TACKLING THE GROWING SPECTRUM OF CYBER RISKS

Considering the scale of the losses that can result from a cyber attack, businesses should ensure they understand, take steps and insure against crime and data breaches

SCARCELY A DAY GOES BY WITHOUT NEWS HEADLINES reporting yet another data breach or cyber crime incident, which can have devastating consequences for any business in terms of reputation and balance sheet. In contrast with many other forms of risk, cyber risk cannot be readily confined. With increasing automation and interconnection between information systems, a compromise of information in one area of the business could affect an entire organisation and its customers. No industry or organisation is immune.

Most cyber attacks are motivated by the desire to secure some form of economic advantage, whether by stealing financial assets, intellectual property or critical personal information of clients or customers. The spectrum of cyber attacks is growing as cyber criminals develop ever more sophisticated ways of attacking network systems: see box.

Cyber criminals are increasingly using subtle social engineering techniques to quietly penetrate an organisation, deploying customised malware (malicious software) that can live undetected in network systems for months. Cyber criminals can then remotely and covertly steal a firm's most valuable information, whether in the form of personal customer information, credit card data or potentially trade secrets or intellectual property. The different types of malware continue to snowball at an alarming rate, which means that keeping ahead of the game in terms of network security has become an increasing challenge. The means of access are also growing as organisations make increasing use of third-party vendors or so-called "cloud" providers, which facilitate storage of data off-site. As FBI director Jane Camey said in October 2014, there are only two types of companies: "those that have been hacked and those that don't know it yet".

The management of cyber risks is not merely an IT issue. Experience has shown that even the most sophisticated, state-of-the-art security systems are breachable. Many attempts to compromise information involve the successful manipulation of people and human nature. It is often easier to trick someone into clicking on a malicious link in an email than it is to hack into an IT system. The attack on Target, the US retailer, whereby hackers gained access to its computer system and stole the financial and personal data of 110 million shoppers is reported to have been the result of hackers tricking the employee of an outside vendor into clicking on a malicious email.

> The loss or compromise of personal customer information or credit card data carries with it not only potential legal and regulatory issues but immediate reputational and brand damage

