WHITE PAPER

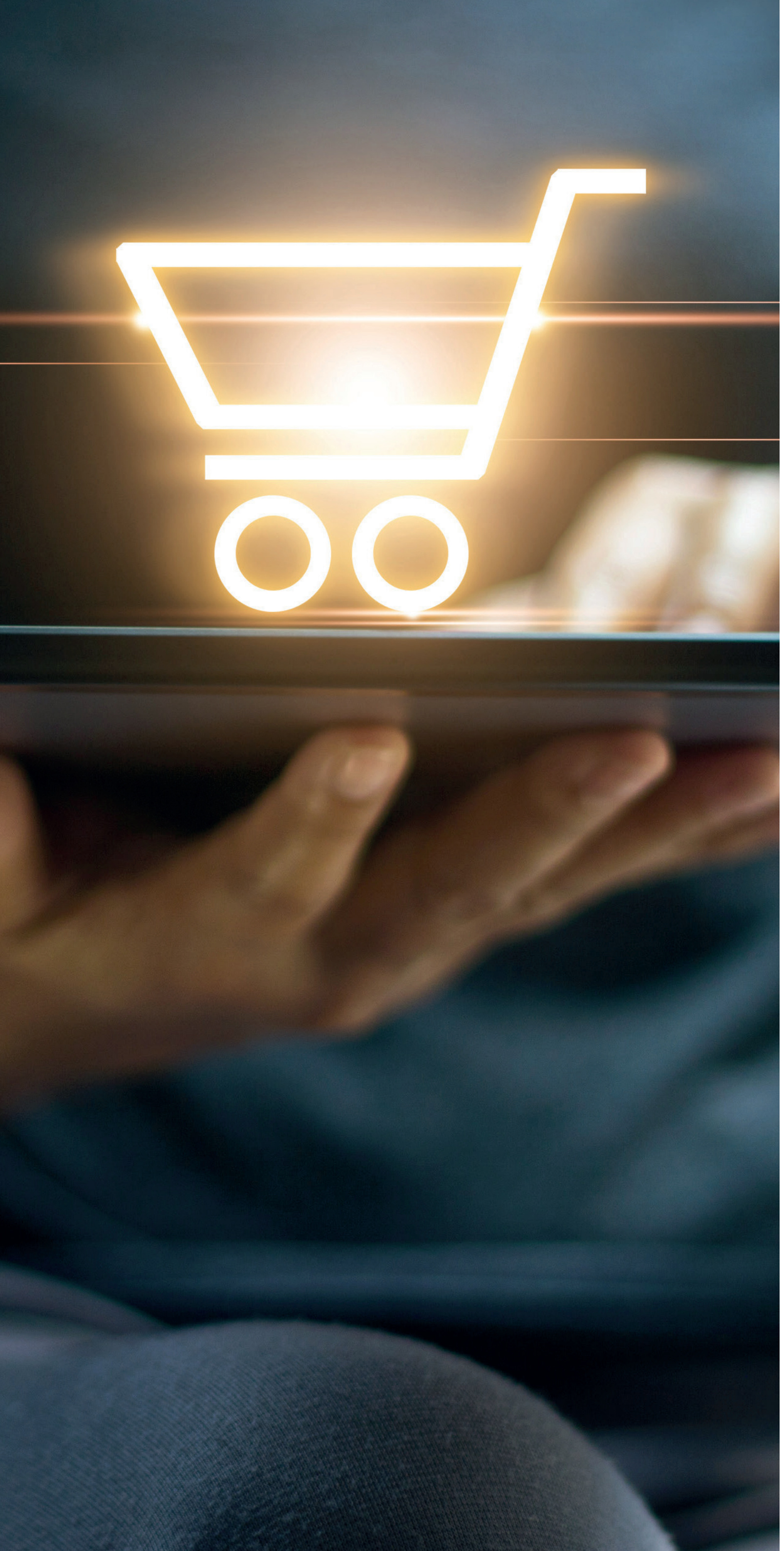
In-store to online

Cyber risks in the retail sector

LOCKTON RETAIL PRACTICE GROUP

LOCKTON®

UNCOMMONLY INDEPENDENT



Introduction

As we all remember, March 2020 saw Covid-19 declared as a global pandemic, forcing all non-essential businesses to shut their doors until further notice. This sudden and rapid operational interruption impacted various sectors enormously, especially the retail sector.

