LOCKTON

UNCOMMONLY INDEPENDENT

Stay connected

Lockton Global Cyber & Technology

Comprehensive guide to cyber insurance

locktoninternational.com

Introduction

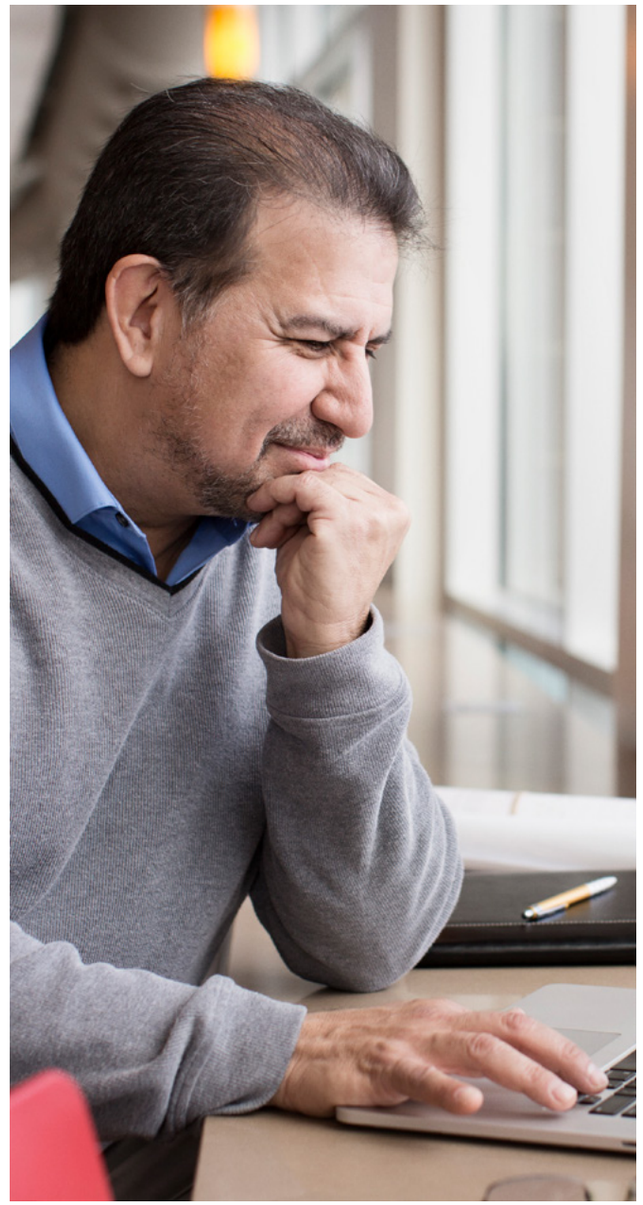
We live in an increasingly interconnected world where reliance on technology has become routine. The digitalisation of business has created huge opportunities and led to increased efficiency and growth, but with that rise has come an urgent need for more diligent focus on cyber-security.

Where is the risk?

We are all familiar with the work of hackers. A steady stream of global headlines over the past few years has introduced us to various types of cyber-attacks on businesses. However, one could be forgiven for thinking that these incidents are typically malicious and only focussed on high-profile organisations.

Nothing could be further from the truth. Virtually all businesses are at risk simply by operating a computer system. The threat increases in response to the number and scope of online services that are offered. Threats may stem from the following:

- Human error
- A disgruntled employee
- Computer system error or technical failure
- A targeted cyber-attack against an organisation
- Fall out from an attack on a supply chain partner
- Systemic infrastructure failure



What are the consequences?

When an organisation suffers a cyber-incident, it can lead to considerable financial loss.

The loss may be 'first party' i.e. loss to the business itself, including IT forensic costs, fees for legal advice, public relations and crisis management costs, business interruption losses or reputational damage.

