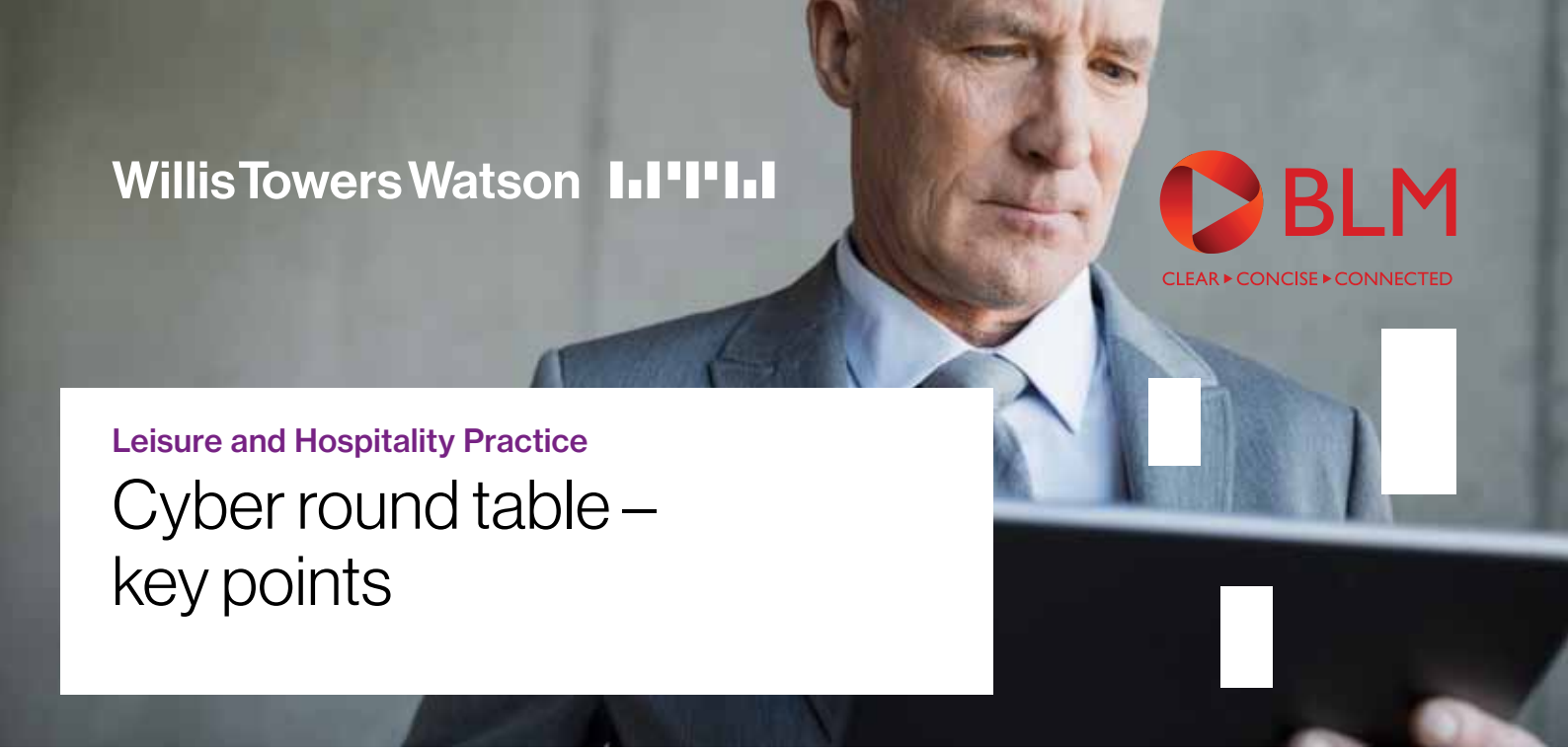


Willis Towers Watson

BLM
CLEAR ▸ CONCISE ▸ CONNECTED

Leisure and Hospitality Practice

Cyber round table – key points

Technology, Big Data and Connectivity are all buzz words that are associated with transacting business in the modern era. Unfortunately, with any advancement there comes an element of risk and we are becoming all too familiar with media reports that involve the terms *hacking, breach, denial of service or cyber extortion*.