In order to resume operations while complying with the imposed governmental restrictions, many retailers had to initiate an instant shift in their business models, moving their activities and operations from in-store to exclusively online.

The sector is now more connected, efficient and reliable than ever, with proprietary sales platforms and online payment processes working more smoothly than in pre-pandemic times. With improved functionality and applications, retail operations have moved forward dramatically, accelerated by lockdown and the surge in online shopping. Digitalisation is now critical to being a successful retailer, and those organisations who get it wrong run the risk of going out of business. In the past 18 months, we witnessed the closure of numerous big brands that struggled to survive the changes triggered by the pandemic. More than 17,000[1] retailers went into insolvency and almost 190,000[2] jobs were lost as a consequence.

Although digitalisation clearly has considerable merits for both retailers and customers, it also has its drawbacks. The greater the drive for network systems to meet the increasing demand for speed, efficiency, control and convenience, the greater the vulnerability to cyber-attacks or to simple human error.

Cyber-related threats were always an appreciable risk to retailers, but that risk has been significantly exacerbated by the rapid shift in the sector’s traditional business model.

Cyber risk within the retail space can be defined as any kind of risk that emerges from the use of information and communication technology. It can take many forms, from distributed denial of service (DDoS) attacks, malware variants or disgruntled employees compromising cyber protocols, to an innocent and accidental click on a malware link embedded within a phishing email. Arguably, the most prevalent cyber threat in the retail sector is ransomware; the industry is particularly susceptible to extortion attempts, often timed to coincide with significant shopping dates to ensure maximum leverage is brought to bear on the retailer.

Regardless of the size, location or sub-sector, all retail businesses face the risk of a major cyber-incident. With the average cost of data breaches rising to £3.36 million[3] per incident in the UK in 2021 due to the increased remote working and utilisation of cloud technologies, retailers are now urged to manage their cybersecurity systems and processes actively.

Beware the ransomware
Case study

A high-profile online retailer recently experienced a cyber-attack in the form of ransomware variation REvil, also known as Sodinokibi. The attack took place during a holiday season, presumably so that the business would be under maximum pressure.

The criminals contacted the retailer advising that its e-commerce site had been encrypted, seeking a ransom in exchange for the decryption key. However, in the manner typical of this 'two-pronged' attack, the criminals also claimed to have copied 1.5 terabytes of private information. Shortly afterwards, the retailer received a second ransom demand, stating that the exfiltrated customer records would be released into the public domain unless the second demand was met within ten days.

The focus was on restoration of critical services and returning the business to usual operation as quickly as possible, with priority given to the online sales platform and the protection of customer data. A disaster recovery process was put in place and managed, and after a hiatus of four days, business and sales were able to continue (although many online shopping carts were left 'abandoned', with a likely attrition of customers to competing retailers). The threat of data breach was managed successfully with the involvement of a specialist ransomware negotiator.

While the online sales platform was down for four days, other aspects of the infrastructure were restored over a much longer period. The company continued to have issues with the following, for a further six months:

- An unstable and slow payroll system
- Unreliable network unavailability
- Slow desktop service
- Some systems still being offline

The business-impact timeline continued during this time, with ongoing financial and reputational effects on the retailer. The full effect of the cyber-attack is still being assessed, but the adverse media surrounding the original attack – coupled with the ongoing operational issues – has caused considerable damage to the retailer's brand and reputation. Loss of revenue due to the original business interruption was significant, but has been exacerbated since by significant customer attrition.

