PASA
assess | aspire | achieve

PASA GUIDANCE

Produced in partnership with:

Crowe

PASA Experts for Cybercrime & Fraud

Cybercrime Guidance

November 2020

Cybercrime Guidance

Acknowledgments

PASA is grateful to the authors of the Guidance and the active Members of the PASA Cybercrime & Fraud Working Group and their employers.

Jim Gee (Chair)	**Crowe U.K. LLP – PASA Experts for Cybercrime & Fraud**
Gillian Baker	**Hymans Robertson LLP**
Andy Cassin	**Willis Towers Watson**
Justin McClelland	**Stephenson Harwood LLP**
Michael Walters	**Invensys Pension Scheme**

1. Introduction

This document provides background to, and guidance on, the topic of cybercrime as it applies to pensions administrators. It sets the scene for the strengthening of the PASA Standards in the near future. This document concerns how pensions administrators should:

1. Meet Legal and Regulatory Standards
2. Understand their organisation's vulnerability to Cybercrime
3. Ensure their organisation is resilient to Cybercrime
4. Remain able to fulfil key functions

Section 1 of the document outlines the current context. Section two focuses on the nature of cybercrime and administrators' vulnerability to it.

1.1. The relevance of Cybercrime as an issue

Cybercrime is a rapidly evolving, serious threat to any organisation. It's described in Section two of this document but the facts speak for themselves:

- In 2019 42% of all crime was cybercrime and fraud[1]
- In the same year 46% of all businesses suffered cyber breaches[2].

This situation has worsened since the Covid-19 crisis and both the UK Government and international agencies have recognised this. Europol commented:

> ***'Cybercriminals have been very quick in devising modi operandi and tools to exploit the current crisis. New and adapted attacks appeared almost immediately from the onset of the crisis and have been among the most visible types of criminality during the Covid-19 pandemic.'***

There are a number of reasons why administrators may be considered attractive targets to cybercriminals. Notably the 'rich' personal data they control and process, which would be valuable to cybercriminals. The crucial importance of continuing to pay pensions uninterrupted, makes administrators potentially vulnerable to ransomware attacks, and hence the large illicit gains to be made. For these reasons, it's vital administrators protect themselves effectively. This is why PASA has developed this Guidance, and will strengthen the PASA Standards.

Cybercrime is clearly a threat to administrators. The latest information revealed by the Information Commissioner's Office (ICO) in July 2020 shows since the introduction of the General Data Protection Regulation (GDPR) the pensions sector has reported 158 breaches – at least 43 of these were categorised as relating to Security, Unauthorised access or Phishing. **This shows cybercrime isn't just something happening to other sectors or other countries, but it's already happening in the UK's pensions sector.**

Given the evolving cybercrime threat and the regulatory response to that threat, administrators will need to monitor developments actively and adapt to the changing legal and regulatory environment.

1.2. Developments in recent years

Both research and practical experience shows cybercrime is so much more sophisticated than it was, say 15 years ago. Some of these changes are described in more detail in Section two.

[1] Crime Statistics for England and Wales
[2] Department for Digital, Culture Media and Sport – 'Cyber security breaches survey 2020'

Cybercrime has risen quickly up the list of risks for pensions organisations because of the level of sophistication being employed by criminals. It will continue to develop and evolve, probably even more quickly as time passes.

1.3. TPR guidance

In April 2018, TPR issued its first focused guidance concerning cybercrime, entitled 'Cyber security principles for pension schemes', intended for trustees and scheme managers. While TPR has no formal powers over administrators, it does have a statutory objective to promote good administration. There's an understanding administrators play a critical role in ensuring good outcomes for savers, and in securing confidence in pensions systems.

David Fairs, Director of Regulatory Policy, Analysis and Advice at TPR has made clear

"It's not a case of if you will be attacked, it's a case of when."[3]

Given the perceived inevitability of a cyber incident, TPR emphasised the importance of understanding schemes' vulnerabilities and the third parties on which they rely, as well as of developing processes to respond to incidents.

TPR has announced it will begin risk-assessing administrators in a number of areas, including cybercrime. We've reviewed and strengthened the PASA Standards to reflect the considerations to be taken into account to prevent Cybercrime. The updated documents will be released shortly and will in turn be incorporated into our Accreditation process, to support administrators in understanding what they need to do to protect themselves and their members from this threat. However, the Standards can be used by all administrators to assess their level of vulnerability and resilience in the face of rising cybercrime.

[3] 13 June 2019 – Hymans Robertson event

2. What is cybercrime?

2.1. Rapidly evolving, continuously changing - unlike some other risks

Cybercrime (like fraud) is a rapidly evolving and continuously changing phenomena. It's unlike some other risks which are relatively static and have long established controls in place to mitigate them.