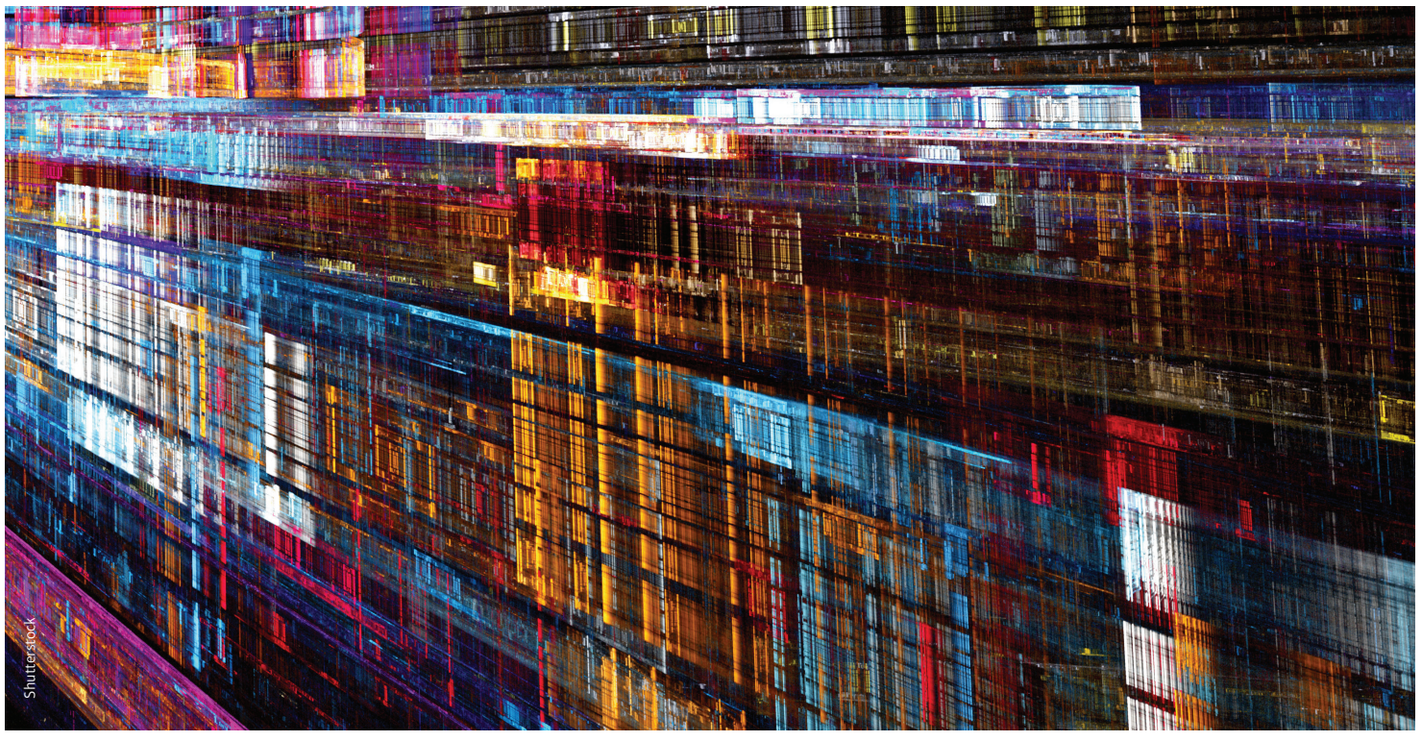
Management of cyber risks needs to be high on the boardroom agenda. Stakeholders and partners are increasingly seeking assurances regarding cyber security and, in the future, this is likely to include regulators, investors, customers, employees and lenders. The board needs to take a proactive approach to cyber risk and ensure that it is given the same level of attention as other legal, regulatory, financial and operational risks. Failure to do so could result in severe criticism being directed at the board and in potential claims against individual directors for breach of fiduciary duty.

Potential consequences of a cyber attack?

Cyber risk can take many forms and can affect the business in a number of ways, many of which can have a devastating effect. The loss of the "crown jewels" in the form of trade secrets or intellectual property could completely undermine competitive advantage, effectively destroying the financial stability of a business overnight. Any retail businesses with an online presence, if subjected to a denial of service attack, might lose customers to competitors with the resulting loss in sales and damage to reputation. This risk is heightened at particularly busy sales periods.

The loss or compromise of personal customer information or credit card data carries with it not only potential legal and regulatory issues but immediate reputational and brand damage. Cyber attacks naturally affect customer confidence, especially when customer funds or data are lost or stolen. In the current digital world, these concerns are likely to be exacerbated by social media and online communication forums that spread news of such an attack at an unprecedented speed. The potential downturn in sales combined with the costs of restoring reputational damage as well as the cost of investigating the cause of the attack and repairing cyber defences can be significant. In addition, a business may face the additional cost of notifying affected customers as well as potential fines and penalties, depending on the relevant legal and regulatory framework. Customers may claim compensation for any losses alleged to have been suffered as a result.

Currently, in the UK, the Information Commissioner has the power to impose fines (up to a maximum of £500,000 (€697000)) for serious contraventions of the Data Protection Act 1998. This is due to increase under the proposed new EU Data Protection Regulation, to fines of up to €1m or up to 2% of annual worldwide turnover for certain compliance failures, including failing



to notify data breaches, transferring data to a territory without ensuring appropriate safeguards or failing to designate a data protection officer. These proposed changes will affect all EU countries and represent a dramatic increase on the level of fines currently being imposed within the EU.

At present, there is no mandatory requirement in the UK to notify the Information Commissioner about data breaches (outside of certain regulated sectors) and this is the case in all EU countries. This could change under the proposed regulation to a system of mandatory reporting. This would require all data controllers to have continuous monitoring and reporting systems in place at all times.

