Cyber Insurance Factsheet

Cyber Insurance. Do I need it?

If your revenue, systems or communications are reliant on computers or the internet or you hold data, particularly sensitive data such as credit card information, the answer is yes.

Connecting to the internet is like opening a door. Physical doors to a building are secured by a lock and perhaps an alarm, but it is also wise to insure the contents in case someone breaks in. With the 'internet door' passwords and firewalls are the locks and alarms, but as most traditional insurance policies exclude cyber risks you are probably not insured if someone 'breaks in'. And it is not just what can get in through the 'internet door', you have to make sure what you send out is protected too.

Everyone using email and the internet is at some risk and we will provide guidance as to what you should consider before deciding whether cyber insurance is for you.

What is Cyber Insurance?

Cyber is a term currently used by the insurance industry to describe a variety of internet based risks. They include the obvious such as hacking and viruses, as well as data breaches, privacy, reputational damage, intellectual property infringement and media risks. They can be those that cause damage or interruption to your business or where you have a liability to others. Within this factsheet we explain the types of cover available, what the main risks are, where and from whom claims can come and why cyber risks are generally not covered by traditional insurance policies.

What to consider

Given the stats available, the chances are high that your business will suffer a cyber breach, even though it may not be directly aimed at you. Loss prevention is obviously the best course of action and adequate IT security is a must, but insurance should also be considered.

You need to assess not just the likely effect of a cyber breach, but also the worst case scenario in terms of physical and reputational damage, loss of revenue (not just if you trade on line) and costs you may incur either putting things right or in damage limitation. What is at risk? What do you store on your computers that are valuable to you or others? What will be the effect of downtime for a day, a week or longer? Are there seasonal variations when downtime could be more significant?

What help do you have available to get up and running again such as an in-house IT manager or external consultancy support? Remember that insurance claims are generally more inconvenient than you think and with IT (in the writer's experience) there always seem to be a few glitches.

Where is data held? If it is in the 'cloud', how much control do you have and are you contractually protected if something goes wrong?

If you find there is a risk to your business you should consider cyber insurance.

Risks

Hardly a day seems to go by without a headline about cyber crime or data breaches. Cyber crime is now big business as criminals seek information and data. They do not just target larger companies, numerous recent surveys show that over 70% of small business have experienced security breaches

in 2015 (Information Security Breaches Survey 2015 – Department for Business, Innovation and Skills).

Some risks will be out of your control. For example, cyber terrorists targeting the UK infrastructure is a major concern to the government, and utilities and internet service providers are high on the list of potential targets.

Other risks could include competitors, ex-staff and some industries will face the threat of those that disapprove of their activities or are politically motivated.

But the biggest risk is generally your staff. Not many are malicious, they are human and just make mistakes or do not fully understand the risks – sharing passwords or soft passwords such as Password123, connecting their own equipment to your system, opening 'dodgy' emails by mistake or falling victim to social engineering. It is easily done; scam emails are now very sophisticated and no longer just come from Nigerian royalty with offers of multi-million dollar investments. Emails purporting to come from managers or the likes of banks look very genuine and it is perfectly understandable that we can be 'duped' into opening them (and in effect the 'internet door') and spreading a virus or malware.

Think outside the box as to what could happen? Look at everything that represents a risk to your business. It may be your supply chain, customer base or infrastructure?

Where could third party claims come from?

If you suffer a data breach claims could come from a number of sources including the following:

- Customers could claim compensation for financial losses or denial of access relating to their data and with the General Data Protection Regulations (GDPR) coming into force on 25th May 2018 there will also be compulsory costs involved in notifying customers of the breach, although firms may also incur additional costs as best practice to avoid reputational damage and loss of income.
- Credit Card information is particularly sensitive and if you suffer a breach you will find that your responsibilities under your mercantile agreement with the card provider will be onerous. Both the forensic costs investigating the cause of the breach and likely fines from the card provider will be substantial (but at least insurable).
- Regulators, specifically the Information Commissioner's Office under Data Protection Legislation, can take action in the event of a breach and the number and size of fines (up to 4 % of turnover) are set to increase once GDPR comes into force. You could face legal costs defending actions and potential fines (which are not always insurable. See Fines and Penalties
- Third parties if you spread viruses, infringe intellectual property rights or for online defamation.

