Technological advances have brought financial companies a wave of new products, services and potential security problems. **Simoney Girard** taps into a few key problem areas

ACCESS ALL AREAS

The recent £980,000 fine slapped on Nationwide Building Society should be a warning to all financial services providers: no matter how many firewalls, security passwords or high-tech gadgets a company may have in place, there is always the possibility of financial fraud, theft or unintentional leaks. With the rise in remote working comes a plethora of problems, not least the question of who has access to your customers' financial data.

In Nationwide's case, a laptop was stolen from the home of one of its employees last year. The building society, which holds information for more than 11 million customers, was found guilty of failing to have adequate information security procedures and controls. This placed its customers at risk of financial crime. Margaret Cole, director of enforcement for the Financial Services Authority (FSA), says: "Firms' internal controls are fundamental in ensuring customers' details remain as secure as they can be. As technology evolves, firms must keep their systems and controls up to date."

Simoney Girard

The corporate laptop

In the space of just six months last year, 4,973 laptops were left in the back of cabs. Remote working and employees taking work home necessitates a significant responsibility as an employer to ensure your customers' details are ring-fenced.

While investigating Nationwide, the FSA found that the building society was unaware that the laptop contained confidential customer information, nor did the company start an enquiry until three weeks after the theft.

This was a contravention of the guidelines in a 2004 report from the FSA – 'Countering Financial Crime Risks in Information Security' – which state that all clients' financial services data must be kept safe at all times.

How confident are you that your clients' details – corporate, high net worth, retail or legal – are secure? Can you afford to shell out nearly £1 million in fines?

A spokesperson for independent fund platform Cofunds, which has more than £8 billion in assets under administration, says: "All our laptops are encrypted – this is just best industry practice.

"If technology-based financial crime was not at the forefront of people's minds several years ago, it certainly is now."

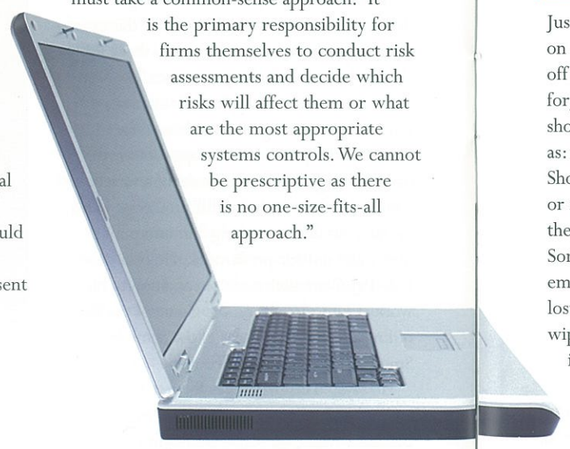
The FSA guidelines state that laptops should not be configured to share or accept files through a wireless card, as this could represent a backdoor into the corporate network.

Data storage & disposal

"You should have a clear understanding of what you must buy and what sort of security controls you need. You can encrypt fobs and laptops, although you should not be storing lots of client information on your laptop," says Paul Sparkes, partner and security leader for Ernst & Young.

Firms can give systems a thorough clean when disposing of the hardware, while banks can get a third party to destroy the disks when the systems are being replaced, so there is no need to have reams of information being left around for others to use. But failure to make sure that laptops or palm pilots have proper security is likely to damage companies financially through fines and loss of reputation.

The FSA is not being unduly hard on firms: as Heidi Ashley, FSA spokesperson states, firms must take a common-sense approach. "It is the primary responsibility for firms themselves to conduct risk assessments and decide which risks will affect them or what are the most appropriate systems controls. We cannot be prescriptive as there is no one-size-fits-all approach."



Social engineering

How often do you conduct full compliance checks on freelance or contract staff? Has HR gone into more detail than was provided by the CV? Paul Sparkes, of Ernst & Young LLP UK, says: "Social engineering is serious. People are coming through the front doors of companies without proper vetting procedures, and siphoning off information over a course of a few weeks or months.

