CMS
law·tax·future

Advising the Board on **Cyber Risk**

Reports looking at the full range of commercial risk

Risk, Resilience
and Reputation

Directors' risk report

A cyber-attack can have a devastating impact on a business's operational activity, lead to regulatory investigations, the imposition of fines and other costs as well as damage to reputation. The increase in home-working, use of new technologies and adoption by many businesses of new security arrangements as a consequence, has reinforced the importance of data security. Failure to understand the company's cyber security arrangements and the impact of an attack could constitute a breach of a director's duties under the Companies Act 2006. Ultimately, directors may face claims by the company (or its shareholders through a derivative action) if their breaches of duty cause the company loss.

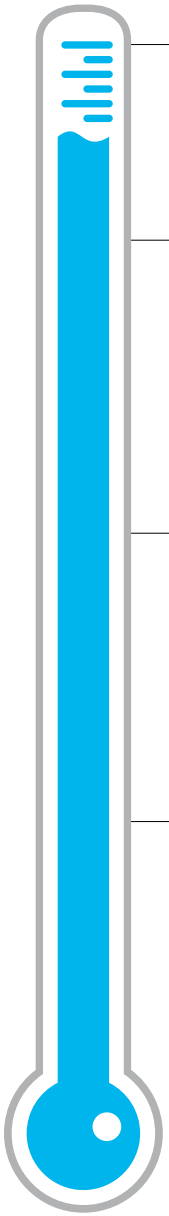
In recent years, it has not been possible to escape news of cyber-attacks affecting established and respected businesses with significant consequences, including large fines imposed by the Information Commissioners' Office (ICO) for breaches of data privacy laws and negative impact on the company's reputation.

For many businesses, the day-to-day management of IT and data security will be the responsibility of a Chief Information Security Officer (CISO)/Head of IT and/or a Data Protection Officer (DPO). However, it is also incumbent on directors to understand the importance of cyber security, be aware of the potential consequences of a cyber-attack and ensure that the business has systems in place to manage risk and respond effectively if it does suffer a cyber-attack.

Directors of regulated entities or those that operate subject to the NIS Directive are under additional scrutiny from regulators and specific consideration must be given by the directors to whether the business is under any further obligations to protect its systems and/or notify affected parties should an incident occur. It is then critical that a director is able to ensure that these additional obligations are followed in a timely and responsible manner.

It is critical that directors assess the risk and formulate a holistic response to potential attacks by ensuring that steps are taken to assist in prevention, preparing for the worst and utilising risk management/mitigation solutions such as specialist cyber insurance that can provide balance sheet protection.

Stakeholder risk thermometer



HIGH RISK

Directors
An avoidable cyber-attack which is not managed effectively can lead to regulatory scrutiny and potentially criminal charges against directors, as well as damage to a director's personal reputation.

Shareholders
A cyber-attack can threaten the future operation of the business. If key systems are affected the business's ability to function may be compromised, leading to financial loss, negative impact on share price and potentially the failure of the business. A poorly managed response to a cyber-attack can result in lasting damage to a business's reputation.

Individuals
A cyber-attack may impact on the data privacy rights of people whose personal information is stored on the business's IT systems, including employees, customers and subscribers to marketing communications. They may be disgruntled, and may seek compensation even if they suffer no financial loss or actual distress.

Business Customers
Customers may be affected if a business is unable to fulfil an order or provide a service as a consequence of a cyber-attack, and may suffer losses as a result.

LOW RISK

Understanding the consequences of a cyber-attack

The consequences of a cyber-attack can be many and varied depending on the scale and nature of the attack, the nature of the business affected and the manner in which the business responds to the attack.

— **Regulatory fines** – Cyber-attacks which lead to compromise of personal data of individuals can attract fines from the ICO of up to €20m or 4% of a business's global turnover, whichever is higher. The ICO will take account of the business's policies to reduce the risk of a cyber-attack and its management of the response to the incident when determining whether to impose a fine. Businesses which are subject to scrutiny of other regulators can face additional sanctions.

— **Claims for compensation by affected individuals** – Under data protection legislation, individuals can seek compensation for breaches of their data privacy rights even if they have suffered no financial loss or distress. Individual claims are modest but collectively they can be significant, especially if the business faces a class action. Infringement of data protection laws or breaching information security requirements can also put a company in breach of its contracts with and/or duties of confidentiality to customers, clients, suppliers or other relevant business partners.

