Cyber security principles for pension schemes

Pension schemes hold large amounts of personal data and assets, which can make them targets for criminals. As trustees and scheme managers, you need to take steps to protect your members and assets accordingly, which includes protecting them against 'cyber risk'.

This guidance sets out the practical steps you can take to meet the expectations set out in our **draft general code of practice**.

Published: April 2018

Last updated: December 2023

See all updates to this guidance

On this page

What is cyber risk?

Cyber risk can be broadly defined as the risk of loss, disruption, or damage to a scheme, or its members associated with using information technology. Risks can arise not only from the technology itself but also from the people using it and the processes supporting it. It includes risks to information (data security) as well as assets, and both internal risks (for example, from staff) and external risks (such as hacking).

Your role

As trustees and scheme managers, you are accountable for the security of scheme information and assets, even though, in practice, others will handle data and manage technology on your behalf.

Under pensions legislation you must ensure that your scheme is administered and managed within the requirements of the law, including data protection legislation.

You must make sure that you:

understand your scheme's cyber risk

ensure that those handling data or managing technology on your behalf have controls in place to

reduce the risk of incidents occurring and their impact

manage incidents that arise

Cyber risk is complex, rapidly evolving and requires a dynamic response. Your assessment of risk, controls and response plans should be reviewed regularly. Normally, this means at least annually and more frequently if there are substantial changes to your scheme's operations (for example, a new IT system or a change of administrator).

You should keep records on how you have assessed cyber risks and the steps taken to ensure the right controls are in place. This will help you demonstrate that you have fulfilled your governance obligations.

You should make sure you have access to the required skills and expertise to assess and manage your scheme's cyber risk. Some schemes may be able to call on such expertise from their employer, while others may need to seek specialist advice. Sharing insights and experiences with trusted stakeholders and peers can also be a valuable source of intelligence.

Working with others

You need to work with all relevant parties within and outside the scheme (including employers and third-party service providers within your supplier chain) to ensure that the risk is appropriately managed.

You should not assume your suppliers and those handling or managing systems on your behalf have taken the required steps. You remain accountable and should seek assurance or evidence that **the right controls are in place**. This may include specialised accreditation, including Cyber Essentials, Cyber Essentials Plus, or ISO 27001.

Check what is and isn't covered by any audits, tests, accreditation or insurance that you may have. You may also consider having the effectiveness of your cyber risk management independently assessed by a cyber specialist.

Cyber security should be an active consideration when selecting a supplier and suitable provisions should be included in contracts. You should agree what metrics to use to monitor your supplier, at a depth and frequency proportionate to their risk.

Agree and receive regular, plain English reports from relevant parties on increasing threats, the volume, nature and impact of any system compromise, and data breach, as well as relevant updates on how any emerging cyber risks are being controlled.

Open, transparent and collaborative working in the pensions industry is particularly important for tackling fast-evolving cyber risk. Seeking appropriate information and advice on emerging cyber security threats will enhance the scheme's ability to respond to and recover from cyber incidents.

Changing third-party suppliers

It's common for schemes to change third-party suppliers, such as administrators or IT providers. You need to know who is legally responsible for the data when they are no longer your supplier. You should understand how long they will hold your data, where it will be held, and how it will be protected. This will assist you in determining whether your scheme is likely to be affected if a cyber incident occurs at your previous supplier.

Assessing and understanding the risk

As trustee or scheme manager, you need to assess the cyber risk and include this in your risk register.

Understand:

your cyber footprint: the digital presence of all parties involved in your scheme. This includes not only your administrator but also:
- the sponsoring or participating employers
- other advisers (auditor, actuaries, investment manager or consultant, lawyers) or service providers (eg annual benefits statement printers)
- members (especially if offering online access)
- trustees or scheme managers

your critical scheme functions (for example, benefit payments) and the systems and assets needed to deliver these

who holds what data, and how and where it flows. Consider not just your member data but also other data used by or for your scheme, for example, investment instructions to advisors

the value to criminals from data theft or corruption, or the interruption of critical services to members

the type and potential severity of incidents your scheme is vulnerable to, whether accidental or intentional and caused by internal or external actions

the potential impact of a cyber incident on your members, the scheme, and where appropriate, the sponsoring employer. The impact assessment should cover multiple elements, such as operational, reputational, and financial impacts

What about you?

