Summary
- Pension schemes and administrators are under constant threat from a multitude of cyber security threats that could cause data loss, resulting in reputational damage and regulatory censure.
- Research suggests many schemes and administrators need to do more to use technologies, risk management and staff training to reduce security risks.
- There is also a need to improve the security of member communications and members' protection of their own confidential data.
- Schemes and administrators must also assess and encourage improvement in the security postures and policies of third-party service providers that access member data.

A constant threat

The vast quantities of personal data that pension schemes and their administrators hold present a tempting target for cyber criminals. David Adams looks at what administrators and trustees need to do to keep member data safe

Cyber crime poses a constant, yet hugely varied threat to individuals and organisations that use online technologies – including every pension scheme and administrator. That threat has intensified in recent years: There was a 43 per cent increase in the volume of computer misuse offences in England and Wales between the year ending June 2019 and that ending June 2021 [figures from the *Office for National Statistics*].

A Freedom of Information request put to the Information Commissioner's Office (ICO) also shows that the number of pension schemes reporting cyber breaches grew from two per month before the pandemic to five per month during 2022, reports Crowe partner and head of national forensics services, Jim Gee, who is also chair of the Pensions Administration Standards Association (Pasa) cybercrime and fraud working group.

Gee says that about 70 per cent of those breaches were caused by ransomware attacks, which lock up computer systems until some form of ransom is paid. Most of the remaining 30 per cent were the result of phishing, in which emails and other media are used to trick recipients into unwittingly enabling fraud or data theft, often by inadvertently downloading malware.

He also points out that while cyber crime was once conducted by individuals or fairly small organisations, today it is an "industry", characterised by "national and international organisations … highly profitable, growing rapidly and able to work from anywhere in the world". Any scheme or administrator that is hit by a cyber incident could suffer significant reputational damage and be exposed to regulatory risks.

Pension industry resilience

Research published by Crowe in April 2022 showed that 43 per cent of pension schemes it surveyed had not tested the resilience of IT systems and processes against cyber threats. Those results followed the findings of The Pensions Regulator's (TPR) 2021 pension scheme administrator survey, which was based on responses from more than 200 in-house and third-party pension scheme administrators.

Although 95 per cent of the administrators did say they had some controls in place, those working for smaller schemes were generally less likely to be using more advanced technological methods to deter cyber attacks or to have incident response plans in place. Fewer than one in five had attained ISO or UK government Cyber Essentials accreditations; and only 25 per cent had followed Pasa's Cyber Crime Guidance.

Target risk

These apparent flaws in scheme and administrator defences are worrying because pension schemes hold so much of exactly the sort of data that cyber criminals want to steal: Personal and some financial data.

Nor should those working with smaller schemes assume they are less likely to be targeted. "There can be a tendency to think that the risks are heightened for larger schemes, but that isn't necessarily the case," says Stephenson Harwood partner, commercial, outsourcing and technology, Simon Bollans.

Administrators must make it more difficult for criminals to access the data they hold, because cyber crime is

conducted according to a basic risk/reward cost/benefit analysis, says Barnett Waddingham information security manager, Janusz Naks. "The more difficult you make it for someone to get the data, the more likely it is that they will go somewhere else," he says.

Guidance and actions

TPR's guidance for scheme administration (due to be updated in the regulator's new single code of practice) emphasises the need to access skills and expertise required to manage cyber risks linked to systems, processes and people; the need to discover whether third-party suppliers have also implemented sufficient security risk controls; the need for an effective incident response; and for regular reviews and testing of controls, processes and incident response.

In addition, the Pasa cyber crime and fraud working group Gee chairs has prepared specific guidance for administrators, encompassing the need to develop controls to mitigate an incident (including use of specialist cyber security service providers), employee training, and response planning.

Bollans suggests administrators use the government's Cyber Essentials scheme to work out how to apply these principles to the practical operations of schemes and the administrator's own businesses. He also highlights some basic principles, such as implementing all necessary software updates, having some form of network monitoring to identify threats, monitoring of emerging risks via updates from the National Cyber Security Centre; and regular testing of internal security processes by expert penetration testing providers.

But any of these measures can be undermined by human error. Staff and trustee awareness of security issues and the precautions they need to take to avoid data breaches is crucial and should be supported by technology usage policies preventing or restricting movement of data (or information that could enable unauthorised access to it) on laptops, phones, USB sticks or other portable devices.

"Internally we need to know that data is locked down, only people who need to access it can access it, and everyone knows what data can and cannot be released," explains Barnett Waddingham head of pensions administration, Paul Latimer.

Other technologies secure mundane but necessary processes, such as email communications. Examples include Beyond Encryption's secure, encryption-enabling email technology Mailock, which enables secure exchange of sensitive documents via email and is protected by multifactor authentication. End users include Royal London and Aegon.

Analysis of potential security risks must also include consideration of security vulnerabilities within schemes' or administrators' supply chains. Crowe's April 2022 research suggested that 28 per cent of the UK pension schemes it surveyed had not assessed the vulnerability of third-party suppliers to cyber crime, with that figure rising to 43 per cent for small schemes.

The final element in best practice for securing member and other scheme data is planning how to respond to security incidents, because there is no such thing as fail-safe security. TPR's guidance highlights the need for an incident response team with clearly defined roles and responsibilities; and plans for reporting an incident to trustees, the ICO, regulators and law enforcement agencies and/or scheme members. It states that schemes and administrators should also have a good understanding of third-party suppliers' own incident response processes, including how and when they would inform the scheme or administrator about an incident.

In the future new security threats will emerge. Gee says he is concerned to see cyber criminals using AI technologies to accelerate and refine attacks; and by the increased availability of cyber crime as a service: provision of malware, DoS attack capability and other threats to anyone prepared to pay for it. "It means a wider group of people can have such attacks undertaken," he explains.

Despite these threats, Gee thinks the pensions world has made some significant progress in recent years. "A lot of schemes have moved this up their risk agenda," he says. "But this changes so quickly. And I still come across schemes that have not done anything very substantive – and some that have not done anything at all."

The bottom line is that schemes and administrators need to keep adapting to these ever-changing, yet continuous threats. Gee draws an analogy with the common cold: "You wouldn't expect never to catch a cold – and you would take steps to ensure that if you caught a cold, you would recover quickly.

"Protecting schemes and their data against cyber attacks is a bit like that: you need to ensure that the protection the scheme has is as good as possible, but that you're also able to recover, adapt and mitigate the effects when you are attacked."

Written by Dave Adams, a freelance journalist

Further information

- Guidance from The Pensions Regulator: https://www.thepensionsregulator.gov.uk/en/document-library/scheme-management-detailed-guidance/administration-detailed-guidance/cyber-security-principles
- Guidance from PASA: https://www.pasa-uk.com/cybercrime-and-fraud/
- National Cyber Security Centre: https://www.ncsc.gov.uk/

Cyber Essentials scheme: https://www.ncsc.gov.uk/cyberessentials/overview

- ICO: https://ico.org.uk/