Cyber Liability Insurance

Cyber risk

As businesses become increasingly dependent on technology for many aspects of their business, the risk of financial loss as a result of things going wrong is growing exponentially. It is estimated that the cost of IT crime has now grown to £27 billion in the UK and the average cost of an information security incident for a small business is currently £60 000 [source: Study conducted by the Ponemon Institute 2013].

Whilst most companies will ensure that their physical assets and liabilities are effectively protected by insurance, consideration given to cyber risk is not always top of the agenda.

Those with a particular exposure are companies engaged in e-commerce, those with transactional websites, those who store sensitive or critical data and/or those with a large amount of information on their websites. However there are very few businesses these days who do not have some exposure.

Managing the risk

It is important to try and mitigate wherever the possible the risk of cyber issues arising in the first place. Whilst not an exhaustive list common techniques include:

- *Carrying out of IT security audits*
- *Encryption of personally (customers and employees) identifiable and confidential information*
- *Regular maintenance of firewalls and anti-virus software*
- *Reviewing relationships and contracts with third party providers of IT services and critical software including such areas as payment processors*
- *Managing third party access to networks*
- *Create and keep under regular review a business continuity plan to deal with potential threats*
- *Awareness of data breach notification protocols both statutory and voluntary codes and assess whether you have the ability and experience to deal with such incidents*
- *Consider potential malicious or negligent acts by employees and how this would be dealt with*

When considering cyber risk no two businesses are the same so it is important as a starting point to spend time in the business considering the threats that could arise, how you would respond to them and quantify the likely costs and expenses that could be incurred.

The role of insurance

Whilst managing the risk is critically important, insurance can assist in both receiving advice when things go wrong and reimbursing what could be substantial costs and expenses in getting a business up and running again as quickly as possible.

It is possible that some elements of cyber risk may be picked up under conventional policies but for a more comprehensive approach a cyber insurance cover should be considered. These policies are tailored to deal with cyber risks specifically and are becoming essential to the secure governance of many businesses.

Types of cover that can be provided include:

- *Data breach and management cover, including the expenses related to investigation and management of an incident, legal and investigation costs, court attendance and regulatory fines*
- *The cost of restoring data, software and programs*
- *The negligent use of electronic media by employees including libelous comments on social media*
- *Passing on a virus to customers or suppliers*
- *Infringement of website and intellectual property rights*
- *Losses and professional costs associated with the threat of extortion*
- *Loss of revenue resulting from a denial of service attack*

Policies can be tailored to meet the specific needs of the business

Examples of what can go wrong

These are just a few examples of the everyday issues that can arise from cyber risk:

- An insurer paid £450 000 to another company when its employee wrongly alleged in an email that the company was to be investigated by the DTI
- A major utility company had to pay £200 000 to an ex-employee arising from comments circulated via the internet that breached their privacy.
- A retailer mispriced a digital camera online and had to honour the contracts which cost them £2.3m
- A dismissed IT employee encrypted the entire database of his previous company and demanded £1m in ransom. The cost of undoing the damage was £5m.
- The IT system of a food and beverage business was hacked and the database of 100 000 customers was stolen leading not only to significant cost but also reputational damage following an investigation by the Information Commissioners Office.
- An unencrypted memory stick was lost by an employee which contained the personal and sensitive details of over 500 employees including addresses and bank details.
- A marketing consultant developing a client's website used logos and images copyrighted to another business and damages in excess of £1m were claimed.
- A haulage company's files were corrupted by a 'phishing' email costing £30 000 of specialist consultants costs to restore.
- Theft of a managing consultant's laptop with unencrypted client data on it led to a cost of £50 000 in notifying clients of the issue.