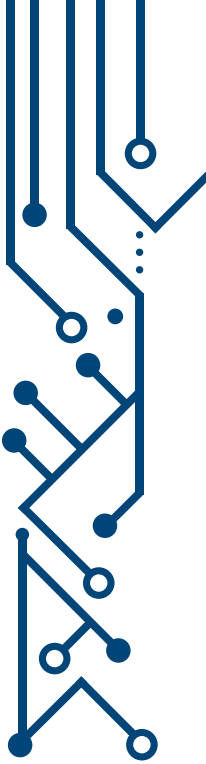
Making Sense of Cyber Insurance:
A Guide for SMEs

ABI Association of British Insurers

abi.org.uk @BritishInsurers

Contents

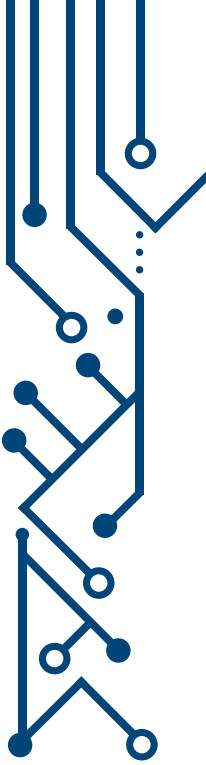


Introduction

Cyber threats are a growing and rapidly changing threat to UK businesses of all types and sizes. Although hacks and data breaches of major companies such as TalkTalk, Sony, Target and Ashley Madison make the headlines, the reality is that smaller companies are just as likely to be impacted by a cyber-attack, which accesses confidential data or business models, steals funds or mis-programmes essential equipment.

According to PwC's annual Global State of Information Security Survey 2016, there was a 38% increase in information security incidents for businesses of all sizes compared to the previous year.[1] The Federation of Small Businesses (FSB) has noted that 66% of SMEs do not consider their business to be vulnerable to cyber threats.[2] Yet the latest data shows that 74% of SMEs report they had suffered an information security breach in the past year and the average cost of the worst breach was between £75,000 and £310,800.[3] These statistics make stark reading. The size and variety of businesses at the SME level make them a natural target for cybercrime and fraud, as companies often hold customer data with lower levels of protection than major corporations.

This is why the insurance industry is playing a key role in supporting businesses of all sizes to both improve their resilience to cyber-attacks and to help them recover if the worst should occur. This guide sets out key features of cyber insurance policies to look for when you are seeking to insure your business. As you explore the protection afforded by cyber insurance it is also important to make sure your business is taking appropriate steps to manage the cyber risks that it faces. Checking the suitability of firewalls, updating malware protection and briefing staff on cyber security best practice are all good first steps; for a useful self-review and further advice, the Government's Cyber Essentials scheme[4] is a great place to start.



"74% of SMEs report they had suffered an information security breach in the past year"

1 http://www.pwc.com/gsiss

2 https://www.cyberstreetwise.com/blog/your-business-falling-any-cyber-security-%E2%80%98myths%E2%80%99

3 http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

Six Key Areas to Look Out For in Cyber Insurance Policies

1. Cyber Business Interruption Loss

This is a core aspect across all cyber insurance policies. Under this agreement if an IT failure or cyber-attack interrupts your business operations, insurers will cover your loss of income during the period of interruption, including if this is caused by increased costs of conducting business in the aftermath of the attack. This can be a critical safety net as you look to recover your normal working pattern.

2. Privacy Breach Costs

This is one of the largest and most critical sections to look for in a cyber insurance policy. It is either an extended single clause or sometimes can be split into two separate clauses: “Breach Costs” and “Privacy Liability”.

“Breach Costs” protection will cover your business for costs arising from dealing with a security breach. For example, notifying customers of a cyber breach, the costs of hiring a call centre to answer customer enquiries, the costs of public relations advice, IT forensic costs, any resulting legal fees or the costs of responding to regulatory bodies.

“Privacy Liability” protection will cover your business against claims of infringement of privacy and associated legal costs in the event of a breach. Usually this cover not only provides for payments to legitimate claimants but also the legal and regulatory defence costs arising from a privacy breach. This form of cover is especially relevant for businesses that handle or store any personal information from their customers.

