Cyber Insurance Guide

Cyber-crime. The threats are out there. In an ever globalised and internet centric world, these threats are becoming more commonplace and with potentially increased severity.

This cyber guide looks into what cyber insurance actually is, what sort of things a cyber insurance policy may cover and the potential risks to businesses (and individuals) if they aren't covered.

BLACK & WHITE

Introduction

News headlines have been littered with high profile examples of cybercrime and the subsequent ramifications. From Sony PlayStation in 2011, and Yahoo over a number of years to Talk Talk in 2015, the Wanacry cyber-attack which affected the NHS in 2017, and Petya cyber-attack spreading from Ukraine across Europe also in 2017. However, this is just the tip of the iceberg . . .

On a daily basis, smaller businesses are being targeted by hackers who are accessing confidential data, stealing funds or locking out access to essential files. In 2015, there was an "Information Security Breaches Survey" carried out which highlighted the costs of attacks to both large and small organisations, and illustrated the need for businesses to take action. The survey revealed some telling statistics:

- **90% of large organisations reported they had suffered an information security breach, while 74% of small and medium-sized businesses reported the same**
- **For companies with more than 500 employees the average cost of the most severe breach is now between £1.46 million and £3.14 million**
- **For small and medium sized business the average cost of the worst breach is between £75,000 and £310,800**
- **75% of large businesses and 30% of small business suffered staff-related breaches**

(https://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles)

The statistics and data don't stop with this report. There has been a tremendous volume of research into this field, with most reporting similar findings. The results make for stark reading, and provide clear rationale for businesses to step up in terms of taking cyber security seriously.

The insurance industry is playing a key role in enabling businesses to offset the risk of cybercrime and cyber threats. In addition the insurers are also making steps to help businesses recover if the worst does occur, because every day that you aren't trading, you are losing customers and income.

What is cyber insurance?

Cyber insurance is the insurance industries response to a growing global cyber threat towards individuals and businesses. Cyber insurance looks to help businesses mitigate against threats, and in the unfortunate event of a successful attack, allow them to get up and running again with the minimum level of negative impact.

It is important to note that for businesses, cyber insurance is not the answer to all of the security issues that a business may face. It is instead part of a toolkit which will allow a business to defend themselves against the threats, and reduce the impact of said threats.

Businesses should look to include cyber insurance in a set of preventative measures which will sure up the business, such as updating security patches, upgrading firewalls and putting processes into place which ensure data can't be ext**RAC**ted from company systems by anyone (note that this list isn't exhaustive).

If **you**r business is taking the above steps, as well as some of the steps included in the National Cyber Security Centre's 10 steps to cyber security document then you are not only giving **you**rself added protection, you are also increasing **you**r chances of getting a lower insurance premium.

What could be included in a cyber insurance policy?

There are several incidents that cyber insurance may be able to cover an individual or a business for. The below list provides an example of the coverage that may be available to you. This list is not exhaustive; however it does showcase a range of options

1) Hardware

Cyber insurance may cover you for hardware issues. This may cover you against loss, theft, damage, cyber events and even to the breakdown of hardware. This can include office equipment with the option to cover numerous insured locations.

Hardware is a critical component to many businesses, if essential systems were to break-down this could have large ramifications. Hardware cover will provide you with peace of mind that in the event of hardware issues, your insurer may be able to help you get back up and running.

2) Data Corruption & Extra Cost

This is cover to restore computer systems following a cyber event, to pre-event health. This can include damage to hardware, as well as costs incurred through loss of access to business data and systems. This cover may not be limited to a business's own computer systems, but could also apply to the computer systems of the insured's service providers. This is likely to include data held by 3rd parties.

3) Cyber Crime

As already discussed, cyber-crime is a growing phenomenon. Your cyber insurance policy may help protect you from some of the threats faced. This can included financial losses from fraud or telephone system hacking. It may also help cover the cost of bringing in a specialist investigator or engineer to help identify and fix the issues.

4) Cyber Liability

Cyber liability cover seeks to help businesses pay for damages and defence costs from claims made against the insured business/individual. These damages could have been caused by failures to secure data or errors in data handling, unintentional transmission of a virus and reputational damage from website, email or distributed content, even defamation.

5) Data-Breach Expense

This looks at covering businesses for the costs of investigating data breaches. It can also cover the costs of notifying customer, legal advice, public relations & crisis management expertise, identity theft assistance for insured's customers or others affected as well as a security audit to identify weaknesses within the business/individual's IT infrastructure.

