Cyber risk and cyber security — current state of play

Annette Hogan, Consultant, Technology & Innovation Group at McCann Fitzgerald, ***highlights recent cases and initiatives in the area of cyber security, before addressing the key question of how best to mitigate risk***

The number of cyber security attacks has increased exponentially in recent years. Barely a week goes by without a new breach being reported.

Yet studies suggest that many organisations are still failing to take the risk of cyber breaches seriously, leaving their most valuable information and assets vulnerable to attack.

This article examines a number of high profile security breaches and recent initiatives, highlights the relevant legal regimes and offers a series of risk mitigation measures to help reduce the likelihood and impact of a cyber attack.

The threat

The recently published UK government 2015 Information Security Breaches Survey highlights the extent to which security breaches are on the increase.

In 2015, 90% of large organisations suffered a security breach as compared with 81% in 2014. The cost of dealing with breaches also continues to soar with an average cost of 1.9m euro – 4.4m in 2015 compared with 850,000 euro – 1.6m in 2014.

Whilst a large number of attacks are due to external factors (69% in 2015), an even higher number originate from within the victim's organisation (75% in 2015), with a significant proportion of these (50%) arising due to human error.

Motivation for cyber attacks

The motivation for cyber attacks varies. Many are the result of organised crime, where the main aim is to steal financial details (e.g. credit/debit card details) with a view to committing fraud.

However, there is increasing evidence of attacks being carried out by sovereign states for international espionage purposes (e.g. a recent attack by Russia on the US Pentagon's systems).

A further potential motivation is terrorism, whereby attackers seek to disable critical infrastructure or services. Attacks may also be carried out by 'hactivists' (e.g. as in the Ashley Madison case) where the aim is to embarrass the company or highlight a particular moral or ethical cause.

One thing is clear: organisations should not underestimate the threat from within, for example from disgruntled or careless employees.

How are attacks perpetrated?

Attacks can be perpetrated in a variety of ways.

One typical approach is that the cyber criminal gains entry to a network and installs malware. The malware seeks out network vulnerabilities and alternative entry points, so that if one entry point is shut down it has an alternative means of access. Once reliable network access is established, the attacker starts to gather data (e.g. usernames, passwords, encrypted data, etc.). The data are then exfiltrated off network.

Often, all evidence of the cyber attack is removed, but the network remains compromised and the attacker may return to steal further data. Alarmingly, the average number of days attackers are on the network before being detected is 243, by which time the damage caused may be significant.

High profile attacks

Sony Pictures suffered a serious attack as a result of which sizeable quantities of intellectual property, corporate data and confidential emails were stolen. The breach was discovered in November 2014, but the network is believed to have been compromised for a considerable period prior to that. Over 100 terabytes of data were stolen, a substantial portion of which were published online. The cyber criminals (which are believed to have had assistance from an insider) used malware to wipe the system and cover their tracks.

US retailer, Target, suffered an attack on its point of sale systems, resulting in the theft of credit and debit card details of 40 million customers. In this case, commercial off-the-shelf malware was

(Continued on page 10)

(Continued from page 9)

used to perpetrate the attack, highlighting that cyber criminals with limited IT expertise can perpetrate highly damaging attacks. Target reported a 46% drop in profits for Q4 2013 as a result of the breach. The estimated cost of the attack (excluding lawsuits and reputational/sale losses) is approximately $148 million.

Former telecommunications giant Nortel suffered a breach whereby spyware was used to steal the passwords of the CEO and a number of other senior executives, resulting in the theft of technical documents, business plans, emails and research reports. It took 10 years from the initial attack to discovery, by which time the damage caused to Nortel's competitive position in the market was irreparable.

Data Protection Acts 1988 and 2003 ('DPAs')

Data protection professionals are aware that any cyber breach affecting personal data is likely to constitute a breach of the obligation in the DPAs to take appropriate security measures against unauthorised access to, alteration, disclosure, destruction or loss of personal data.

The DPAs do not specify what is appropriate in any given case, as security standards are continuously evolving and data controllers need to decide what is appropriate for their particular organisation.

However, the DPAs provide that regard may be had to: the state of technological development; the cost of implementing security measures; the sensitivity of the data; and the degree of harm that might result from unauthorised disclosure.

Data controllers are further obliged to have written contracts in place with their data processors (e.g. data back-up/hosting/other outsourced service providers), which oblige the data processor to only process data in accordance with the data controller's instructions and to comply with the security obligations in the DPAs. Companies should also reserve the right to audit those security measures to ensure they are adequate.

In the event of a data breach, the provisions of the Personal Data Security Breach Code of Practice (which applies to all data controllers and processors except telcos and ISPs) will apply.