Why the retail sector?

The case study discussed is one of many cyber incidents that highlight the drastic impact of cyber risks on an organisation's financial health, business continuity and reputation.

Cyber risks are inherent to the retail sector, especially during this era of digitalisation. The Covid-19 pandemic had prompted a surge in dependence on IT systems, whereby retail businesses had to rely fully on their online presence to continue their operations during the global lockdown. Amid the increase in online shopping and use of shopping applications, retailers are accumulating large volumes of personal data and credit card information. Unsurprisingly, the retail sector is now exposed to greater cyber risk than ever.

In a survey conducted by the British Retail Consortium (BRC)[4] this year, it was evident that 54% of the surveyed retailers had witnessed an increase in cyber-attacks and threats in comparison to 2020. Ransomware, malware and theft of data were seen as significant threats by the majority of the surveyed retailers, with ransomware in particular ranked as the biggest threat by over 70% of the retailers. Furthermore, 38% of the retailers said that cyber security was a significant cause of concern over the next couple of years in terms of retail crime. To mitigate the risk of cyber threats and aid crime prevention, the retail sector collectively spent £160 million between 2019 and 2020 on cyber security.

In addition to the rapid advancement in e-commerce, innovation, and the storage of more personal data online, retailers have become a prime target for cybercrime. Attackers will target retailers for a number of reasons, notably:

- To create major financial chaos. For example, distributed denial of service (DDoS) attacks, which are designed to flood the target's network with huge traffic volumes, and are often deliberately timed to coincide with peak sales periods to increase the threat
- To steal store credits, gift cards and loyalty points
- The increasing use of IoT devices in physical stores (e.g. to control temperature, vibration, humidity) create a larger attack surface
- Hackers can take advantage of a lack of ongoing training and vigilance among staff when it comes to phishing attacks

Understanding your cyber risks

To prepare and prevent cyber-attacks effectively, every retail business should thoroughly understand the diverse nature, impact, and origin of cyber risks, which will typically involve privacy breaches and/or business interruption losses.

It is important to acknowledge that cyber risks are not always external or malicious, they could also arise internally from human error, negligence, system faults and weaknesses, or even deliberate criminal acts by the employees.

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) or 'third party' (i.e. losses related to claims made against a retailer).

Retailer exposures following a cyber-attack

- Cyber extortion demands and expenses
- Liability to third parties for data breaches and the failure to protect confidential information
- Liability to third parties for cyber events, such as spreading of malware, or an inability to access online services
- Regulatory investigations, fines and penalties
- First party costs to remediate a cyber-attack, including legal fees, public relations costs, IT forensic costs
- Reallocation of internal resources
- Business interruption loss
- Reputational harm
- Damage to hardware and/or software including digital assets

The supply chain

As discussed in the Cyber Resilience Toolkit for Retailers by BRC[5], to protect a retail business against a potential cyber incident, any retailer should identify the key areas of the business that would be impacted in the event of a cyber-incident in addition to the assets that could be jeopardised.

Retailers are part of a long chain of suppliers, any of which could be targeted at any point in time. In fact, to feel the effects of an attack, a business does not need to be a 'target' per se, as evidenced by the SolarWinds, Microsoft Exchange and Accellion supply chain attacks.. Hence, understanding one's own business is not sufficient; a full appreciation of potential cyber threats to its suppliers is critical.

Furthermore, considering the changing nature of cyber threats, businesses are advised to assess and monitor the evolving cyber arena, adapting its business continuity plan, and disaster recovery response accordingly.

Examples of cyber risk

External threats

DATA BREACH

The ICO defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss or unlawful destructions, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service'.

WEB APPLICATION BASED ATTACKS

For example SQL injection attacks (SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker))

DENIAL OF SERVICE ATTACK (DOS)

A method of taking a website out of action by overloading or 'flooding' the server.