Additional losses may be 'third party' i.e. losses related to claims made against an organisation, including for example, claims relating to: passing on a computer virus, costs associated with regulatory investigations, not providing access to online services, theft of a third party's confidential information, or release of private information into the public sphere. When these third-party losses are the subject of a legal claim against the business, there are also claim expenses to consider, on top of any damages.

Statistics

$3.86m

The average data breach cost in 2020[1]

23%

Human error caused 23% of breaches in 2020 [2]

52%

Percent of breaches caused by malicious attacks in 2020[3]

50%

Percent of organisations were hit by ransomware in 2020[4]

73%

Percent of cybercriminals succeeded in encrypting data[5]

1. Ponemon Institute and IBM Security: Cost of a Data Breach Report 2020. 2. Ibid. 3. Ibid. 4. Sophos: The State of Ransomware 2020: Results of an independent study of 5000 IT managers across 26 countries. 5. Ibid.

Cyber risk trends

By definition, the above statistics are a reflection of historical data. What are we likely to see in the future in relation to cyber risk?

Increased regulation

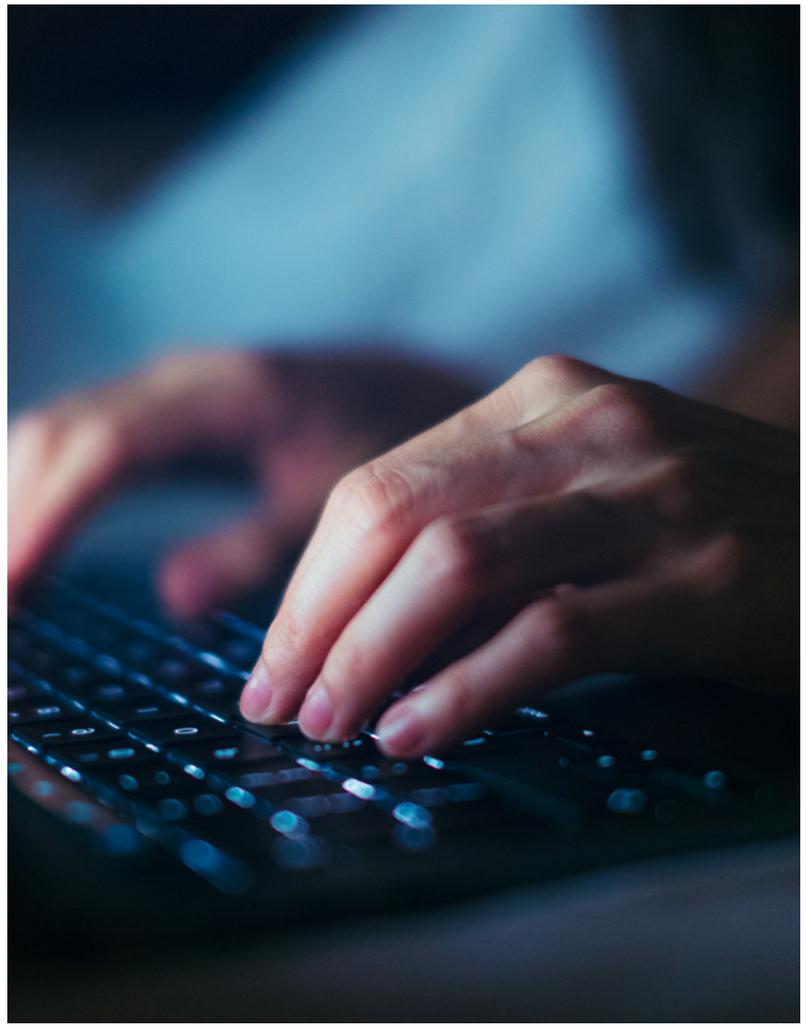
In response to the growing threat of cyber-crime and recognising the need to protect data subjects, regulators across the world are introducing new privacy regulation. Laws such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have put strict compliance regimes in place with significant consequences for breaches, including rigorous notification timeframes and hefty fines for non-compliance.