Cybercrime has increased in sophistication and is mostly undertaken by rapidly growing, highly profitable criminal 'businesses':

- They undertake 'market research' to see what type of 'client' might be most likely to buy their stolen data
- They make 'business' decisions about what organisations to target – What would be the time needed, cost and risk? What would they gain, in terms of stolen personal data, diverted financial flows or ransomware payments?
- Once a decision is made to target a particular organisation they undertake 'research' to find the interests and weaknesses of key individuals, often trawling social media for information
- They often hack organisations without pre-existing clients to 'stock' their criminal enterprise with a variety of data which a subsequent 'customer' might want
- False identities are sometimes key and so different teams will focus on gathering together financial, address, property ownership, employment and identity documentation
- Alongside those undertaking cybercrime directly, other parts of the 'business' will earn money from the manufacture of documentation to facilitate other types of crime and fraud
- Most recently, there is evidence of cybercriminals starting to use Artificial Intelligence to analyse the most promising weaknesses to exploit
- 'Cybercrime as a Service' (CAAS) has developed, where, for a set series of tariffs, cybercriminals will attack an organisation for a 'client'

2.2. Distinction between fraud and cybercrime

It's important to be clear about defining a problem if it's to be tackled effectively. Cybercrime is not fraud which is a different issue with different solutions.

When a computer is used to undertake fraud (as is often the case now) this is cyber-enabled fraud not cybercrime.

Cybercrime involves illicit intrusions into computers and networks (hacking) and/or the disruption of computer functionality, such as malware, ransomware and Distributed Denial of Service ('DDoS') attacks. Data stolen by means of cybercrime can then be used for fraudulent purposes.

2.3. Cybercrime techniques

Two main cybercrime techniques are 'phishing' and the insertion of ransomware into a computer.

Phishing has been around for many years. It's been defined as 'the dishonest attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication'[4]. It's the most successful and dangerous of all cyber-attacks. Research has found 91% of all cyber-attacks start with a phishing email[5] and people are four times more likely to fall victim whilst using a mobile phone.

It's become much more sophisticated in recent years, so it now includes:

- **Spear phishing**: the sending of targeted emails, directed at a specific individual, rather than being sent randomly to multiple recipients (often preceded by research on the recipient)
- **Clone phishing**: the altering of previously sent (legitimate) emails to include new (illegitimate) links with the intention of familiarity triggering opening of the email
- **Whaling**: a form of spear phishing targeted at celebrities and senior executives
- **Link manipulation**: the use of similar looking URL links (for example: www.abcbank.com/customer services (genuine) might be changed to www.abcbank.customerservices.com)
- **Filter evasion**: the sending of a photo or video which when clicked requires the victim to provide their email and password
- **Website forgery**: the development of similar but fake websites, which can infect the victim's computer
- **Covert re-direct**: Typically by the use of illegitimate pop ups on legitimate websites which can infect the victim's computer
- **Vishing**: voice phishing. This can now be quite sophisticated, for example commonly available apps can be used to alter the number appearing to be that of the caller, alter the caller's voice and add background office or other noise so the caller appears genuine and recognised.

Ransomware can encrypt the victim's files, making them inaccessible, and result in a demand for a ransom payment to decrypt them. By the end of 2021 ransomware attacks on businesses are expected to happen every 11 seconds[6].

The May 2017 'Wannacry' global cybercrime attack (named after the particular malware virus) is estimated to have encrypted up to 70,000 computers in the NHS[7], other networks in 150 countries and cost in the region of $4 billion.

[4] A common definition used by various government, bank and commercial sources identified by internet searches
[5] Cofense solutions
[6] Cybercrime magazine
[7] National Health Executive

However, ransomware can also be non-encrypting. It can involve the loading of pornographic images on to computer screens or requiring the re-installing of Windows software – both to be avoided in return for the payment of a ransom. There is also Leakware which threatens to publish stolen information from the victim's computer system.

Mobile ransomware is used to display a blocking message over the top of all other applications for Android phones and to use the Find My iPhone system to lock access to an iPhone.

Ransomware is particularly dangerous when deployed against organisations with a vital function, because the inability to perform that function can sometimes lead those running it to be tempted to pay the ransom. The National Cyber Security Centre supports the National Crime Agency (NCA) advice not to pay a ransom, as there's no guarantee you'll get access to your device (or data). Also, being known to have paid a ransom makes the victim more attractive to other cybercriminals.

2.4. Examples of cybercrime (generally and in the pensions sector)

The U.S. Pentagon, the White House and the Central Intelligence Agency have all successfully been hacked, as have TalkTalk, Ladbrokes and Travelex in the UK. The Japan Pensions Service, the U.S. Federal Retirement Thrift Investment Board and the Pittsburg Police Pension Fund have also fallen victim. As mentioned above there's been more than 150 data breaches in the UK pensions sector which have been reported to the ICO since the introduction of the Data Protection Act 2018.