LOCKED ACCOUNTS

Where customers are (usually temporarily) unable to log into their accounts as a result of criminal activity on systems such as, for example, DOS attacks.

WHALING

A type of spear phising (i.e. specifically directed) attack, such as an email spoofing attempt, that targets senior members ('big fish') of a specific organisation, seeking unauthorised access to confidential data.

DOXING

Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.

HALWARE

A program or malicious software that consists of programming, for example code or scripts, designed to disrupt the performance of PCs, laptops, handheld devices etc.

PORT SCANNING

A technique employed to identify open ports and services on a network, potentially with a view to exploiting weakness illegally.

SOCIAL ENGINEERING

In cyber security context, the general art of manipulating people online so they give up confidential information.

PHISHING

A method of accessing valuable personal details, such as username and passwords, often through bogus communications such as emails, letters, instant messages or text messages.

PHARMING

A method of deceiving an individual into ending up at a fake website, even through the correct URL has been entered.

SPEAR PHISING

As per phishing, except that it is a directed attack against a specific target.

THEFT OF DATA

Stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

RANSOMWARE

A type of malware that prevents the us of a system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

Source: BRC Crime Survey 2021 – types of cyber risks

External cyber threats are varied and diverse by nature. Each threat is driven by a specific motive and a desired end result. For example, a Denial of Service (DOS) attack may disrupt a retailer's servers and prevent clients from accessing their accounts or processing orders, while a data breach not only exposes the targeted entity, but also a business's customers.

Taking account of this rapidly changing cyber space and the varying motives driving cyber-attacks, retailers are urged not only to understand the nature and types of cyber risks, but also the elements of their business that increases their exposure and appeal to cyber criminals. These include: software vulnerabilities, dependence on online platforms and payments systems, or the type of customer data held.

External threats loom large and necessitate a strong cyber security stance.

Internal threats

However, no number of fire walls or versions of anti-virus software will protect against insider threats. One survey[6] showed that about 62% of employees believed it acceptable to transfer work documents to personal devices. A more recent report[7] showed the average global costs of insider threat rose by 31% in two years.

Insider threat profiles include:

- Negligent insiders: employees or contractors unintentionally leaking data
- Criminal and malicious insiders: those intentionally leaking data
- Credential thieves: those who target insiders' login information.

Cyber risk management

Implementing a robust cyber risk management framework is crucial. It is important for retailers to consider four parts of the process as follows:

GOVERNANCE

- Appoint individuals with clear responsibility for cyber security and develop a clear plan 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 off-line communication protocol