Growing sophistication of cyber attacks

In recent years, cyber-attacks have become increasingly sophisticated with threat actors constantly finding new ways to exploit vulnerabilities and avoid detection. We have seen a surge in ransomware attacks over the last few years, affecting organisations across a range of industries. The severity of these attacks has also increased, with eight figure ransoms now not uncommon.

Adoption of cloud-based software as a service

Organisations are becoming increasingly dependent on cloud-based infrastructure for running their business systems and storing sensitive information. Using cloud-based services can reduce operating costs and enable businesses to upscale their IT departments according to organisational demands. However, attacks against these services are on the rise, often due to misconfigured settings.



Protecting your organisation

There are several measures that businesses can take to minimise their cyber risk.

GOVERNANCE

- Appoint individuals with clear responsibility for cyber security and develop a clear plan of reporting through to the board/ management
- Invest in an incident response plan
- Invest in a business continuity plan
- Invest in a crisis communications plan, including an offline communication protocol

HUMAN FACTORS

- Invest in ongoing employee education, including the publication and distribution of policies and procedures covering phishing, transfer of funds, information security etc.
- Operate a 'safe' work environment where employees feel comfortable sharing information regarding possible compromised security

SECURITY

- Invest in vulnerability assessments, including penetration testing and red teaming
- Ensure additional procedures are put in place to counter increased network weaknesses involved in having a remote workforce, including multi-factor authentication, endpoint protection, the operation of remote desktops or VPNs, separation of employee and work data, safe use of portable devices, limited use of public Wi-Fi, security controls for video-conferencing etc.
- Install software updates, especially critical updates, on a regular and prioritised basis
- Backup data to secure platforms, preferably off-line. Generate multiple back-ups

RISK TRANSFER

- No matter how much a company invests in IT security, it will never be 100% secure. Furthermore, no firewall or virus protection will protect against human error or a rogue employee. While IT security is one part of the puzzle, cyber insurance is another. They are not mutually exclusive and should go hand-in-hand at all times
- A risk and insurance specialist can help you understand and quantify risk, and investing in a well-written cyber insurance policy will protect your balance sheet when an incident occurs

What is cyber insurance?

Background

Many people believe that cyber cover may already be addressed in other insurance policies they have purchased, such as property, or professional indemnity. Some overlaps exist (as they do with all lines of insurance) but traditional insurance policies lack the depth and breadth of standalone cyber cover, and won't come with experienced cyber claims and incident response capabilities.

Standalone cyber insurance is a relatively recent form of insurance that, in general terms, covers losses relating to damage to computer systems and networks. Cover extends in some policies, to incidents involving media as well as some data breaches. Issues relating to media acts and omissions, and relating to data breaches, are typically included because they often arise in the 'cyber' context.

Cyber policies have matured considerably since the earliest policies were developed some 20 years ago. While cyber insurance has not traditionally formed part of the 'standard business insurance suite', the exponential rise of cyber threats means that for any businesses, a standalone cyber policy should no longer be considered a discretionary spend.

A well-written cyber policy will have two components: first-party coverage (essentially to cover costs of investigating the incident and helping the business to become operational again, as quickly as possible), and third-party coverage (covering liabilities).

A market-leading policy will, as part of its first-party coverage, include access to a breach response team, whereby the insured obtains immediate access to expert consultants. This assistance is very welcome when the business is in a particularly vulnerable position post-incident. Cyber threats create considerable pressure, confusion and concern, so having immediate access to experts (including experienced ransom negotiators where necessary) is critical.

Recent data indicates that cyber insurance policies have one of the highest claims acceptance rates across all insurance products.

Find out more here

What does cyber insurance typically include?