The leisure and hospitality industry's use of technology is evolving with increasing use of the internet for marketing, Wi-Fi, information and booking. This has created great benefits in terms of cost, efficiency, transparency, accessibility and customer service. Consumers have, conversely, become far more sophisticated and demanding due to the easily comparable, price, menu, booking and information available to them via multiple devices (for example laptops, tablets and smartphones). The increasing use of computers and the internet has, however, also exposed operators to a far greater risk of cybercrime and system malfunction.

These issues were discussed at a round table on Cyber risk in the leisure and hospitality industry hosted by Willis Tower Watson and BLM on 11th May 2016. The key points are set out in this document.

The growth of "cybercrime made simple" and industrial cybercrime

Cybercrime has become much more commonplace in recent years. This is because it is very easy for ordinary criminals to acquire effective hacking tools on the internet quickly and cheaply and because sophisticated, professional and multinational cyber gangs have formed, which perpetrate cybercrimes on an industrial scale, attacking and blackmailing businesses of all sizes in all industries.

Cyber criminals of all types have been assisted by software which harvests open source intelligence about businesses' cyber vulnerabilities which is publicly available on the web and easy for any reasonably sophisticated hacker to access.

The commoditisation of hacking tools and techniques has also become an industry in itself enabling cyber criminals to keep up with new innovation. By way of example it is widely predicted that Near Field Communication (NFC) technology such as contactless cards is likely to develop into the number one cyber risk. This is because sophisticated hackers have already cracked NFC security and that knowledge will rapidly be disseminated to common criminals who can use it as they wish.

Key security problems: People and perimeter risk

The majority of cyber incidents are caused or made much worse because the board and management are not sufficiently knowledgeable or in control of cyber risk management and staff are inadequately trained and tested.

IT teams and consultants are by no means infallible and communicating with and managing them is often hindered by poor communication with the rest of a business, due to difficulties in understanding technical language and little or no comprehension of key issues and risks by staff and management.

Cyber risk management must therefore consider not just technical security but also board, management and staff knowledge and properly implemented cyber security policies and procedures.

Perimeter risk is another key risk, even if a business has addressed its own internal cyber security issues. Given the interconnectedness and interdependence of businesses in the digital world, companies remain exposed to possibly inadequate security of their business partners, suppliers, service providers and advisors.

According to a UK Government survey:

- 42% of large organisations don't provide any ongoing security awareness training to their staff (and 10% don't even brief staff on induction);
- 26% of respondents haven't briefed their board on security risks in the last year (and 19% have never done so);
- 33% of large organisations say responsibilities for ensuring data is protected aren't clear (and only 22% say they are very clear);
- 93% of companies in which security policy was poorly understood had incidents related to human failure; and
- Proactive steps must therefore be taken to check and address both internal and perimeter cyber security.

Proposed changes to EU data protection legislation

On 14 April 2016 the European Parliament voted to adopt new data protection law for Europe, the General Data Protection Regulation (GDPR). Notwithstanding the Brexit referendum vote, businesses should assume that they will need to comply with this regulation because it will come into effect on 25th May 2018, before the two year period for exit under Article 50 of the Lisbon Treaty could possibly end. Pursuant to the GDPR, Data protection law will be significantly tightened, and individuals' rights (including to bring claims) will be strengthened. Fines will rise to as much as 4% of global turnover for breach of the law, including inadequate cyber security which results in data breach. The Regulation is due to take effect in 2018, and will impact all business sectors. Organisations should start to assess now how the Regulation will change their current data protection compliance obligations.

The Regulation is likely to require company-wide changes for many businesses. As a first step, businesses need to take stock of their existing data assets and compliance profile, and then systematically assess how the Regulation will impact existing compliance. For most organisations, this will be a sizeable project. Organisations in the UK, which until now have enjoyed a light touch data protection regime, arguably will have the most to do to prepare for data protection under a harmonised European wide regime.

Case study: Hard times cafe

The Hard Times Café in Rockville was closed for several days following a ransomware attack on its point of sale and back office systems earlier this year. The company decided to completely rebuild its systems following the attack rather than pay the ransom.

Ransomware has become an increasingly common tool for hackers. It is cheap and easy for hackers to use and can therefore be deployed against numerous targets as a basis for low ransom demands which make it very tempting for the target business to "pay up and move on". The refusal by Hard Times Café to pay a ransom demand of $10,000 is in this regard unusual.

