The cost of cyber attacks

Gill Wadsworth reveals the costs of cyber-attacks and how schemes can best protect against this risk

Summary
- Cyber-attacks are becoming more frequent and costly, and trustees are directly liable for the risk.
- The Pensions Regulator expects trustees to have adequate protection plans in place.
- Outdated and ineffective cybersecurity makes pension schemes vulnerable to attack.

Protecting against cyber-attacks is an expensive business, but failing to take effective security measures can cost pension schemes an awful lot more.

In 2022 cyber-crime cost UK businesses on average £4,200, while the average cost to remedy is five times as much at £21,000.

This is something Capita found in March 2023, when the firm suffered a serious cyber security breach in which customer data was exfiltrated.

The attack affected thousands of pension members who had their personal data compromised and led to £25 million in costs, as well as reputational damage, potential loss of business and customers, increased regulatory scrutiny and investigations from the Information Commissioners Office and The Pensions Regulator (TPR).

And the threat from cyber criminals is only set to worsen. Cyber research firm Cybersecurity Ventures expects global cybercrime costs to grow by 15 per cent every year over the next five years, reaching $10.5 trillion (£7.92 trillion) annually by 2025, up from $3 trillion in 2015.

In the UK, cyber is the fastest growing fraud with around £37 billion a year lost to all types, and of the £6 billion a year lost to pension fraud each year, the lion's share is now believed to be cyber.

And this could be a vast underestimation, since Pension Scams Industry Group chair, Margaret Snowdon, notes the industry "does not collect enough data to be able to be sure of the figures, as companies and schemes do not always report ransomware attacks".

Ripe for the picking

Pension schemes are ripe for the picking for cyber criminals; holding trillions of pounds in assets and with deep reserves of member data make them a particularly attractive prospect.

Trafalgar House client director, Daniel Taylor, says: "Cybersecurity is one of the biggest threats facing pension schemes today. The message has finally sunk in; schemes hold massive amounts of sensitive data and significant sums of money, and many are still relying on outdated or cobbled-together systems that leave dangerous gaps. The industry is traditionally slow-moving, with legacy tech and data stores that create serious vulnerabilities."

In December 2023, TPR issued updated guidance for pension scheme trustees on how to manage cyber risk to schemes. This was followed in February 2024 by a *Regulatory Intervention Report* on the Capita cyber security incident.

The watchdog is clear that trustees and scheme managers are responsible for protecting their members, and that they must have risk mitigation in place and adequate procedures in the event that the worst should happen.

Aon partner, Paul McGlone, highlights how TPR expects every scheme to have an incident response plan that could be used in the event of a cyber incident, and to have tested it.

"The details of each plan will differ, as processes should be suitable for their specific scheme, structure, size, and people. For many schemes, the plan isn't so much about a rigid process as guidelines and checklists to refer to. Common elements of a plan would include some sort of severity assessment, an escalation process, guidelines on reporting, draft member communication, as well as emergency contact details and checklists to ensure that key tasks are not forgotten," he explains.

TPR acknowledges the "amount of work involved in this type of exercise" but says trustees "should factor this in as part of effective contingency planning".

Sackers partner, Olly Topping, says the level of resource needed will depend on the size of scheme and the number or different third-party providers it employs, but irrespective of the amount of commitment required, trustees must take cyber security seriously.

"Schemes are already very busy, and cybersecurity can a lot of resource, but the regulator feels, and we would agree, that this is a serious risk and requires the appropriate level of time and investment to manage if it is to be mitigated adequately."

Topping notes that while larger schemes may have the resources to put cybersecurity in place, they may also have multiple third-party providers making oversight of all data and assets more complex.

Meanwhile smaller schemes, according to Snowdon, "tend to keep their heads down or rely on third-party service providers", but she notes that there is "no foolproof protection because cyber criminals are organised and sophisticated".

"If criminals want to get in, they almost certainly will. A scheme should aim to be better protected than others; like a burglar alarm makes thieves move on to easier prey," Snowdon says.

Prevention better than cure

Stephenson Harwood cyber lead, Joanne Elieli, says there are several prevention measures that pension trustees can enforce to ensure they are cyber resilient.

These include regular security audits and vulnerability assessments; robust data encryption; multi-factor authentication and strong password policies; and regular cybersecurity training for trustees, administrators and staff.

"Human error is the biggest vulnerability any organisation has and so regular, meaningful training can dramatically reduce this risk," Elieli says.

Elieli encourages pension trustees to discuss their cyber security needs with their in-house and/or external legal counsel, together with their relevant technical team.

"The most effective type of support at a high level though is that which is collaborative, specifically between the legal and technical teams. You want your key stakeholders engaged too to ensure that best practices and cyber resilient measures are in place and being endorsed from the top down," she says.

According to McGlone, prevention measures need to cover the trustees themselves, their various service providers, and the scheme sponsor.

"Most trustees start by reviewing the controls at their critical providers, typically administrators, and then work through other providers based on potential impact of a cyber incident. But it's important to include the sponsor in that assessment, as well as the trustees' own controls. Having the most secure administrator is no help if the weakest link is a trustee using a Hotmail account on a laptop with no virus software," he explains.

"Cybersecurity is one of the biggest threats facing pension schemes today"

Control, monitor, test

LawDeb director, Sean Burnard, says his independent professional trustee firm follows a strict cyber-security process.

"We have a mantra when it comes to cyber security: Control, monitor, test. It is this mantra that guides our behaviours and our recommendations to trustees. As the world becomes more digital, cyber presents an increased risk to schemes, trustees, and their members – it should be high on the risk register for schemes of all sizes."

McGlone recommends that trustees have both preventative support and response support.

"Preventative support includes general cyber governance (e.g. setting up cyber policies and incident plans), specialist cyber expertise (e.g. assessing controls at providers) and legal advice (ensuring contracts are robust). Response support is quite different and can be practical support (e.g. project management), forensic IT expertise (e.g. if an incident needs investigating), legal advice (e.g. data privacy issues) as well as advice around member communication, media enquiries, credit monitoring services etc," he explains.

TPR also expects trustees and scheme managers to have robust policies in place should the worst happen. Every scheme should have a cyber incident response plan that includes communication strategies, legal and recovery procedures.

Snowdon says: "The most important thing is for trustees to have a cyber expert on tap, whether directly or via cyber insurance. Doing your own thing when facing a cyber threat can often lead to a worse outcome, including you possibly going to jail. Ensure you have a plan on what to do if something goes wrong and have someone in charge of executing that plan. And keep on testing and replanning. Seems a lot, but the cost of doing nothing is much more than you can ever imagine."

But the cost of such cybersecurity is an issue for some schemes, and since TPR places the burden of risk squarely with the trustees, they will need to find the resources to make sure they are protected.

Taylor says: "Tackling cyber threats isn't a cost-free exercise. Schemes must recognise that it's not just down to the administrator to plug every gap. Trustees need to be prepared to shoulder some of the costs and work together with their advisers in a spirit of cooperation. It's a shared responsibility, and without the right level of investment and collaboration, it's impossible to effectively defend against the growing cyber threat."

In a world where cyber criminals are getting ever more sophisticated and the spoils from pension funds increasingly tempting, trustees will need to keep security both tight and responsive.

As Burnard concludes: "This is not a once and done. The cyber risk landscape is evolving as fast as the world's technology, and trustees must regularly and thoroughly review their cyber approach to ensure they're as prepared as they can be. The mantra holds true – control, monitor, test."

Written by Gill Wadsworth, a freelance journalist