Data Security Focus:
Protecting client data

In association with
The recent hacking of the personal and financial details of 2.4 million Carphone Warehouse customers was a high profile reminder that we live in a world where so much of our personal information is held by organisations with which we trade – and just how vulnerable it can be to determined criminals.

While relatively few breaches of data security have been recorded officially, it is thought that data loss occurs on a far more frequent basis than gets out into the public domain.

Adviser firms may not be high profile like Carphone Warehouse but they do hold considerable amounts of information and personal details on their clients. This can be in the form of physical records, documents and electronically held data. All of which is vulnerable to theft, misuse and loss.

Having a security strategy in place is essential and it must embrace every aspect of a firm’s data storage, no matter how or where it is kept. Where physical records are kept and used, having strictly upheld policies around storage and access and a clear desk policy, can help ensure that anyone accessing the building when staff are not around, does not have sight of confidential and financial information.

Where data is stored electronically, access can be restricted and controlled via password protection and by having a robust IT structure in place.

Often the chink in the security chain is human. Which is why criminals focus on phishing and email scams. Tricking a person into giving out details or even making a fraudulent transaction can be far more effective than trying to hack a system.

In this special report, a number of firms talk about how they deal with data security and we provide some take-aways from those conversations on page 9.

Rob Kingsbury, editor, Adviser Business Review
In an age of data misuse and identity fraud, keeping client information confidential is of paramount importance to financial advisers. Years of relationship building means advisers are privy to hundreds, if not thousands, of individual’s personal details and financial records; knowledge which could prove invaluable to others.

To safeguard their businesses, advisers are employing a host of different methods. Encrypted emails, a clear desk policy and third party security checks are just some of the ways adviser firms are investing in keeping their data secure.

Donald Reid, chief operating officer, Tilney Bestinvest, says the company has strict procedures and protocols in place.

“We take protection of client data extremely seriously and adhere to industry best practice. All our staff sign a standard non-disclosure agreement, which is issued by HR. We also perform an annual social engineering test, which is designed to...”

Donald Reid, Tilney Bestinvest
“We are careful to restrict what action employees can perform... in many cases, information is provided on a view-only basis”
measure the effectiveness of our security and employee discretion, and incorporates on-site and electronic based exercises,” he says.

Employees wishing to print a document must swipe a security card at the printer to collect their papers, ensuring that no other member of staff can view the document. And, like many advisory firms, Tilney Bestinvest also operates a clear-desk policy, which is set at executive level and stringently enforced.

Reid says: “Desk inspections take place regularly. I will often go round the office, once staff have left for the day, to ensure no confidential data or company-sensitive information is lying out on a desk. If we do find something, a discussion would immediately take place with the employee in question and if it were to happen on two occasions it would be deemed a disciplinary offence.”

Ensuring employees are fully aware of the FCA guidelines and individual data protection rights is key in avoiding a breach in confidentiality.

Patrick Connolly, Chase de Vere
“All employees must pass a competency test to ensure they know exactly what they should do and the implications of getting it wrong”
Patrick Connolly, head of communications, Chase de Vere, says: “All employees receive annual training on data protection and must also then pass a competency test to ensure they know exactly what they should do and the implications of getting it wrong.”

Connolly says educating employees is part of Chase de Vere’s "robust policies on data protection issues”, including breach reporting and management, client authentication and verification, and a clear desk policy.

**GOING PAPERLESS**

Some advisers, however, have taken the clear-desk approach a step further and banished paper altogether. So-called ‘paperless’ offices are growing in popularity among firms, with many praising the operational efficiencies and extra security it provides. Developments in technology mean advisers can now store all of their clients’ data electronically, making it only accessible online to authorised staff.

Carl Lamb, managing director, Almary Green, made the decision to go paperless in 2006.

**Carl Lamb, Almary Green**

“It’s a big commitment, but I would say we have more than got our money back. You need to invest in your own firm if you’re going to grow the business”
“There were four key reasons we opted to go paperless; storage, development of the business, ease of data and data security. The need to ensure client data is easily accessible and secure is absolutely vital in this industry,” he says.

