PANGEAINSURANCE

CYBER INSURANCE

Pangea Insurance Brokers – Michael Piper

WHAT IS CYBER INSURANCE?

Cyber insurance (also known as cyber liability insurance or cyber security insurance) is designed to protect businesses against the financial loss resulting from a range of cyber threats and exposures, including cybercrime, data breach and system interruption.

PANGEAINSURANCE

WHAT DOES CYBER INSURANCE COVER?

- Cyber insurance covers financial losses caused by cyber events, cybercrime, and privacy breaches.
- Primarily covering the business loss of income caused by a cyber-attack, but additionally the costs to deal with and recover from the attack.
- Cover is also in place for your liability to third parties arising from a breach of privacy or loss of date.
- Business interruption losses are most often caused by ransomware and targeted extortion attacks. These attacks are not only frequent but can be incredibly expensive. In recent years, the sophistication of these attacks has made it more difficult to recover files, which can lead to extended system downtime, loss of profits, and reputational harm.
- Privacy breaches are also addressed under cyber insurance policies. If sensitive data is lost or stolen, businesses will need to notify affected individuals and regulators depending on their legal or regulatory requirements.

PANGEAINSURANCE

HOW IS A CYBER INSURANCE POLICY STRUCTURED?

FIRST PARTY COVERAGE - For losses that you experience yourself –

THIRD PARTY COVERAGE - For losses that a third party experiences but which you are responsible for.

With nearly all cyber insurance claims stemming from financial losses experienced by the business directly – such as ransomware – the main sections of cover are for first party coverages.

These include:

- Incident response, which picks up the costs associated with responding to a cyber incident such as forensic investigations and legal advice
- System damage and business interruption, which helps keep businesses up and running by covering the costs of data being restored and reimbursing loss of profits caused by the downtime

CYBER-CRIME, SOCIAL ENGINEERING AND FRAUD

Crime policies provide cover for fraud caused by employees and fraudulent acts by third parties. It is important to note such frauds and dishonesty are often now committed using computers, hence the confusion with cyber policies.

Some cyber policies offer a crime extension, but this still may not cover a business for all eventualities. The issue with crime extensions on cyber policies is that the cover can be narrower, even when the crime is perpetrated electronically.

Some extensions only cover pure electronic theft; therefore, if you are involved in any way – for example, if you open an attachment or transfer the money to the criminal, there is limited or even no cover at all.

It's also essential to remember that a cyber policy will not cover theft by an employee or a face-to-face trick, and a simple crime extension won't cover many traditional standalone crimes.

PANGEAINSURANCE

RISK MANAGEMENT AND SUPPORT

As well as putting adequate insurance in place, it is important for you to manage your own cyber risks as a business. This includes:

- Evaluating first and third party risks associated with the IT systems and networks in your business

- Assessing the potential events that could cause first or third party risks to materialise

- Analysing the controls that are currently in place and whether they need further improvement

Many insurers include technical assistance with managing a breach as part of the insurance policy, to offer specialist support from the legal, communications, and forensics assistance from experienced and knowledgeable companies.

Increasingly, insurers are adopting a similar approach in advance of any incidents, offering assessments, training, analysis in varying forms as part of a proactive management approach.

PANGEAINSURANCE

WHAT DO INSURERS LOOK FOR?

To varying degrees depending on the individual underwriter and their perception of your exposure insurers typically look for the following security to be in place:

- You encrypt sensitive information stored on portable media devices or laptops
- You have access control procedures around critical data stored on your network
- You have (either) encryption of hard drives and/or databases containing critical data
- You have Multi Factor Authentication (with a randomly generated token) enabled for remote access
- At least two members of staff review and authorise any transfers or funds, signing of cheques or the issuance of instructions for

the disbursement of assets, funds or investments above GBP 10,000

- You verify all requests to change customer/vendor/supplier details by confirming via a direct call, using known contact information
- Your back-ups are done on a weekly basis, stored off-site and segregated from your usual systems
- You have firewalls and anti-virus in place and they are updated in line with recommendations
- You or your IT outsourced service provider, have a patch management policy in place to implement

PANGEAINSURANCE

DO YOU NEED COVER?

Do you send or receive payments electronically?

Do you collect or store personally identifiable information (PII) like credit card numbers or health information?

Do you store business-critical information on your computer systems, such as client contracts, designs and plans, stock levels and other corporate information?

How long can your business operate without access to computer systems and the data they hold?

Do any of your employees work remotely?

Are you confident that you or your employees will never make a mistake?

PANGEAINSURANCE

CLAIMS EXAMPLES

Computer lockdown

A company director at a construction firm quite innocently clicks on a link in an email that he believes has come from one of his customers. To his horror his computer and the company's entire computer network are instantly locked with a message demanding a ransom payment of £2000 in bitcoin to restore things back to normal

Denial of service

A small online retailer makes the majority of their turnover in small windows of time, with seasonal goods. When their e-commerce website crashes it is suspected that a competitor has used a 'botnet' to shut the business down during a busy period, leading to severe business interruption and substantial impact on company finances.

Notifying customers

Following a cyber attack a retailer has to notify all customers affected that their personal information, including credit card details, may have been hacked. As well as the cost of sending out thousands of notifications, over the next few days the company is inundated with telephone calls and emails and has to cope with increased workloads to handle the volume of enquiries

Frozen food

A cold storage facility endures two days of business downtime and is forced to write off thousands of pounds worth of stock that has defrosted due to their warehouse management computer system being hacked.

PANGEAINSURANCE

THANK YOU

Pangea Insurance Brokers Ltd

Michael Piper

www.pangeainsurance.co.uk