Every 19 seconds – the cyber threat

Cyber crime has arguably been the pre-eminent emerging threat of the last decade, but new legislation across Europe threatens to make cyber issues even more pressing as regulators wake up to the fact that changes in data privacy laws are required.

President Barack Obama’s US administration and the European justice commissioner, Viviane Reding, are both proposing new national and cross-border data breach notification and data privacy laws. These will have a major impact on companies, forcing them to notify regulators and consumers every time a data breach occurs, even if no records have been accessed.

But what are the cost implications? The EU data privacy proposals include fines of up to two per cent of global annual turnover if a company breaches the proposed data laws, a requirement for companies with over 250 employees to appoint a data protection officer, and for all breaches to be reported to the regulator – ideally within 24 hours. These regulations present a significant new burden for risk managers.

Compliance headache
The exact changes are still at least two years off, requiring approval from EU member states and ratification by the European parliament. However, one certainty in this complex and fast-moving area is that data breaches are becoming more common and dealing with them increasingly costly, complex and damaging for the organisation that owns the data.

It is has become apparent that there is not going to be a ‘one size fits all’ solution to the problem. The end result is a headache for international companies attempting to comply with, or anticipate
Learning the hard way

Sony
Earlier this year Sony discovered that 77 million PlayStation network and Qriocity (its entertainment network) user names, email addresses, phone numbers and – reportedly – credit card details had been maliciously breached. The first breach was followed by a second of the personal details of its 24.6 million Sony online entertainment customers. The breaches led to a 23-day closure of the PlayStation network, with Sony suffering an estimated loss of $171 million excluding any subsequent lawsuits. The costs do, however, include the cost of notifying and assisting customers, IT forensic costs and system overhaul as well as reputation management. The Sony brand suffered and its share price dropped 55 per cent in just four months as a result of the breach and resulting negative publicity.

Estimated financial loss: $171 million
Fall in share value over four months: 55 per cent

TJX Companies
In 2007 TJX companies - the parent company for TJ Maxx in the US and TK Maxx in the UK - discovered it had been using an unsecured wireless network for around 18 months. During this time a hacker accessed over 45.5 million credit and debit card numbers, and the personal data of 451,000 shoppers. The cost of client notification, IT system overhaul, business interruption, fines, credit card repayments and legal costs is estimated to have been over $1 billion.

Estimated financial loss: $1 billion
Number of records accessed: 45.5 million

the law, and for risk managers trying to advise on best practice.
The EU is now considering how firms intend to comply with the requirement to notify, and what type of breaches should require notification. It also wants to find out more about cross-border breaches and compliance obligations.

Myriad of methods
Individual European countries have their own varying regulations. For example, Germany, Austria and Norway have national laws which require mandatory notification of data breaches. The UK and Ireland have codes of practice on personal data security breaches but no mandatory client notification, while Finland and the Netherlands are pushing to have mandatory notification laws in place. Cyprus, the Czech Republic, Estonia, Sweden and Hungary currently have non-mandatory laws which imply a duty to notify.

In the UK, organisations are expected by the Information Commissioner’s Office (ICO) to report all serious data breaches. The ICO also requires organisations that process personal data to take strict protective and precautionary security measures and, if these measures are found wanting, it has the power to impose fines of up to £500,000 for data loss. The Financial Services Authority (FSA) has the power to issue fines (which have been known to run into millions of pounds) on any financial services company deemed to have put customers’ data at risk.

In the US there is no single law covering data privacy – but the Obama administration has recently announced support for a federal privacy and national data breach notification law. Laws and regulations currently vary by state. The vast majority (46) of states have laws which impose mandatory data breach notifications on organisations. US law also states that the responsibility for protecting sensitive data lies with the data owner.

A matter of time
Norton’s Cybercrime Report for 2011 estimates that stolen cash and the time spent on identifying and resolving data breaches to businesses and governments costs around $388bn globally.

And Lockton’s latest report, Cyber risks decoded: a report on data risks, the law, risk mitigation and insurance, found that an individual falls victim to a type of cyber crime every 19 seconds.

Andrew McClelland, chief operations and policy officer at IMRG, says “it is only a matter of time before a major UK retailer suffers a serious data breach”. He adds: “Given the current economic climate, data protection is not as high up the corporate risk agenda as it should be. It will take a major incident to force boards to concentrate, because this would undoubtedly lead to a fall in consumer trust. This would alarm shareholders and senior managers and make cyber risk an agenda item at board meetings.”

McClelland adds: “Insurance is not yet seen as a critical priority unless retailers have already suffered a cyber attack.

“However, I anticipate that this situation
may be about to change as legislation across the EU is moving towards mandatory client notification, as has been the case in the majority of the states in the USA for several years."

**Not keeping quiet**
Research shows there are a number of commonalities between data breach incidents and that many systems are easy to breach. Breaches are often discovered by third parties, not the data owner, suggesting that online security and risk management measures are often not up to the required standard.

Criminals looking to steal and exploit data for financial gain appear to be in an increasingly strong position. Not only does new technology and growing access to technology provide ever more opportunity, but governments and private enterprises are aware that they can no longer keep quiet about data leaks and malicious attacks.

While it is good to keep the public informed, any release of information on the nature and extent of cyber attacks and how to prevent them also educates the fraudsters, raising the threat level.

**Insurance solutions**
And as the frequency and severity of cyber data risk increases, so the insurance world is becoming more concerned about the financial risks associated with a data breach and cyber crime.

There is a growing insurance market for both first and third party data liability business, and also first party business interruption cover. These products and covers are likely to continue to develop over the coming years.

