KEY POINTS

- As well as the better known hacking, cyber threats encompass a wide range of risks, the consequences of which can be severe.
- Banks could face regulatory sanction and may be deemed undercapitalised if a large number of customer accounts are affected.
- Organisations need a better awareness of the benefits of cyber insurance through extensions to specific policies or ideally, standalone cyber policies.

Feature

Authors Tom Webley and Peter Hardy

What can be done to mitigate cyber risk?

In this article, the authors consider the consequences of a cyber breach, the regulatory and legal issues posed by cyber threats and the role of insurance in mitigating the risks.

The risks posed by cyber breaches continue, justifiably, to dominate the press. Governments, regulators and risk officers are rightly taking these risks very seriously. Some sectors are more at risk than others, with the financial services industry having some of the most serious exposure.

Financial institutions are an obvious target for criminals. After all, criminals have been targeting banks since the earliest days of banking. In addition, the risk is exacerbated by the size of the potential damage caused by a breach. Financial services institutions hold a vast amount of personal and financial data about their customers. They are now heavily reliant on computer systems (including for most types of payment and transaction) and the cost of any business interruption can be enormous.

So what can be done to limit these risks, given that cyber criminals tend to develop forms of attack faster than even sophisticated organisations can update their defences and as systems become increasingly complex, the risk of accidental error also increases? Organisations need to consider what they can do to limit the damage once an attack or breach takes place.

Two obvious steps are: (i) to have in place a clear disaster response plan; and (ii) to make sure there is cyber insurance in place which is tailored to the specific needs of the business and provides the most comprehensive cover for specific cyber risk and losses.

The take-up of cyber insurance has been surprisingly slow in the UK and Europe. However, the British and European markets are starting to catch up with their US counterparts and regulators are pushing this issue by increasingly seeing insurance as an important part of adequate cyber risk mitigation. In fact, the UK Government has recently published a report on "*UK Cyber Security - The Role of Insurance in Managing and Mitigating the Risk*".

WHAT ARE CYBER RISKS?

ISACA (previously the Information Systems Audit and Control Association) defined cyber risk as the "business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise". Given the core role that most organisations' IT systems play in their business operations, this definition will naturally encompass an incredibly wide range of risks, both "first party" (loss of the insured's own assets/property) and "third party" (potential liability to others).

Different organisations will face different threats. These will be specific to their business operations, systems and the data they hold. However, as well as the better known hacking, cyber threats faced by most organisations include:

- Accidental loss or deletion of data.
- "Phishing" by third parties to gain access to the systems.
- Viruses or malware.
- Accidental misuse of private data.
- Software malfunction.
- Deliberate damage to data or systems.

These threats can be internal as well as external, and defences and risk mitigation steps need to factor this in. Statistics suggest that over half of all cyber breaches are caused by accidents or human error, rather than a deliberate attack by a third party.

Whatever the causes of the breach, the consequences can be severe. Table 1 below summarises just some of the significant losses which an organisation can suffer due to a cyber breach.

It is not just the potential size of the harm which cyber breaches can cause which makes them such a significant risk. It is also the difficulty in defending against them. For large organisations, there is often something of an expensive arms race in trying to stay ahead of the hackers and cyber criminals. Sophisticated organisations, particularly regulated financial services institutions, or other firms which hold financial data for clients, are likely to have robust defences in place. However, these might not be enough to protect them from human error of their own employees.

In addition, criminals are increasingly trying to circumvent the defences that large organisations have in place by getting to their systems via their smaller suppliers and customers, which would typically have less sophisticated cyber defences. The increased vulnerability of SMEs also makes them a target in their own right, particularly for companies that have valuable IP or hold valuable data.

WHAT ARE THE REGULATORY AND LEGAL ISSUES POSED BY CYBER THREATS?

Cyber breaches do not only pose the risk of direct financial losses being suffered by organisations. There are also indirect regulatory and legal issues which can arise from a breach.