While there is no 'standard' cyber policy, typically a policy will include the following:

First-party coverage

Breach event costs	Including all reasonable and necessary fees, costs and outside expenses, including IT forensics, legal expenses, public relations and crisis management expenses in the event of a system security breach and/or a privacy breach.
Business interruption loss	Addresses difference in net profit/loss as a result of network downtime (as a result of a system security breach or first-party administrative error). This can include fixed operating expenses.
Cyber extortion	Reimbursements for reasonable and necessary costs to end a ransomware event, including a ransom payment.
Digital asset loss	Including costs to replace, recreate or restore digital assets that have been damaged, destroyed, altered, misused or stolen as a result of a system security breach or first party administrative error.
Reputational harm reimbursement	Addresses difference in net profit/loss as a result of an adverse media event about the insured having experienced a system security breach or a privacy breach.

Third-party coverage

Privacy liability coverage	For the insured's legal liability to pay damages and claims expenses arising from a privacy breach.
Privacy regulatory liability	For the insured's legal liability to pay regulatory loss as a result of a civil regulatory action. This may include compensation awarded by the regulator, civil penalties or fines, to the extent insurable by law.
System security liability	For the insured's legal liability to pay damages and claims expenses arising from a system security breach.
Media liability coverage	For the insured's legal and contractual liability to pay damages and claims expenses as a result of wrongful acts of the insured in connection with the gathering, creation, broadcasting, publication and display of media.

What does cyber insurance not cover?

Bodily injury and property damage

Unless additional coverage is specifically purchased, standalone cyber insurance generally does not cover bodily injury or property damage claims arising out of a cyber-security incident. Nevertheless, coverage is available through specialist markets and subject to an additional premium.

System failure

Cyber insurance does not typically cover system failure liability to a third party brought about by a non-malicious incident (although business interruption losses to the insured may well be covered).

Systemic infrastructure failure

Losses from systemic infrastructure failure are not typically covered, for example, if there were a large-scale internet failure.

Loss of funds

Theft or loss of funds (even those due to a cyber-attack) are not generally covered under a cyber policy, but may be covered under a separate crime policy. Some cyber policies may have a modest sub-limit for monetary loss, but for larger risks, separate crime cover should be considered.

Final note

As a final note, some underwriting markets have more appetite than others when it comes to cyber risk, and may be more inclined to write business in a particular industry sector than others.

Case studies

1

A medium-sized law firm's network is breached, putting confidential client information at risk. The information includes a draft acquisition letter for a company merger and a draft prospectus for a public energy company. The firm later receives an email from an unknown source requesting a payment of £50,000 in bitcoin in exchange for a promise not to sell the information on the black market.

How should the cyber insurance policy respond?

Breach response costs:

- Legal expertise to manage and advise on incident response.
- Cost for IT forensics to establish the scope of the incident.
- Cost of PR firm to manage the incident response communication.
- Notification costs to notify any affected individuals and the regulatory agency.

Cyber extortion loss:

- Cost related to the extortion event, plus any ransom payment.

Privacy liability coverage:

- Cost to respond to third party claims and reimbursement of damages.

Privacy regulatory liability coverage:

- Costs to respond to regulatory claims and regulatory penalties or fines when insurable by law.

2

The HR administrator of an accountancy firm receives an email pertaining to be from the Chief Operating Officer (COO) asking for all staff and contractors' personal details for an audit. After the information is sent, it is revealed that the email did not come from the COO and the information has been stolen by an attacker.

How should the cyber insurance policy respond?

Breach response costs:

- Cost of legal expertise to manage and advise on incident response.
- Cost of IT Forensics to establish the scope of the incident.
- Cost of PR firm to manage the incident response communication.
- Notification costs for notify any affected individuals and the regulatory agency.

Privacy liability coverage:

- Cost to respond to third party claims and reimbursement of damages.

Regulatory liability coverage:

- Cost to respond to regulatory claims and regulatory penalties or fines, when insurable by law.

3

An employee intends to forward a client email to a colleague with some negative comments about the individual who had sent the email. Instead of forwarding, the employee accidently replied to everyone in copy. The individual affected brought a defamation lawsuit against the organisation for harming their reputation.

How should the cyber insurance policy respond?

Media liability coverage:

- Costs to respond to the defamation lawsuit and reimbursement of any damages.

