OBF
INSURANCE GROUP

THE COMPLETE GUIDE:

CYBER SECURITY RISKS, CLAIMS AND INSURANCE

THE MOST COMMON CYBER RISKS FACING SMEs

Regardless of company size, any business that stores and collects data electronically is at risk from a cyber attack every day. In 2017, 62% of cyber attacks targeted small-medium businesses and 64% of those were web-based attacks. While newspaper articles largely focus on cyber attacks on large businesses, the threat of cyber attack on small and medium sized businesses is very real.

With that in mind, our cyber insurance experts have developed a quick guide to the most common cyber security risks facing SMEs.

LOST AND STOLEN DEVICES

More and more of our work tasks are now being completed on mobile devices such as smart phones, laptops and tablets. Since such devices are often used outside of the work environment, the risk of theft or loss is high. Research shows that over 70 million smart phones are lost each year and one laptop is stolen every 53 seconds.

Worryingly, 52% of these devices are stolen from the office or workplace while 24% are stolen from conferences. This means that any data stored on misplaced or stolen devices can be easily compromised and potentially place your business and clients in danger of hacking or some other form of data breach.

E-MAILS

Spam and junk e-mails constantly manage to find their way to businesses' inboxes and they are appearing more and more genuine all the time. If such an e-mail is opened unintentionally, you could be opening the way to a third party accessing your data, leaving you and your business exposed.

In addition, using auto-fill forms may save time, but they can also easily result in security breaches. If you're discussing a sensitive matter in an email, the last thing you want to do is accidentally send it to the wrong person. Unfortunately, this is an easy mistake to make and indeed, one most of us have made at some point.

OUTSOURCING TASKS

Outsourcing tasks is increasingly common, with many companies seeking outside help on at least one project a year. Although doing so allows managers and employees more time to focus on other tasks, it can also present a threat to data security.

According to a report undertaken by PWC, hiring service providers, consultants and contractors can present one of the highest cyber security risks. For example, there is a risk that outsourced personnel may fail to comply with a firm's data security measures and inadvertently or otherwise allow undesirable sources access to its data.

PRINTERS AND COPIERS

While your computers may have ample firewall protection, printers and copiers are often overlooked. In fact, Columbia University recently completed two studies on how easy it was for hackers to exploit these devices' weaknesses in a cyber attack.

Additionally, if you are replacing your current printer or photocopier systems, you should ensure to wipe the hard drives clean before you dispose of them, to ensure that no private data can be retrieved from them afterwards.

HACKING

Hacking is perhaps the most common cyber risk facing SMEs and is of particular concern if you are storing clients' private data on your systems. However, customer confidentiality isn't the only part of your business at risk from hacking.

Hackers can also damage your website and delete archived information you may need to facilitate orders or sales and conduct your everyday business. A reputable firewall is an absolute necessity on all I.T. systems and your company website to provide vital protection against hacking.

If you believe your I.T. systems have been compromised, cyber insurance can help to cover the cost of contracting forensic experts to examine your system and trace any breaches.

HOW TO PROTECT YOUR BUSINESS AGAINST CYBER SECURITY THREATS

As technology has a more significant role in the business world, so does the threat of cyber attack. Data breaches can have a damaging impact on your business and can have an even more devastating effect if your clients' information is also compromised.

Use these simple steps to protect your company against cyber security threats.

1 CONDUCT REGULAR SECURITY AND RISK ASSESSMENTS

One of the first steps you should take to protect a business against cyber security threats is to conduct a risk assessment. Essentially, your company needs to determine what data requires protection, what security already exists, and if there are any gaps in this.

Once this has been completed, you can then develop a plan to protect the most important information, as well as identify the software, protocols and other steps you will need to implement to safeguard your business.

2 KEEP SECURITY SOFTWARE UP TO DATE

Though it may seem like a simple measure, keeping security software up to date is something many firms forget to do. This doesn't just include making sure any software subscriptions are renewed, but also modernising your anti-virus software and any other security measures whenever possible.

After all, cyber threats continue to become more sophisticated, making up to date software and firewalls essential to guard against new threats and keep your business's information secure.

3 DEVELOP A COMPANY SECURITY PROTOCOL

Once you have security protocols in place, it's time to educate your staff on how and why they should adhere to these. Inform staff regarding warning signs of malicious software or account takeovers, as well as how to respond to any suspected security threats. It should also be company policy that strong passwords are used, which are unique to their work accounts, and that no record of these is kept.