TABLE 1: LOSSES DUE TO CYBER BREACH

Consequence of Breach	Description
Loss or theft of intellectual property	For many organisations, their IP is one of their most valuable assets. Any such value could be lost or diminished if IP is lost or stolen as a result of an accidental or deliberate breach. Many organisations see this as the biggest threat posed by cyber.
Loss of data or software	As with IP, data is an incredibly valuable asset for most organisations and an organisation can suffer considerable financial damage if data is lost due to a cyber breach. The same is true of expensive software used by commercial organisations.
Business interruption	This has the potential to be one of the most severe consequences of a cyber breach. Any business which is reliant on IT to operate (which, nowadays, will be the vast majority of businesses) can easily grind to a halt as a result of a breach. Given the impact this might have on customers, for regulated organisations, there could also be severe sanctions imposed by a regulator.
Breach of privacy	It is possible that much of the data held by an organisation is private (such as the personal or financial details of its customers). Breaches of that privacy could result in investigation costs, regulatory fines or claims from third parties. Unauthorised disclosure of personal data is one of the most frequent cyber breaches.
Fraud and economic crime	Organised criminals are becoming increasingly sophisticated in their use of IT to commit large scale fraud or theft on organisations, particularly financial institutions.
Extortion	Another form of criminal attack which can result in considerable financial loss is an organisation having its data, systems or IP etc held to ransom, often by cyber criminals using "ransomware" software.
Regulatory issues	The regulators are clearly very concerned about cyber risks. Andrew Bailey, chief executive officer of the UK's financial regulator, the Prudential Regulation Authority (PRA), claimed that cyber security is the issue which keeps him awake at night. Anything that poses either systemic/macro risks to an organisation or industry, or which poses more micro-risks to customers, is likely to be a key focus for regulators. For example, where account records have been changed and back-up data has been corrupted – customers with electronic statements only, would not be able to work out how much money was in their accounts and would not be able to pay bills. Where a large number of customer accounts was affected, banks could be deemed undercapitalised. In the UK, the Financial Services Compensation Scheme would only compensate customers for account balances it could verify. It will be vital, therefore, to ensure that an organisation has in place robust defences, systems and controls to protect it from cyber threats and be able to show that such issues are being taken seriously at the highest level within the organisation. Any failure to do this, particularly if it results in negative outcomes for customers, is likely to result in regulatory sanction.
Civil liabilities resulting from systems failures	Systems failures can result in a variety of claims from third parties, such as customers and suppliers. Even if the claims are small individually, the fact that any systems failure will often affect a large number of customers means the effects can cumulatively be quite large and the costs of defending claims significant. This is particularly true of banks and financial services institutions, which are a favourite target of claims management companies. (See further Table 2 opposite).
Reputational damage	There have been several high profile examples in the last few years of cyber breaches involving household names (such as retailers and banks). This can cause considerable reputational damage, including eroding shareholder, investor and customer confidence.
Physical loss and bodily harm	Cyber attacks and breaches can result in physical harm, as well as the loss of more intangible assets. Hardware or machinery could be damaged or employees could be injured or killed. Although this is rare, it is possible. For example, imagine a factory whose systems are hacked and the safety procedures shut down. This could have serious consequences.

Regulators are becoming increasingly aware of the significance, and impact, of cyber attacks and breaches. This is not simply the case with regulators which deal with data protection and data privacy, such as the UK's Information Commissioner's Office.

