Summary

- According to the government's recent *Information security breaches survey,* more than 90 per cent of large organisations and 74 per cent of smaller ones have been hacked, with the average cost of a breach standing at £2.3 million.
- The pension sector is a prime target for criminals, on account of the high-value nature of the data companies hold.
- Employees are often the weakest link. However, staff can be an integral part of security procedures; they are on the front line and have to deal with the threat of cyber criminals and opportunistic attacks on a daily basis.
- Staff education should focus on basic cyber security hygiene, educating employees about the importance of strong passwords and how to spot phishing emails.
- Showing the potential damage that can be done can have a powerful effect. Other options include computer-based training modules, face-to-face sessions and producing clearly structured process and policy documentation.

Educate against attack

Nick Martindale explores how pension schemes can improve their cyber security and the importance of employees in fighting threats

In this digital age, any large organisation that controls significant amounts of data, and potentially access to cash, is likely to be at risk of a cyber-attack. According to the government's recent *Information security breaches survey*, more than 90 per cent of large organisations and 74 per cent of smaller ones have been hacked, with the average cost of a breach standing at £2.3 million. Just as big a danger, though, is the organisation's reputation, which could potentially wreak untold damage on a brand or share price.

My1Login head of marketing Norman Begg says the pension sector is a prime target for criminals, on account of the high-value nature of the data companies hold. "Pension records include invaluable information coveted by hackers, including names, national insurance numbers, dates of birth, current pension, fund data and family member details," he points out.

Nor is it just the pension providers that need to understand and cope with the cyber threat. Trustees, too, need to better appreciate the value of the data they hold, and the risks they may inadvertently be exposing members to. "Pension trustees often think that cyber threat is a risk that affects large companies and that schemes are somehow below the radar of cyber criminals and hacktivists," PASA chair Margaret Snowdon warns.

"This naivety makes pension schemes particularly vulnerable. The more trustees make information readily available to members through channels such as mobiles and tablets, the more they need to protect themselves."

Employees

There are a number of basic measures of which any organisation handling data should be aware – including encrypting data and making sure multi-layered security software is installed on all servers and workstations – but the reality is that it is employees that are often the weakest link.

"Naivety makes pension schemes particularly vulnerable. The more trustees make information readily available to members through channels such as mobiles and tablets, the more they need to protect themselves"

"Staff can be an integral part of your security procedures; they are on the front line and have to deal on a daily basis with cyber criminals and opportunistic attacks from the moment they log on through their interaction with emails, files and the internet," ESET security specialist Mark James says.

"With the right knowledge and understanding, they can be taught what to look out for and how to report suspicious behaviour."

The key to this is effective education of employees, outlining basic security measures they can take to avoid helping criminals gain access to data through, for instance, by installing ransomware or phishing software. "Attacks often start with an end-user, using them as a gateway to the wider network," Avecto vice president Andrew Avanessian says.

"Staff education should focus on basic cyber security hygiene, educating employees about the importance of strong passwords and how to spot phishing emails."

Passwords are a particularly problematic area, says Begg. "Employees are typically guilty of a plethora of weak practices such as using the same password for multiple applications, choosing weak and easy-to-remember passwords, writing passwords down or storing them in spreadsheets, on their mobile, in Dropbox, or sharing them insecurely via email or text," he says.

"Commonly, employees will also use personal passwords for business applications. When these consumer services are hacked there's a domino effect, resulting in breaches to business applications protected by those same passwords."

Preventions

There are a number of different ways in which organisations can deliver training to demonstrate just where employees need to improve. Showing the potential damage that can be done can have a powerful effect. "Employees typically underestimate what malicious software can do," Barracuda Networks general manager EMEA Wieland Alge states.

"When you demonstrate to them that their computer can extract millions of datasets within a short time, many employees are flabbergasted. I would recommend annual or bi-annual face-to-face training by two people, one familiar with the daily workflows and one familiar with the actual digital threat." This can then be followed up with e-learning modules, he adds.

Other options include computer-based training modules, face-to-face sessions and producing clearly structured process and policy documentation, Administration Limited managing director David Watkins states.

"In particular, key hints or tips and escalation measures are all relevant to the job of increasing awareness of cyber security threats, and how to protect against them," he says.

James, meanwhile, suggests using a mix of in-house trainers and external providers to ensure nothing is left to chance. "The training should be relatively short and to the point, with an emphasis on how they can be part of the team and not part of the problem," he says.

Once any education has been carried out, it's a good idea to test out whether the learning has been applied, Fitzrovia IT managing director Daren Oliver says. "We would recommend phishing email tests to see which employees open up the email and then proceed to click on the embedded hyperlink," he says. "Additional training and education can then provided to the employees failing the test." The same level of scrutiny should be applied to their own devices if they are used to access work systems, he adds, whether at home or in the office.

