Cyber Risk Management

A short guide to best practice

Bond Dickinson

October 2014

Insight

So what exactly is 'cyber risk'?

In essence, cyber risk means the risk connected to online activity and internet trading but also generally to the use of electronic systems and networks and the storage of personal data.

Due to the prevalence of use and dependence upon electronic systems it is a growing risk that can affect all businesses, regardless of size.

Accordingly, while cyberspace has revolutionised how many of us live and work, it is crucial to understand the threats that it brings with it.

The risks:
Implications of a cyber incident

Cyber security is an increasingly high profile issue with cyber-crime now ranking alongside international terrorism as one of the top global threats.

A primary objective of the UK Government's National Cyber Security Strategy is to make the UK a safer place to conduct business online.

However, cyber incidents can range from hacking and virus transmission to theft or accidental loss of data. While external actors such as hackers often steal the headlines, problems can arise from internal sources such as malicious, or even just careless, employees or inadequately protected buildings and systems. The impact of a cyber incident can be significant and the potential costs immense, with wide-ranging implications:

- data loss - accidental loss or theft or copying of data
- breach of contract to third parties caused by the loss of data
- business interruption
- property damage
- personal injury
- extortion – for example by a hacker
- damage to reputation
- copyright infringement
- libel.

Prevention:
Steps to manage cyber security and reduce the risks

Determining the benefits of cyber security and knowing where to start are a significant challenge to many organisations.

The UK Government has said that the majority of successful external cyber attacks could have been avoided by implementation of basic IT security such as firewalls and malware protection. Unfortunately as cyber criminals become increasingly sophisticated, it is often difficult to keep one step ahead of them. At a recent cyber seminar for the IT market, a leading software provider announced that there was no such thing as cyber security and that the focus instead should be on how quickly an attack can be identified in order to limit damage.

Pro-active management of cyber risk at board level is critical in reducing the risks. Recommended measures include:

- identifying key information, data and systems and thoroughly assessing their vulnerability to attack
- allocating responsibility for cyber risk management appropriately
- having a clear information security policy in place and supporting this with staff training and reminders so the business can be confident that the entire workforce understands and follows it
- assessing the extent to which the business shares information with suppliers and clients and customers and how they protect the business' information and data
- acquiring better systems or updating existing systems to maintain security standards
- checking existing cover and buying appropriate levels of cyber cover to mitigate risks in the same way as other risks such as traditional property damage or errors and omissions cover are mitigated.

Many organisations allow employees to use their own computers, tablets and smart phones for business purposes. This obviously increases the business's risk so IT provision should include ensuring that all devices used to handle business information have the same level of protection in place.

By implementing the above, organisations can at least help to mitigate cyber incidents.

When approaching the market for cyber insurance, one of the first questions the underwriters will often ask is what procedures are currently in place and what the business is doing about managing the risk. Insurers can demand that appropriate risk procedures are in place and implemented in order to reduce the risks of a cyber related incident.

Mitigation:
Steps to take on discovering a problem

A cyber breach can be devastating for any business, with the effects ranging from operational disruption, liability to third parties, reputational damage and regulatory issues.

These will all need to be dealt with quickly and effectively or order to limit further damage.

It is crucial therefore to have a unified business-wide incident management process. A clear response strategy which staff understand and can implement promptly can not only help recover more quickly from an incident but can also help prevent future incidents.

Many cyber insurance policies include a cyber incident management and response service following a data breach. While policies differ, this will often include expert IT, legal and PR support which will provide practical support in the form of technical forensic investigations, legal advice, notifying customers or regulators, and providing credit monitoring to affected customers.

Insurance:
Key considerations for insurers

Cyber cover is a growing opportunity for the insurance market in the UK and Europe but in order for the industry to avoid being caught out, a clear understanding of the risks is necessary.

The methods used by cyber criminals are evolving and society's dependence on being able to access data and use electronic systems is growing rapidly. Therefore the risks for insureds who do not take these issues seriously and consequently their insurers are significant too. Perhaps the biggest challenge for the industry is quantifying exposure to the risks given just how fast-evolving those risks are, coupled with the lack of historical data available.

Market insiders warn that it is only a matter of time before a systemic cyber event brings down the internet or a sector in the economy and with it, widespread problems, liabilities and claims.

Buyers of cyber insurance are also now spreading beyond financial, technology and healthcare companies, to include sectors such as retail, manufacturing and energy and small to medium-sized enterprises as well as large corporates. The trend is showing no sign of abating.

Insurance products are evolving and responding to the increasing take up with new and developed offerings in the product line. However, the scope of its cover can vary enormously from policy to policy.

As the field of cyber risk insurance matures, policies are becoming more specific and customisable. Accordingly, it is essential that businesses, their brokers and insurers consider the level of cover required so that the appropriate protection is provided and customers are not paying for unnecessary cover or leaving key gaps in cover.

Here to help:
Key contacts

Andrew Kimble

Partner
Data Protection
T:+44(0)845 415 8422
E: andrew.kimble
@bonddickinson.com

Justin Tivey

Legal Director
Insurance Claims
T:+44(0)845 415 8128
E: justin.tivey
@bonddickinson.com

Andrew Parsons

Managing Associate
Dispute Resolution
T:+44(0)845 415 8115
E: andrew.parsons
@bonddickinson.com

www.bonddickinson.com/cyber-risks

www.bonddickinson.com