Cyber and data security in the hotel industry

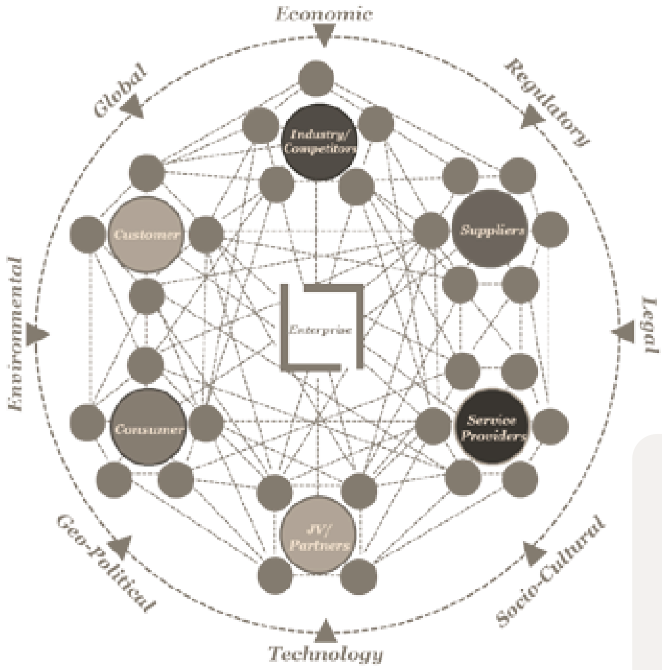
Cyber breaches are continually in the headlines both globally and in the Middle East. They impact operations, financial performance and reputation. With increasing global regulatory attention, they can also affect executives' jobs and the long-term viability of hotel businesses. This paper examines some of the key themes and trends in the industry and outlines key activities for operators and owners to undertake.

The shifting paradigm

In the Digital Era, technology is everywhere; people can connect to your company, your employees, customers, providers and competitors through laptops, smartphones and even wearable devices. We rely on connected technology for the safe operations of our energy, utilities, transport, healthcare, government and financial systems.

The Digital Era: *ubiquitous data, everyone and everything online, greater connectivity, porous perimeters and external drivers.*

With increasing reliance comes increasing risk, many of which are outside the Enterprise's control.



Cyber Security and Data Privacy risks in the hotel sector

1. Awareness levels about cyber security and data privacy issues are rising

The simple truth is that cyber security and data privacy problems can be big news and newsworthiness drives awareness levels. The public, law makers, regulators and judges are all sighted on the risks. These people provide "adverse scrutiny" to entities when things go wrong and they are fully aware of the fact that some of the world's biggest, richest and more powerful entities have been humbled by poor approaches to security and privacy.

Awareness levels are only going one way and we are rapidly approaching a tipping point, when entities realise that they have no choice: they have to do much more to tackle the security and cyber risks they face and to live up to the expectations that society places in them. If the full roll call of entities that have been humbled in the news is considered, the conclusion seems to be obvious: security and privacy issues are not being accorded the priority they deserve.

2. Hotels are already in the spotlight due to high profile breaches

2015 was a really bad year for the hotel industry globally. Cyber and data security emerged to prominence as a massive risk area, due to a series of high profile breaches affecting payment cards. Just before Christmas 2015 the Federal Trade Commission in the United States concluded long running proceedings against a hotel. This case has established a need for the development of comprehensive information security programmes, annual security audit cycles and post-incident investigations in the hotel sector. Looking at this from the customer's side, security experts are now advising travellers to be on heightened alert when using hotels.

Hotels have been propelled to the forefront of the mind and it is inevitable that this will play out in further legal and regulatory problems over time.