Practical steps to mitigate cyber risk

Every organisation should consider a number of key steps as part of its risk management regime in an effort to mitigate cyber risk, including:

- establish a cyber risk management policy and ensure that this is part of the company's governance framework and, as such, give it the same level of attention as financial and other risk management regimes;
- undertake an initial risk assessment which includes consideration of the amount and type of personally identifiable information, customer data and confidential corporate data maintained by the organisation and the manner in which that information is used, transmitted and stored. The company's technology infrastructure needs to be evaluated as well as potential threats to the network security and the likely consequences of significant interruptions to online working or customer transactions. Also consider the risk of third party claims arising from the company's media content and the services provided to support e-commerce;
- ensure internet safety and network security. Networks should be protected against external and internal attack and steps taken to reduce the scope for penetration, for example by controlling access to removable media (such as memory sticks) and scanning all media before incorporating them into network systems. Consider who needs access to what. If an employee does not need access to sensitive data, they should not have it;
- adequate training and user awareness. Every organisation has a cyber defence weak spot in its own employees. An adequate cyber security system should not only have the relevant defences and policies in place, but staff should be adequately trained on all relevant policies and procedures;
- ongoing management. Planning and analysis of risk serves no proper purpose unless a company properly implements its findings. As cyber crime continues to evolve, companies must constantly monitor the adequacy of their cyber security and re-evaluate the threats pertinent to their business; and
- establish an incident response and disaster recovery team and put in place an incident response plan that has been adequately tried and tested. This should include legal team members to be called on to advise in relation to potential legal or regulatory issues, including the need to notify regulators and customers. Their advice may benefit from legal professional privilege. The umbrella of legal privilege can be particularly beneficial in the cyber crime context given the potential legal, regulatory and reputational ramifications.

Insurance for cyber risk

Insurance can play a vital role in the management of cyber risk, particularly when preceded by a thorough risk assessment, which should facilitate an in-depth understanding of the types of cyber risk, and the potential losses and liabilities that could affect the business following a cyber attack or data breach.

The question that first needs to be addressed is the extent of coverage already provided for cyber risk under existing insurance policies, including professional indemnity/civil liability, crime/fidelity and property/business interruption policies. Such policies have not historically been designed to cover the risks revolving around intangible assets, and network related risks, so a careful assessment of the coverage provided by these policies is essential. There are likely to be gaps in cover and the company will need to consider how those gaps should be filled, whether by enhancements to existing policies or through new cyber products being offered by insurers.

The cyber insurance market has developed rapidly in recent years and a number of insurers are now offering dedicated cyber insurance policies. However, the wording of cyber policies varies enormously and there can be huge discrepancies in the scope of cover provided. Some policies contain particularly onerous terms and conditions and others have exclusions that may serve to undermine the purpose for which the cover is being bought. A careful analysis of the coverage being offered is essential to ensure, not only that the particular risks and exposures faced by the company are covered, but there are no exclusions or conditions that could prevent pay out in the event of a significant claim.

The types of loss and liabilities that cyber policies typically cover include:

- **Data liability**. This should cover damages and defence costs resulting from any claim against the insured resulting from any data breach that compromises personal information or any claim alleging that

information has been lost or compromised as a result of unauthorised access to or use of the insured's computer systems. It is important to ensure that this covers not only loss of an individual's personal information but employee data and confidential corporate data, including third-party trade secrets, customer lists, marketing plans and other information that could be beneficial to competitors and could result in liability if compromised.