HUMAN FACTORS

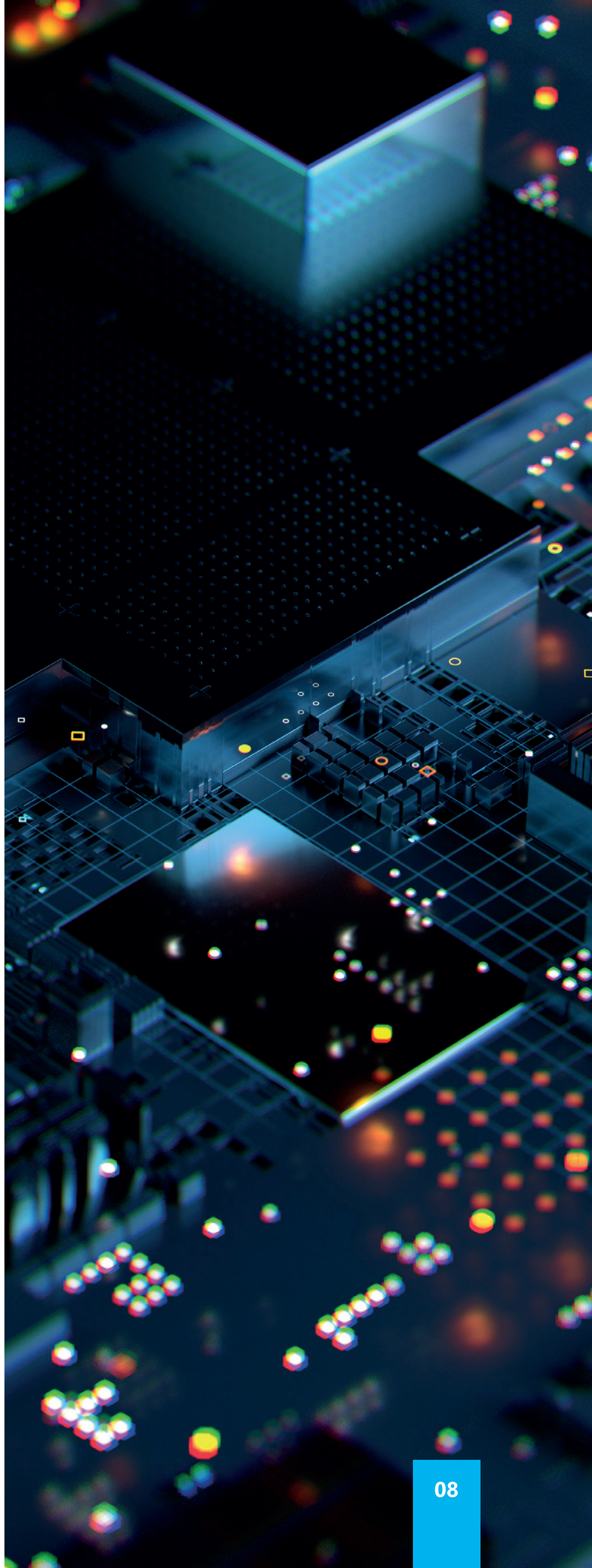
- Invest in ongoing employee education, including the publication and distribution of policies and procedures covering phishing, transfer of funds, information security etc.
- Operate a 'safe' work environment where employees feel comfortable sharing information regarding possible compromised security

SECURITY

- Invest in vulnerability assessments, including penetration testing and red teaming
- Ensure additional procedures are put in place to counter increased network weaknesses 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 us 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
- Back-up 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



Governance

Cyber risks pose a serious threat to the financial health, operational continuity and reputation of any retail business. Retailers are at risk simply by operating a computer system. The threat increases in relation to the number and scope of online services that are offered, consequently this needs to be identified, assessed, mitigated and, where appropriate, transferred.

Cyber risk is not just a technical issue, it is an organisational risk that threatens all aspects of a retail business and needs to be dealt with at governance level. In order to protect the business appropriately, the management team must ensure clear responsibility and ongoing vigilance; this will help to protect the retailer from the potentially catastrophic financial or reputational effects of a cyber-incident.

To ensure that the management fully understands the potential cyber threats and their consequences, it is crucial for the board and IT team to communicate openly and regularly, ensuring proper protocols are in place.

Despite the recent surge in cyber-attacks, and particularly ransomware assaults, research by the Institute of Directors indicates a disconnect between IT staff, who live and breathe cyber-security and understand the consequences, and the management team.

Quite apart from the business management of risk, the issue of potential personal exposure for directors and officers for failing to mitigate cyber risk is a real and ever-present issue.

Human factors

Human error remains the greatest cyber threat to an organisation and arguably the most underrated. Error can occur in many ways including:

- Clicking on phishing links
- Inadvertent data breaches or sharing of other sensitive information
- Weak passwords
- Inappropriate use of public Wi-Fi
- Failing to implement software updates regularly

Investing in cyber security awareness and education for employees is critical and dynamic, as threats change and become increasingly sophisticated.

Security

As cyber-attacks morph and threat actors find new ways to exploit vulnerabilities and avoid detection, it is vital for retailers to look very closely at the cyber hygiene protocols. Examples of such protocols are set out above, many of which have now become ‘mandatory’ rather than discretionary or simply ‘good practice’.