Trustees and scheme managers themselves receive and send large amounts of potentially sensitive scheme information. You should ensure you have the right controls around your own work, eg clear policies on what can and can't be sent to personal email addresses or accessed on tablets and mobile phones.

Ensuring controls are in place

You should seek assurance that those handling data or managing systems on your behalf have controls in place to:

- reduce the likelihood of a cyber incident occurring and the impact of an incident
- detect cyber incidents when they occur
- respond effectively

Controls should cover people, processes and technology and be proportionate to your cyber risk. Larger schemes, and those more exposed to cyber risk, will need more robust controls.

We encourage the largest and highest risk schemes, their advisors and suppliers to fully meet the expectations set out in the National Cyber Security Centre (NCSC) **10 steps to cyber security**. The smallest and lowest risk schemes and suppliers should at least consider having the controls as set out in **NCSC's small business guide: cyber security**.

The rest of this section sets out the key controls we would expect to see in place across the pension scheme's cyber footprint.

Prevention

Ensure that adequate controls are in place for the following:

Staff engagement and training

- All staff and trustees should receive training relevant to their role as often as required, include:
  - cyber risks awareness and how to report incidents, in particular phishing, which remains one of the most prevalent forms of cyber-attack
  - policies for device (including removable and personal) use, covering home and mobile working
  - policies for using email and internet (including social media)
- Clear governance structures with well-defined lines of responsibility and accountability for information technology systems and processes.

Data security

- Policies and processes around data access and protection:
  - include encryption, use and transmission, in line with data protection legislation and guidance
- Clear records of your scheme data and assets:
  - include where they are held, transmitted and stored. This is to swiftly determine which data has been compromised and who might be affected in the event of an incident
- Back up critical systems and data regularly:
  - include, if appropriate, one or more offline backups, to stop these from being affected by a cyber incident
  - test processes that restore backed-up data to ensure they work as expected

Technical controls

- Multiple layers of technical controls around systems in line with **cyber essentials**.
- Relevant policies and processes in place to control the user access:
  - physical and virtual access to systems
  - staff should be suitably vetted with the right level of access
  - review access regularly and remove it for leavers or where no longer relevant to a role
  - passwords and other layers of authentication, for example, multi-factor authentication (MFA)

Correctly configure devices, including mobile phones, with firewalls (or firewall functionality) and malware protection.

Systems and network vulnerabilities should be tested and managed. In some cases, it may be appropriate to seek independent security testing, including penetration testing. The NCSC provides a free online **cyber security tool** which can be used to check common vulnerabilities in public-facing IT.

All software should be kept up to date. Monitor publicly available information for vulnerabilities that have been exploited during previous cyber attacks and update your system accordingly.

Importance of patching and updating

Viruses and malware are constantly evolving to exploit vulnerabilities. Hardware and software developers try to fix these flaws as soon as they are discovered.

Many infections occur because people delay software updates, which would fix them. Installing software updates promptly is a simple yet effective way of reducing cyber risk.

Detection

Detecting cyber incidents early is critical to minimising the risk to members' data and scheme assets.

Systems and networks should be monitored so incidents can be identified and responded to. An automatic audit trail of digital processing activity is also useful when investigating cyber incidents.

There should be clear processes for staff to report cyber risks and incidents, and be able to do so confidently. Log reports to identify any significant or recurring issues.

Incident response planning

All organisations will experience security incidents at some point, even those with the most rigorous controls, so it is critical to plan for an incident.

Design and maintain a plan which sets out how to respond to a cyber incident. The NCSC provides advice on **planning a cyber incident response** and **developing a response process**.

Document:

- the roles and responsibilities of the incident response team and main decision-makers
- procedures for escalating and responding to incidents
- system shut down procedures to prevent malware and viruses from spreading
- procedures for identifying which systems, data and assets may be compromised, and affected operations and services
- the priority order for recovering data and services
- procedures and timescales for recovering backup data and scheme services. Systems and data should only be brought back online when they are secure
- processes for how and when the trustees will be informed about a cyber incident
- internal and external communication plans, including to scheme members
- processes for how and when to report to regulators

Test and update your response plan regularly. The NCSC provides a **free test tool**.

