# Prepare and protect

**Summary**

- Pension schemes have billions of pounds of assets and vast amounts of member data spread across multiple access points, making them an attractive prospect for scammers and hackers.
- Policies such as auto-enrolment have increased the number of pension savers and therefore their exposure to cyber crime.
- As technology advances, so have cyber criminals' techniques, and the industry is having to adapt to stay ahead.
- TPR and Pasa have published guidance for trustees, who have to be increasingly wary of the threat posed by cyber crime.

**Pension policy and technological advancements have led to savers' money and data being more exposed to cyber crime. Jack Gray examines what the industry is doing to tackle the risk, whether what is being done is enough, and the challenges that the future holds as cyber criminals' techniques evolve**

As we hurtle into the future, it can seem as if the advancement of technology is passing us by and it is often difficult to keep pace. However, the pensions industry must do exactly that in order to protect pension savers and their money. Recent guidance from The Pensions Regulator (TPR) and the Pensions Administration Standards Association (Pasa) gives trustees and scheme managers some assistance in safeguarding members, but more could be done to ensure that peoples' savings are protected.

### The size of the problem

The regulator's guidance and campaigns, such as ScamSmart, highlight that there are concerns regarding members' cyber security, but how big is the problem? "It's not possible to put a figure on cyber risk, but most corporates have cyber risk in their top few global risks, and pension schemes should be equally cautious," begins Aon partner, Paul McGlone. "Pension schemes have millions of records and billions of pounds of assets, set up in a way that means multiple stakeholders and providers, giving many different access routes for a cyber criminal. The risk is therefore material and trustees should be taking steps to ensure that their schemes are well protected."

The amount of information that schemes manage can make them a particularly attractive prospect to cyber criminals, with the amount of automated data only set to increase as the world moves to be more computer centric. Dalriada Trustees professional trustee, Charles Ward, comments: "Pension scheme trustees and administrators hold a vast amount of data in respect of millions of members and beneficiaries, all of whom will expect their information to be properly protected. However, such rich seams of data mean that pension schemes are also on the radar of cyber criminals.

"Trustees and their service providers therefore need to take cyber security seriously and put in place measures that, whilst proportionate, are also holistic."

Not only do pension schemes have large amounts of data and members' savings, but the number of savers is increasing as the government looks to drive up pension engagement. "Concerns have been growing across the industry regarding cyber security," adds LifeSight risk and compliance manager, Louise Williamson. "The success of auto-enrolment has led to an increase in exposure with many more savers and savings potentially at risk. This risk is concentrated over a relatively small number of administrators and providers in the market."

### Scheme preparation

Despite the concerns, the issues can be addressed, or at least minimised, if schemes are prepared. Pasa's guidance urges that "trustees prepare for when a cyber-security incident occurs, rather than if an incident occurs," says Burges Salmon associate, Samantha Howell.

Williamson believes that the pension industry is "very alert to the challenges" posed by cyber crime. She continues: "Schemes and trustees need to commit time and resources to proactively ensuring security measures in place meet a minimum threshold and robust controls are in place to mitigate risk, alongside focusing on their response should an incident occur, which is more reactive."

Although many are doing what they can to address the issue, Aon's recent study – *Global Pension Risk Survey 2019* – finds that almost a quarter (23 per cent) had no training on the risk posed by cyber crime.

Despite the survey finding that 95 per cent of respondents had not had their scheme affected by cyber crime, there were still some that reported being affected and the number is expected to increase, according to Aon.

McGlone warns that although schemes may be aware of the security needed to minimise cyber crime, they may not know how to react. He says: "A bigger unknown for many schemes at the present time is not the level of security, but how they would respond if that security was breached and they faced a real cyber incident."

Howell adds that, although schemes may not have seen much cyber crime to date, it is likely to become more commonplace. "It is expected that the trend of high-profile, cyber-security incidents will continue for the rest of the year and the rest of the decade. It is only a matter of time before we see significant incidents for a range of pension schemes," she comments.

