Are you cyber secure?

Davinia Brennan, Associate at A&L Goodbody, gives some practical strategies for avoiding data breaches, and mitigating damage if they do occur

Due to the increasing frequency and scale of attacks, cyber security — as well as continuing to grab headlines — is featuring high on company boardroom agendas. Boards are recognising the need to be proactive, rather than reactive, in safeguarding their companies against cyber risks. As cyber-crime 'follows the money', financial services, particularly banks, are an obvious target. Major retailers have also found themselves victim to significant data breaches. However, any company that has a significant cash flow and stores personal data is at risk of cyber-attack.

Due to the newness of cyber risks, there remains some uncertainty as to how best to prepare for, and deal with them. In fact, recent research by the UK government found that 22% of small businesses admit they "don't know where to start with cyber security".

What is cyber security and why is it important?

Cyber security is about protecting computer-based information from unauthorised access, alteration, disclosure or destruction. Doing business on the internet brings risks, and there has been a continuing flurry of attacks on the IT systems of companies seeking to steal information and money or disrupt businesses. Information is an asset that can take many forms, including client lists, customer databases, employees' financial details, customers' financial details, deals that the organisation is involved in, pricing information, product designs, or manufacturing processes.

Cyber security is important because a successful cyber-attack can cause massive damage to a business, including data loss, intellectual property theft, business interruption, financial loss, reputational damage and loss of consumer confidence, compensation claims and regulatory sanctions or fines.

Whilst the majority of high-severity losses are caused by deliberate malicious acts, companies should be aware that employee negligence is the leading cause of data breaches. The last Annual Report of the Data Protection Commissioner (published May 2014) shows that the ODPC dealt with 1507 data security breach notifications in 2013, with almost 1100 caused by human error. Accordingly, companies need to ensure security investments are not just aimed at new technologies preventing cyber-attacks, but also on fostering a company-wide culture of awareness of cyber and data security.

Nothing can guarantee protection against security breaches, but data controllers can certainly reduce the likelihood of a breach or mitigate its adverse effects, if they take basic administrative and technical security measures. Cyber security is becoming a business necessity, with most businesses now demanding that their suppliers are secure.

The Target breach — lessons to be learned

There have been numerous high profile security breaches both at home and abroad. However, the mega data breach suffered by Target in the US in 2013, which compromised 70 million customer accounts and 40 million credit and debit card accounts, is a particularly good example of the consequences of being inadequately prepared for a cyber-attack.

Supply chain risk — Whilst most large firms have taken efforts to make themselves cyber secure, an organisation is only as strong as its weakest link, and so remains exposed to cyber risks via third parties in its supply chain, who may not have taken adequate, or any, cyber security measures.

The Target breach allegedly occurred due to a third party air conditioning contractor of Target, who had access to some of the Target network, being subject to a phishing email. The hackers were then able to break into Target's network using login credentials stolen from the air conditioning contractor, and access the credit card details of Target customers. This shows the importance of organisations carefully scrutinising their supply chain connections when assessing their cyber security risks, and ensuring third

(Continued on page 6)

(Continued from page 5)

parties have appropriate security measures in place.

Educating employees — The Target breach also shows that having cyber security software in place is pointless if employees are not adequately trained in relation to cyber risk, and there is no data breach incident plan or procedure in place. The Target breach was detected by its malware detection system and its head office was allegedly notified on two occasions of suspicious activities, but the warnings were not acted upon.

Costs — The costs of dealing with a breach should not be underestimated.

Target has stated that the costs associated with its data breach totalled $252 million as of the end of January 2015 (which would be partly offset by an expected $90 million in insurance policies). This includes the costs of defending or settling legal actions against it. In March 2015, a US court gave preliminary approval to a $10 million settlement of a class action to enable customers affected by the breach to be awarded up to $10,000 each in damages.

Reputation — Target's breach shook consumer confidence in the retailer and executives have said that it had a noticeable effect on the bottom line.

Board level oversight —The breach shows the potential for board members to be held accountable for security breaches where they fail to provide effective oversight. The CIO and CEO both resigned as a result of the breach, and a report for shareholders of the company recommended that 7 of the other 10 members of the Board should also be replaced. This highlights the importance of Boards staying informed of cyber risks and being proactive to ensure that appropriate mechanisms are in place to deal with them.

> ***"The Target breach also shows that having cyber security software in place is pointless if employees are not adequately trained in relation to cyber risk, and there is no data breach incident plan or procedure in place."***

Preparing for cyber risk

Having an effective cyber risk strategy in place can help a company preserve its reputation and mitigate the adverse effects of a breach. Below are some steps which might be taken to prepare for cyber risk.