— **Claims for compensation or damages by business customers** – If a business is unable to meet its contractual commitments to customers such as fulfilling orders for delivery of goods and services due to its IT systems being inoperable, it could face claims for breach of contract.

— **Ransomware payments** – Many cyber-attacks involve the encryption of a business's IT systems and a demand for a ransom payment for provision of a decryption key. Some cyber-attacks also involve the exfiltration of data (including personal data) and the demand of a ransom payment in return for not disseminating that data.

— **Business disruption** – Business operations may be disrupted if access to data is compromised or data cannot be used compliantly. No organisation is immune from such disruption, and few organisations would be able to operate effectively without access to their IT systems. The 2017 WannaCry cyber-attack caused mass disruption worldwide. In the UK, the NHS was hit particularly hard, with the hack causing over 19,000 appointments to be cancelled and 200,000 computers to lock out users with messages demanding ransom payments in Bitcoin.

— **Remedial costs and incident management costs** – Managing and remedying a cyber-attack can be an extensive (and expensive) exercise involving replacing affected IT system, restoring data, engaging with the media and customers and dealing with regulators. The legal, PR and IT consultancy cost can be considerable.

— **Damage to reputation** – Consumer and shareholder confidence can be shaken by a cyber-attack, especially if the business handles the incident badly. High profile cyber-attacks remain news items for a lengthy period and are often restated as comparisons when other unconnected attacks are reported. It can take many years for a business to recover its reputation.

— **Directors' liability** – Whilst the company will suffer the main financial fallout from a cyber-attack and will be the primary target for claims and enforcement measures, directors can be personally affected. They could face claims by shareholders for mismanagement of the company if they are considered to have failed to perform their duties as directors by not ensuring that adequate measures were taken by the company to manage the risk of a cyber-attack. Regardless of the merits of such claims, the impact on a director's reputation can be long-standing.

Understanding and managing the vulnerabilities and areas of risk

Unsurprisingly, IT security plays a key role in managing risk, but poor IT security is only one factor which can affect a business's vulnerability to a cyber-attack. A large proportion of cyber-attacks result from employee engagement with spam and phishing emails requiring them to input information or click on weblinks. These actions can result in downloading of malware which can lock IT systems or exfiltrate data. Some vulnerabilities will lie outside the business's IT perimeter and may require extra vigilance.

(A) Risks within the business's IT perimeter

It is important for a business to consider its IT security in the context of its broader business practices. Directors should ensure that the business has good security policies in place and also a plan to manage the impact of a cyber-attack.

- **Employee training and awareness** – Employees should be made aware of the risks of cyber-attacks, especially in relation to suspicious emails, and should be required to complete regular training modules on cyber-security threats and good practice concerning IT usage.
- **Policies and Procedures** – This training should be supported by policies and procedures concerning IT usage, such as the requirement for use of strong passwords and if possible two-factor authentication. All IT users should be aware of the business's data protection policy and the policies for home working and the use by employees of their own IT devices.
- **IT security** – IT systems should be regularly reviewed to ensure that software releases are up to date including latest updates and patches. Anti-virus and anti-malware software should be installed, regularly reviewed and kept up to date.
- **Restoration of data** – All businesses should have procedures in place to ensure regular backing up of data, with the ability to restore data or implement other disaster recovery arrangements as soon as possible to minimise business disruption. These procedures should include the storage of back-ups offsite and/or on a separate system to avoid them also being encrypted in any ransomware attack.

(B) Risks outside the business's IT perimeter

Some areas of vulnerability are more difficult to manage. In particular, many businesses will be dependent on suppliers to provide IT and other services, potentially exposing them to vulnerabilities outside the business's own IT systems.

For example, many companies outsource critical business functions which may require suppliers to access their IT systems, such as finance or HR functions. Suppliers or consultants which have access to the business's IT systems should be expected to adhere to the same standards as employees of the business. Policies should be in place to ensure awareness and compliance. Service contracts should contain appropriate clauses to safeguard the business and pass on any financial liability which may arise from non-compliance.

Some businesses allow customers to access their IT systems for example to track orders. Similar standards should be applied.

A company which acquires another business should ensure that the target company has good cyber security measures in place to minimise the risk of inheriting a business which is vulnerable to a cyber-attack. Due diligence should extend to detailed consideration of IT security, with appropriate indemnities.

(C) Incident Response Plan

Even businesses with the strongest cyber security can fall victim of a cyber-attack. It is important that directors ensure that if a business does suffer a cyber-attack it responds in an effective and responsible manner and takes measures to minimise and recover its losses.