Almary Green spent close to £45,000 on the six-month project, but says the cost was justified: “It’s a big commitment, but I would say we have more than got our money back. You need to invest in your own firm if you’re going to grow the business and take it forward.”

Transferring to online has been welcomed by clients, Lamb says, with many requesting access to documentation at short notice.

It is an opinion shared by Jason Witcombe, director, Evolve Financial Planning, who says clients are increasingly expecting their records to be held electronically.

“We operate a paperless environment and have done since we set up in 2004. It feels a much
more sensible approach than contending with storage issues. All documents sent to our office are scanned and saved online, which means I can log into my client’s records wherever I am in the world.”

Witcombe says every single piece of documentation, email and meeting notes related to each client is saved in their individual record and is password-protected.

Tilney Bestinvest also offers part of its proposition as paperless, with clients given the option to view their account online, but Reid says there remains an expectation for paper documents among some clients, especially those with significant accounts, and believes the move towards a paperless industry will be gradual.

ONLINE SECURITY
Of course, making the transition to online brings with it a different set of risks. To date, emphasis has been placed on compliance and protecting client assets, but advisers now have to contend with the responsibility of preventing online security breaches.

Lamb says: “With everything centrally stored, your database becomes a very powerful hub and you need to ensure you have incredibly strong IT support in place. It’s vital to us that data is kept safe at all times; we carry out regular testing of the system to ensure no external forces can access it and we keep everything encrypted.”

Almary Green hires an external IT company to ensure its technology runs smoothly and securely.

Lamb says: “It’s an extra cost you have to factor in, but it’s all about having peace of mind and ensuring your business runs smoothly. If something went wrong, it poses a huge reputational risk.”

The 2014 Information Security Breaches Survey revealed almost three quarters of all UK large businesses were affected by viruses or malicious software in 2013, and 16 per cent reported a theft of confidential data by external hackers. The financial cost of those breaches soared compared to the previous year as attacks grew more sophisticated.
As such, access and permission rights to information need to be carefully defined. Almary Green grades employees and their visibility of client information is dependent upon their rating. It is an approach familiar with many advisers.

Reid says: “We are careful to restrict what action employees can perform – in many cases, information is provided on a view-only basis.”

Tilney Bestinvest undergoes frequent third party security checks to ensure personal information cannot be hacked and says any client data accessible on a mobile is always encrypted.

Increasingly, clients will expect enhanced levels of protection, and advisers will have to ensure their data management and security systems deliver.

Witcombe says: “Inevitably, there is a risk with everything you do, be it paper or electronic. The key is to be very vigilant and ensure the server you use has the most up-to-date anti-virus software, firewalls and regular back ups.”

Email communications remain the most vulnerable, he says, and the company is especially attentive in looking out for fraudulent emails.

“Insurance companies have flagged the dangers of fraudulent emails to us and it is an area we are very strict on. If we receive a request to transfer funds to a different bank account to the one we have registered, we would not do so without further checks and client verification,” he says.

As hackers grow more advanced in their attacks on data, so too must advisers’ technology to keep their clients’ personal information safe.
TAKE AWAYS FROM THIS SPECIAL REPORT

Tilney Bestinvest has all staff sign a standard non-disclosure agreement and employs an annual social engineering test, designed to measure the effectiveness of security and employee discretion.

Implementing a clear desk policy will help ensure that no confidential information is accessible to non-authorised staff after hours.

Regular training and refreshers on FCA guidelines and individual data protection rights can also help prevent potential breaches.

Online data can be restricted to authorised staff only through password protection and to view-only where appropriate.

But electronic storage brings its own risks from hacking and phishing attacks, which are growing ever more sophisticated. A security breach poses huge reputational risk. Up-to-date anti-virus software, firewalls, regular back-ups, and encrypted emails and third party security checks can all help to prevent a breach.

Insurance companies are flagging fraudulent emails as potential areas of concern. Staff need to be reminded to stay vigilant around these attempts to access data and firms need to have processes, procedures and training in place to help prevent members of staff unwittingly giving away information or transferring funds in response to these often sophisticated scams.