Cyber Risk Assessment — Companies should start by identifying their key information assets and their vulnerability to attack. The most important data needs the highest level of protection and the most strictly limited access.

Cyber Security Legal Obligations — Companies are legally required to take 'appropriate security measures' against 'unauthorised access to, or unauthorised alteration, disclosure or destruction of data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing' (Section 2(1)(d) of the Data Protection Acts 1988 and 2003 ('the DPAs')).

In determining what 'appropriate security measures' are, companies may have regard to the state of technological development and the cost of implementing the security measures, and must ensure that the measures taken provide a level of security appropriate to the harm that might result from a data security breach and the nature of the data concerned (Section 2C of the DPAs). Companies should also consider applicable industry technical standards.

In addition, companies are obliged to take all reasonable steps to ensure that employees and others at its premises are aware of and comply with the relevant security measures.

Cyber security policy — Having a written cybersecurity policy, dealing with how to keep data safe and how to respond to security incidents, is essential. It will also help demonstrate a commitment to compliance with data security obligations in the event of any subsequent regulatory investigation.

The policy should be easily accessible, so that employees are aware of their data security obligations. Data controllers should also ensure that third parties in the supply chain which handle data are aware of security policy requirements.

Ideally, the policy should set out the organisation's governance structure, to enable cyber risk management across the organisation and ensure board level engagement with cyber risk, including a board level owner for cyber risk. It should also contain policies and procedures dealing with the following:

- staff training;
- home and mobile working to ensure mobile devices are used securely and the safety of company data is not jeopardised;
- removable media storage device controls, limiting their use and the type of information which can be stored on same;
- incident response plans (discussed further below);
- access controls, particularly in regard to sensitive information and audit trail monitoring;
- monitoring of network traffic for unusual activity;
- secure configuration settings of all IT equipment;
- malware prevention; and
- network security.

Security breach incident response plan — It is vital that organisations

have a clear plan of action to follow in the event of a security breach incident. It should be similar to a fire drill and practised like the same, so that companies can understand quickly what has happened, how it happened, the type and extent of data compromised, and who has been affected. This will help the company to decide upon what type of response is required.

Cyber Security Officer/Team — It is important to be clear about who in the organisation is responsible for cyber security, and have a solid security breach team in place, who have the skills and expertise to address the range of breaches that might occur. Large companies, in particular, need to ensure that no time is lost due to confusion over who is responsible for making executive decisions in response to a breach.

The team should ideally include a designated board level member responsible for oversight of cyber risks, and/or another designated senior executive(s), key IT personnel and internal/external legal counsel (to ensure legal privilege over the internal investigation and in preparation for any legal action which might emerge such as compensation claims and regulatory investigations).

Third party breach partners might also be identified ahead of an incident, to ensure they can be engaged quickly, such as forensic consultants to assess and remedy the breach; a PR agency to advise on reputation management and assist with media communications, and credit monitoring services to monitor financial and credit data.

Cyber insurance — Organisations should consider investing in cyber-insurance. Increasing awareness of the costs of dealing with cyber-attacks and data breaches has led to more businesses taking out cyber insurance policies; however there has been no real boom yet. The benefits of cyber insurance include access to a network of data breach experts.

According to the UK government's report, 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk' ('the Report') (www.pdp.ie/docs/10088), only 2% of large UK businesses and practically no small businesses have cyber insurance in place. The Report notes a significant gap in awareness around the use of cyber insurance, with 52% of CEOs believing they have cyber risk cover, whereas less than 10% actually do.

The Report highlights, however, that whilst cyber insurance provides solutions for a broad range of cyber risks, some important risks are difficult to insure or completely uninsurable. For example, insurers may not cover direct losses from intellectual property theft (i.e. compensation for the value of the IP asset compromised or the lost revenues as a result of diminished market share) as such losses are difficult to prove and quantify. Though some insurers will provide legal expenses cover for the pursuit of claims against third parties that are infringing the organisation's intellectual property.

Develop a relationship with the Data Protection Commissioner ('DPC') — Having a good relationship with the DPC and keeping an open line of communication should ensure you have a faster and smoother response to any breach.

Dealing with data security breaches

In Ireland, there is no legal obligation to notify the DPC or affected data subjects of a data security breach, except in the electronic communications sector. However, the DPC has approved a non-binding 'Personal Data Security Breach Code of Practice' (www.pdp.ie/docs/10089), which recommends reporting security breaches to the DPC within two working days. The only exception to the Code's notification requirement is where the data subjects have already been informed and the loss affects less than 100 data subjects and involves only non-sensitive, non-financial personal data.