3. Trust, confidence and brand put at risk

Legal and regulatory problems bring their own special range of issues. Locking horns with regulators, litigants and judges is the last thing that business needs. Judicial and Regulator design of business models has to be avoided at all costs. In landmark EU litigation in 2014, the way global web search operates in Europe was redesigned by the European Court of Justice, in a case that has delivered into law the so-called “right to be forgotten”. The security of mobile phone operating systems has just been re-designed by a District Court in Los Angeles, massively inflaming the passions of the technology sector and security experts alike. But legal and regulatory problems are just one arc of the consequences of bad security and privacy. Businesses need to think about trust, confidence and brand health and reputation.

These points are commonly understood, but some business people point to share prices, saying that prices don’t dip much, or for long, after big security and privacy problems. That may be the case at the moment, but the absence of share price volatility does not mean that value is not being eroded. Moreover, if share prices do not dip, that points to another problem, namely defects in market behaviour.

That is a dangerous place to go, because the classic response to market imperfection is the expansion of regulation: regulation is seen as the antidote to market imperfection.

Businesses that trumpet the share price issue, merely bring-on the risk of more red tape and bureaucracy, as well as serious penalties and sanctions risk.

Trust, confidence and brand health may operate in a different timeframe to share prices. The absence of share price volatility does not mean that trust, confidence and brand health are not being eroded. If that is true, then the logic points, perhaps, to a convergence in the future of value erosion. Entities that are damaging their trust, confidence and brand health today may pay in share price in the future. In other words, suffering security and privacy failure might be like a cancer, where the harm is hidden from view until it is too late. This returns the focus to legal risk.

4. The legal risks are significant

The EU will soon adopt the General Data Protection Regulation (GDPR).

This is a landmark piece of legislation that will radically change our perceptions on how personal data should be handled in business. The GDPR will also have global effect. This is not just law-making for the inside of Europe’s borders.

The purpose of the GDPR is to put people back in control of their personal information and to improve how entities look after personal information while it is in their custody.

5. Hotels need a vision for security and privacy

There is much more to security and privacy than compliance and risk.

There is also the economic interest in gaining commercial advantages from the use of personal data. Gaining better customer insights and providing them with personalised services are now recognised by many in the hotel industry as core business goals.

In order to properly bring together the interests of economic advantage, risk management and compliance with legal obligations, entities need to develop an appropriate Vision for their desired end state. That Vision will take account of the entity’s “special characteristics” and the points of view of all necessary stakeholders. Once a Vision has been set, a strategy to deliver the Vision can be developed and appropriate structures can be put in place.

When the lessons of failure are examined (failure of data handling projects, such as Single Customer View systems, and failure in the sense of security and privacy breaches), it becomes obvious that the absence of an appropriate Vision is at root cause.

People responsible for security and privacy in hotels ought to ask themselves whether their entities have appropriate Visions for desired end states. If not, they should bring together the stakeholders to discuss ways to take things forward.

Five key questions to ask yourself

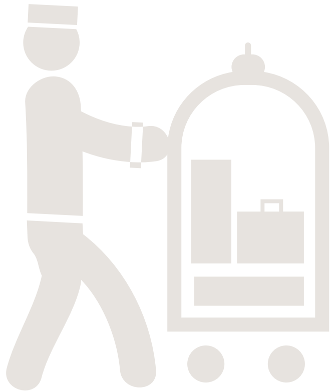
Are you already compromised? Have you checked? How compromised are you? Do you know your threats?

How good are your defences? Do you test like a real ‘hacker’? Have you considered all risk options? Insurance? Third parties?

Do you know where your data is and who has access to it? Are you sure it is only in your company? Sleep walking into cloud?

What would you do if you were breached today? Do your crisis plans cover reputational, legal, regulatory fall out?

How do you compare? Whats your RoI? How do you compare to peers and best practice? What looks good? Innovation in a Digital era?



Mike Maddison
Partner, Middle East Risk Assurance Services Leader
+971 56 683 8253
mike.maddison@ae.pwc.com

Alison Grinnell
Hotels Leader
+971 (0) 55 267 3636 or +971 (0) 50 900 7830
alison.grinnell@ae.pwc.com

Creative Design Centre CDC 1220 042016