Subject to certain limited exceptions, the Code requires the Office of the Data Protection Commissioner ('ODPC') to be notified, within 2 working days, of any incident where personal data have been placed at risk of unauthorised disclosure, loss, destruction or alteration. The ODPC may require a detailed report of the incident, as well as requiring notification of data subjects and remediation of any security deficiencies.

The sanctions for breach of the DPAs are mainly civil and include: the issue of an enforcement notice (with which failure to comply is an offence); naming and shaming in the DPC's Annual Report; deletion of data; increased likelihood of DPC audit; and damages claims by affected data subjects based on breach of the duty of care in the DPAs.

The DPC does not currently have power to levy fines against non-compliant organisations, but this is likely to change when the General Data Protection Regulation is enacted. Under the draft Regulation, fines of up to the greater of 5% annual worldwide turnover or €100 million have been proposed.

It is relatively unusual for the DPC to proceed directly to enforcement proceedings in the context of a security breach. However, following a cyber attack in late 2013, Loyalty-build's security deficiencies were considered to be so egregious that immediately following notification of the incident, the DPC issued an enforcement notice preventing all forms of data processing until such deficiencies were rectified.

Other reporting obligations

Telecommunications companies and internet service providers are generally obliged to report security breaches to the DPC and to data subjects under the EC (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the 'e-Privacy Regulations').

The reporting requirements are similar to those under the Personal Data Security Breach Code of Practice, save that failure to report the breach is a criminal offence under the e-Privacy Regulations.

Currently, there is no specific legal requirement for entities regulated by the Central Bank of Ireland to notify the Bank of any security breaches. However, this is recommended as a matter of best practice on the basis that any failure to take appropriate security measures could be construed as a breach of the duty to act fairly towards customers in the Consumer Protection Code 2012, or a breach of the customer terms and conditions (e.g. where the regulated entity has represented that it will keep customer data secure).

Recent guidance issued by the Bank (discussed further below) also provides that serious security incidents should be reported to the Bank. Potential sanctions include fines, negative publicity, damages claims and complaints to the Financial Services Ombudsman. US financial services company Standard & Poor also indicated recently that security breaches may result in negative ratings action against the relevant institution.

Directors' duties

Directors are subject to a number of duties to their company under the Companies Act 2014. A number of these duties could be construed as requiring the directors to take appropriate steps to protect the company against cyber attacks, including duties to: act in good faith in the best interests of the company; act honestly and responsibly in relation to the conduct of the affairs of the company; exercise the same degree of skill, care and diligence as a person having similar knowledge and experience would in the same circumstances; and act in the best interests of the employees,

shareholders and creditors of the company.

Where a cyber breach is shown to have arisen as a result of a director's breach of any of these duties, the director may be required under the Companies Act 2014 to indemnify the company for any losses arising as a result of the breach.

Criminal liability

Various criminal offences may be committed in the process of carrying out a cyber attack.

The Criminal Damage Act 1991 creates separate offences of causing damage to a computer and unauthorised access to a computer.

The Criminal Justice (Theft and Fraud Offences) Act 2001 makes it an offence to dishonestly operate a computer (from inside or outside the State) with intent to make a gain or cause loss.

It is an offence under the DPAs to knowingly access and disclose personal data without the authority of the data controller or data processor, Further, an offence will be committed under the Postal and Telecommunications Services Act 1983 (as amended) if a communication is unlawfully intercepted in the course of transmission.

The victims of cyber attacks may also commit certain offences in relation to them. For example, failure to report certain cyber crimes to the Gardai (e.g. damage to computer, dishonest operation of computer) is an offence under the Criminal Justice Act 2011. The directors of a company may also be guilty of an offence, punishable by fines of up to €100,000, where a contravention of the DPAs has occurred (e.g. failure to comply with an enforcement notice) with their consent or connivance, or due to their neglect.

The government will shortly publish the Criminal Justice (Offences relating to Information Systems) Bill. This will enable ratification of the 2001 Council of Europe Convention on Cybercrime (Budapest Convention) and transposition of EU Directive 2013/40 on attacks against Information Systems. This is a welcome development as the criminal law in this area is currently piecemeal and, in many cases, outdated.

"Any company considering cyber insurance should assess the risks which are specific to its organisation, and check carefully whether the following key items are included: data loss, reputational damage, theft of intellectual property, third party claims and business interruption."

Cyber insurance

As traditional insurance policies generally exclude cyber liability, companies may wish to consider taking out a specific cyber insurance policy.

