Institute and Faculty of Actuaries

Pension scheme cyber risk

1. Introduction

This paper seeks to address the following:

- the key cyber risks faced by pension schemes;
- who is responsible for managing these risks; whilst schemes typically outsource the day to day running to third parties, the trustees or the employer will ultimately be responsible;
- how these risks may be managed.

For this paper we are focusing on deliberate acts, rather than the accidental loss of data e.g. through loss of data files[1], though the implications of this may be similar to cyber data theft, nor does it cover other inadvertent breaches of data protection legislation.

2. What are the key risks faced by pension scheme?

To identify the key risks, it's important to understand what assets could be at risk from cyber criminals. As well as billions of pounds of assets, with millions moving around regularly from member to scheme bank accounts, employers and fund managers, pension schemes have an abundance of member data which are also attractive assets for a criminal. In addition, for pension scheme sponsors, there is the added risk of reputational damage from their pension scheme being impacted by a cyber-attack, which could also increase scheme deficits.

2.1 Ransomware attacks

These involve cyber criminals encrypting scheme data and demanding a ransom to unlock this. They could do this by tricking third party administrator (TPA) staff into downloading malware as part of an e-mail. However, the 2017 WannaCry ransomware attack infected computers automatically without user interaction, exploiting weaknesses in Microsoft Windows operating systems which were either unsupported or not updated for security patches. There is anecdotal evidence that at least one TPA has already been affected by a ransomware attack.

For many, it may be possible to recreate data from backs-ups but even this would involve some disruption to the operation of the scheme and additional costs due to the need to re-process transactions from the back-up date.

---

[1] One example of this is Zurich Insurance who lost a back-up tape containing 46,000 customer records and were fined £2,275,000 by the FSA as a result – see https://www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal

There could also be fines under data protection legislation if the attack succeeded due to failings on the part of the scheme or service providers e.g. failure to apply software patches or running unsupported software[2].

Unfortunately, ransomware attacks are increasingly infecting back-ups as well, so in some cases, the scheme and/or their service providers may have to pay a ransom to unlock data. In the worst case, there have been incidents outside the pensions sphere where the ransom was paid but the encryption key was unable to unlock encrypted data, which was lost entirely. This would have catastrophic impacts on scheme administration with scheme pensions unable to be paid, members unable to take their benefits or change their investment choices and/or create delays with the movements of money such as the investment of member and/or employer contributions.

2.2 Data theft

Pension schemes are exposed to the theft of scheme data. This could follow a similar initial route to ransomware with staff inadvertently downloading malware, perhaps through e-mail attachments. Data theft attacks vary in sophistication. At one end, there have been instances of teenagers stealing data from major firms using generic hacking tools downloaded from the dark web. At the other end of the scale, Advanced Persistent Threat (APT) attacks might involve professional hackers patiently probing systems over a year or more, exploiting any success to gain access to multiple systems, stealing data repeatedly and then covering tracks such that firms may be unaware data has been stolen.

There have been numerous examples of major data thefts over the years including Yahoo! and Equifax[3]. As well as the invasion of privacy, stolen bank and other details could be used to defraud members and other beneficiaries e.g. through fraudulent loan applications. Pension scheme data is quite valuable for fraudsters who may use stolen data to identify members to target for pension scams, or other forms of identity theft. There is anecdotal evidence of UK pension scheme data being sold on the dark web.

Data theft may give rise to remediation costs to address breaches; a need to put in place credit monitoring for affected members to prevent stolen data being used to defraud these; compensation for fraud and/or for distress caused; and regulatory fines for any deficiencies on controls which might have prevented theft. Note that data stolen could include records of past as well as current members – a breach of the US health insurer Anthem resulted in nearly 80 million records being stolen, half of which related to historic customers. In assessing potential exposure, schemes should consider legacy as well as current records, and hold records for no longer than is necessary.

Post-Brexit, data protection breaches come under the UK General Data Protection Regulation (UK-GDPR), which is broadly similar to the EU's GDPR[4], and which amongst other things give the Information Commissioners Office (ICO) the power to levy fines of up to 4% of turnover or €20m.

While it may seem perverse to levy a fine on a scheme, reducing assets available to support member benefits, it should be noted that although the ICO has not fined a scheme in recent times, it has fined a number of charities[5] so trustees should not assume they won't be fined.

---

[2] The May 2017 WannaCry ransomware attack exploited a vulnerability that should have been closed off if those affected with supported software had applied a Microsoft patch released in March – see https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[3] https://en.wikipedia.org/wiki/Data_breach

[4] For more details, see for example: https://www.crystalriskconsulting.co.uk/docs/GDPR-Briefing-Note-Q4-2017-v3a-CRC-Version.pdf

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/04/ico-fines-eleven-more-charities/
- details of recent ICO fines can be found at: https://ico.org.uk/action-weve-taken/enforcement/

2.3 Cyber theft and fraud

Cyber risk encompasses not just theft of data but also of assets. There are many ways they could do this. For instance, cyber criminals could hack pension scheme systems to re-direct beneficiary payments. Alternatively, they could create fraudulent transfers of funds. A spectacular example of this was the cyber-attack which compromised the Bangladesh Central Bank SWIFT payment system resulting in the fraudulent transfers of over US$100m[6]. For pension schemes, there's already anecdotal evidence that within days of the mandatory requirement for publicly publishing the scheme's Statement of Investment Principles, this information and trustee signatures are being used to facilitate fraudulent disinvestment attempts.