The UK Government, PRA and Financial Conduct Authority (FCA) are all focusing on the need for firms to improve their cyber resilience. Their view is clear. Cyber threats are not a purely technical issue. Cyber issues need to be considered at board level. This should also be considered in the context of another strong message coming out of many

TABLE 2: LEGAL AND REGULATORY ISSUES

Issue	Description
Internal investigations	When it comes to cyber breaches, internal investigations can and should be pre-emptive, as well as reactive. Organisations should regularly review, test and update their cyber defences and emergency action plans before any serious breaches have taken place. However, such investigations do carry their own risks. One such risk is a lack of privilege in the findings. Any documents or conclusions that suggest the organisation's systems and controls are insufficient have the potential to result in legal or regulatory liability for the organisation. To limit and manage this risk it is important, therefore, that lawyers (whether in-house or external) are involved in, and preferably run, the investigation. Another issue in relation to the findings of any internal investigations is the potential need for self-reporting. If any issues are uncovered, an organisation will need to take legal advice as to whether there is a regulatory or legal obligation to report those findings (eg to a regulator or contractual counterparty) and, if so, how best to limit the damage caused by doing so.
Data privacy breaches	Data privacy issues remain one of the most frequent forms of cyber breach. Any cyber breaches involving data privacy might result in the organisation being in breach of its statutory and regulatory obligations, such as the data security standard prescribed by the UK's Data Protection Act 1998 and equivalent European or other international legislation.
Regulatory investigations	The increasing regulatory scrutiny of cyber security and resilience is likely to lead to an increase in regulatory investigations in this area. As is often the case with regulatory activity, the U.S. regulators are leading the charge and the Securities and Exchange Commission already investigates regulated companies that have suffered a data breach. In the UK, the FCA could follow this lead and investigate any financial services companies that have suffered a breach which the FCA suspects might have been the result of inadequate systems and controls and/or lead to negative outcomes for customers. Breaches can have more macro-regulatory interest. For example, both the Bank of England and the FCA are looking into the reliance placed by traders and investors on Bloomberg terminals, after a recent systems outage at Bloomberg led to widespread disruption.
Third party claims	Most breaches will have the potential to result in third party claims, such as from customers or suppliers whose data has been lost or used inappropriately. There might also be breach of contract and lost opportunity claims arising from business interruption caused by a cyber breach or IP claims. How these claims are defended will depend on the nature of the claim and the knock-on effect. For example, it might make sense to settle a claim brought by a single commercial customer, whereas doing so for a retail customer might lead to a raft of speculative litigation encouraged by claims management companies. There might also be regulatory consequences in fighting claims, particularly if the end result is that the defence is unsuccessful and the organisation is found liable. One other factor to consider is insurance. If proper insurance is in place (as it should be – see further below), it will be important to ensure that no steps are taken in relation to claims brought that could undermine the potential cover.
Claims/ action against individuals	As well as claims against the organisation, there is also the possibility that claims or regulatory action could be brought against individuals. Board directors and risk officers will have to ensure that they take responsibility and ownership for the firm's cyber defences, as they are likely to be the ones held ultimately liable by regulators. Insurance cover should also reflect this. There is also the possibility of civil action being taken against directors. In the US, derivative actions against directors are more common than in the UK, despite such claims being made possible by the Companies Act 2006. However, the risk is still there and directors need to understand these risks and, to the extent possible, insure against them as part of their D&O cover.
Jurisdictional considerations	Cyber threats are global and in no way limited by national boundaries. For example, in the case of hacking, where was the hacker based? Where are the servers? Was the data stored in the cloud? Where are the customers based? Where did the loss or harm occur? Which regulators can take enforcement action? All of these factors need to be considered by the organisation when putting in place cyber defences and an emergency plan, when reacting to potential breaches and when considering insurance cover.

regulators around the world: the need for increased personal accountability. Board directors and risk officers should certainly take note of this.

Depending on the nature of the organisation, the industry and jurisdiction in which it operates, and the relevant regulatory regimes, there are a number of legal and regulatory issues which will need to be considered. Some of the more common ones are summarised in Table 2 above.

WHAT ROLE DOES INSURANCE PLAY IN MITIGATING THE RISKS?

Risk and insurance are natural, if not opposing, bedfellows. However, the insurance market in Europe has been slower to adopt cyber insurance than in the US,

where its adoption has in a large part been driven by regulatory requirements around data breaches.