2.5. The role of the Dark Web

The Dark Web is the World Wide Web content (a series of 'darknets') requiring specific software, configurations or authorisation to access it. It forms a small part of the Deep Web, the part of the Web not indexed by web search engines.

It's a marketplace for illegal goods such as drugs and weapons. However, it's also used by cybercriminals to target organisations. Cybercrime tools, consultancy and compromised email accounts (with their passwords) are all for sale.

The Dark Web is where most cybercrime is organised and monetised. Research in 2018 revealed extensive discussions about attacking (and monetising attacks) on leading UK brands[8].

2.6. What research tells us

Recent research[8] has looked at what makes organisations vulnerable to cybercrime and identified three main factors with a number of questions associated with each:

[8] 'The Dark Web – Bad for Business' – Crowe UK LLP and the Centre for Counter Fraud Studies at University of Portsmouth

Factor 1

- How attractive is an organisation to cybercriminals?

  (a) Does the organisation concerned control a lot of detailed personal and financial data which can be used to defraud victims?
  (b) Does it control a lot of sensitive data which can be used to threaten and extract ransom payments?
  (c) Does it have high value intellectual property which can be stolen and sold?
  (d) Is it a potential gateway to mount attacks on other victim organisations (e.g. an outsourced technology provider)?
  (e) Is it known to have weak defences?
  (f) Is it known to have strong defences and therefore representing a challenge?

Factor 1 (a) is especially relevant to administrators.

Factor 2

- What would be the extent of the damage caused by a cybercrime attack?

  (a) Does the organisation concerned have a strong, trusted public profile (and therefore is particularly vulnerable to reputational damage)?
  (b) Are its income sources vulnerable?
  (c) If its information and data was stolen, could it be used to attack other organisations (for example clients) or individuals?
  (d) Is there a public expectation the organisation would be secure (with the resultant reputational damage if it's proven not to be)?
  (e) Is financial damage likely?

Factors 2 (a), (c) and (d) are especially relevant to administrators.

Factor 3

- How cybercrime resilient is an organisation (and its suppliers)?

  (a) Does it regularly map and document its data to understand where it's held, on what systems and how the data is combined?
  (b) Is the organisation data protection compliant?
  (c) Does it regularly complete penetration testing of its systems?
  (d) Where and how is the data backed up and how quickly can it be restored?
  (e) Are arrangements in place to crisis-manage a cybercrime attack if one takes place?
  (f) Are arrangements in place to investigate a potential cybercrime breach?
  (g) Are arrangements in place to manage the consequent public relations issues?
  (h) Are arrangements in place to make sure any breach is promptly and properly reported to the Information Commissioner's Office (ICO) – whether it's the administrator or the pension scheme's responsibility to do this?
  (i) Are there clear processes in place to notify all Data Controllers and other stakeholders?
  (j) Is there an IT and Cyber Security policy in place covering all systems and networks?

All of the elements of Factor 3 are relevant to administrators.

Some lessons learnt from this research include the importance of understanding vulnerabilities, of complying with legal and regulatory standards, and of becoming cyber resilient (managing an attack if it does take place, minimising any damage, and maintaining key functions).

APPENDIX 1 – THE LEGAL AND REGULATORY ENVIRONMENT

The complexity of the legal and regulatory environment can't be summarised in short form in this Guidance. However, the principles deriving from it require administrators to:

- Put good governance in place;
- Identify what needs to be protected;
- Protect assets/data appropriately;
- Use appropriate detection systems;
- Be aware of emerging threats and issues;
- Be ready to respond to attacks and to recover from them;
- Test and refine systems to ensure that resilience is maintained.

The following sources (not comprehensive and ever-evolving) provide a useful source of guidance from the relevant regulatory and other bodies as at the date of publication:

TPR:

- https://www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/cyber-security-principles-for-trustees.ashx

ICO:

- https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

NCSC:

- https://www.ncsc.gov.uk/cyberessentials/overview
- https://www.ncsc.gov.uk/section/advice-guidance/all-topics

ICO and NCSC:

- https://ico.org.uk/for-organisations/security-outcomes/

FCA:

- https://www.handbook.fca.org.uk/handbook/FCG/5/?view=chapter
- https://www.fca.org.uk/publications/research/cyber-security-industry-insights
- https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf
- https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

There are two ISO Standards which are relevant:

- ISO27001 – https://www.iso.org/isoiec-27001-information-security.html
- ISO27032 – https://www.iso.org/standard/44375.html

Whereas any guidance from TPR isn't binding on administrators, TPR's risk assessment of the top 75 administrators will be the most extensive such exercise ever undertaken in the industry and there are likely to be important lessons to be learned.

PASA

assess | aspire | achieve

THE PENSIONS ADMINISTRATION STANDARDS ASSOCIATION

Get in touch:
info@pasa-uk.com
www.pasa-uk.com