Additionally, a 'clean desk environment' should be implemented, wherein no confidential files are left exposed. Instead, they should be locked away in filing cabinets when not in use. Another key security measure all staff should take is to be sure not to work on confidential files on anything other than company devices, which should not leave the building without managerial permission.

4 ENSURE GDPR COMPLIANCE

In May 2018, the General Data Protection Regulation was implemented across Europe. The GDPR imposes strict rules on how companies control and process personal and identifiable information. Non–compliance with this regulation can result in fines up to 4% of the annual worldwide turnover or €20 million, whichever amount is greater.

Many larger businesses are required to hire a Data Protection Officer, who is responsible for ensuring GDPR compliance. However, it is still recommended that small to medium sized businesses consider hiring an external Data Protection Officer to help manage the task of compliance.

5 TAKE OUT CYBER INSURANCE COVER

Though having security measures and protocols in place protects your data, it's important to also take steps to safeguard your business in case your information is compromised. That's why every company, large or small, should take out comprehensive cyber security insurance.

Cyber insurance protects against data liability, administration obligations, as well as any risks to your company's reputation for security through slanderous accusations.

For full protection, ensure that your cyber risk insurance policy also includes liability coverage for claims that may occur due to your data vendors' errors and omission, as well as any accidental loss of data.

UNDERSTANDING YOUR CYBER INSURANCE NEEDS

Cyber insurance is commonly mistaken for something only big corporations need. Many smaller businesses view cyber cover as an unnecessary expense or are unclear what they are covered for.

To help you understand your specific business needs for cyber insurance, we have answered the most frequently asked questions.

1 WHAT EXACTLY IS CYBER INSURANCE?

Cyber insurance mitigates the repercussions of a data breach. Essentially, it makes sure your company is financially secure across all online activity (once it's legal). It covers the costs caused by loss of data, leaked information and network interruptions.

It even covers the cost of defending your reputation, and any expenses involved in responding to the situation. And yes, your policy will safeguard your business if your database is hacked.

2 WHY IS CYBER INSURANCE IMPORTANT?

Cyber insurance protects your business and its data. While it's all too easy to think that the only cyber security threat comes from hackers, who wouldn't be interested in attacking your business, unfortunately, that's not the case. Security threats come in all shapes and sizes and aren't all the result of malicious actions.

From an employee accidentally hitting 'send' to the wrong recipient when discussing confidential dealings to opening an innocent looking message with a nasty virus, there is a range of ways by which using the internet can hamper your business as much as it aids it.

3 WHO NEEDS CYBER INSURANCE?

If your business relies on information technology, you need cyber insurance. Businesses that store sensitive client information should be investing in a comprehensive policy.

For example, if you're a financial institution and details of your clients' business dealings leak, you could face a serious lawsuit. Similarly, if you're a medical centre that stores patient records, you need to have measures in place to protect yourself if the information is compromised.

However, it's just as important for any other business that relies on an internet connection to complete their work. From digital design agencies to gyms that use online booking systems – if you use a computer in your business, you need cyber insurance.

4 WHEN DO YOU NEED CYBER INSURANCE?

Cyber insurance can be considered something that's only relevant if your systems are undergoing updates or your security measures are temporarily not in place, but that's not the case. Your company should have a comprehensive policy in place at all times. Even businesses that are doing everything right can be the victims of cyber crime, or accidental data breaches.

You should also consider cyber insurance protection if you contract vendors to do digital, online or I.T. work on your behalf. After all, if they make an error or omission in their work that has consequences, you may be liable for a claim. As a result, you should make sure your policy includes a clause protecting your finances if a claim arises from the work a contracted company has completed.

Not all cyber security insurance policies are created equal. By getting expert advice, you'll know what's covered and what's not, how and when to notify the insurer about a possible claim and all the other important features of the policy.

OBF INSURANCE

OBF Insurance Group are one of the leading cyber insurance brokers and are happy to discuss your requirements today, simply call us on **01 660 1033** and one of our expert brokers will advise you.

OBF

INSURANCE GROUP

OBF are one of Ireland's leading cyber insurance brokers. Our team of experts understand the value of your business and professional reputation and will be happy to advise on the right cover to protect your business. Call us, e-mail us or visit our website today to get a competitive quote for comprehensive cyber insurance cover.

PHONE: +353 1 660 1033
FAX: +353 1 668 7985
E-MAIL: info@obf.ie
SITE: www.obf.ie

OBF Insurance Group Ltd.
Bridge House,
Baggot Street Bridge,
Dublin 4, Ireland, DO4 X2P1