Empower Results®

Mitigating and managing cyber risk: ten issues to consider

The board of directors is responsible for managing and mitigating risk exposure.

A recent study conducted by the Ponemon Institute[1] revealed that companies rank cyber security risks as greater than natural disasters and other major business risks.

In light of its potentially significant effect on corporate reputation and financial performance, the board needs to consider the impact a cyber event may have on its business by identifying the organisation's risk exposure and exploring risk transfer and mitigation strategies.

The following factors highlight the main areas that directors should consider in mitigating and managing cyber risk:

1 Understand the risks

Consider your client base. Now consider how your organisation would cope if more than three quarters of your clients stopped doing business with you. Should your organisation fall victim to a cyber attack, such an outcome could be a possibility. According to a 2011 Unisys survey, 82% of the UK public would stop dealing with an organisation, such as closing their online account, if their data was breached. Damage to brand and reputation can be irreparable.

A cyber attack or data breach can take many forms including deliberate attacks, technology issues and human error or negligence. The perpetrators of a cyber attack can include organised crime groups, competitors, disgruntled employees and politically motivated groups.

The UK's increasing reliance on computer systems, web-enabled communications and cloud technology has left many organisations open to new exposures. Although most risk managers and business decision makers recognise that data breaches represent a major threat to their organisations, developing a better understanding of their organisation's specific network security and privacy risks is an important first step to aligning the exposures to appropriate risk transfer options.

1. Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age (August 2013)

Empower Results®

Cyber risks: cause and effect examples

Event

- Accidental
- Intentional
- Malicious
- Accidental
- Third party

Nature of event

- Hacking
- Virus
- Cyber extortion
- Identity theft
- Unauthorised access
- System error
- Loss/destruction of information
- Theft of information
- Defamatory
- Privacy breach
- Breach of intellectual property
- Wrongful collection

Outcome spectrum

- Breach notification
- Brand and reputation damage
- System disruption
- Forensic investigations
- Damage to digital assets
- Legal proceedings
- Regulatory security
- Extortion demands
- Data loss

Consequences

- Legal liability to your suppliers and employees
- Notification costs
- Fines and penalties
- Increased compliance costs
- Enforceable undertakings
- Replacement of digital assets
- Loss of revenue
- Customer confidence
- Impact on share price
- Data restoration costs
- Forensic consultation costs

2 Data breaches and your organisation's reputation

The amount of personal and confidential information maintained electronically by public companies increases every day. As a consequence, the likelihood that a material data breach will adversely affect an organisation's reputation, bottom line and share price is a real exposure. In the US, the Securities and Exchange Commission has responded to this ever-increasing risk by requiring greater disclosure related to data security; it is likely that the UK and other European countries will follow suit in the near future.

3 Are you aware of the changing regulatory landscape?

The European Commission is planning to overhaul the regulation of data protection and privacy across all member states by introducing a General Data Protection Regulation that would create a single set of rules for all organisations processing personal data in the European Union.[2]

2. The European Commission, Proposal for a Regulation of the European Parliament and of the Council, 25 January 2012

If the draft regulation is adopted, it would lead to a substantial reform of the 1995 data protection directive and could potentially impose much tougher rules on any affected organisation. More importantly, the potential consequences of failing to comply with the new rules could compound the possible financial, brand and reputational damage which can befall an organisation after a data breach.

The regulation is currently expected to come into force in 2015 or later.

In a separate move, the Commission is also proposing a directive on network and information security that may affect a range of organisations including those that are involved in the provision of critical infrastructure, banking and healthcare as well as those that are enablers of information society services – for example, e-commerce platforms and social networks – by requiring them to meet minimum IT security standards as well as disclose cyber breaches to their national regulators.[3]

4 The proposed General Data Protection Regulation may create a number of challenges

One of its most important elements is a plan to allow the national data protection authorities of each member state to impose fines of up to 2% of worldwide revenues on any organisation that processes personal data. In the UK, the current maximum fine that can be imposed on an organisation is £500,000.[4]

5 Mandatory notification may be on the horizon

As things stand, any organisation that comes under the new data protection regulation will be required to notify its local data protection authority and its data subjects within 24 hours, if possible, should it suffer a data breach. There is, at present, no requirement to provide such notification in the UK.

6 Increasing data protection and privacy compliance burden

Perhaps the most significant elements of the draft data protection regulation are those that directly seek to enhance the privacy rights of the individual, particularly the intention to create the right to be forgotten.

Under this plan, an individual can require any organisation to delete personal data when there is no longer a legitimate reason for keeping it. Moreover, an organisation can no longer process personal data that requires the consent of the individual.

In future, it will have to have explicit consent before proceeding.

3. The European Commission, Digital Agenda for Europe , Policy/Legislation, 07/02/2013
4. ICO - Taking action: data protection and privacy and electronic communications, http://www.ico.org.uk

7 Hackers are already two steps ahead of you

Some organisations mistakenly believe that because they have a firewall, a quality IT team, or antivirus protection, they will not be targeted. However, various major organisations around the world have been victims of cyber crime in recent years and have experienced significant data and security breaches including the details of bank accounts, medical records and confidential business information.

These incidents have affected millions of customers and exposed some of these companies to litigation and liability, significant financial recovery costs as well as loss of future business and reputational damage.

8 Cyber threats can pose merger risks

Boards need to closely consider cyber security and other data protection measures in the context of corporate M&A activity. If a company acquires a target with a malware-infested IT system, there is a potential for a wide range of liabilities. Cyber security and other data protection methods should be added to the list of criteria a board should consider when evaluating a potential acquisition. In addition, acquisition documents should include appropriate representations, warranties, and indemnities related to cyber risks.

9 Have you considered the legal and risk governance issues around data hosting and jurisdiction?

The decision by many UK organisations to outsource their software applications, technology platforms and IT infrastructures to third-party providers has created a raft of new legal issues that may have significant risk management ramifications. Businesses should balance the flexibility and potential cost savings of outsourced services such as cloud computing with the risks inherent in storing data, infrastructure and platforms offsite, beyond the company's direct control, and possibly even in a foreign country with different laws.

It may be helpful to obtain detailed information from cloud providers about their security programs including who can access the data, where it will be located (country of jurisdiction, for the evaluation of legal obligations), technical aspects of the infrastructure, and what steps the provider has taken to protect the integrity and security of the data.

10 Insurance coverage is available through tailored cyber risk policies

Ramifications of a breach can be very costly to a company's business, both fiscally and for brand and reputation. In addition to notification costs (PR, call centre costs and credit monitoring services), investigations response and compliance, and compensation to affected individuals, there are additional concerns such as engagement of forensic experts, and defence of claims for misleading conduct, negligence, breach of contract, breach of confidence and interference of privacy.

Most of these exposures are not covered under conventional insurance. It is, therefore, important for companies to thoroughly evaluate existing exposures and insurance coverage and consider purchasing tailored network security and privacy insurance to cover identified gaps.