PASA

assess | aspire | achieve

PASA GUIDANCE

Cyber Security

June 2019

PASA – Cyber Security

Acknowledgments

PASA is grateful to the authors and reviewers of the Guidance and their employers.

Donna McGuire (Author)	SAUL – PASA Standards Committee
Paul Blackmur (Reviewer)	Pi Partnership Group – PASA Standards Committee

PASA is also grateful to the organisations shown below, who generously gave time to review and provide technical input to the Guidance.

- PASA eAdmin Working Group
- Equiniti
- Baker & McKenzie LLP

1. Introduction

Cyber security is becoming an increasingly regular topic for pension schemes. The introduction of the General Data Protection Regulation (GDPR) reaffirms the need for pension schemes and trustees to have an active cyber security review. This is supported by the Pensions Regulator's (TPR) statement that pension scheme trustees need to take active steps to protect members and assets against cyber risk. These reviews should be completed on a proportionate basis and a number of key areas require careful consideration.

The National Cyber Security Centre also provides information such as the '10 steps to cyber security' to help organisations protect themselves.

2. Risk Assessment

A typical risk assessment process is based on the following stages:

1. Understanding what you need to protect (assets). e.g. Pension scheme members personal data (data)
2. Identifying the threats to those assets. e.g. Unauthorised access to data by outsiders through hacking
3. Defining the level of risk by considering the likelihood of the threat, against the potential impact. e.g. Likelihood of threat assessed as 3/5 and the impact of the threat assessed as 5/5.
4. Establishing the controls already in place to mitigate threats and assessing how effective those controls are. e.g. IT secure design and build, firewalls in place, anti-virus software deployed, regular patching, etc.
5. Assessing the net likelihood and impact defined in point 3 above.
6. Determining whether the resultant risk is acceptable. If not, the risk should be treated by implementing an additional control

To carry out a successful risk assessment, you must first agree what you are trying to protect (e.g. pension scheme member data), establish the potential risks and how to identify them.

The scheme's existing controls and processes should first be assessed. It's important to understand your scheme's data flows to highlight vulnerabilities. Mapping these scheme data flows is also required under the GDPR, so you may already have it recorded. The scheme's stakeholders and suppliers should also be considered, as they can introduce cyber security risks. You should particularly focus on your scheme's third-party suppliers (such as the pension scheme administrators), They should all confirm the controls they use to minimise the risk of a cyber security to your scheme's data.

Assessment of the approach and controls in place can be approached in different ways. Importantly, the review should be on a pragmatic and proportionate basis to suit the size of your scheme and the amount of personal data held. If you do not have access to an internal specialist, you may need to engage an external independent specialist to carry out the review.

3. Types of cyber risk

Threat	Main Techniques	Comments
External targeted attacks	• Malware • Denial of Service • Credential stuffing • Brute-force attacks • Social engineering e.g. Phishing • Exploit web application vulnerabilities	Increased reported attacks against UK financial targets.
Internal accidental	• Loss of data including removable storage media • Weak passwords • Enable malicious content in email (link/attachment) • Improper use of administrative access or credentials	Contributed to most security breaches.
Internal deliberate	• Exfiltration of data e.g. prints, cameras, mobile storage media/devices	Difficult to protect against and can require significant investment.
Supplier chain	• Breaches using the above techniques	Can be partly mitigated through contractual terms and robust due diligence/on-going assessment.

4. Governance

The risks faced by pension schemes are increasing both in volume and sophistication. TPR has published a set of governance principles trustees and managers of pension schemes should apply. The principles include:

- Having clear responsibilities and accountabilities
- Undertaking regular training to understand cyber risks and how they are evolving
- Updating and regularly reviewing cyber risks within the Risk Register
- Imbedding controls both for trustees and third parties to protect the scheme
- Having awareness of the auditor's role and of any insurance in place for the scheme
- Considering an independent assessment such as Cyber Essentials/Cyber Essentials Plus or ISO 27001
- Protecting personal data and other stored data and assets with suitable controls
- Having a response plan to minimise the impact of a cyber incident. Remember: organisations have 72 hours to report Personal Data Breaches under the GDPR

5. Risk Management

Ownership of cyber risk should be at board level and feature on the scheme Risk Register. It won't be possible to mitigate all risks by completing thorough and regular reviews. However, they can be mitigated, reduced or at least measured. For large schemes it may be appropriate to create a Chief Information Security Officer (CISO) role and create a sub-committee to encourage regular detailed assessment.

6. Key Risks

The use of laptops, external drives and other forms of removable storage media and devices has increased over recent years, leading to an increased risk of data loss. The use of more traditional hard copy reports or data should still be considered a risk. All data leaving the secure office environment

should be carefully considered and necessary safeguards put in place to mitigate the associated risks to the scheme.

The most common causes of security breaches relate to human error. These can be complex and wide ranging in nature. It's essential all stakeholders with access to data have had appropriate training and understand they're responsible for keeping the scheme's data safe. All organisations should review their controls regularly, to reduce and manage human error. A strong focus should be placed on what to do when something goes wrong, rather than if it'll go wrong.