Ben Maidment, an underwriter in the global markets team at Brit Insurance, says: “Risk managers have started to recognise the potentially huge cost to their business that data breach events present and the value of purchasing insurance for such a scenario, not solely for the risk transfer but also to access insurers’ specific expertise and specialist vendor relationships to respond to breach events quickly and cost effectively.”

Malcolm Randles, an underwriter at Kiln Group, says insurers will look to work with firms that take data breach and cyber risk seriously. He says: “What we want to see is that the company has the appropriate risk management procedures to deal with that particular sector’s risks and regulatory requirements. We look at all aspects – kick the tyres and lift the engine hood – when assessing if we want to take a risk on or not.”

Iain Ainslie, an underwriter at Ace Group, agrees. He says: “We want to be reassured that there is a strong compliance culture that runs right through our clients’ organisations. All employees need to be aware of the risk as human error still plays a big role in most breaches, so ownership by key stakeholders is vital.

“We also like to see evidence that the IT department is sophisticated and switched on. For example, sophisticated hackers know that Microsoft releases its anti-virus patches on Tuesday evenings – so the hackers work over Tuesday night to amend their viruses to work around the new patches.”

With data breaches estimated to have cost over $600 million between 2008-10 in the US alone, one thing is for certain: the changing compliance climate for data breaches and the potential insurance solutions are something that risk professionals and organisations need to address sooner rather than later.

Lockton says:
“Data privacy is, and will continue to be, the biggest emerging risk for businesses in the 21st century. Any company that does not put appropriate risk management and mitigation measures in place to deal with a potential data breach will suffer significant financial loss and irreversible damage to their brand reputation. However, companies that do plan for a breach, have robust risk management measures and systems in place and respond in a responsible and appropriate manner can emerge from a data breach incident relatively unscathed. Insurance can provide essential financial assistance and access to highly experienced legal, IT forensic and crisis PR advice – which can help companies preserve reputation and get back to trading as rapidly as possible.”

Sponsored by Lockton says:
“Data privacy is, and will continue to be, the biggest emerging risk for businesses in the 21st century. Any company that does not put appropriate risk management and mitigation measures in place to deal with a potential data breach will suffer significant financial loss and irreversible damage to their brand reputation. However, companies that do plan for a breach, have robust risk management measures and systems in place and respond in a responsible and appropriate manner can emerge from a data breach incident relatively unscathed. Insurance can provide essential financial assistance and access to highly experienced legal, IT forensic and crisis PR advice – which can help companies preserve reputation and get back to trading as rapidly as possible.”
Little angers customers more than learning their personal data has been unwillingly shared. Risk Management Professional looks at the steps businesses can take to minimise the threat.

W

ith some of the world's biggest organisations subject to successful cyber attacks, businesses' attempts to protect data from online criminals can seem futile at times, especially when poor compliance or shoddy procedures can be to blame. So what options exist for anxious businesses?

Organisations are increasingly at risk - whether it is cyber-extortion or denial of service (DoS) attacks, or hacktivism or human error - with more and more sensitive data stored on a computer system somewhere in our interconnected world.

IRM's Professional Development Forum, taking place in Manchester, UK, on 23-25 April, will feature a seminar on cyber risks featuring case studies and scenarios on data loss, content issues and exposures.

David Canham MIRM, chairman of IRM's risk in information systems and e-business special interest group (RISE SIG), and Aviva UK IT risk manager, says there are two angles to the issue – the risks and public expectation of how companies manage data.

Waking up to reality

He tells Risk Management Professional: “Organisations should ensure they are confident that they have done the basics – the hygiene factors, such as payment card industry (compliance) and ensuring virus software is up-to-date – but then there is the new breed of mobile working that is of real concern”

In terms of the public, Canham says there is a distinction between anxiety and expectation. He says: “Do people worry – absolutely. Are people more accepting of it? I think those aged around 18 to 25 realise that we live in an increasingly digital age.”

Data directive

The European Data Protection Directive proposals call for data to be used by businesses with transparency, legitimate purpose and proportionality, and the US administration is said to be looking at similar measures.

The directive calls for each member state to set up a supervisory authority - an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated.

Costly threat

According to the European Commission, the executive body of the European Union, the directive should benefit European businesses by unifying the current fragmented legislation. A firm conducting business across multiple European territories currently has to comply with several different interpretations of data privacy, whereas the directive should bring a level playing field – and estimated savings of €2.3 billion per year.

And this is an area where firms cannot afford to make mistakes. One of the commission's research papers, Attitudes on data protection and electronic identity in the European Union, found that most (51 per cent) Europeans think that companies breaching data protection rules should be fined, banned from using such data in the future (40 per cent), or compelled to compensate the victims (39 per cent).

Future-proofing

While data protection will continue to be a difficult challenge, one proposal for businesses from the commission is for firms to carry out data protection impact assessments (DPIA) to ensure effective compliance with data protection rules.

Beyond that, businesses can also consider measures such as outsourcing data protection work to vendors, but the legal and regulatory liability primarily remains with the data owner.

The bottom line is that the data privacy risk, while significant and growing, appears best managed through a combination of insurance options, due diligence, and adherence to contractual and regulatory requirements.
As every business sector changes significantly through the growth of the internet and network-based technologies, Lockton’s Global Technology and Privacy Practice has expanded its risk transfer solutions across a range of industries including technology, hospitality, financial services, retail and healthcare.

Lockton provides experience, advice, and insurance solutions for:

Security & Privacy Liability
Network Interruption
Technology Errors & Omissions
Media Liability

For more information, contact:
Ben Beeson on 020 7933 2857 or email: ben.beeson@uk.lockton.com

Scan to learn

www.lockton.com