### Trustee responsibility

TPR's guidance says that trustees and scheme managers are accountable for the security of scheme information and assets, and that the schemes' cyber risks should be on their risk register and regularly reviewed.

Howell notes that the first step should be to review the "current security levels and consider whether there are any weak links", before auditing advisers, considering the insurance in place, having trustee training and "monitoring the cyber risk".

McGlone adds: "Trustees should be assessing risk at both ends of the process. First, the risk of a cyber incident taking place, by discussing protection with their providers and sponsor, as well as considering their own cyber resilience. Second, their preparedness to respond to an incident should it occur.

"It's also important to remember that reviewing cyber risk is not just a once only exercise, as techniques and tactics continue to evolve pension schemes need to stay on top of the issues to ensure that they continue to follow best practice guidelines."

An important step that trustees may want to take to best protect members is assessing how their scheme is operating against the recommendations. "The trustee should look at the wealth of available information and really challenge how their scheme stacks up against available evidence," explains Williamson. "They should also look for tangible evidence of security, for example independent oversight, penetration testing or data on any attempted attacks."

Sackers senior associate, Oliver Topping, notes that research points to human error and phishing emails as areas for trustees to be aware of: "Recent research by CybSafe has shown that human error caused 90 per cent of cyber data breaches in 2019, and 45 per cent of all breach reports to the Independent Commissioner's Office (ICO) were caused by phishing. Being aware of the risk of phishing emails through training is a key step to prevent risks in this area."

Although the responsibility of scheme data and assets falls at the feet of trustees and scheme managers in the eyes of TPR, most use third-party administrators (TPAs). "Trustees' priority should be to ensure that TPAs and other service providers have put sufficient controls and incident response processes in place," says Ward. "There are recognised standards and accreditations that can help suppliers demonstrate their cyber resilience. We have seen many trustees simply assume that the administrators are properly looking after the data without knowing for sure. If anything happens to the member data, then it is the trustees that will be on the hook, not the third-party providers."

### Evolving legislation

As the world becomes more tech-oriented, legislation has had to adapt to minimise the risks posed by a data breach or cyber attack. The most significant piece of legislation was the General Data Protection Regulation (GDPR). "It sets standards in terms of the data protection cyber security issues that anyone who holds data would have to abide by to protect members' data," explains Squire Patton Boggs (SPB) partner, Garon Anthony. "As a result, that includes the potential access to scheme assets. It also prescribes the system of fines."

SPB senior associate, Chris Harper, notes that, although "a number of schemes had policies in place" before the legislation, the level of fines outlined in GDPR "have focused the minds".

Anthony adds that, since the introduction of GDPR, he is unaware of any fines by the ICO for pension schemes that may have fallen foul of the legislation. However, he warns that it will be "just a matter of time" before it happens "because you have pension scheme trustees, administrators, all the various advisers running the scheme on a day-to-day basis and they have a vast amount of data, and it's really valuable data".

He continues: "If you were a cyber attacker, you may think it would be worth targeting a scheme and its administrators. It has to be inevitable that there will be a breach just because of the vast quantities of data that schemes hold and the fact that there will either be human error that leads to an inadvertent data breach or a cyber attack."

TPR's updated code of practice is expected in the near future and Harper says that it would be surprising if it didn't include "adequate measures in place for cyber security issues".

## Future challenges

With the continued automation of scheme data, the challenges posed by cyber security are likely to continue and possibly worsen. Trustees will continue to be tested, but in an ideal world they will be prepared to face the issues that arise. To achieve this, the industry will have to keep pace with potential scammers and technological advancements.

"Change is inevitable and the increased desire to have information at your fingertips and transact as seamlessly as possible does need to be balanced with ensuring the platform and permissions are secure throughout. Keeping pace with developments and committing to continual oversight is essential to keep savers data secure in the long term," concludes Williamson.

**Written by Jack Gray**