2.3.1 E-mail spoofing

This is a variation of cyber fraud involving cyber criminals impersonating e-mails to de-fraud schemes and their stakeholders. For instance, a cyber-criminal could send an e-mail to a sponsor, purportedly from the trustees, asking for a fraudulent invoice to be paid or to change a third-party provider's bank details. Alternatively, a fraudster could impersonate a member about to retire, asking by e-mail for the money to be paid to the fraudsters account.

2.4 Distributed denial of service (DDOS)

DDOS attacks involve criminals hijacking multiple computers to flood host servers with superfluous traffic in a bid to overload systems and deny internet service. Increasingly, the Internet of Things is being exploited with smart fridges and other applications used to facilitate DDOS attacks, increasing the volume of traffic that can be directed by criminals. Even if a pension scheme is not the intended target, if it shares a host with a target it could find it online service offering compromised. Whilst typically this may not have any significant financial impact for a pension scheme, it may create member dissatisfaction if self-service online offerings are down for a prolonged period. It may also create member uncertainty about the security of their benefits.

This list is not exhaustive. Among other threats is cyber-jacking, where computers are hacked to mine Bitcoin; cyber vandalism where websites are defaced; and cyber-attacks on infrastructure.

3. Who is responsible?

For a Trust based scheme the trustees are ultimately accountable for managing cyber risk. The 2004 Pensions Act requires trustees to establish and operate adequate internal controls. For contract-based schemes, this would rest with the provider, but with the onus on the employer to do their due diligence. The Pension Regulator (TPR) has issued guidelines which include the need for controls around computer systems and databases[7] as well as cyber security principles for pension schemes[8]. In addition to their responsibilities under the Pensions Act and TPR guidelines, trustees are the Data Controller under GDPR with primary responsibility for compliance with data protection legislation[9].

In practice, most schemes outsource administration to a TPA who would usually manage the cyber risk on their systems which hold member records and handle payments. However, from time to time data is shared with the trustees to assist with decision making on discretionary member cases. In

[6] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

[7] https://www.thepensionsregulator.gov.uk/en/document-library/codes-of-practice/code-9-internal-controls

[8] https://www.thepensionsregulator.gov.uk/en/document-library/regulatory-guidance/cyber-security-principles-the-pensions-regulator

[9] Though small occupational pensions schemes may be eligible for a discount on ICO fees for data controllers – see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/

some cases, the data shared could include health information and this would be classed as special personal data requiring particular care and attention under GDPR.

Member details would also be shared with actuarial firms for the purposes of valuations. While personal data won't be shared with investment managers, the scheme may be exposed to cyber theft in relation to transfers of funds for investment.

To the extent third parties are affected by cyber-attacks, they are likely to be held responsible in the first place[10]. However, this does not absolve the responsibility of trustees for ensuring the third parties they use have adequate cyber risk controls, nor eliminate the possibility that a scheme may be fined under GDPR for data breaches by third parties processing data on their behalf (who would be classed as Data Processors under GDPR). We would anticipate that a scheme where questions have been asked about the cyber credentials of TPAs would be treated more favourably than one which has assumed that TPAs operate in line with best practice.

Another dimension for firms to consider is the relationship between the scheme and the employer (/sponsor). Following on from the e-mail spoofing example above, the pension scheme could be an unwitting conduit on cyber-attacks on the employer. Also, cyber-attack costs borne by the scheme may increase IAS19 deficits on the employer's balance sheet.

However, the risk goes both ways – a scheme may be reliant on employer's payroll and other system, so attacks on these could affect the scheme as well as the firm. More generally, interfaces between employer and scheme systems could be a conduit for breaches of employer systems to in turn infect scheme administration systems.

4. What can be done to mitigate cyber risk?

4.1 Trustees

In considering a scheme's exposure, trustees should first consider their own personal cyber hygiene.

- How strong are their passwords?
- Do they have adequate virus protection and anti-malware protection in place?
- Do they fail to regularly apply security updates and patches that help protect against attacks? Or worse, use unsupported software like Windows 7 which is even more vulnerable to attack[11]?

In terms of specific vulnerabilities, trustees should consider how secure is the e-mail they use for scheme correspondence.

- Do they retain scheme correspondence which includes personal data which could be stolen?
- If e-signatures are used for investment and other instructions, how easy would it be for a cyber-criminal to use these to commit fraud?

