Leisure and Hospitality Practice

managing digital risks in the leisure and hospitality industry

The leisure and hospitality industry is dependent on consumer confidence and is facing growing pressure to deliver innovation, quality and value. The industry is increasingly engaging with digitally active consumers who expect to be able to interact with brands on a personalised, multichannel basis and who are harnessing social media and mobile technology at an ever faster rate. As more companies in this industry increase their IT capital expenditure, many now see digital risk as an inevitable risk which could cause major disruption, significant financial loss and lasting reputational damage.

Perception vs reality

There is a perception that IT failure and cyber-crime are confined to websites or the loss of data such as customers' personal data or credit card details. The reality is that without working internal IT systems, such as booking and payment processing, businesses could cease trading for a substantial period, resulting in huge financial losses and potentially extensive costs of hiring external expertise to fix technical problems.

Another common misconception is that most cyber incidents occur as a result of external hackers. In fact it is a combination of external hacking attacks (42% of cyber incidents), internal negligence such as lost laptops and files or deliberate acts e.g. insider collusion (30%), and system glitches (28%)*. Often businesses will not know they have experienced a cyber-breach until an external source notifies them, meaning that breaches reportedly take 240 days on average to detect**.

The assumption that responsibility for managing and understanding digital risks lies solely with IT departments is gradually changing. There is growing recognition that everyone in an organisation should be accountable for cyber security. Despite this change in attitude, few staff are trained and many boards still lack a comprehensive understanding of the risks their business faces and the measures needed to address them. This can be due to the technical language used to describe and articulate cyber exposures, as well as optionality around the disclosure of cyber breaches.

Although investment in cyber security will not prevent every incident, managing digital risks effectively can significantly reduce the impact of cyber incidents.

Legal responsibilities

There are certain laws and regulations that companies and those that service and supply them must abide by and adhere to, including:

- Data Protection Act
- Law of Confidence
- Law of Contract
- Law of Tort
- Payment Card Industry Standards
- Financial Services Act
- Legal Services Act

In order to satisfy these obligations, effective cyber security measures must be implemented. Although not every law would apply to every business, all would be bound by one or more to maintain cyber security.

Digital dependence

All leisure and hospitality operators have become increasingly dependent on the internet and IT systems in many areas of their business, including:

Office administration and general business functions (e.g. accountancy, law, marketing, sales and business strategy).

Point of sale technology (e.g. tills, self-service check-out scanners and debit/credit card processing).

Reservation and cancellation systems.

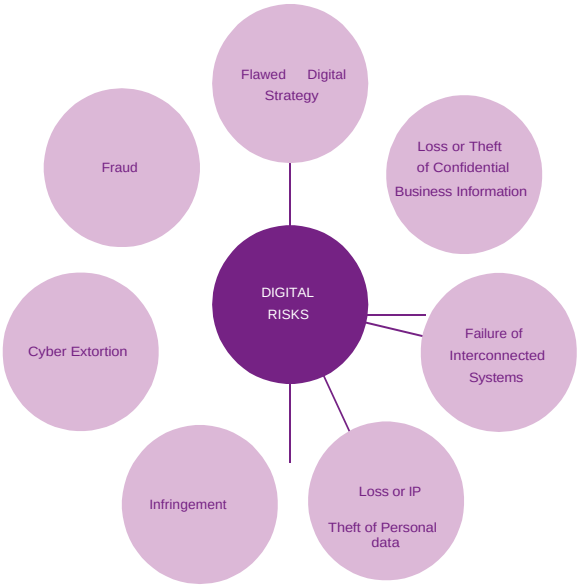
Customer Relationship Management.

Regulatory and reporting compliance.

Marketing.

Provision of Wi-Fi.

What are the risks?



Digital risk	Detail
Flawed digital strategy	Companies tend to focus on incidents such as a hack or service downtime, however with online bookings now contributing a large proportion of revenue, a poorly received website revamp, for example, could have a significant impact on bookings.
Loss or theft of confidential business information	Confidential and commercially sensitive information could be useful to competitors as well as fraudsters, for example; pricing strategies, current financial position, advertising and marketing campaigns and any other information that is not publicly available. If this information is lost, stolen or widely disseminated it will result not only in damage to reputation but could impact trading.
Failure of interconnected systems	Computer based services are interdependent and the failure of one organisation's computer system can have a dramatic knock-on effect on all those with which it is connected. Examples of such issues include: Till or chip and pin machine failure - prevents a service provider from processing credit/ debit card payments. Website issues (server down-time, denial of service and web app attacks) result in the inability to process online bookings.
Loss or theft of personal data	Service providers collect, maintain, transmit or store private information including customer, member and employee data, as well as credit card information. This personal and confidential data may be shared between individual organisations increasing the number of touch points and therefore the potential risk of a data breach.
IP infringement	IP infringement for service providers can include violation of design, copyright, trademark, domain name rights and copycat websites.
Cyber extortion	Cyber extortion has become far more common in almost all industries, partly as a result of the low cost and easy availability of hacking tools which are simple for even the most technically challenged criminal to use. Denial of service (DoS) attacks can block access to essential systems and online reservation platforms, leaving service providers unable to trade and at the mercy of cyber criminals.
Fraud	Hospitality is one of the industries particularly prone to payment card skimming, with fraudsters using stolen details from individuals' credit cards to make bookings. Increasingly this type of activity is happening online where a physical card is not required to make a booking and appropriate checks are more difficult to carry out - the cost of such activity can be significant.

What are the impacts?