Managing and Mitigating the Risk" leaves no doubt as to the severity of the risk posed by cyber attacks and threats, but also the benefit that can be gained from insuring specifically against those risks. Firms need to consider the extent to which there are gaps in their existing cover in relation to cyber and what cover they need which might be met by standalone cyber policies.

> There are figures which suggest that in the UK only 2% of large firms and almost no smaller firms have specific cyber policies.

There are figures which suggest that in the UK only 2% of large firms and almost no smaller firms have specific cyber policies. These surprising statistics appear to be the result of a combination of organisations believing that cyber risks are sufficiently covered by existing more general policies, or that there are no specific cyber policies which would insure such risks. In fact there are, and cyber risks can be covered either by extensions to specific policies or, ideally, by standalone cyber policies. The key is to be aware of the scope of cover currently available in the market, whether through existing coverage extensions or, preferably, specific cyber policies.

The UK Government's report on "*UK Cyber Security - The Role of Insurance in*

Not only are existing policies unlikely to insure adequately against cyber risks, but the availability of specific cyber cover is likely to mean that the more general policies will look to expressly exclude cyber risks. As with all categories of risk, it is possible (subject to comments below) to purchase cover for almost every eventuality. The question is, have you in fact bought the cover that you subsequently need?

There are benefits to having cyber insurance on top of the obvious benefit of increased protection. For example, one of the difficulties with quantifying and mitigating against cyber threats is the paucity of the data. Insurers and brokers can provide good insight here, based on their wider experience with different clients in different industries, and this can help with building defences and contingency plans, as well as with the insurance cover itself.

Some risks are uninsurable, such as the direct loss caused by the theft of IP or the impact of espionage on an organisation. However, the available cyber-specific cover is far more extensive than many organisations realise. Table 3 summarises some of the key insurable risks.

TABLE 3: KEY INSURABLE RISKS

Risk	Summary
Data breach	Organisations can insure against both the direct costs of investigating the breach, as well as third party liabilities arising from it.
Security breach	Insurance cover is available for third party liabilities resulting from some network security breaches and IT assets being used for cyber attacks.
Damage to software and data	Some attacks and cyber breaches result in loss, deletion or corruption of software or the data held by an organisation. It is possible to insure against the costs of third party experts used to reconstruct the data or software.
Cyber crime	This might traditionally be included as part of a comprehensive crime policy, but organisations have to be increasingly mindful of cyber-exceptions in traditional policies.
Extortion	Both the costs of the external experts dealing with the breach and the ransom itself can be insured.
Business interruption	This is one of the most potentially harmful results of cyber breach. It is insurable, but with certain limitations, as insurers fear that one cyber event might have a considerable aggregate impact.
Physical damage to assets	This can be covered as part of a standalone cyber policy and might well be excluded from traditional property insurance.

Given the increasing prevalence and severity of cyber breaches, it is likely that the uptake in (and reliance upon) cyber-specific policies will be on a steep upward curve. However, it is important to ensure that any policy in place is fit for purpose. This will involve a careful analysis of the risks posed by cyber breaches to all elements of the business and an assessment of the potential financial value of those risks. This analysis should include:

- Identifying the generic risks posed by cyber breaches.
- Identifying specific or esoteric risks faced by specific business units within the organisation.
- Carrying out a cyber gap analysis to identify gaps in existing insurance cover.
- Discussing these gaps with brokers (if relevant) to ensure that any cyber-specific cover is comprehensive and for a sufficient level of cover.
- Ensuring that any policies are able to keep up with what is a fast-evolving threat.
- Considering how the policy would actually respond to any claims.
- Making sure that individuals within the organisation are sufficiently protected.
- Preparing a cyber report confirming that sufficient cover is in place (thus providing protection for the risk of-

Biog box

Tom Webley is Counsel in the Banking and Financial Services Litigation Group at Reed Smith in London. Email: twebley@reedsmith.com

Peter Hardy is a partner and head of the London office team in the firmwide Insurance Recoveries Group at Reed Smith. Email: phardy@reedsmith.com

ficers and comfort for the board).

