ONCE MORE
UNTO THE BREACH

An extract from Perspective:
The fraud and identity issue
Essential insights into the issues facing your industry today
David Higginson, ID & Fraud Consultant at Equifax, outlines the risks that regulated firms face around securing sensitive customer data and what they should do to protect themselves.

Once more unto the breach

Not a week goes by without another incident hitting the press where confidential consumer information has been hacked or brought out into the public domain. Why are these incidents so common?

The answer is because sensitive personal information, like names, addresses, dates of birth and bank details, is highly prized by the criminal community: they’re proverbial gold dust. Just a limited subset of this information will provide enough detail for criminals to commit a wide range of financial crimes, from out-and-out fraud (e.g. bogus loan applications) to sophisticated money laundering operations.

Such is the availability and demand for this information that within the dark and murky corners of the web are forums and marketplaces that specialise in the sale of this data, often at relatively modest prices.

How the hackers work

So, how do these data breaches occur? Through a variety of means – some very sophisticated, others less so. At the larger end of the scale were the 2013/14 hacking incidents involving a well-known US email provider, which illustrates the scale of the problem, when 1.5 billion email addresses were compromised in the largest breach ever seen. This provided the criminal network, behind the hack, with enough sensitive customer information to commit fraud on an industrial scale. Just think about how much information flows through a typical person’s email account(s), and how key this is to the running of their everyday life. It may contain details of who they bank with, who they shop with, details of their friends, family and associates.

Other methods employed include the use of malicious computer programs (malware), specifically designed to steal or copy confidential information, such as online banking credentials. We have also seen a rise in the use of phishing emails designed to trick consumers into disclosing sensitive information by being directed to bogus websites. Phishing, as it’s known, is just another means of social engineering, where fraudsters attempt to psychologically manipulate either consumers or staff within organisations to persuade them to release confidential information.

Digital danger

When it comes to cybercrime, this is low-risk, high-reward territory for the organised gangs involved, which is why this type of crime has seen a surge in recent years. The challenge for law enforcement agencies is the speed and size of these attacks and the complexities of bringing to justice organised criminal groups who may be spread across a number of different legal jurisdictions. What’s more, there is also evidence to suggest that some of these attacks are actually state-sponsored.

The digital age has brought about great changes in how the world operates, and allows customers much greater flexibility in how they communicate and interact with their bank or service provider. However, advances in technology have also exacerbated risks, in that vast amounts of data can be easily stored but also easily compromised. The price of data storage has dropped significantly in recent years and portable storage devices, like USB sticks, are now commonplace.

Additionally, the rise of cloud computing has offered both businesses and consumers an easier and more flexible method of storing significant amounts of data using remote servers, all of which are at risk, unless access is sufficiently controlled. It’s a real challenge for firms to adequately control and protect all of their digital assets, some of which are held across multiple sites within different geographies.

But remember, whilst computer-aided crime has seen exponential growth over the last few years, data lost through more routine, low-tech methods can be just as damaging. A method still favoured by criminals is the interception of post, whether by setting up a fraudulent mail redirection facility or the direct theft of letters from letter and post boxes. It may be that a single up-to-date bank statement and utility bill is all that is required to assume another person’s identity to go on to commit all manner of other crimes.

It’s also worth noting that the risk of data loss is not just consigned to external groups. There is a significant fraud risk associated with individuals within an organisation, whether employed on a full time basis, or perhaps as contractors. These staff members may have access to significant amounts of sensitive consumer data and may be tempted to commit fraud due to external pressures like money worries, high levels of debt, gambling addiction and more.
Both data protection and industry regulators have long understood the link between poor data security and financial crime. The FCA, in their most recent Financial Crime Guides, spell out in detail what it expects of firms in this area and what it constitutes as best practice. This is laid down in overarching requirements contained within the heading of ‘Systems and Controls’ in that it requires firms to have adequate safeguards in place to counter the risk that it might be used to further financial crime. Senior management within firms is under a specific obligation to mitigate these risks.

Protecting data

So, bringing these threats together, how can firms control and protect sensitive customer information? There are probably too many potential solutions to go into detail for the purposes of this article, however, a robust Information Security Framework should be established to include the following elements:

Culture – It starts with the ‘tone from the top’. Senior management is expected to set the standard and should make it clear to all staff the importance of data security within the firm and what part they play in keeping customer data confidential.

Training and awareness – Senior management needs to ensure that all staff are aware of the ways in which data can be compromised and the reporting procedures should there be concerns or a breach identified. This also extends to ensuring customers are made aware of the most common methods that fraudsters will use to steal their information. Some firms are offering their customers free antivirus software in order to protect their machines.

Governance – Firms should define the roles and responsibilities for both the operational and IT elements of the organisation, along with clear reporting lines.

Risk management – Consider all aspects of the business where data could be rendered insecure and where the highest risks lie. These assessments should be carried out using up-to-date and accurate management information. Firms should be prepared to reassess these risks continually, particularly where new or emerging threats surface.

System and Controls – Once threats have been identified, suitable checks and balances need to be put into place. Examples include the controls required to protect digital assets, secure disposal of data, data protection policies, physical access controls, incident response plans and more. These systems and controls need to be documented and tested at regular intervals to assess their effectiveness, whether this is done internally or carried out by third party advisers. Has the firm been affected by a data breach in the past and if so, has it learnt from previous mistakes?

These are challenging times for regulated firms when it comes to data security and minimising financial crime – often it’s an arms race between organisations and the criminal gangs looking to steal customer information. One thing is for sure, it’s a challenge that is not going away and is subject to continual change. Get it wrong, and the consequences for firms could be far-reaching.

To find out more, contact David on 07771 856 848 or by emailing david.higginson@equifax.com.

Idea in brief

THE SITUATION
Rarely a week goes by without another incident hitting the press where confidential consumer information has been hacked or brought into the public domain. Why are these incidents so common?

THE CHALLENGE
Both data protection and industry regulators have long understood the link between poor data security and financial crime. Senior management within firms has a specific obligation.

THE TAKE AWAY
These are challenging times for firms when it comes to data security and minimising financial crime. To control and protect sensitive customer information a robust Information Security Framework needs to be established.