The Code also encourages organisations to give immediate consideration to notifying affected data subjects of the breach, except where there is no risk to personal data due to the adoption of technological measures that make the data inaccessible. Whilst it may be beneficial for customers to be informed of any breach affecting them as soon as possible, there is a danger of over-notifying and causing undue anxiety and concern. Accordingly, depending on the circumstances of the breach, it may, on occasion, be appropriate to wait for precise details of the loss and the remediation plan.

The Code also requires organisations to consider notifying third parties such as An Garda Siochána, or financial institutions, who may be in a position to assist in reducing the risk of financial loss to individuals.

Articles 31 and Recital 67 of the draft EU Data Protection Regulation, as adopted by the European Parliament in March 2014, propose mandatory breach reporting of data security breaches to national regulatory authorities without undue delay, and not later than 72 hours of becoming aware of the breach. Article 32 further requires individuals to be notified where the breach is likely to have an adverse impact on their rights or legitimate interests.

Regulatory sanctions for data breaches

In Ireland, the DPC does not have the power to impose fines for data breaches, nor is it an offence per se to fail to implement 'appropriate security measures'. Rather, the DPC will review the breach notification, and may require the organisation to submit a detailed report. Depending on the nature of the breach incident and the security measures in place, the DPC may also decide to investigate the breach. If necessary, the DPC may further serve an Enforcement Notice requiring the organisation to take certain steps to limit the adverse effects of the breach, such as notifying customers of the breach. Failure to comply with such a notice is an offence, for which an organisation can be prosecuted by the DPC. An organisation may be liable,

(Continued on page 8)

(Continued from page 7)

on summary conviction, to a fine up to €3,000, and on indictment, to a fine up to €100,000.

Organisations across all sectors of the economy will soon be subject to severe sanctions for non-compliance with data security obligations or failure to notify data security breaches, as the draft Data Protection Regulation provides for fines up to €100 million or up to 5% of annual worldwide turnover (whichever is greater).

Compensation claims

Any individual who suffers damage or loss resulting from a data security breach can take civil proceedings against an organisation for breach of its legal duty of care in handling their personal data.

In *Collins v FBD Insurance* [2013] 137, the Irish High Court held that no matter how obvious the breach, it is necessary to show loss or damage from the breach, and damages are not recoverable for non-pecuniary loss. Feeney J. expressly stated: "an entitlement to damages for distress, damage to reputation or upset, are not recoverable save where extreme distress results in actual damage, such as a recognisable psychiatric injury".

However, more recently, in *Google v Vidal Hall* [2015] EWCA Civ. 311 (27 March 2015), the UK Court of Appeal held that pecuniary loss is not necessary, and data subjects can recover damages for distress. As decisions of the UK courts are of persuasive authority in Ireland, it remains to be seen whether the decision will open the floodgates here to distress claims against organisations in relation to data breaches.

Contractual and corporate responsibilities

In addition to the data protection concerns outlined above, a data security breach also raises the risk of breach of contractual obligations in relation to the protection of personal data and confidential information.

Contracts are a key means of preparing for cyber risk, mitigating the impact of cyber-attacks and enabling the recovery of losses caused by cyber-attacks. Contracts, for example, may provide for allocation of risk and liability in the event of a breach of cyber security, such as non-compliance with legal obligations or any confidentiality restrictions. In particular, contracts may provide for uncapped liability and/or indemnity protection for losses arising from IT systems and data being compromised.

Furthermore, companies should be aware that directors may be held accountable if it can be established that a cyber-attack or its consequences are attributable to breach of their fiduciary duty. Section 232 of the Companies Act 2014 (which comes into effect on 1st June 2015) requires a director to indemnify a company for any loss or damage arising from a breach of such duty.

In addition, section 29 of the DPAs provides for the prosecution of directors, or other officers of a company, where an offence is proved to have been committed with their consent or connivance or to be attributable to any neglect of their part. In late 2014, a number of private investigators were prosecuted under this section. These provisions demonstrate, once again, that cyber security is an important company boardroom priority.

Conclusion

Taking simple cyber security measures, such as adopting an efficient cyber security policy and data breach incident response plan, and educating staff on their cyber security responsibilities, makes good business sense. It will not only ensure compliance with legal obligations, but will ensure that assets, reputation and customers are protected too.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com