One of the most effective ways to protect your scheme is to ensure virus and malware protections are in place and regularly updated. When software patches are issue they need to be applied as soon as they become available. Many schemes will engage an external specialist to review and regularly test the processes in place.

Social engineering techniques, such as Phishing, are used to target organisations causing them to inadvertently transfer funds or sensitive information to a criminal third party. This is typically achieved by issuing a spoof email, mimicking a legitimate individual or company request. The spoof email could potentially direct the recipient to a fake website or platform to obtain log in, passwords or access codes. The information collected could then enable the unauthorised party to enact a transfer of funds, or to access internal systems.

Many pension schemes' stakeholders hold information needing protection. This includes trustees, administrators and actuaries, as well as several other third parties. You should seek assurance from all your third-party suppliers they have the necessary protections in place on your scheme's data. This could include formal certification to Cyber Essentials (Plus) or ISO27001, where an independent third-party assessor reviews the adequacy of the control environment against the respective framework.

You should also seek assurance Anti-Fraud measures are in place and followed. This could include access and user privileges, up to date mandates, approval procedures and management of key man risks.

7. Controls

There are several additional key organisational controls which can mitigate cyber security risks. You should consider how these apply to your scheme and any applicable stakeholders, such as administrators or advisors. These include:

Monitoring and logging

Monitoring and logging digital processing activity are key controls for all organisations. A log file or event log creates an automatic audit trail of any device's operations. This will include details of user access, file creation/modification time, etc. Examples include authentication logs, audit logs, system logs and administration logs. In case of a security incident, the log files can serve as the primary source of investigation, and may assist organisations to understand the root cause of a cyber security incident (which may also need to be reported in the event of a Personal Data Breach).

Penetration testing

Having a regular and effective penetration test is best practice and will identify weaknesses or improvements for consideration. The exercise should be completed by an independent, external specialist, ideally with experience in the pensions industry. The scope should include internet facing applications and infrastructure.

Business Continuity Plan / Disaster Recovery (BCP/DR)

Having a robust and updated BCP/DR plan is a key consideration for any business and plays an active role in protecting your scheme from certain cyber security and other risks. The BCP/DR should be reviewed and updated on a regular basis. It should also be regularly tested. Tests may range from a desktop walkthrough, scenario tests through to full-blown alternative site service recovery. All failures or advisories should be assessed and fed through into process improvement under lessons learned.

Data Protection

Increased data protection regulation requires organisations to review and update their data protection policies. Data protection and cyber security measures run hand in hand, so they should complement each other. Under data protection legislation, all data processors should have a valid legally binding contract with any data processor who processes personal data on the controller's behalf. The contract must demonstrate certain data protection requirements have been met.

Where you share data with another (independent) data controller, such as an employer, it's best practice to have a formal data sharing agreement. When sharing data, the mechanism used should be robust. This could be encryption, a secure data sharing site or pseudonymisation (enhancing privacy by replacing most identifying fields within a data record by one or more artificial identifiers).

Infrastructure

Whilst infrastructure can be tested by penetration and BCP/DR exercises, you should review the structure to make sure it's fit for purpose and appropriate in light of the cyber risks identified. This also applies to external stakeholders. Organisations might consider the benefits of internal or external hosting, as well as the use of resilient links. Infrastructure specialists could be consulted to provide an independent review of the current infrastructure arrangements.

Accessibility

Protecting a pension scheme from *external* cyber threats is just one area where protection will be needed. Internal user management is needed to keep the scheme safe too. Keeping access details (log in and physical building access) up to date, will minimize the chance internal fraud. Your cyber risk review should also confirm whether the access levels granted are suitable for the individual employees and not excessive. A regular review of access levels by senior line managers is best practice. You should also consider bank mandates and other online authorisations, which will change over time. For

some roles, you should consider running individual background checks, particularly around financial fraud or dishonesty. As a general rule, organisations should provide only the minimum level of system privileges needed for any user to do their job.

Third parties or external specialists should also be regularly considered when reviewing user access and security.

A further area where risk can be introduced is flexible or remote working, for example where individual trustees work from varying locations. This will also be relevant in relation to the third party suppliers. Where it is relevant, the organisation should have a remote working policy in place, which clearly sets out the requirements for employees to protect the scheme's assets and personal data. This should be supported by appropriate technology.

Robust password policies should be in place. You should consider whether two-factor or multi-factor authentication should be implemented for remote working, or for access to programs or assets which container large volume and/or sensitive data.

8. Incident management

You should have a data breach incident response plan to support you in the event of a cyber-attack, or other data breach incident (e.g. a Personal Data Breach under data protection law). Being prepared is a necessity, as experts believe if you haven't already suffered a cyber-attack in some form you should expect it.

Having a plan in place for employees, trustees and third-party suppliers so they are clear on where responsibilities lie and the mechanisms/processes they'll need to trigger is essential.

You could consider additional insurance, which can help an organisation recover from and protect it against an attack.

9. Useful links

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

http://www.thepensionsregulator.gov.uk/guidance/cyber-security-principles-for-pension-schemes.aspx

https://www.cyberessentials.ncsc.gov.uk/

PASA

assess | aspire | achieve

THE PENSIONS ADMINISTRATION STANDARDS ASSOCIATION

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