The hospitality industry is particularly vulnerable to cyber-attacks due to the extensive use of credit cards, provision of Wi-Fi for customers and storage of customer and employee data. The impact of any digital incident can be disastrous in terms of reputational damage and financial loss.

Financial losses can include forensic investigations, notifying customers and defending lawsuits. Reputational damage is however potentially more costly and harder to measure. A reputation can take years to build and, in the age of social media, hours to destroy.

Questions to consider

Operators in the leisure and hospitality industry who wish to effectively manage their digital exposures should begin by asking themselves some basic questions, including:

Has the company's key information been identified and are all digital threats to that information being effectively managed?

Is the allocation of responsibility for digital risks clear and is this included on the risk register?

Is there a complete and accurate prediction of what the impact would be on the company's reputation, share price (if applicable) and financials if confidential business information or customer data were to be lost or stolen?

Is there a complete and accurate prediction of what the impact would be on the business if its online services were disrupted for a short or longer period?

Does the business have a written cyber security policy in place? Is this championed by the board and supported by management through regular staff training and monitoring?

Is there a comprehensive incident management plan in place to be followed for each type of cyber incident? Does this plan include access to external expert response teams and does it contain procedures for managing external PR, with a focus on minimising reputational damage in the wake of an incident?

Has the cyber security of the company's suppliers, service providers, business partners and professional advisers been checked?

Key risks

The leisure and hospitality industry holds valuable information that is very attractive to cyber criminals, including personal data and payment details.
The following are the key risks:

Loss of personal data relating to customers, resulting in breaches of privacy law obligations.

Loss of confidential information, which may amount to a breach of contract and/or loss of commercial advantage.

Denial-of-service attacks, preventing the use of operational systems.

Financial fraud through the use of customer credit card information.

Reputational damage following an incident.

isk from Business Partners; including suppliers, designers, marketing and PR companies, webhosting companies, cloud service providers, solicitors, accountants, surveyors, distribution and shipping companies, warehousing companies, IT supply and service companies, customers and banks/financial services.

Case study***

What happened?

The credit card information of the customers of a global hotel operator was stolen by hackers.

The impact

After disclosing information about the attack to customers, the company was subject to numerous tribulations and regulatory investigations, which were later followed by civil lawsuits by regulators as well as private plaintiffs. This resulted in significant costs for the company along with reputational damage and lost management time.

Lessons to learn

The importance of co-operating with regulators once a cyber-breach occurs. The company in this case made the decision not to self-report the breach and took an aggressive stance in the investigation.

Data breaches are expensive endeavours even though the number of accounts hacked can be relatively small. Also, the response to a breach needs to focus on managing reputation and customer perceptions, in addition to the technical and legal elements.

A solid cyber defence programme is essential to cybersecurity. This programme needs to be supervised at the highest level i.e. directors needs to take a hands-on approach and actively participate in resolving cybersecurity problems after a breach.

About us

Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

The Leisure and Hospitality Practice has worked with customer facing businesses for over 30 years and as a result we have a deep insight into the opportunities and challenges our clients face. Our team of specialists are based throughout the UK and work with clients operating within all industry sub-sectors, including hotels, pubs and restaurants.

Our industry focus combined with our risk management, claims and insurance placement expertise means we are well placed to assist with both traditional and emerging business exposures.

BLM

BLM is the UK and Ireland's leading risk and insurance law business, with over 200 partners and 800 lawyers and technical experts totally dedicated to risk and insurance.

Our strong presence in the hospitality sector reflects our expertise across the whole range of legal issues affecting operators in the UK. Cases always have to be handled in a way that reflects the client's strategy and priorities, including customer service issues.

Everything we do is designed to reduce the time and money our clients spend managing risk, resolving disputes and managing claims. Clients' interests are at the very heart of all processes, delivering value for money at every stage to assist in controlling costs and indemnity spend, sharing knowledge and protecting brand and reputation.

Our specialist team is adept at building relationships at all levels to gain a better understanding of a client's organisation, business and brand. Risk management and defensibility training are also integral elements of our service, enabling us to make a real contribution to our clients' operations.

Sources:

http://www.pwc.co.uk/hospitality-leisure/index.jhtml (accessed October 2015)

http://www.insurancedaily.co.uk/2011/08/03/hospitality-and-leisure-attract-cyber-attacks/ (accessed October 2015)

http://plusweb.org/Portals/0/Chapter%20Material/Southern%20California%20Chapter%20Data%20Security%20and%20Privacy%20Workshop%20-%20September%208,%202011.pdf (accessed October 2015)

http://www.metrocorpcounsel.com/articles/31991/wyndham-%E2%80%93-case-study-cybersecurity-how-cost-relatively-small-breach-can-rival-major-h (accessed October 2015)

http://hotelexecutive.com/business_review/3982/with-cyberattacks-on-the-rise-is-your-hotel-protected (accessed October 2015)

* Poneman Institute - 2014 Cost of Data Breach Study: Global Analysis

** Advisen's 4th Annual Cyber Risk Insights Conference, London, 10/02/2015

*** Metropolitan Corporate Counsel - A Case Study in Cybersecurity, March 2015

Contact

Please do not hesitate to contact us to discuss your risk management and insurance strategy further and find out how we can help you implement the right approach for your business.

Willis Towers Watson

Michael McLaverty
Account Director
Belfast
T +44 (0)28 9089 5225
E michael.mclaverty@willistowerswatson.com
www.willistowerswatson.com

BLM

Nick Gibbons
Partner and Cyber Specialist - London
T +44 (0)20 7457 3567
E nick.gibbons@blmlaw.com
www.blmlaw.com

15840/06/16