4

The IT department of a PR firm is undertaking work to upgrade its systems when it experiences a failure. The system takes several days to restore fully, during which time employees do not have access to email or files. This causes significant disruption to the business.

How should the cyber insurance policy respond?

Breach response costs:

- Cost of legal expertise to manage and advise on incident response.
- Cost of IT forensics to establish the scope of the incident.
- Cost of PR firm to manage the incident response communication.

Digital asset reimbursement:

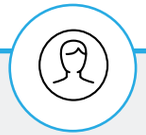
- Cost to replace, recreate or restore digital assets which have been damaged, destroyed or altered as a result of the system failure.

Network interruption event:

- Reimbursement of the difference in net profit/ loss as a result of the network downtime.

The process and cost

Each carrier will have a multi-page application for what it considers to be normal elements of a healthy and secure network and might (per industry) have specialised questions that fit the specific business vertical in which they are underwriting. Generally, carriers will want to know how an organisation is performing in the following areas:

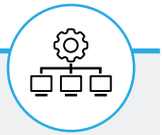


People

- Training and awareness
- Access control

Process

- Governance frameworks
- Policies and procedures
- Management of vendors
- Management systems
- Audit regimes



Technology

- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Detection and monitoring

It is helpful to have a methodology that demonstrates that both the business and network are prepared to deal with any cyber eventuality. These steps can include: employing a fully operational 'patching' policy, multi-factor authentication, endpoint protection, employee training, back-up policies, supply chain risk identification and management, and a vulnerability assessment. If an organisation is part of a regulatory body, a description of regulated-entity compliance processes would be beneficial. While not mandatory, such information demonstrates robust cyber hygiene.

The cost of a policy is based upon the limit of liability sought, together with the risk perceived by the insurance underwriter. There is generally no set formula nor 'standard' premium, although underwriters will take into consideration the size of the company's revenues, the amount and type of sensitive data it holds, the industry to which it belongs, and the risk controls in place.

Coverage levels

Whether buying for the first time or renewing a cyber policy, one of the key considerations is how much limit to purchase. There are several factors that need to be considered here.

Firstly, any limit purchased needs to be weighed against the perceived exposure of the business. Cyber exposure is difficult to quantify and insurers, together with other risk professionals, are trying to gather as much data as possible to assist in this. Listed below are some broad considerations, though these should be discussed with your Lockton broker prior to deciding on an appropriate limit.

Estimating costs

- The majority of cyber claims are made up of first-party costs that the business incurs directly. These include breach response costs such as IT forensic fees (to triage, contain and then rebuild systems), legal advice (necessary in the aftermath of an incident), as well as any notification costs required.
- Another cost to consider is that of ransomware; a threat that is currently growing exponentially, driving up breach response costs as a result. Ransomware can come with a sizeable ransom demand. These types of claims are now regularly hitting six and sometimes seven or eight figures.
- A key exposure for any business is the sensitive data held on its clients. When considering cover limits, estimates around the cost of losing this data and dealing with claims that may arise is critical. This exposure will vary for all types of businesses but has particular relevance for professional service firms.
- Conversely, a key exposure for other businesses (particularly in the manufacturing sector) will be business interruption. How long can a business sustain itself offline before its business interruption losses necessitate the purchase of cyber cover? Also important in this context will be the 'waiting period' – the period of time which must pass prior to a valid claim being notified (typically 8-12 hours). Needs will vary from business to business and different waiting periods will be sustainable.
- Another consideration is the impact of the 'silent cyber' effect. Historically, many businesses have relied on their professional indemnity (PI) policy for cover in the event of a cyber incident. From 1 January 2021, many Lloyd's markets are excluding or reducing cyber risk from PI policies and non-Lloyd's markets are also reviewing their positions. This could mean that there is limited or reduced cyber cover available under your existing PI policy, thereby increasing the need of a standalone cyber policy. If you already have a cyber policy in place then the limit ought to be reviewed. Further, even if cyber cover is not excluded per se, it is important to note that PI polices may only include limited (if any) first-party costs. For further details, see the **'Silent cyber'** section of this brochure.