6) Cyber Event – Loss of Income

This cover is as simple as the name suggests. It looks to cover businesses/individuals for loss of income following a cyber attack/event, which includes prevention of access to business data.

Like other types of insurance products, Cyber insurance comes with many options of cover. Whether you're a freelance consultant, a new start-up or you're running a growing SME, Cyber insurance policies come with different levels of cover and different price options. Cyber insurance comes at a low premium in comparison to the potentially detrimental repercussions of a data breach.

"For small businesses, nothing is more important than protecting their livelihood. Cyber liability insurance is another tool they can use to prevent financial disaster in the event of a malicious attack"

Natalie Cooper, editor of BankingSense.com

What are the potential risks to businesses if not covered?

As already established, all businesses are at risk to cyber-crime. Without adequate protective measures in place, which includes but isn't limited to insurance, there is a real threat to incomes and reputations.

Financial Risks

The financial risks to businesses are well documented. A cyber event has the ability to cut off a business's access to crucial data and essential information systems and most businesses, especially small ones which may be forced to close in order to deal with the repercussions.

Costly and time consuming security overhauls will have to take place in order to prevent the attack from happening again and staff may even need to be re-trained. It could also have the effect of wiping databases and corrupting files to the point at which a business can no longer operate.

Without these IT and business systems in place it is unfeasible for many companies to continue to operate and provide their customers with the service they demand.

These financial risks are not restricted to the short term. A cyber-event can affect a business for a long period of time, with customers opting to choose a perceptively more reliable provider, or because of the cost of potentially replacing old/obsolete IT infrastructure.

In 2016, 2.9 million British companies were hit by some sort of cyber-crime at a total cost of £29.1 billion (https://www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion/).

Non-Financial Risks

The risks of cyber-events are not limited to financial losses; the impact is far wider reaching. As it has been documented with the examples provided at the beginning of this guide, businesses can suffer with a great deal of subsequent issues following an event.

Reputation is a key risk to businesses who have suffered a cyber-attack. A successful invasion of a company's IT infrastructure leads to a loss of trust from both current and potential customers. This damaged reputation will take a long time to rebuild.

Your customers can naturally become very disgruntled if their personal data and information is leaked and they could even be affected by damaging identity theft.

Although it can be argued that time has a financial impact, it is also a non-financial risk. Subsequent to a cyber-event time has to be spent investigating the breach, reporting the impact and solving the issue. This could be done by either internal or external parties, which could delay the implementation of other projects across the business.

What may not be covered

As with any insurance policy, it is crucial to review not only what is covered by your insurer but what is excluded under the agreement. Most exclusions in cyber insurance are the same as those in other insurance policies such as war and terrorism. For cyber insurance in particular, some common exclusions to be aware of are as follows:

“Court Jurisdiction”

It is always worth checking which territories a cyber policy applies to. While policies purchased in the UK normally include territories in the European Union and much of the rest of the world in their cover, the United States and Canada are often excluded.

“Claims by Related Entities”

Whilst cyber insurance will protect your business from loss of customer data and any claims which arise as a result of this loss, policies do not normally include the claims for the loss of employees’ personal information who may seek redress from a data breach. This exclusion normally extends to contractors and even to partially owned subsidiaries of your business.

“Bodily Injury and Property Damage”

Digital Asset Replacement clauses will replace losses in the digital sphere, but cyber insurance policies will not usually cover damage to physical property or bodily injury which results from a cyber incident.

“Cyber crime vs Cyber insurance”

Cyber insurance is designed to protect and reimburse your business in the event of loss of data as well as providing the necessary support for legal, notification and other costs in the event of a breach. However, cyber insurance will NOT reimburse your business for a financial loss (such as a hacker stealing money from a bank account); this would be covered under a crime insurance policy which many businesses may already have.

We are always ready, always accountable, always helpful no matter what the circumstance, no matter whether you are a client or not.

If you have any questions or concerns about how cyber-crime can affect your business, or would like a **quotation for Cyber Insurance**, please get in touch with us.

Quick, Simple, Hassle-free

GET A QUOTE

www.**blackandwhite**insurance.co.uk/**cyber-insurance**

or call 029 2080 8921

BLACK & WHITE

HEAD OFFICE
2-3 Sir Alfred Owen Way
Tudor House
Caerphilly CF83 3HU

Email: cs@blackandwhiteinsurance.co.uk

Need to talk to us **029 2080 8921**

Mon-Fri 8:30am-5pm, Sat 9am-1pm
Bank Holiday's 9am-1pm

www.blackandwhiteinsurance.co.uk