WHITE PAPER

In today's digital environment, what is the value of cyber risk management for hotels?

LOCKTON'S HOSPITALITY PRACTICE – HOTEL SECTOR

LOCKTON®

Introduction

Technological innovation and development now touches almost every aspect of our lives, as a rapidly expanding network enables us to connect with products and services faster than ever before.

In response to this relentless demand for speed and efficiency, most sectors are adapting to embrace digitalisation and automation – and the hotel sector is no different. Hoteliers are increasingly utilising advanced connectivity to meet these changing needs and transform their offering. By evolving with the times, they are staying competitive through a technological evolution.

Historically, 'customer experience' for hotel guests was nothing more complicated than the level of physical comfort encountered during their stay. However, today's customer brings a much wider set of expectations that begin long before they step through the hotel door. They are looking for a unique and personalised service that is carefully tailored to their individual interests and preferences. An experience that spans their journey before, during and after their stay, and that is designed to reflect their lifestyle.

As a result, the hospitality industry is now widely connected. Online customers are given the option to book flights, vehicles, tourist attractions and restaurants as 'additional extras' when they book their hotel rooms. This streamlines the process of planning their stay, giving them an enhanced experienced based around choice.

They are also able to compare prices and facilities instantaneously, so hoteliers must work hard to attract and retain customers in the face of fierce competition. They must also showcase what makes them different and justify their charges, in addition to satisfying their customers' varied needs and demands.

The in-person customer experience is evolving too. Third-party vendors, including retail stores, restaurants, cafes, and beauty parlours, are often allocated space within a hotel to provide their services and products, offering a range of options within the same premises. Often, these small businesses-within-a-business are connected by smart technology.

It is clear that digitalisation is here to stay, bringing with it significant efficiencies and a heightened customer experience. However, the evolution of the digital landscape is not without risk – and the transition undoubtedly exposes the hospitality sector to greater cyber threats. For hoteliers, these rapid technological advances are constantly expanding the entry points for a cyber-attack – and the risk is becoming increasingly urgent.

Cyber risks specific to the hospitality sector

Digital technologies

In addition to the traditional use of technology in areas such as payment transactions, guest bookings and managing smart card access to hotel facilities, the hospitality sector is subject to increased cyber risk from digital technologies.

Shared digital platforms and the increased use of 'smart technologies' (controlling hotel lighting, temperature, smart TVs, curtains, robotic butlers, porters, etc.), while critical in delivering an elevated customer experience, also have the effect of widening the cyber threat landscape.

While the threats themselves may not have necessarily changed, the susceptibility of the hotel's network has expanded due to the number of 'access points' for cyber criminals. These threats can be external or internal and should be identified, assessed, mitigated and, where appropriate, transferred.

External threats

External threats loom large and necessitate a strong cyber security stance. They include deliberate, malicious and criminal threats from stereotypical hackers (thrill seekers), nation-state actors (geo-political), hacktivists (ideological), and terrorist groups (ideological violence).

External threats also include supply chain attacks on third parties such as software suppliers, causing collateral damage to many end users of the software.

The types of attack can range from ransomware, data exfiltration, malware, phishing, and social engineering, to distributed denial of service attacks.

Internal threats

Notwithstanding the wide and varied cyber security protocols that businesses undertake to protect their network perimeters, no firewall, multi-factor authentication or antiviral software will protect a business against insider threats.

Insider threat profiles include:

- **Negligent insiders:** employees or contractors unintentionally mishandling data (either directly or through lost devices), or compromising security, e.g. via phishing emails, incorporating unclean memory sticks, inappropriate use of social media/posting photos
- **Criminal and malicious insiders**: those intentionally mishandling data or compromising network security for personal gain
- **Credential thieves:** those who target insiders' login information

Data breaches

The hotel sector is at particular risk of cyber threat, due to the large amounts of sensitive and confidential personal information held on its customers, both present and past.

This includes emails, addresses, names and dates of birth, credit card numbers, passport and driving licence details. The sector also has some additional challenges that may increase its vulnerability to data breaches, including high employee turnover and, traditionally at least, somewhat modest data security policies.

Personal data is particularly vulnerable on the open market and particularly valuable on the dark market. Credit card fraud and identity theft, for example, are very real consequences of stolen or compromised data. In response to this threat, and recognising the need to protect data subjects, regulators across the world are introducing new privacy laws. As a result, the liability risk to the hotel sector is growing in proportion to the increased global regulatory landscape.