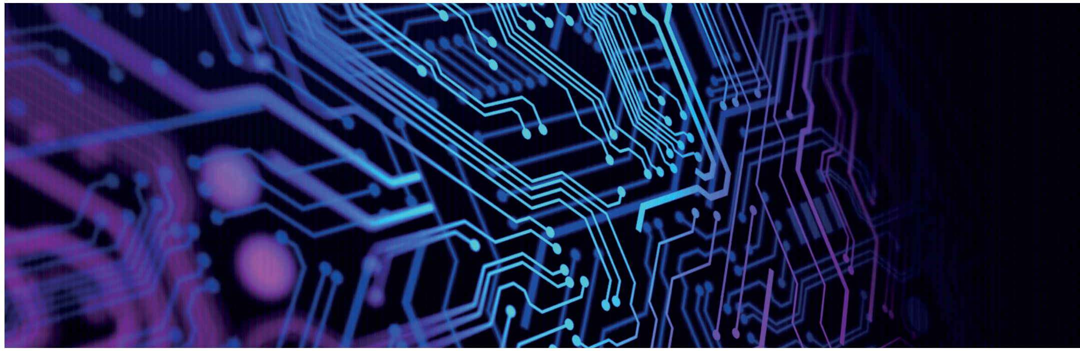
Partnering with a good cyber security firm will be of real benefit in the identification and mitigation of cyber threats, both internal and external.

Risk transfer

An important risk mitigation process is the transfer of risk to insurance.

Contrary to popular belief, property, casualty and other traditional policies are not always designed to respond to a cyber-incident. In fact, in the last several years, insurers in these areas have taken steps to specifically exclude coverage related to a cyber-attack from their policies. Specialist cyber insurance is often a better option.

Although some overlaps exist, as they do with all lines of insurance, traditional insurance policies lack the depth and breadth of standalone cyber cover and will not come with experienced cyber claims and incident response capabilities. 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.



10 Steps to Cyber Security

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. The NCSC recommends you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives

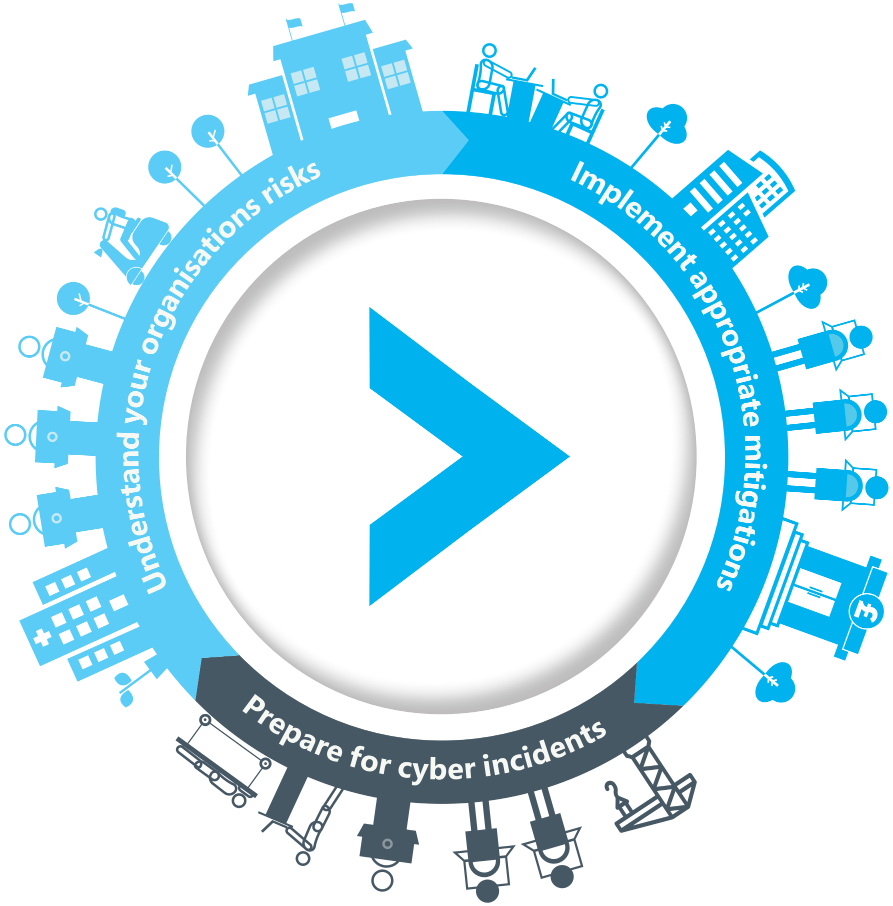
Risk Management
Take a risk-based approach to securing your data and systems.