The uptake on such policies has so far been low for a number of reasons. It tends to be expensive due to the high impact nature of risk and the fact that losses may be difficult to quantify. Low uptake also keeps the premiums high and the global cyber risk insurance market is small, making it less competitive. In many cases, cyber insurance has also proven inadequate. For example, Target is reported to have recovered $90million under its cyber insurance policy yet its losses were closer to $248 million.

However, cyber insurance does have a number of benefits (e.g. payouts for third party claims, access to experts). Any company considering cyber insurance should assess the risks which are specific to its organisation, and check carefully whether the following key items are included: data loss, reputational damage, theft of intellectual property, third party claims and business interruption. It is also worth checking whether any territorial restrictions apply (which might be an issue in respect of remote working), and whether the company is expected to have carried out any due diligence to ensure that its systems have not already been compromised.

Finally, cyber insurance should not be the sole form of protection but instead should form part of a comprehensive cyber protection strategy driven from the top down.

Recent initiatives

To date, many organisations have failed to take proper cognisance of cyber risk. However, a number of recent initiatives should help to raise awareness of the issue.

The Draft EU Network and Information Security Directive — which is expected to be finalised by the end of 2015 — will apply to organisations in various sectors, including the energy, transport, food supply, banking and financial sectors, which are regarded as providing critical goods and services. The Directive provides for mandatory reporting of breaches to national competent authorities, and aims to ensure greater harmonisation throughout EU Member States in their approach to combating cyber crime.

Ireland's National Cyber Security Strategy for 2015 to 2017 proposes a number of measures, including the establishment of a National Cyber Security Centre, further engagement on an EU and international level on how to tackle cyber crime, and various training and public awareness campaigns to ensure that cyber security becomes a priority item for every business.

A recent investigation by the Central Bank of Ireland into the management of operational risk surrounding cyber security within various regulated enti-

(Continued on page 12)

(Continued from page 11)

ties identified a number of deficiencies. As a result, the Bank recommended a series of risk mitigation measures which regulated entities should be taking to protect against cyber attacks.

The Bank further indicated that it will take into account any non-compliance with these recommendations when exercising its regulatory and enforcement powers.

Mitigation measures

Giving the prevailing risks, companies need to look seriously at their risk prevention and mitigation strategies to ensure that they are appropriately protected. As a minimum, the following measures should be adopted:

Clear and comprehensive cyber security policies and incident response procedures approved by the Board — Such policies should include a clear allocation of responsibilities in the event of an attack, actual or suspected, so that activities aimed at mitigating the harmful effects of an attack are co-ordinated to maximum effect. There should, for example, be clear internal reporting lines and timeframes, and clearly stated responsibility for notifying external agencies such as the Gardai, the DPC, other regulators and financial institutions.

Regular (not less than one per year) penetration testing of systems and incident response testing — Such services can be provided by external experts who can then work with the organisation to help plug any security gaps (technical or human generated) which are identified.

Appropriate staff training — Policies and procedures in respect of attacks should be clearly communicated to staff, with refresher training to be provided on a regular basis and following annual penetration testing of systems, to ensure that staff are aware of any new security measures adopted by the organisation and how to implement them.

Ensuring third party service providers (particularly those responsible for hosting or backing up company data) have appropriate cyber security measures in place — This means having written contracts in place with each service provider, whereby the service provider agrees to process data in accordance with the instructions of the customer, and to comply with the data security obligations in the DPAs.

The customer should reserve itself the right to conduct security audits on the service provider's security procedures, and ideally require the service provider to submit to regular penetration testing and implement any recommendations arising from such testing. The contract should also require the service provider to inform the customer immediately in the event of any security breach, actual or suspected.

Contingency plans in the event of data or systems being compromised – If business critical systems are affected, the company should have appropriate disaster recovery and business continuity measures in place so as to minimise downtime and the financial consequences of any business interruption.

Taking out cyber insurance — This should be appropriate to the particular risks faced by the organisation, bearing in mind that certain forms of loss (e.g. theft of intellectual property) may be harder to recover than others (e.g. loss of data). Insurance should also be viewed as an additional protection, rather than being a substitute for a comprehensive cyber risk management strategy.

Regular review of cyber security measures — This is necessary to ensure that existing measures remain fit for purpose in light of evolving cyber risk.

Conclusion

Although the measures suggested above will not eliminate the risk of suffering a cyber attack, they will assist organisations in demonstrating that they did all they reasonably could in the circumstances to prevent and minimise the effects of attacks. This will be important from the perspective of minimising potential losses to the victim, defending third party claims and avoiding regulatory sanction.

Robert S. Mueller III, Director of the FBI is reported to have said: "There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." This serves to highlight that cyber-risk is not something that any of us can afford to ignore.

Annette Hogan
McCann Fitzgerald
annette.hogan@mccannfitzgerald.ie