I don't need Cyber and Data Protection Insurance… Do I?

Insurance. Not the most exciting topic to talk about, but vital to discuss when you consider just how vulnerable all business really are. So, what makes a business so vulnerable?

Are you vulnerable?

The first thing to question yourself on is if your business holds any sensitive customer data; this includes customer names, addresses, banking information and more. The next factor to consider is whether your business is reliant on computer systems to conduct business and/or if you have a website (though in 2020 it's hard not to take advantage of the exposure the internet can bring a business).

Finally, you must question whether your company is subject to a payment card industry (PCI) merchant services agreement. The PCI data security standard is used by businesses to enhance cardholder data security, and it applies to all merchants and service providers that process, transmit or store cardholder data.

Although, however safe you think you are with these card transactions, every business using this method to transfer money is subject to a data breach. In fact, any business that practices any of the above could be vulnerable to a data breach or loss of vital business services in the future. For this reason it's extremely important for every modern business to have cyber and data protection insurance, as you can never predict who the next cyber-attack victim will be.

Frankly Insurance and how cyber-crime can impact you

One of the best cyber and data protection insurance businesses is Frankly Insurance, who's policy cover's a vast range of accidents and breaches that may occur…

Covering breach costs is a general cover surrounding cyber and data protection, with Frankly Insurance offering support in the event of a data breach (electronic or otherwise) including forensic investigations, legal advice, notifying customers or regulators, and offering support such as credit monitoring to affected customers.

Some scams are a threat that this cover includes, such as social engineering scams; where access is gained to your network via an email link. Social engineering is extremely common as hackers will pretend to be someone they're not, either in person or through communication platforms such as email. They will then gain your trust, with you unknowingly giving them information they may need to hack into your system. Traditional protection from malware and viruses will not protect you from a social engineering attack, as the hacker here gathers pieces of information surrounding the business in order to exploit them, which can be very hard to pick up on.

Frankly Insurance also provides crisis containment cover, with a public relations firm who can provide expert support. This firm offers developing communication strategies and run a 24/7 crisis press office; allowing you to feel supported consistently knowing that there's a solution to any crisis you may have (and it's just a phone call way).
Cyber-crime can financially ruin a business, and all it takes is one hacker. This has been proven time and time again with both large and small corporations, therefore having cyber extortion protection on your side is a must have.

Having this means you will be protected if a hacker attempts to hold your business to ransom through ransomware (you will also have access to the services of a risk consultancy firm to help manage the situation if need be). Cyber-crime is also generally covered financially, as Frankly Insurance will cover direct financial loss following an external hack into your company's computer network. This could be ranging from theft of money, property, or your digital assets by hackers. They will also reimburse you for the costs of repair, restoration or replacement if a hacker causes damage to your websites, programmes or electronic data, as well as covering any external hack costs.

There are many different types of cyber-crime and accidental data breaches that may affect you, with the main five being social engineering, phishing attacks, employee breaching accidents, traditional hacking, and fraud artists. All five of these are just as dangerous to each other, and will cause a lot of damage to your business if any one of them occurs…

Telephone hacking is also covered; many aren't aware but phone systems get hacked more than you may think, with hackers getting into your system and making calls to high rate premium numbers that then pay themselves. So you may need to ask yourself: when did you

last update and check the security of your phones system, and how would you cope with a security breach such as this if you had no insurance to cover it?

Frankly Insurance will pay the costs of unauthorised telephone calls made by an external hacker following a breach of your computer network, therefore you would be secure knowing that even if this breach did happen, there would be no financial losses for your business.

Furthermore, compensation for loss of income will be provided generally, in case of an incident such as a hacker targeting your systems- therefore preventing your business from earning any revenue. This is known as cyber business interruption and can also be covered through gaining the cyber and data protection insurance.

Privacy protection is a big deal, and when a breach occurs and data is leaked: a big loss in finance and customers can follow. At Frankly Insurance, the costs associated with regulatory investigations and settle civil penalties levied by regulators will be paid when a situation like this happens (where allowed), and they will also pay to defend and settle claims made against your company for failing to keep customers' personal data secure, taking a huge weight off of your shoulders.
Finally, multimedia liability is covered, therefore you can feel secure with the knowledge that you are protected if you or any of your colleagues/ employees mistakenly infringe someone's copyright by using a picture online, for example, or inadvertently libel a third party in an email or other electronic communication.

Always have an action plan

Having a strong action plan for a cyber-attack or data breach is more important than ever, with these attacks in 2020 being a question of when it will happen; not if it will happen, as any business can become affected at any time. Getting cyber and data protection insurance such as this is your first step as a business in having a secure action plan, especially when you consider what you could lose if an attack were to happen.

This article was written by Catherine Smith from FreshStanceIT, using the information provided by Earl Franklin from Frankly Insurance.

Earl Franklin contact information:
Frankly Insurance Services Ltd Tel: 01727 634 300
Mobile: 07949 036 750 Email: earl@franklyinsurance.co.uk
Web: www.franklyinsurance.co.uk