Engagement and training
Collaboratively build security that works for people in your organisation.

Asset management
Know what data and systems you have and what business need they support.

Architecture and configuration
Design, build, maintain and manage systems securely.

Vulnerability management
Keep your systems protected throughout their lifecycle.


Understand your organisations risks
Implement appropriate mitigations
Prepare for cyber incidents

Identity and access management
Control who and what can access your systems and data.

Data security
Protect data where it is vulnerable.

Logging and monitoring
Design your systems to be able to detect and investigate incidents.

Incident management
Plan your response to cuber incidents in advance.

Supply chain security
Collaborate with your suppliers and partners.

Cyber insurance

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 the media and 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.

A fundamental part of a standalone cyber policy is the first party breach response services. These include IT forensics and legal counsel, as well as public relations and crisis management consultants to mitigate damage and ensure the business is operational again as soon as possible. This is in addition to the third-party liability cover.

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 business, 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.

Cyber liability purchase process and cost

Each insurer 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, insurers will want to know how a retail business 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.

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.

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 broker prior to deciding on an appropriate limit.

There are several factors to be considered when estimating costs, including:

- 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. Due to the exponential growth in ransomware threats, a drive in breach response costs has occurred in the past few years. 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 retail business is the sensitive data held on its customers. When considering cover limits, it is crucial to estimate the cost of losing this data and dealing with claims that may arise.
- Another significant exposure for a retail business is 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.
- The impact of the 'silent cyber' effect must also be considered. 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 for a standalone cyber policy. If you already have a cyber-policy in place, 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.

Cyber market appetite

Cyber risk and the costs of dealing with a cyber incident are headline news for all business sectors in 2021 - the retail sector is no exception. The sector remains under consistent threat, with over 60% of UK retailers having experienced a cyber attack in 2020. The cyber insurance market has been 'hardening' very quickly over the past two years. As a result, insurers are understandably nervous, creating uncertain market dynamics.

The retail sector is witnessing a massive increase in cyber insurance premiums and deductibles, where retentions are being adjusted to a multiple of what they used to be and premiums are increasing by circa 100%. The change in the way risks are viewed and scrutinised by insurers means that better cyber hygiene is necessary for all retail businesses looking to obtain cyber cover. Cyber insurers are demanding minimum controls and standards to be in place to procure or even renew a cyber insurance policy.

Key changes in the cyber insurance landscape to consider and prepare for include:

Premium rate

- A minimum of a 75% premium increase is to be expected at renewal.
- Recently, the market has seen a few examples where the premium rate has increased by more than 400%! Such drastic increases are not necessarily the norm, but it provides an indication that nothing is 'off the table'. If a business has also suffered from losses, the renewal outcome could be even worse.
- Self-insured retentions are up by an average of 100%, but 200-300% increases are not uncommon.

Capacity

- Global capacity has reduced substantially with the majority of insurance companies reducing maximum capacity by 25-50% on any single layer.
- Certain markets require higher attachment points (e.g. £40-50m) for more exposed risks.