All businesses should have an incident response plan setting out how an incident will be managed. This should include procedures for containing the incident, engaging with regulators and if appropriate affected individuals, and managing media attention. Directors should take responsibility for ensuring that the incident response plan is appropriate and adequate for the business's needs, taking into account the potential impact of a cyber-attack. Ideally an incident response plan should be tested in a table-top mock breach scenario to ensure that all aspects are adequately addressed, if possible involving those third parties that will assist in management of an actual breach, including lawyers, forensics consultants and PR specialists. Directors should satisfy themselves that the incident response plan can be quickly and effectively implemented if necessary.

A business will often be judged on how it responds to a cyber-attack and an incident response plan can be vital in protecting the business's reputation (and reputation of directors) in the crucial period following a cyber-attack.

Directors should also be aware of the types of specialist cyber insurance policies which are available and ensure that the business has appropriate policies in place, again taking into account the potential impact of a cyber-attack on the business.

Insurer's perspective

Lucy Russell
Underwriter – Cyber & Technology, Canopius

The benefits of cyber insurance

Cyber incidents can no longer be considered unusual or unexpected. The growth in the number of cyber incidents affecting businesses has been exponential in recent years and the nature of the attacks has become ever more sophisticated. Every business is vulnerable to attackers and can become a target irrespective of its size, whether it holds substantial customer data or relies on IT to conduct its business operations.

Cyber insurance is an essential line of defence for any company in order to cope with the financial consequences of an incident. Cyber insurers can assist with the incident in a variety of different ways:

— **Breach response:** Providing a range of suitable experts (identified in advance by the insurer) ready to get to work on the incident immediately, to detect what has gone wrong, to protect against further losses.

— **Advice and action:** What steps should the business take to get back up and running, inform its customers about the incident, establish what has been lost and what can be recovered, decide whether a ransom should be paid to recover data/systems, put security in place to prevent a similar incident from happening again, address any loss of reputation or public relations.

— **Losses & Defence Costs:** In the event that the business suffers losses or receives claims from third parties (for example, its customers) as a consequence of the incident, the insurance will respond and pay or reimburse the business. There is coverage for losses arising from business interruption and damage to digital assets. It is also important to recognise that the costs associated with dealing with the incident may be very substantial.

In the event of a crisis, every business needs to have a plan of action to respond to what has happened. It is crucial for businesses to have the right experts and resources in place before an incident has occurred. A cyber insurance policy is an invaluable addition to the risk management toolkit for directors, helping them to prepare for an incident and providing access to the support network required to minimise the impact of the incident and equip the business with the tools that it needs to recover as quickly as possible.

Flexible working practices

Recent years have seen many businesses adapting their operations to involve flexible working practices. The challenges associated with this trend have been further accelerated by the COVID-19 pandemic, which has seen significant numbers of businesses change their working arrangements to allow staff to work from home. Often these changes were made at short notice, remain in place months later and for many businesses are set to become permanent arrangements as working practices are restructured towards a mix of office and home-based working.

Unfortunately, these difficult circumstances have created vulnerabilities that threat actors have been seeking to exploit, and there has been an escalation in the number of cyber-attacks associated with remote working arrangements.

Some practical measures that businesses should take with their remotely working workforce include:

— Introducing additional security for remote working, such as two-factor authentication to access systems or emails remotely, and maintaining high security standards for any new systems and tools that are introduced to facilitate remote working.
— Reminding staff of the need for extra vigilance to combat hackers or malicious actors (on top of usual security and data protection obligations).
— Regularly assessing and mitigating the risks the business would face if it was the victim of a cyber-attack.
— Monitoring the supply chain to determine whether COVID-19 has forced important suppliers to operate in a riskier manner. Consider whether changes or alternatives are required, or whether there are ways to work together to mitigate risks.
— Updating the incident management plan to ensure it meets the additional risks which may arise from large-scale remote working.

If the business is attacked, the priority will be limiting any losses, returning to operational activity and ensuring that the business complies with its regulatory obligations. Any steps directors can take before an attack happens will lead to valuable time gained at the time of crisis.

PR perspective

Hannah Cambridge
Director, FleishmanHillard UK

How a business responds to a crisis is just as important as the crisis itself. If your response falls short, a business could unintentionally escalate the issue among its stakeholders and damage both trust and reputation.