- **Media liability**. This should cover damages and defence costs resulting from any claim against the insured for infringement of copyright and other intellectual property rights, misappropriation or theft of ideas or media content. This may not extend to content published in a personal capacity, but this should ideally be included because the organisation may face significant liabilities as a result of the use by employees of Twitter, Facebook and other social sites and networks.
- **Regulatory coverage**. This should cover the cost of responding to any administrative, government or regulatory investigation following a data breach or cyber attack (for example by the Information Commissioner's Office, the Financial Conduct Authority and the Securities Exchange Commission) and any fines or penalties imposed. However, coverage will typically be limited to civil fines and penalties (criminal fines and penalties are not insurable in many jurisdictions) and some regulators prohibit regulated firms from recovering any fines or penalties they impose from insurers.
- **Remediation coverage**. Most policies provide coverage for the additional costs associated with a data breach. This should include costs incurred by the company in notifying those affected, notifying relevant authorities (where required), credit monitoring those affected and setting up call centres to field enquiries from concerned clients. Coverage may also extend to the costs of forensic services to determine the cause and scope of breach as well as PR expenses and other crisis management costs.
- **Information assets coverage**. The policy may include coverage for the cost of recreating, restoring or repairing the company's own data and computer systems. Such coverage may also extend to third-party data that has not been captured by back-up systems or has been corrupted or lost, for example, as a result of negligence or technical failure.
- **Network interruption coverage**. The policy may cover lost revenue owing to network interruptions or disruptions resulting from a denial of service attack, malicious code or other security threats to networks.
- **Extortion coverage**. Many policies include cover for the costs of responding to demands for ransom or extortion to prevent a threatened cyber attack.

As mentioned, the scope of coverage provided by cyber policies varies and the specific policy terms and conditions should be analysed carefully to ensure that the coverage provided meets the company's likely loss scenarios and potential exposures. One particularly important consideration is whether the coverage extends to information in the hands of third parties where data handling, processing and storage has been outsourced to third parties, including cloud service providers. If the organisation has outsourced data handling, coverage should be sought for any loss or business interruption arising from data that is managed by third-party service providers.

Another point to watch out for is the "retroactive date" as cyber policies will often limit coverage to cyber attacks or data breaches that occur after a specified date, which may be consistent with the policy inception date. It is important to request retroactive coverage for network security breaches that may have occurred before the inception date, given that it is not uncommon for cyber attacks to remain undetected for a considerable period.

Although it can take six months or more after a breach to determine the full financial consequences of a cyber attack, estimates suggest that one of the latest cyber attacks on a technology and media company will cost about $100m. The financial cost of the reputational damage and lost business opportunities is hard to quantify. Given the scale of the losses that can flow from a cyber attack, it is ever more important that businesses understand, take steps to mitigate and where possible insure against cyber risks. A proactive approach to cyber risks and insurance is essential.

Sarah Turpin *is a partner in the cyber law and cybersecurity and insurance coverage groups and* ***Sasi-Kanth Mallela*** *is special counsel in the cyber law and cybersecurity and government enforcement groups at K&L Gates in London*

THE SPECTRUM OF CYBER ATTACKS

- **Advanced oersistent threats (APTs)**: nation state-sponsored attacks that are targeted, persistent and advanced and typically result in loss of trade secrets or intellectual property.
- **Cyber criminals** typically attack using exploits and malware (malicious software designed to remain undetected) as a means of stealing valuable information or financial assets. Cyber criminals also deploy ransomware, a form of malware that makes itself known on purpose and gives criminals the ability to lock the victim's computer from a remote location, claiming the victim will not be able to access it unless they pay a ransom.
- **Denial of service attacks** or **distributed denial of service (DDoS)** attacks that are designed to make a machine or network resource unavailable to its intended users.
- **Domain name hijacking** or **domain theft**, whereby registration of a currently registered domain name is transferred without the permission of its original registrant.
- **Corporate impersonation** and **phishing**, whereby emails purporting to be from reputable companies are used to induce individuals to reveal personal information, such as passwords or credit card numbers.
- **Employee mobility** or disgruntled former employees who may seek revenge by compromising network systems or stealing valuable information.
- **Lost or stolen** laptops and mobile devices that may contain valuable commercial or client data.
- **Inadequate security and systems**: third party vendors that may provide another means for criminals to access network systems.