Scrutiny and exposure

- If a retail business does not have multi-factor authentication (MFA) for remote access, Office 365 and Remote Desktop Protocol (RDP) in place at renewal, there is a strong possibility that they will not be able to renew or purchase cyber insurance.
- If Ransomware controls are deemed to be insufficient, there is a strong possibility that insurers will impose sub-limits and co-insurance for any losses arising out of Ransomware.
- Insurers are requiring full ransomware applications at renewal, in addition to a regular application. These are detailed documents, which can take time to complete. In addition to ransomware supplements, there will be a request for further information or clarification as the threat landscape continues to change.

Lockton's credentials

Lockton's global cyber and technology team of more than 20 specialist cyber brokers and advisors offers a wide range of expertise in risk identification, protection and management.

How we work with our clients

We support our clients in this difficult market by maximising insurer interest to obtain the best possible terms. We ensure the pre-submission stage is comprehensive and that every point is reviewed so that our clients are not negatively impacted by a lack of information. Our leading proprietary wording is supported by some of the biggest syndicates. It is updated annually and has backed some of the largest claims in the market. Our expertise is integrated, with our cyber claims specialists working alongside the placement team.

Michael Kay
Head of Retail Practice
Lockton Companies LLP
E. michael.kay@lockton.com

Authors

Reem El Khatib
Associate, Research & Project Manager
Lockton Companies LLP
E. reem.elkhatib@lockton.com

Carlo Ramadoro
Vice President
Lockton Companies LLP
E. carlo.ramadoro@lockton.com

Vanessa Cathie
Vice President
Lockton Companies LLP
E. rvanessa.cathie@lockton.com

Lockton is the world’s largest privately owned insurance broker

Lockton is a **global professional services** firm with over 8,000 Associates who advise clients on protecting their people, property and reputations.

As such, our focus is our clients and our people rather than external shareholders. We can make long-term decisions that benefit our clients and improve service delivery.

Our 8,000 associates help over 60,000 clients in over 120 countries. They place over $38 billion of insurance premiums each year.

For nine consecutive years, Business Insurance magazine has recognised Lockton as a **‘Best Place to Work in Insurance’.**

Our clients value our bespoke solutions, innovative ideas and great service rather than efforts to sell more products. StrategicRISK’s 2015 UK Corporate Insurance Buyers Survey (a survey of insurance buyers in FTSE 250 companies) ranked Lockton top of all brokers for ‘client responsiveness’.

Our **96% client retention** rate speaks for itself.

Over 8,000 associates

Exceptional client retention rate (96%)

Over $38 billion premiums placed

Clients in over 125 countries

Over 60,000 clients

Over 100 offices worldwide

10.3% annual organic growth since 2000

$1.8 billion revenues

90% reinvestment due to our private ownership

Sources

1. https://inews.co.uk/news/consumer/retail-shop-closures-high-street-crisis-17500-chain-stores-closed-2020-915033
2. https://www.theguardian.com/business/2021/apr/03/almost-190000-uk-retail-jobs-lost-since-first-covid-lockdown
3. https://www.itpro.co.uk/security/data-breaches/360389/data-breach-costs-surge-to-record-high-in-2021#:~:text=The%20average%20cost%20of%20a,the%20adoption%20of%20cloud%20technologies
4. https://brc.org.uk/news/operations/crime-survey-2021/
5. https://brc.org.uk/media/676128/cyber-resilience-toolkit-for-retail.pdf
6. https://www.ponemon.org/research/ponemon-library/security/thales-e-security-and-ponemon-institute-collaborate-to-produce-2013-global-encryption-trends-study.html
7. https://www.ponemon.org/research/ponemon-library/

LOCKTON®

UNCOMMONLY INDEPENDENT

Lockton Companies LLP
Authorised and regulated by the Financial Conduct Authority. A Lloyd's broker.
Registered in England & Wales at The St Botolph Building, 138 Houndsditch, London EC3A 7AG.
Company No. OC353198.

global.lockton.com