Benchmarking

In order to provide clients with further detail on potential cyber losses and assess appropriate levels of cover, Lockton has partnered with CyberCube. This analytics firm takes data on a particular business and models that against 50,000 possible cyber events and loss scenarios. A simple loss curve is then produced, which facilitates the discussion as to how much risk a business ought to transfer by way of insurance.

This valuable tool is available to Lockton clients, providing a snapshot of the potential cyber exposure a business faces.

Silent cyber

Background

Cyber risk is everywhere and as such threatens many lines of insurance. Elements of cyber cover have traditionally been found under policies other than cyber, such as property, kidnap and ransom, or professional indemnity. However, this threat is not always affirmatively addressed within these policies. Insurers in non-cyber markets have not always fully considered the implications of cyber exposures, nor have they tackled the potential aggregation over their various types of policies.

This 'silence' in non-cyber policies does not necessarily mean cover is not there – just that it is not affirmative and coverage cannot be guaranteed, potentially leading to both coverage and claim reporting issues.

The growing size and sophistication of the standalone cyber market and the increased cyber risk, have been additional factors prompting a re-evaluation of cyber-specific risks over various lines of insurance.

Regulatory scrutiny by the Prudential Regulation Authority (PRA) into these risks, and the PRA's requirement that insurers suitably identify, assess and manage their cyber liabilities, were factors in Lloyd's issuing a mandate in July 2019. The mandate required Lloyd's underwriters either to affirm or exclude cyber cover in various lines of insurance. Cyber should no longer remain 'silent'.

Effects of the mandate

The insurance markets are responding to the Lloyd's mandate in a variety of ways, and there are countless versions of cyber endorsements currently in play on non-cyber lines of insurance, reflecting these differing interpretations, as well as market appetite. The preparedness to affirm or exclude cyber cover in non-cyber policies, is by no means consistent, and some "silent" cyber currently available may no longer be offered by non-cyber underwriters.

This necessitates a close consideration of standalone cyber insurance, as well as a reassessment of limits for any existing cyber cover. Every scenario is different and each situation should be assessed on its facts.

How Lockton can help

Led by a premier global team of more than 50 cyber brokers and advisors, Lockton's Global Cyber & Technology team is dedicated to delivering unparalleled service and innovative programmes for your organisational needs.

The team offers a wide range of expertise in risk identification, protection and management, as well as the proven delivery of results. Specialists from across the cyber industry are on hand to support the team, including cyber claims experts, ex-CISOs and legally qualified technicians.

For further information, please contact the Global Cyber & Technology team.

Mark Luckin
Head of Cyber & Technology
Lockton Global Cyber & Technology

T: +61 433 337 922
E. mark.luckin@au.lockton.com

What can we offer?

Broad and extensive insurer relationships, across both London and international markets

Market leading proprietary policy forms

More than 300 incidents handled each year with a 99% covered claim rate to date

Lockton is the world's largest independent insurance brokerage.

8,000+	96%	$38	125	60,000+
Associates	Client retention rate	Over $38 billion premiums placed	Clients in over 125 countries	Clients

100+	10.3%	$1.8	90%
Offices worldwide	Annual organic growth since 2000	Billion revenue	Reinvestment due to our private ownership

Lockton is a global professional services firm with over 8,000 Associates who advise clients on protecting their people, property and reputations. Lockton has grown to become the world's largest privately held, independent insurance broker by helping clients achieve their business objectives. For nine consecutive years, Business Insurance magazine has recognised Lockton as a 'Best Place to Work in Insurance'.

Our 96% client retention rate speaks for itself.

Independence changes everything.

As a family-owned organisation, we're not driven by the quarterly pressure of financial markets. This kind of independence frees us to always act in the best interest of our clients and creates an entirely different dynamic—one that's focused on your success.

locktoninternational.com

Stay connected

LOCKTON®

UNCOMMONLY INDEPENDENT