- What other steps should organisations be taking to mitigate risks?
- Insurance should play a key role in mitigating the risks caused by cyber breaches. However, when it comes to cyber, not all risks can be transferred.

There are other steps which organisations and their risk managers need to take to ensure they are in the best possible position to defend against and respond to cyber breaches. As with insurance, a "one-size-fits-all" approach will not be appropriate.

Adequate defences

Almost all organisations will now realise the need for robust defences against cyber breaches. These defences must be:

- tailored to the specific nature and needs of the business;
- nimble enough to keep up to date with the evolving nature of the threat; and
- regularly tested to ensure they work in practice.

Unfortunately, cyber criminals appear to be winning the race to adopt and evolve and companies' cyber defences struggle to keep up with the pace of change. This has increased the risk of significant attacks. Increasingly sophisticated criminals are constantly on the lookout for areas of vulnerability in cyber defences.

Many larger companies spend a great deal of time and effort on such defences. Banks are an obvious example. Given the sensitive nature of the personal and financial data they hold, the regulatory pressures on them and the potential financial impact of business interruption, banks and other financial institutions take the need for robust defences very seriously. However, sophisticated criminals still target banks directly and indirectly through third parties as described above, given the spoils on offer and the fact that the evolution of the methods of attack tend to outpace the development of the defences.

Disaster recovery plans

As well as regular stress testing of the defences, it is important for organisations to have a clear and robust disaster recovery plan should there be a breach. As with everything else, this should be tailored to the main threats posed to each business unit and set out clearly and concisely what should be done in the event of a breach. The plan should be regularly updated, including the most basic things, such as making sure contact names and numbers are current.

> It is ... important to work out as accurately as possible what the maximum financial impact of an attack or breach might be ...

Appropriate supervision and ownership of risks

Many organisations originally saw cyber threats as a technical issue which sat most appropriately with the IT teams. The technical side of cyber defence is clearly important, particularly in ensuring that the technology of the gamekeepers keeps up with that of the poachers. However, in order for an organisation to have fully robust defences and disaster plans in place, this issue has to be considered at board level. It is likely to be only at this level that there is a full understanding of the business as a whole and what impact a cyber breach might have.

Cyber security should be a standing agenda item at board meetings and there should be documented evidence to show that the board has taken steps to understand the risks and mitigate against them. This is particularly important for regulated organisations where regulators will expect the board and senior management to be on top of these issues and, given the rhetoric coming out of most regulators, are likely to hold individuals personally liable if this is not the case.

Quantification of potential risks

Quantifying cyber risks in financial terms is not straightforward. It is very hard, for example, to attribute with any accuracy a value for intellectual property. However, attempting to quantify the threats is important for a number of reasons. The business needs to be able to survive an attack. Severe cyber breaches can be fatal to a commercial entity. For example, severe business interruption could mean no money coming in while bills still need to be paid. It is, therefore, important to work out as accurately as possible what the maximum financial impact of an attack or breach might be and take steps to mitigate the risk; the most obvious being to ensure there is adequate insurance cover. The steps taken to quantify the risks could form part of the process of placing the insurance. Brokers and insurers, with their expertise in this area, could help work out what financial exposure there might be.

So the message is that cyber risk is serious and here to stay. Organisations need to take appropriate steps to defend themselves from cyber threats, including protecting their business and customers and having adequate insurance in place. If nothing else, it is clear that regulators will expect these issues to have been considered at the highest levels within organisations. There might be difficult questions to answer if there is not clear evidence to show that they have been. ■

Further Reading:

- Implications of the failure of the Bank of England RTGS system [2015] 2 JIBFL 69.
- Protecting the bank's position when customers fall hook, (on)line and sinker for vishing frauds [2014] 8 JIBFL 540.
- LexisPSL: Corporate: ICSA guidance on cyber risk.