EVERSHEDS

Clicking into place

Cyber liability: how can businesses protect themselves against underestimated cyber risks?

Digital Financial Services

The cyber threats facing businesses are more sophisticated than ever. The widespread use of cloud computing and the continuing emergence of new technologies creates additional risks for businesses to consider. Data and IT systems are crucial to the effective operation of almost every business. Cyber liability is not an IT risk, it is a strategic business risk. Virtually every business relies on IT infrastructure and, as such, will be exposed to the risks of business interruption, income loss and reputational damage if IT equipment or systems fail or are interrupted, or if data is lost or misused. The average cost of data breaches is $3.8m for companies around the world.[1]

What is cyber risk?

Cyber risk is the risk of financial loss, disruption, or damage to reputation as a result of breaches of data security, including unauthorised disclosure of data, and compromise or failures of IT systems.

Specific examples include:

- security breaches where sensitive information (e.g. customer or employee bank details) is stolen or inadvertently disclosed
- theft or loss of digital assets, e.g. customer lists and business trade secrets
- business interruption due to a virus shutting down a network
- costs associated with damage to data records caused by a hacker

Who is at risk?

All types and sizes of organisations are at risk. Cases of large-scale data breaches are well-publicised. However, it is not just the organisations which make the headlines that are at risk.

In addition to business interruption and reputational damage, a business is also at risk of claims for compensation from third parties, e.g. employees or customers, in the event of data breaches; criminal and civil penalties; and investigation costs.

A 'Cyber Breaches Survey' published by HM Government in May 2016 reported that 65% of large businesses have experienced one or more cyber security breaches in the last 12 months.[2]

Examples of cybersecurity breaches, and the loss caused by these breaches could include companies:

- suffering losses of thousands of customers which could affect a company's profits by millions of pounds if customers personal details are hacked
- incoming regulatory fines if their security does not meet regulatory standards and customer details are stolen by computer hackers
- being sued by employees if a security breach causes those employee details to be leaked

Cyber-crime is estimated to cost the UK economy $4.3 billion a year.[3]

1. 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute
2. Cyber Breaches Survey 2016, Main Report
3. Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee

Insurance considerations

The difficulty facing businesses is that the usual insurance policies which a business maintains would not respond in the event that data is lost or stolen – the insurance would not cover the costs of restoring the data, the costs of any reputational damage and claims from third parties. Traditional business interruption insurance would not cover losses suffered if an IT system fails as a result of a virus or other cyber-attack.

Managing cyber risks through insurance is relatively new and many businesses do not realise that they may not have insurance cover for these risks, and may only realise when it is too late. It is, therefore, important for businesses to recognise that they may not have cover for these risks but that cover is available.

Insurance cover for cyber risks is best achieved by way of a specialised cyber liability policy, although insurers may provide cyber cover by extensions to liability policies. Cyber risks fall into direct losses to the business and liability to third party claims. Cyber risk insurance can cover either or both of these types of risk.

Cover in relation to direct losses to the business may include:

- computer restoration and data recovery
- business interruption from systems failures
- reputational damage arising from a breach of data that results in loss of intellectual property or customers
- theft of money or digital assets through theft of equipment or electronic theft

Cover in relation to claims by third parties, typically customers, may include:

- investigation, defence costs and civil damages associated with security and privacy breaches
- customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- multi-media liability, including investigation costs, defence costs and damages arising from defamation, breach of privacy or negligence in publication in electronic or print media

Cover is usually available in relation to assistance with and management of the incident, which can be essential when faced with reputational damage or regulatory enforcement.

What next?

Businesses should spend time evaluating the potential risks it faces in relation to the IT and network systems it uses. They should then, with the assistance of their insurance brokers, establish what cover they have in place in relation to these potential risks and, in conjunction with their insurance brokers and insurance lawyers, ensure that so far as possible they have the necessary insurance for the cyber risks.

A failure to ensure insurance protection is in place for the cyber risks could prove very costly in the long run.

How can we help?

Eversheds Insurance and Reinsurance team is experienced in advising on digital security issues and can provide guidance and assistance in a number of ways, including:

- reviewing and advising on the terms of existing and proposed insurance programmes to advise on gaps in relation to cyber liabilities
- negotiating the terms of cover with insurers
- providing advice and assistance in the event of a claim in respect of a digital security loss
- advising on coverage disputes
- advising on cyber-security compliance and risk management

For further information please contact:

Matthew Gough
Head of Digital Financial Services
T: +44 29 2047 7943
M: +44 779 532 8532
matthewgough@eversheds.com

Paula Gaddum
Partner
T: +44 161 831 8165
M: +44 797 981 8845
paulagaddum@eversheds.com

Philippa Laughton
Senior Associate
T: +44 20 7919 4744
M: +44 750 095 1513
philippalaughton@eversheds.com

eversheds.com/digitalfinancialservices