Any education programme needs to involve third parties, such as freelancers, contractors or consultants, who also have access to the systems, Carbon Black national security strategist Rick McElroy adds. "Lots of attacks come through third parties," he says. "Many times, third parties have elevated access to IT systems. It's paramount they understand the guidelines and rules." Anyone accessing systems should also sign policies on acceptable use, he adds, while the education itself needs to be delivered through various formats, including videos, posters and self-phishing campaigns.

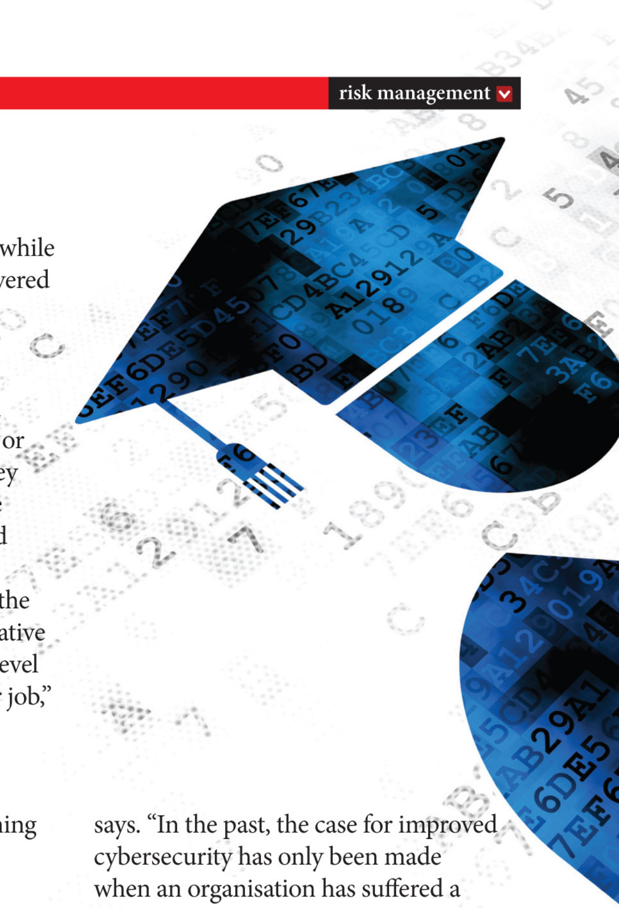
Organisations should also think about the potential for employees – or contractors – to abuse the access they have to data, and devise appropriate policies. "Temporary employees and freelancers are a particular threat in this case, and this really underlines the importance of restricting administrative rights, ensuring staff only have the level of access they need to perform their job," says Avanessian.

"That's where data segregation has to come in," says James. "All employees should undergo the training but temporary staff and consultants should have limited contact with sensitive information. When it comes to encryption and safe storage, these procedures should automatically happen where possible and require no user interaction to take place."

There are other basic steps, too, which any organisation should take to ensure they reduce the chances of falling victim to cyber crime. "Investing in strong preventative measures and defences is key to limiting any damage that could be caused by a breach," says Oliver.

"These should include encrypted version control backups, fully tested disaster recovery and business continuity solutions, a stacked security system – for example, firewalls, anti-virus software, anti-malware – user training and awareness, 2-factor authentication, cyber essentials accreditation and independent vulnerability tests. Certainly in the case of the recent high-profile ransomware attacks, robust data backup and recovery strategies are crucial to safeguarding businesses from fraudsters."

It's also vital that senior management buys into any initiative, Skybox Security VP EMEA Justin Coker warns. "Cybersecurity and business leaders also need to be of one mind when it comes to addressing these threats strategically," he says. "In the past, the case for improved cybersecurity has only been made when an organisation has suffered a breach; that simply isn't acceptable as organisations like pension firms become end-to-end digital businesses. They simply can't afford to be a victim of something like a ransomware or denial of service attack that would shut them down for hours, if not days."



Large-scale breach

Indeed, it is only a matter of time before there is a large-scale breach affecting a pensions business, warns Avanessian.

"Although there hasn't been a high-profile public one as yet, the large pots of data and cash, including defined contribution schemes, is a gold mine for cyber criminals looking to take advantage of the UK's £3 trillion market," he warns. "Scheme trustees should work closer with scheme administrators to identify areas of risk and make security a number one priority, and don't wait for regulation to enforce it. We also need to remember that many attacks start with the end-user rather than going straight to the data centre, so it's advisable to look to reduce the risk there first, then work back through the network."

Written by Nick Martindale, a freelance journalist