Summary
- Cyber attacks, both in pensions and the broader financial sector, are on the rise.
- Pension schemes may need to pay more attention to evolving methods used by cybercriminals.
- Artificial intelligence, as well as the introduction of pensions dashboards, presents opportunities and challenges for cyber security.

Sink or swim: The rising tide of cyber threats

Callum Conway looks at why pension fund trustees and members are facing an increasing wave of cyber threats – and what they can do to stay protected

Unless you were living under a pension-proof rock, you'll recall that in March 2023, Capita suffered a serious cyber security breach.

The cyber attack affected thousands of pension holders whose personal data was compromised. Capita estimated that the financial cost of the incident was £25 million. As a result, the company faced increased regulatory scrutiny and investigations from the Information Commissioner's Office (ICO) and The Pensions Regulator (TPR).

Although it might be tempting to think of this devastating incident as recent history or a one-off, cyber security attacks are not going away – in fact, they're very much on the rise, both in pensions and the broader financial sector.

Last year, the BBC Pension Scheme experienced a data security incident affecting over 25,000 members, where sensitive information such as names, national insurance numbers, dates of birth and home addresses was compromised. A similar data breach at J.P. Morgan Chase impacted over 451,000 people with retirement plans.

In 2024, there was a staggering 4,000 per cent increase in pension scheme data breach reports, according to the ICO.

TPR head of policy, Fiona Frobisher, says pension schemes are at increasing risk of being targeted by cyber attacks because they hold large amounts of personal data and assets.

"The multiple high-profile cyber attacks in recent years should leave pension trustees and their administrators in no doubt of the need for robust cyber resilience," says Frobisher.

Norton Rose Fulbright partner, Tim Jones, senior associate, Suzie Kemp, and associate, Alexander McGuire, all agree. They say the pensions industry faces particular risks associated with business email compromise, given some trustees and managers may operate with private mailboxes and domestic hardware without enterprise-level security.

They also highlight a recent surge in browser-based cyber threats – programmes that modify web browser settings without the user's permission and redirects the user to websites the user had not intended to visit – with browser-based malware accounting for 70 per cent of malware cases last year.

"These new methods increase the risks of an attack, illustrating the importance of training and ensuring staff are aware of threat actor's evolving tactics," they explain.

Norton's team also says there are increased risks associated with the growing complexity of supplier networks and the lack of visibility into how third parties store, process and protect data.

According to the World Economic Forum, 54 per cent of large organisations cite supply chain weaknesses as their biggest challenge in pursuing cyber resilience.

So, is the industry aware of these evolving risks, and is it doing enough to stop them?

The *Core Alternative Managers' Mood Index* report by Gen II Fund Services reveals cyber security has become the foremost operational concern for investors during fundraising due diligence.

The report indicates that 27 per cent of investors now prioritise cyber security in operational due diligence conversations, reflecting a heightened awareness of digital threats in the private capital industry.

However, Norton's experts suggest pension schemes may need to pay more attention to these risks.

"We would advise trustees and managers to take steps beyond policy reviews and consider other protection and governance measures that may be incorporated into a scheme's controls," they say.

Echoing this, Frobisher claims trustees are increasingly focusing on

the cyber risk to members through administration and digital services, but they are not as focused on their other suppliers, such as offshore third-party suppliers and their advisers.

She says that some schemes may also be over-reliant on employers' and administrators' cyber security plans, which are sometimes accepted without the appropriate scrutiny.

Currently, TPR requires occupational pension schemes to establish an effective system of governance that includes controls to manage cyber risk.

In February 2024, it issued updated guidance for pension scheme trustees on managing cyber risk, including its General Code, which requires trustees and managers to know and understand their scheme's cyber risks.

In addition, TPR makes clear that having an incident response plan is key to lessening impacts on members, according to Independent Governance Group trustee director, Michael Do.

"Well-rehearsed playbooks can help to significantly hasten trustee decision-making and action-taking, ensuring that the adverse consequences for members are reduced as far as possible," he says.

Similarly, the ICO, which has a remit to protect individuals' rights and freedoms, expects pension scheme trustees and managers to implement appropriate technical and organisational measures to protect personal data commensurate to the risk posed.

Cyber security and counter fraud forensic services partner, Tim Robinson, says awareness training can help put cyber security in plain English for trustees.

"Working through the General Code will also support the delivery of an achievable and comprehensive cyber strategy that will help to raise resilience across a scheme's full ecosystem, manage cyber resilience on an ongoing basis and leave [*trustees*] better equipped to respond to incidents if they arise," says Robinson.

Looking ahead, it's impossible to discuss the cyber security landscape without assessing the impact of artificial intelligence (AI) as a force for both good and evil.

On the one hand, technology will play a pivotal role in preventing cyber security risks, Norton's experts argue.

"Its ability to process large quantities of data, spot patterns and anomalies makes delivering services easier and strengthens cyber defences," they say.

"The multiple high-profile cyber attacks in recent years should leave pension trustees and their administrators in no doubt of the need for robust cyber resilience"

"AI has been incorporated into cyber-security frameworks, such as intrusion detection systems and automated response protocols, enabling organisations to better deal with increasingly sophisticated attackers."

On the other hand, cybercriminals can use AI to exploit users through deep-fakes and create more sophisticated attacks. Approximately 40 per cent of phishing emails targeting businesses are now generated using AI, leading to a 60 per cent success rate in deceiving recipients, as reported in the *Harvard Business Review*.

Meanwhile, financial institutions are also facing a significant increase in deep-fake fraud attempts, which have grown by over 2,000 per cent over the past three years, according to data from Signicat's *The Battle Against AI-Driven Identity Fraud* report.

Despite this increase, only 22 per cent of financial institutions have implemented AI-based fraud prevention tools, leaving many companies vulnerable to more sophisticated attacks, the report says.

The introduction of pensions dashboards will also present opportunities and challenges for cyber security in pension schemes.

Centralised monitoring and transparency should encourage stronger regulatory compliance and improved data accuracy, but if not properly secured, a single breach could expose millions of pension holders' sensitive information.

Burges Salmon partner, Richard Pettit, identifies two main risks from a trustee perspective in relation to dashboards. First, the ever-increasing chance of scams, which is a joint cyber and data protection risk, and second, the risks associated with uploading member data to the dashboards ecosystem.

"Trustees should reconsider their obligations as data controllers under the General Data Protection Regulations and update the provisions of their scheme administration contract in connection with pensions dashboards," says Pettit.

The Pensions Dashboards Programme claims it has "identified risks of misusing personal data and inappropriate entities gaining access to the ecosystem".

Clearly, strong cyber security measures – including encryption, AI-driven fraud detection, and continuous risk assessments – will be crucial to ensuring that dashboards enhance rather than hinder security.

Overall, trustees remain in an "unenvious" position when it comes to cyber security, concludes Robinson.

"Due to the volume of rich personal member data, management of significant assets, and the need to pay pensions uninterrupted, schemes are targets and potentially very vulnerable to ransomware attacks," he says.

As the industry continues on the path to digitalisation, it must remain aware of the evolving and increasing risk of cyber attacks and be proactive in its efforts to prevent them.

Written by Callum Conway