3. Cyber Extortion

Cyber Extortion cover protects your business from ransomware and other malicious attempts to seize control of, and withhold access to, your operational or personal data until a fee is paid. This clause will typically provide for a reimbursement of the ransom amount demanded by the attacker as well as any consultant's fees to oversee the negotiation and transfer of funds to solve the ransom request. This clause is included as standard in most cyber insurance policies and is growing in prominence as more businesses move online and the use of ransomware proliferates. Ransomware systems such as "CryptoLocker" and "Cryptowall" have accrued millions of dollars in illegal profits according to reports by law enforcement agencies[5,6].

Paying an attacker to unlock your systems should not be the first course of action. Before any decision to pursue this course of action you should report the matter to the police, and also speak with your insurer to establish the conditions for them paying any cyber extortion expenses. Upon the resolution of a ransomware attack, your business should then look to repair the breach and improve security.

4. Digital Asset Replacement Expenses/"Hacker Damage"

This clause protects your business from damage inflicted by a hacker on digital assets. In particular it provides protection against the loss, corruption or alteration of data as well as the misuse of computer programmes and systems. Asset replacement expenses are especially relevant for firms that rely on online business models or on automated manufacturing systems where a hack could inflict significant damage to business operations.

5 http://www.washingtontimes.com/news/2015/nov/2/cybercriminals-rake-in-325m-cryptowall-ransomware/

6 http://www.theguardian.com/technology/2014/jun/02/cryptolocker-virus-nca-malware-protection

5. Media Liability

Media liability insures a business in the event that your digital media presence leads to a party bringing a claim against your business for libel, slander, defamation or the infringement of intellectual property rights. This clause is especially pertinent for companies that rely on the transmission of digital data via email or a website, rely on a large social media or digital content creation business model, or have significant advertising on their site that may lead to a liability.

6. Cyber Forensic Support

Cyber Forensic support is often included by insurers as a standalone clause or can sometimes be located under the more generic “Breach costs” clause explained above. In practice, cyber forensic support translates to having near-immediate 24/7 support from cyber specialists recommended by your insurer in the period following a hack or data breach. These specialists are able to assess your systems, identifying the source of any breach and suggesting preventative measures for the future. In addition, this support can often include advice on your legal, regulatory requirements as well as what steps to take to notify your customers of a data breach.

Potential Exclusions to Look Out For

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.

"Crime vs Cyber Insurance"

Cyber insurance will 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.

Further Information

This guide provides an introduction to the protection offered by cyber insurance, and is a starting point for those looking to enhance the protection of their business. Insurance can only ever be one part of the toolkit of preventative measures though, and as cyber threats continue to develop it is crucial that businesses also take steps to put in place strong cyber security. More information on cyber security can be found on the cyber pages of www.abi.org.uk or at the links below, which can further your understanding of cyber security initiatives in the UK.

Cyber Essentials

(www.cyberstreetwise.com/cyberessentials) is part of the Government's Cyber Street Wise initiative and provides businesses of all sizes with good standards of basic cyber security practice. Cyber Essentials is mandatory for businesses working on central government contracts which involve handling personal information and certain IT services. Available in two levels, Cyber Essentials and Cyber Essentials Plus, the assessments provide an identifiable certification to demonstrate that your business adheres to government standards.

The Cyber-security Information Sharing Partnership – CiSP

(www.cert.gov.uk/cisp) is a joint industry-government initiative for the sharing of cyber threat and vulnerability information. It is a free-to-join service provided and managed by CERT-UK. Members vary from large multi-nationals to SMEs across sectors, and the platform enables all participants to share cyber threat information. This helps increase the overall situational awareness of the cyber threat and therefore reduce the impact on UK businesses.

Responsible for Information

(www.nationalarchives.gov.uk/sme) is a free e-learning course aimed at the staff of SMEs. With a focus on helping staff to understand information security and cyber risks it can be used as an introductory step towards better cyber security awareness.

Association of British Insurers

May 2016

For more information
Association of British Insurers
One America Square
17 Crosswall
London EC3N 2LB
020 7600 3333

abi.org.uk **@BritishInsurers**