When a cyber incident occurs, business leaders may find themselves having to make decisions with limited information. They may also face a lot of technical and regulatory detail that is hard to grapple with, even alongside expert advisors. These decisions, and especially those made in the early stages of a response, are critical in setting the stage for how the business will handle the issue.

There's a lot to consider, but there are some key things that are always worth keeping in mind.

— **Remember your values**. Most businesses have a list of values that guide the organisation in every decision it makes. As a leader, you should be the voice of those values in a crisis. Values can help when making tough calls, defining key messaging, pre-empting expectations and explaining why you responded the way you did.

— **Call in the experts**. Tap into the experts you have available to you. Cyber incident response teams often involve an insurer, external counsel, IT forensics and communications. Experts in these fields know the process involved, understand their role and know how to work together. They can offer in depth experience and an essential, external perspective.

— **Agree your guiding light strategy**. With your values in mind and the information you have to hand, define your response strategy. This should include your aims, key messages, the tone you will take and the stakeholders that you must prioritise.

— **Don't rush into communicating**. It can be tempting to tell everyone what has happened when you become aware of a cyber incident, even when you know very little. In practice though, this can cause confusion and panic in the short term and potential claims of distress in the longer term. Work closely with legal and communications to understand what your stakeholders need to be told, whilst you continue to gather information.

— **Once it's public, demonstrate proactivity**. After an initial communication about what has happened, there's often a period with very little to say whilst the investigation is ongoing. Remember to demonstrate proactivity with your key stakeholders by updating them on how any impacted systems may have been restored or what temporary measures are in place to limit business impact. Balance this proactivity with the risk of overcommunicating and you will find the right fit to suit your business and your stakeholders.

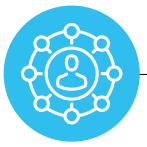
— **Remember employees**. If the cyber incident has impacted the business's servicing, your employees will want to know why they can't do their day jobs as normal. However, you'll also need those employees to help manage communications with clients or consumers. Finally, they may also be data subjects, directly impacted by the incident – a fact you may not know for many weeks or months. All of this means that what and how you communicate with employees is critical.

— **Care about cyber security**. Before an incident even occurs, ensure that business leaders are fully engaged with cyber security. They should be leading by example in messaging to employees about the importance of data security and following good practices. Not only may this improve good practices, but it will also help to shape stronger messaging in the event of an incident.

— **Key to a good response is practice**. Responding to an incident is much easier when you've had some practice and been through the motions before. It can also help to define roles and responsibilities. Many simulations will identify processes or measures that could be strengthened to not only reduce the risk of a cyber incident occurring but also strengthen your reputational response in that event.

Summary: practical risk management for directors

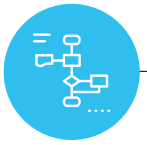
The nature and scale of the cyber security threat is ever-changing and directors have a vital role to play in ensuring that the business has robust procedures and practices to manage the risks and mitigate the potential impacts. By ensuring effective measures are in place they will be helping to safeguard the future of the business and protect the business's reputation, as well as their own reputations.



Awareness
Ensure that the board, CISO, DPO and other stakeholders are aware of the threat the business could face from a cyber-attack and the potential impact that an attack could have on the business's operations.

Policies and procedures
Ensure that the business's policies and procedures to minimise the risk of a cyber-attack are up to date and that there is employee training to support the protective measures which are put in place.

External vulnerabilities
Ensure that due consideration is given to vulnerabilities outside the business's IT systems and that the business's suppliers follow acceptable cyber security standards.



Incident response plan
Ensure that the business has a readily accessible plan to respond to an incident, including engagement with the media and regulators, containment of the incident and restoration of IT systems.

Insurance
Ensure that the business has adequate insurance in place to cover all the insurable losses which may arise from a cyber-attack.

Engagement
Ensure that directors are fully engaged with cyber security and are seen to be engaged, leading by example in messaging to employees about the importance of data security and following good practices.

Contacts

Lee Gluyas
Partner
T +44 20 7524 6283
E lee.gluyas@cms-cmno.com

Tristan Hall
Partner
T +44 20 7367 3105
E tristan.hall@cms-cmno.com

Amit Tyagi
Partner
T +44 20 7367 3578
E amit.tyagi@cms-cmno.com

Colin Hutton
Partner
T +44 131 200 7517
E colin.hutton@cms-cmno.com

Cathryn Hopkins
Senior Associate
T +44 20 7067 3310
E cathryn.hopkins@cms-cmno.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

2104-0143643-5