Significant financial and legal consequences follow for organisations who do not comply with these regulations across their operations; the potential for liability should not be underestimated.

Data is now arguably the most valuable asset in the world. Like any other business asset, it can be exploited and manipulated, causing considerable harm if not protected. Some of the biggest cyber- related claims in history have resulted from data privacy breaches.

Cyber risk management

Regardless of the type of cyber exposure your business has, implementing a robust cyber risk management framework is crucial. It is important that hotel owners and managers give careful consideration to four distinct elements of the process.

Governance

Cyber risk is not just a 'technical issue', but a business risk that threatens every part of a hotelier's business and needs to be dealt with at governance level.

The operational, financial and reputational consequences of a cyber-incident can be hugely detrimental and impact the survival of any hospitality business, regardless of size.

To protect your organisation appropriately, your management team must ensure clear responsibility and ongoing vigilance.

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

It is vital that there is a strong alliance between your management team and your business's cyber risk professionals. This doesn't just mean communicating the relevant cyber performance figures, but also establishing the contextual and situational awareness that will bring those performance measures to life.

If improvements are required, costs should be measured against the benefits, for example:

- Expedited international expansion
- Reinforced security
- An embedded competitive differentiator
- Well-informed management of the supply chain risk

The board needs this information to allow a translation of the raw performance numbers into opportunities and financial return. This contextual level of discussion will instil confidence in non-technical directors, customers and other stakeholders, as well as allow the management to understand, rationalise and fulfil its oversight responsibilities appropriately.

The cyber threat does not stand still – it is a dynamic environment that requires constant monitoring to allow for the development of appropriate response measures.

Security

As cyber-attacks morph and threat perpetrators find new ways to exploit vulnerabilities and avoid detection, it is vital that hotel businesses look very closely at their cyber hygiene protocols.

Examples of good protocols include:

- Multi-factor authentication for remote access (MFA)
- An endpoint detection and response (EDR) solution rolled out across the IT environment
- Privileged access management (PAM) and permissions across the IT environment
- Secure offline backups
- An incident response plan specific to ransomware that is updated and tested regularly
- A business continuity plan addressing network outages, offline communication, and data recovery protocols
- Remote desk protocol access from outside the network
- Updated software and patching protocols
- High-level employee awareness training
- Password management software
- Vulnerability assessments, including penetration testing, red-teaming and table-top exercises
- Appropriate separation of operational technology and information technology, as well as customer, payment, and back-office networks

Partnering with a good cyber security firm will be of real benefit in the identification and mitigation of cyber threats, both internal and external. It will ensure that your business is well-protected from cyber threats, but also adequately prepared in the event of your organisation experiencing a cyber-incident.

Human factors

Human error remains the greatest cyber threat to any organisation and arguably the most under-rated.

Error can manifest 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 constantly and become increasingly sophisticated.

Risk transfer

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

Contrary to popular belief, property, casualty and other traditional insurance 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 include 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.

NCSC's ten steps to cyber security

The chart below, from the National Cyber Security Centre, highlights ten steps to cyber security. These work together with the four factors listed above.