The background

Cyber risks such as hacking, viruses and denial of service attacks were excluded from most insurance policies in 2002, although at the time they were generally called Electronic or E Risks. This followed a series of attacks on big institutions to include the likes of the US military. Many of the attacks were by 'geeks in bedsits' having 'fun' and testing their hacking skills, but insurers were very concerned

about the potential for a worm or virus to be spread throughout computer systems worldwide and insurers do not like unlimited exposure.

Since then specialist insurance cover has become available, but was initially expensive and restrictive. This has changed and a number of insurers now offer cover for most cyber risks at affordable prices for most businesses.

Typically, the 'E Risk' exclusion applies to hacking and damage caused by a virus or similar mechanism to include the likes of worms, trojan horses and logic bombs.

Insurance Market

The cyber insurance market is in its infancy and is evolving to try and respond to the risks faced by business. At the moment there is no real uniformity with the products offered by insurers and the level of cover and excesses can vary enormously, as can the amount of information required for a quotation. There are cyber packages that offer a good level of cover, at premiums starting from as little as £100 for small companies and are suitable for most SME business. More sophisticated or client/sector specific risks will require a more bespoke approach.

Many insurers are now seeing cyber as a growth opportunity and introducing policies, although keeping pace with the emergence of new cyber risks is a challenge and the insurance market's reaction should a major cyber attack occur on the UK's infrastructure will be interesting.

Types of cyber insurance available:

System Damage and Corruption – cover for rectification costs, incurred in retrieving, restoring or replacing any of your computer systems or programs.

Cyber Crime – Providing cover for financial loss from computer crime, fraudulent transactions, identity theft, telephone hacking, cyber threats and extortion, but the position with losses arising from social engineering varies from insurer to insurer. Many only cover losses from criminals gaining access to your system and exclude losses due to deception ie being 'duped' into making payments to a criminal following social engineering. However, some insurers offer a crime extension or policy to provide cover for losses from social engineering.

Business Interruption –cover for a reduction in profit as a result of system downtime or reputational damage.

Cyber Liability – cover for any third party damages and defence costs arising from your legal liability for:

- General Liability – for the transmission of viruses emanating or passing through your computer systems
- Data Breach/ Privacy Liability – cover for claims arising out of a security breach of any data and personally identifiable information, such as credit card details, including breach notification costs, forensic investigations and contractual fines levied by the credit card providers.
- Fines and Penalties – cover (if provided) will vary from insurer to insurer. Those that provide cover may say 'if insurable by law'. As stated above, contractual fines can be insured, but criminal fines cannot. Fines by regulators such as The Information Commissioners Office are not criminal fines, but the position is not totally straight forward. They are insurable, but

not if the result of deliberate or dishonest misconduct, intentionally illegal or morally reprehensible acts. So, fines or penalties resulting from fraud would not be insurable, but non-fraudulent negligent, acts or omissions would be insurable. The individual circumstances of a case would need to be considered before an insurer pays a claim.

- Media Liability – cover for claims arising from defamation from websites or distributed contents, infringement of intellectual property rights or invasion of privacy.

Generally, these covers flow from a 'cyber peril' being triggered which is a malicious attack to include the likes of hacking, phishing and denial of service attacks, but check the detail of policies, including the definition of terms carefully.

Most policies exclude:

- the whole internet going down (either a whole country or globally)
- wilful, reckless or dishonest acts of directors and senior managers (but not ex-directors or senior managers)
- fines and penalties (unless specifically included), but see comments above.
- some policies exclude cyber-terrorism

Most policies will include professional support in the form of crisis management and public relation consultants.

We hope that you have found this factsheet of use and for further information please speak to your usual contact at Nsure.

Telephone 01903 520200 or email michael.bickers@nsure.co.uk