"Cybercrime is no longer a fringe issue but a genuine, serious and growing problem"

Hotel sector faces 'cyber crime wave'
FT November 27, 2015

Cyber incidents in the leisure and hospitality industry are not confined to the theft of personal data of customers and employees. Companies may suffer a business interruption through system malfunction or denial of service attack, claims against them for intellectual property infringement and the theft of commercially sensitive confidential information.

The effect of a cyber-attack can have a disastrous impact on brand and reputation, exacerbated by the increasing use of social media and speed of interaction. A public cyber incident can itself damage a customer's perception of the company's security but the manner in which an incident is handled can be just as detrimental.

It is important to plan ahead, building on existing crisis management plans, brainstorming different scenarios and creating draft statements for different audiences/ outcomes. Testing plans through scenario simulations will also identify weaknesses and help people prepare for the emotional stress that handling a crisis can entail.

Cyber incidents cause significant financial loss

Crunching the numbers for the different heads of loss that will affect a business following a cyber-incident demonstrates that losses are very likely to be tangible and significant.

The impact on profitability is also likely to last far longer than the duration of a cyber-incident with reputational damage being a major concern for most companies in the leisure and hospitality industry, with the loss of market share often difficult to regain.

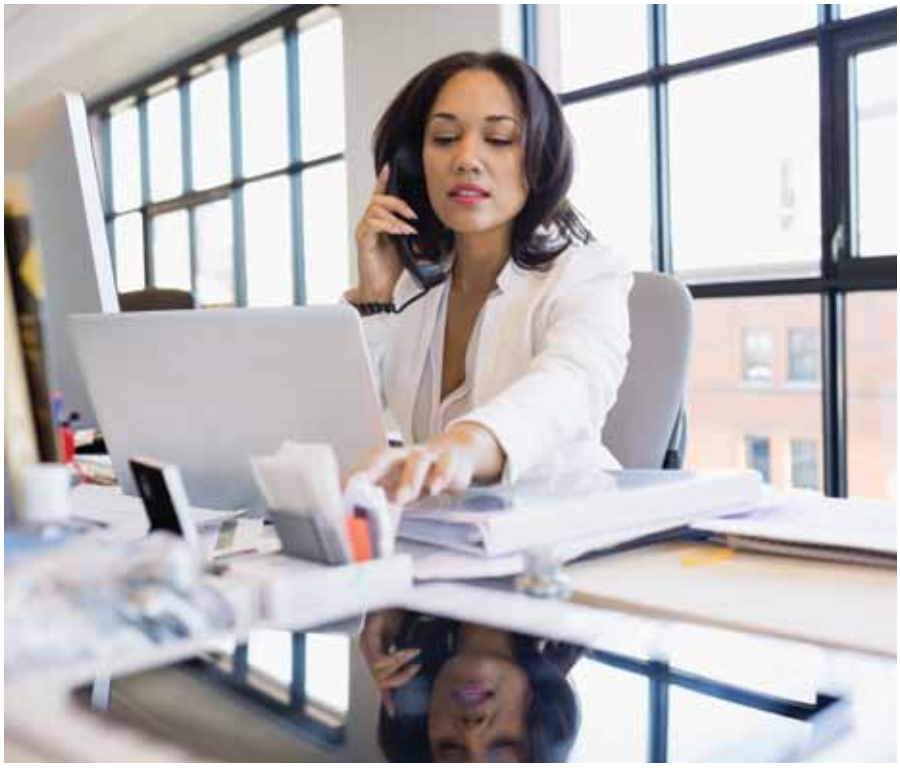
Cyber insurance

Although some cyber risks may be covered by general insurance, many won't be. A gap analysis of existing insurance cover is therefore essential.

Cyber insurance cover generally includes expert incident response services which are vitally important in terms of minimising the consequences of a cyber-incident which typically grow quickly and exponentially.

Underwriters want to know what companies will do to respond to an incident, and do not want to just hear about all the measures in place to prevent an incident.

The process of applying for cyber insurance and addressing issues raised by a typical cyber insurance proposal form will serve to heighten awareness and improve cyber security, even if a business ultimately decides not to purchase the policy.



Contact us

Please do not hesitate to contact us to discuss your risk management and insurance strategy further:

Willis Towers Watson

Kelvyn Sampson
Retail and Leisure & Hospitality
Industry Practice Leader
T: 44 (0)14 7322 2990
E: kelvyn.sampson@willistowerswatson.com

BLM

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

FP2084/15883/06/16