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

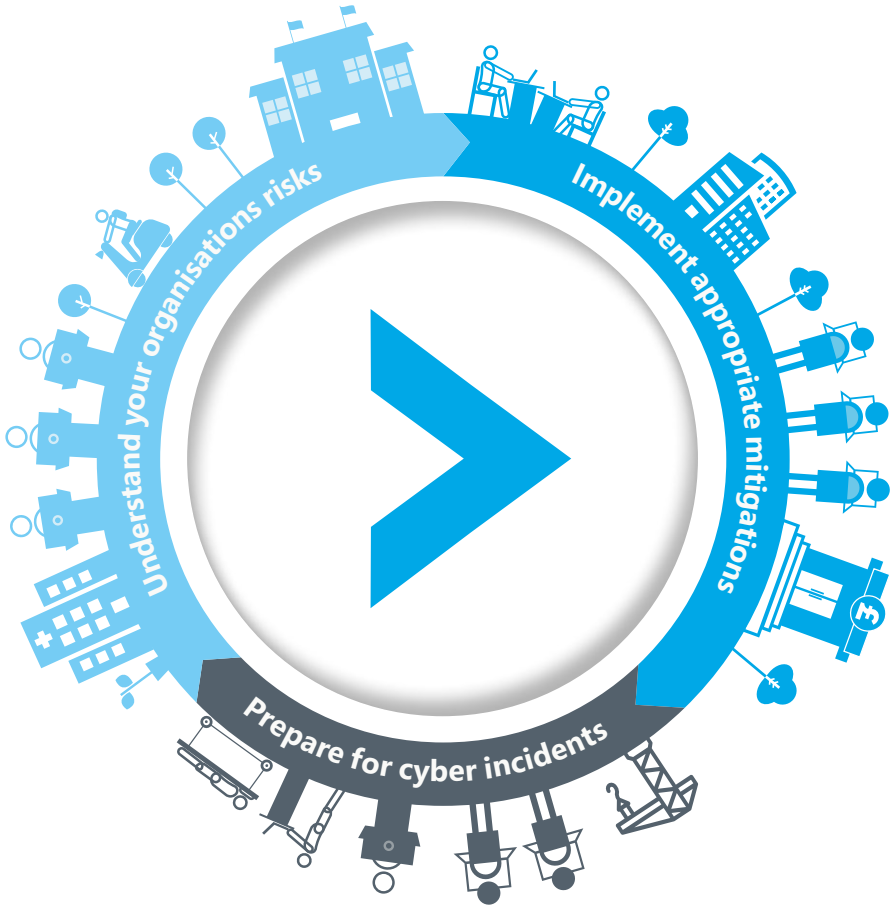
Risk Management
Take a risk-based approach to securing your data and systems.

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.



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.

Reservation system breach
Case study

In 2021, a hotel chain suffered a breach of its hotel reservation system. The incident allowed unauthorised access to customers' card details and credit card security codes. An extortion demand was received to pay a seven-figure ransom in exchange for the promise not to release the stolen data to the public domain.

The hotel had purchased cyber insurance and took immediate steps to notify its brokers. A breach response team was swiftly put in place, including a legal team (which was able to advise on notification obligations to data subjects and the privacy regulator), IT forensics, PR and crisis management consultants, and a ransomware negotiator.

It transpired that unauthorised access to the reservation system had taken place over an extended period of months. The IT forensic consultants determined the scope of the damage and were able to take immediate action to rescue the network. Negotiations with the cybercriminals reduced the ransom to 30% of the figure initially demanded. The hackers agreed to delete the stolen information in exchange for the payment of the (considerably reduced) ransom.

The total expenses and losses were significant, including the ransom, various consultancy fees, business interruption losses and reputational damage.

The standalone cyber policy met the costs to the limit of the policy (after payment of the retention).

NOTE: The Lockton Global, Cyber and Technology team works with clients to help protect their business from cyber risks, from ransomware to phishing, targeted hacks, malware, IP theft and various cyber complexities. Due to the sensitive and confidential nature of such risks, we have created a fictional case study to demonstrate examples of cyber complexities a client might experience. This case study is inspired by real matters; however, some facts have been amended to protect client confidentiality. These case studies do not constitute advice. Please seek appropriate advice before taking any action.

Cyber insurance

Standalone cyber insurance is a relatively new 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, with the provision of IT forensics and legal counsel, as well as public relations and crisis management consultants to mitigate damage and ensure that 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 organisation, 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 organisation 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 purchasing process, limits and cost

Each insurer will have a multi-page application for what it considers to be normal elements of a healthy and secure network. Generally, insurers will want to know how a hospitality 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

Cyber threats create considerable pressure, confusion and concern, so having immediate access to experts, including experienced ransom negotiators where necessary, is critical.

The cost of a policy is based on 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, and the risk controls in place.

Any limit purchased needs to be weighed against the perceived exposure of the business. Some broad considerations are listed below, although you should discuss these with your risk and insurance broker prior to deciding on an appropriate limit.

- Many 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, as well as legal advice (necessary in the aftermath of an incident) and any notification costs required. An estimate of these costs should be undertaken to gauge exposure.
- We have seen an exponential growth in ransomware threats over the past few years. The hospitality sector is a vulnerable industry due to the number of sensitive data records held by businesses, which provide additional leverage to cybercriminals. 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 hotel business is the sensitive data held on their customers. When considering cover limits, estimates around the cost of dealing with potential privacy breaches are useful.
- Another significant exposure for hotels is business interruption losses, i.e. the lost revenue while the business is offline or the systems compromised. Also important in this context will be the 'waiting period', the period of time that must pass prior to a valid claim being notified (typically 8–12 hours). The period will vary from business to business.
- The impact of the 'silent cyber' effect must also be considered. Historically, many businesses may have relied on more traditional policies for some 'silent cyber' cover in the event of a cyber-incident (i.e. cover which is non-affirmative, but nor is it specifically excluded). In a phased roll-out from 1 January 2020, Lloyd's markets have required cyber-related losses in non-cyber policies to be dealt with more clearly, i.e. with cyber cover either specifically affirmed or excluded. Non-Lloyd's markets are also reviewing their positions. This could mean that there is now limited or reduced cyber cover available to an insured under an existing non-cyber policy, thereby possibly increasing the need for a standalone cyber policy. If there is an existing cyber-policy in place, the limit ought to be reviewed.