Ensure that you have sufficient capability to investigate a cyber incident. This may include using a NCSC-approved incident response provider.

Document incidents and follow up major ones with a post-incident review, updating response plans in light of lessons learned as appropriate.

Post incident monitoring may be necessary in some cases, for example, tracking increased or unusual transfer requests following a data breach.

Responding to incidents

You need to have your own robust incident response plan in place and test this through internal exercises, looking at a range of scenarios appropriate to your scheme. This may be a stand-alone plan or part of your business continuity plan.

You should consider the plans of those handling data or managing technology on your behalf, to ensure these appropriately cover the scheme. For example:

- employers' plans covering in-house administration must specifically cover scheme data, systems

and functions

third-party suppliers' plans must specifically cover the pension schemes services provided to you

Understand how your scheme's core services are covered, such as pensioner payments, retirement processing and bereavement services, and the timeframe for bringing these back online. This should be done as soon as it is safe to do so, and ideally within 24 hours.

Communicating to members

While this can be outsourced, you remain responsible for communicating to members and should be clear when this would happen. A data breach is likely to cause them concern, so be prepared for any queries.

For some cyber incidents or schemes with a complex cyber footprint, it can take a considerable period of time to identify whether or what data has been exfiltrated. You do not need to wait until this is confirmed to contact your members. Keep them updated while investigations progress.

To protect your members from the effects of a data breach, direct them to more information on: **identity theft** and **pension scams**, and the **ICO's guidance for the public** as well as the **NCSC's phishing guidance**. You can also offer them support services, such as credit monitoring, in the event of a breach.

Reporting an incident

We are keen to work with the industry to ensure that savers are adequately protected, and share good practice and insight. Open and transparent dialogue is particularly important for handling cyber risk.

We are asking schemes, their advisers and providers to report significant cyber incidents to us on a voluntary basis, in an open and co-operative way, as soon as reasonably practicable. You do not need to conduct the full incident investigation before reporting to us.

A significant cyber incident is likely to result in:

a significant loss of member data

major disruption to member services

a negative impact on a number of other pension schemes or pension service providers

Report cyber incidents to us at: **report@tpr.gov.uk**. Urgent reports should be marked as such and highlight anything particularly serious. If appropriate, you can call us after sending the report. Your advisers and service providers can also report to us for incidents at their end.

Reporting to us does not replace your existing legal requirements, such as to **report a personal data breach to the ICO** without undue delay (if it meets the threshold for reporting) and within 72 hours.

You are also legally required to **report breaches of pensions law** where these are likely to be of material significance to us. This includes where these arise from a cyber incident, for example if it leaves you unable to process core transactions promptly and accurately, such as benefit payments. For authorised master trusts, you should also report this to us via the existing **significant event reporting process**.

When a significant cyber incident occurs, you may also need to report it to the National Cyber Security Centre (NCSC). Read the **NCSC 's guidance about their role** and the type of incidents that you should report. If you proactively engage with the NCSC on any significant cyber incidents, the ICO will take this into account.

Incidents that are not considered significant and those that might lead to a heightened risk of individuals being affected by fraud, should be reported to **Action Fraud** – the UK's national fraud and cybercrime reporting centre. If your organisation is in Scotland, then reports should be made to **Police Scotland**.

Links to more information

National Cyber Security Centre

Advice & guidance

Threat reports

Cyber essentials

10 steps to cyber security

Glossary

Cyber security check tool - a free online tool which can use to check common vulnerabilities in your public-facing IT

Information Commissioner's Office

- Breach response and monitoring
- A guide to data security
- Personal data breaches: a guide
- Information security checklist
- Responding to a cybersecurity incident
- Encryption
- Working from home
- Ransomware and data protection compliance

PLSA

- Cyber risk – made simple guide

PASA

- Cybercrime protection checklist
- Cybercrime guidance