---

[10] An example of this, albeit relating to data loss, was the £875,000 fine levied by the FSA on HSBC Actuaries for the loss of a disk containing unencrypted member data – see https://www.fca.org.uk/publication/final-notices/hsbc_actuaris0709.pdf; this was part of a wider fine of £3.2m levied on HSBC firms relating to the breach – see https://uk.reuters.com/article/uk-hsbc-idUKTRE56L26820090722

[11] For a list of products approaching the end of their support life, see https://docs.microsoft.com/en-us/lifecycle/end-of-support/end-of-support-2020. A fuller list of discontinued / unsupported Microsoft software can be found at: https://www.versionmuseum.com/history-of/discontinued-microsoft-products

Trustees should seek to undertake regular training to ensure that they stay up to date as threats and tactics evolve. This could be from advisers, the sponsor or using online tools such as UK National Cyber Security Centre (NCSC) guidance. Trustees could also take part in phishing exercises to assist them with staying alert to potentially harmful emails.

4.2 Assess other parties

For those schemes with in-house operations, TPR's cyber risk principles are a good starting point for considering the strength of cyber risk controls. At a minimum, the scheme should look to follow basic cyber hygiene frameworks such as the NCSC Cyber Essentials framework[12] or the US National Institute of Standards and Technology (NIST) Cybersecurity framework[13]. The scheme may also wish for all parties to comply with the ISO 27001 Information Security Management standard.

As for outsourced operations, trustees may delegate the day to day task of managing cyber risk to TPAs and others but not the ultimate responsibility. Trustees / employers should assure themselves of the strength of third-party cyber controls both at outset and on an ongoing basis. As part of initial due diligence of third parties, at a minimum trustee should look for evidence of compliance with NCSC or NIST frameworks, or ISO 27001 certification. The contract should address obligations to the scheme if the TPA is the cause of a cyber incident.

For Trust based schemes, cyber security reviews should also include the sponsor and the extent to which an attack on the sponsor's payroll and other systems could affect the scheme.

As part of subsequent monitoring, trustees or employers should seek evidence that cyber risk controls and standards are being adhered to, with notification of any changes which may affect cyber risk profile. An example of such a change may be increased home working as a result of the Covid-19 pandemic, which could expose the scheme to weaknesses in the computers of third-party staff, their VPN connections and/or their WiFi networks.

4.3 Reducing financial impact

Even with robust controls in place, successful cyber-attacks are still possible. Trustees may wish to consider if the third-party has sufficient financial resources to deal with the costs of such attacks. This might include the third-party's cyber insurance cover, but note that cyber insurance is unlikely to cover GDPR fines which would need to be borne from other resources.

Another limitation of cyber insurance is that it does not eliminate the need to maintain basic cyber hygiene, and failure to do so could result in claims being declined – in the same way as leaving keys in ignition would invalidate a motor theft claim.

Trustees should also have regard to exposure they have to the employer and should seek assurances as to the strength of employer cyber controls. Employers provide such indemnities by way of the scheme rules, but, for those employers with weaker covenants, trustee may need to consider alternative protections. For example, trustees should also enquire about the employer's insurance policies and whether any of these would cover the scheme as well as the employer from cyber-attacks.

In addition to third party and employer cyber insurance, in the event of a cyber loss, the trustees may also be able to claim on trustee liability insurance in respect of claims from members, and possibly the employer D&O policy in respect of any claims against them personally. However, in many instances cyber claims may be excluded from the policy and/or a claim by the scheme could be contested by the insurer.

[12] https://www.ncsc.gov.uk/cyberessentials/overview
[13] https://www.nist.gov/cyberframework

Therefore, the scheme may also wish to have its own bespoke cyber insurance policy, particularly if it has in house operations. These policies may cover response costs – with the notable exception of GDPR and other regulatory fines – and may also provide practical assistance in managing any breach that may occur.

4.4 Ability to deal with an incident

Whilst not a mitigation action as such, having a plan in place and access to specialist advice can be essential when a cyber-attack does happen. By thinking in advance about the actions and decisions which may need to be taken when an incident happens, trustees can calmly plan the steps they may need to take to resolve and recover.

5. Conclusion

Cyber risk poses a significant threat to pension schemes with the ability to cripple the administration of the scheme, breach the confidentiality of member records or defraud the scheme and the employer. Trustees are ultimately responsible for ensuring adequate cyber risks are in place, and should seek for both in-house and third-party operations to adhere to basic cyber hygiene principles at a minimum. Insurance can also help mitigate losses and provide valuable assistance, though attention needs to be paid to exclusions and other potential limitations of cover.

Acknowledgements

The authors would like to thank Visesh Gorani BSc FIA, Head of the IFoA Cyber Risk Working Party, and Allan Martin BSc FFA of ACMCA Limited for their valuable contributions to this paper.

Patrick Kelliher & Vanessa Jaeger

October 2020

Patrick Kelliher FIA CERA, CEO Crystal Risk Consulting Ltd., Chair of the Institute and Faculty of Actuaries (IFoA) Operational Risk Working Party

Vanessa Jaeger FIA, IFoA Cyber Risk Working Party