Cyber market appetite

The cyber market continues to harden as ransomware losses hit the marketplace with regularity, driving the following responses from cyber underwriters:

- Retentions are typically being increased
- Coverage is often restricted by the inclusion of ransomware-related sub-limits and coinsurance (or both)
- Where sufficient cyber hygiene controls are lacking, ransomware-related exclusionary language is increasingly common
- Minimum rate increases of 100% – 150% are typical, even for clean risks with best-in-class controls
- Rate increases of 150% and above are not uncommon for highly exposed industries, such as hospitality
- Supply chain exposure is causing reverberations around the marketplace and sharpening underwriter focus. Additional questions are being asked of clients, specifically in relation to their exposure to the Accellion, Microsoft Exchange, SolarWinds and Kaseya supply chain events

Greater scrutiny around security controls, which mitigate the ransomware threat, are also front and centre of the market's underwriting process. In our experience, the following cyber hygiene protocols are a bare minimum, without which it will be challenging to obtain a cyber quote:

- Multi-factor authentication (MFA)
- Endpoint detection and response (EDR)
- Privileged access management (PAM)
- Secure offline backups

While the insurers are bringing greater scrutiny to the underwriting process, and potentially reducing available limits while increasing premiums and retentions, the benefits of a market-leading standalone cyber policy should not be underestimated.

Typical coverages include:

- Privacy third-party liability
- Privacy regulatory fines and expenses (to the extent insurable)
- System security third-party liability
- Multi-media liability
- Breach response costs
- Extortion demands
- Extortion expenses (e.g., ransomware negotiations)
- Digital asset losses
- Computer hardware losses
- Business interruption losses
- Reputational harm reimbursement

The breach response process is particularly helpful when an organisation has suffered a cyber-event, providing 24/7 access to a team of legal, IT, PR and crisis management consultants who can assist with getting the hospitality business operational again, as quickly and efficiently as possible.

Note: Typically theft of funds is not covered within a cyber policy. A separate crime policy might be appropriate for this type of cover.

Lockton's Global Cyber and Technology practice

At Lockton, we understand the many pressures and challenges that hoteliers are now facing. Our dedicated Global Cyber and Technology practice can help you address the increasingly urgent issue of cyber risk with bespoke insurance and risk solutions that meet your specific requirements.

Our expert team of independent, specialist cyber brokers and advisers will take the time to understand your business, identify your priorities and deliver reliable, effective and innovative cover.

How we help you protect your business

- A broad range of broking experience across all aspects of cyber and technology
- Specialist technology and risk consultancy through Lockton Cyber Risk Advisory Services (LCRAS)
- Navigation through the best cyber security process with our unique three-step approach: inform, improve and insure
- Partnered services on managed detection and response, forensic accounting, data landscaping and more
- Unmatched insurance and risk transfer program advisory and placement solutions
- 50+ Cyber & Technology Associates globally
- Relationships with over 175 insurance companies globally
- Over 300 incidents handled each year with a 99% covered claim rate to date

Talk to us

It is vital to plan ahead and prepare as early as possible for your renewal with a detailed presentation. We can provide you with advice and guidance on your next steps, helping you face the future with confidence and peace of mind.

If you would like to find out more, please contact:

Andrew Nicholson
Partner, Head of Lockton's Hospitality Practice
Lockton Companies LLP
E. andrew.nicholson@lockton.com

Authors

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

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

Lockton is the world's largest privately owned insurance broker.

- Over 8,500 associates
- Exceptional client retention rate (97%)
- Over $39.5 billion premiums placed
- Clients in over 125 countries
- Over 65,000 clients
- Over 100 offices worldwide
- 13.4% annual organic growth since 2000
- $2.16 billion revenues
- 90% reinvestment due to our private ownership
- Certified carbon neutral

Independence changes everything.