These are important but compliance doesn't always mean good security. It's more important to understand how companies are implementing these standards and what controls they're choosing to implement and why.

Continued on next page

Case study 3: **Nest thematic research (continued)**

While the Chair and CEO need to take ownership of this issue, it is important to understand the role of the Chief Information Security Officer (CISO) and their reporting line to the board. The NCSC has developed a range of questions that it believes will help generate constructive cyber security discussions between board members and their CISOs.

It is difficult to measure cyber risk and therefore hard to identify the laggards. An increase in disclosure may create a scenario where both weak and strong companies become targets. This acts as a disincentive to companies to improve their cyber security reporting by too much, which is not beneficial to investors. There is, however, a level of disclosure that we can expect from companies which would not be counterproductive. For example, assurance that they adhere to best practice standards, have a strong cyber security awareness culture that spans across the organisation to all employees and disclose their process for managing cyber threats.

As an index investor, Nest was keen to understand how to identify the biggest cyber security risks across it's investments, given the lack of reporting from companies. Nest found that certain types of companies are susceptible to attack and make them a bigger target. Investors can look to target and engage with companies that:

- hold the most data
- carry the most systemic risk in the market
- are conglomerates that are likely to have old legacy systems
- have recently undergone a merger or acquisition
- have global supply chains
- have just been hacked to assess the company's resilience, response and recovery and what might need to change or improve going forward.

Next phase of research:

Nest have started to give some support to a project commissioned by the National Cyber Security Centre, a branch of GCHQ, to develop a cyber security awareness index which will be freely available and published much like the FTSE indices.

The index stands to bring much needed transparency on the cyber security awareness of the UK companies we invest in. The principal aim of having a transparent index of companies is to encourage positive behavioural change within the boardrooms of companies that are the least cyber security risk aware. At the same time, understanding of companies' cyber security risk by pension funds will improve, and we can use that to help manage and reduce this common area of risk among all companies through investment stewardship and investment choices. By offering our support to the research team, we can help shape the cyber security awareness index in ways that are most relevant to us and other pension funds.

2.5 Hold fund managers to account

Part of understanding the fund manager's investment process is knowing how they incorporate material environmental, social and governance factors into investment decision-making.

Case study 4: **Brunel Pension Partnership (Brunel) raises cyber security pre-investment**

Cyber security is first raised with asset managers prior to appointment and is integrated within the tender questions. It forms part of the rigorous due diligence undertaken to assess how the manager is handling cyber security directly, both initially and on an ongoing basis.

Any concerns are discussed with the manager and conditions may be set around cyber security, where required, prior to entering any agreement. Where such conditions are set, managers are monitored more frequently in Brunel's ongoing monitoring plans. In addition, the Responsible Investment team reviews how ESG risks are implemented into the manager's investment process and engagement activities. As Brunel onboards new mandates, the Responsible Investment team will continue to engage with asset managers on how they are developing their integration and engagement on cyber security.

BRUNEL
Pension Partnership

Post-investment, most asset managers produce regular responsible investment reports which disclose the topics raised in company engagements. There was no coverage on cyber security by three of the largest index managers in their 2018 sustainability or stewardship reports. Asset owners need to encourage asset managers to prioritise this issue and adequately report on how they address it. The case study above shows how Brunel is approaching the issue.

RPMI RAILPEN

7th Floor, Exchange House ■ 12 Exchange Square London ■ EC2A 2NY
@ contactus@rpmi.co.uk
020 7330 6800