"IT can set up codes of access controls, keeping systems usage restricted to a few key staff. Other procedures can be put in place, such as ensuring that people who make the purchase orders are not the same people that also approve payment."

Heidi Ashley, press officer in the City team at the FSA, added: "Firms must ensure that people hired to carry out controlled functions are deemed to be fit and proper.

"There are certificates to prove this, and firms need to have a look at our rulebook to ascertain what is required for different financial job functions."

Companies should also beware the instant messaging phenomenon – these do not use encrypted communication and can present a threat, as instant messages can sneak through a firewall. If you use a lot of freelance or contracting staff, it is worthwhile ensuring that messaging applications do not work on company equipment.

BlackBerry jam

Just recently, I rang a fund of funds manager on his mobile the second before he leapt off a ski boat on a family holiday; he had forgotten he'd strapped his phone to his shorts. This raises important questions, such as: who is listening to your conversation? Should your employees be discussing legal or financial business on trains, especially if they are working on winning a new client? Some common-sense ground rules should be employed. Thankfully, if a BlackBerry gets lost or stolen, all data stored on it can be wiped remotely and immediately. It is worth investing in this sort of technology for staff who travel often.

Secure hosting

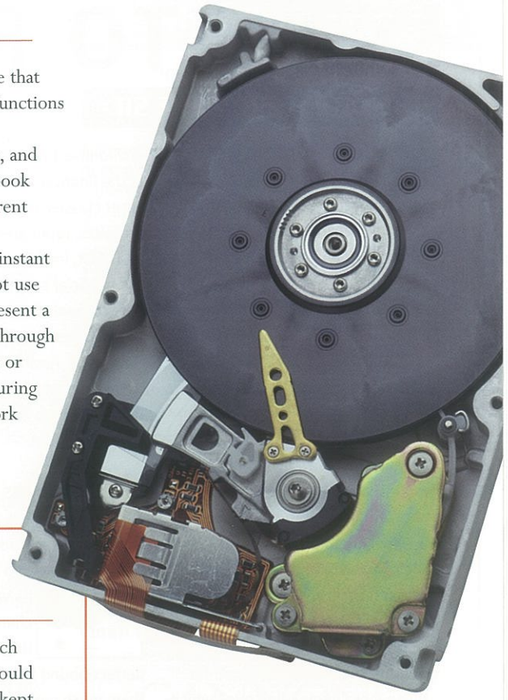
The FSA's report is clear on threats such as phishing and identity theft: firms should take greater care to ensure clients are kept informed about potential fraudulent activity.

The UK payments association APACS has raised many issues, such as: tracking an increase of emails bounced back from spoof sites; using third-party monitoring services to scan emails; and having a central email address for customers to send suspect emails to, with an automatic response highlighting anti-phishing tips.

Companies must also implement a top-class information security framework, with scalable governance mechanisms in place, as well as standards and guidelines covering networks, operating systems and databases.

No system, of course, is totally hack-proof. However, firms should ensure, especially if they are hosting personal data such as clients' bank account details and home addresses, that software – whether on PCs or Macs – are as fortified as possible.

One way is to check, check and check again. As the spokesperson for independent funds platform Cofunds explains: "We use both external and internal testing to make sure people cannot hack into client information. There are many companies that test systems externally to challenge whether these are robust enough." This is what the FSA calls the penetration test.



Conclusion

"As part of our general supervision we assess firms on different internal controls, risk impact and probability in relation to our regulatory objectives such as treating customers fairly and the prevention of financial crime," the FSA spokesperson warns, adding that Nationwide's fine was not for losing the laptop but for the wider failings that this opened up.

With a growing number of internet-based transactions and applications, remote working and online portfolio management, it is crucial that systems have belt and braces in place.

After all, it's certainly better to be safe than £1 million sorrier. ■