Cyber Security and Data Privacy in the Hotel Industry

Your digital world just got bigger

The world has changed but not everyone has changed with the world.

The ‘digital age’ is bringing rapid change: new customer connections; tighter supply chain integration; new sourcing models; new ways of exploiting bulk data; faster R&D processes; mobility; and much more. Businesses now operate in an interconnected ecosystem. As a result, securing critical data, transactions and operations means working beyond the walls of the enterprise.

The new reality:

- Increase in reliance on technology
- Organisations are built on trust and collaboration
- Information and data ubiquity throughout the business ecosystem
- Transactions and operations span multiple parties
- New and advanced threats which take advantage of the new reality
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.

2. Hotels are already in the spotlight due to high volume of personal data

Cyber and data security emerged to prominence as a massive risk area, due to a series of high profile breaches on the hotel industry globally and due to the high volume of personal data held by the hotels. 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

Digital risk and the need to build trust should be treated as an enterprise issue for which boards need to develop a clear risk appetite to suit their specific business circumstances. Alongside this, there needs to be a clear action plan and frequent monitoring and assurance that the risks are appropriately managed.

Enterprises need to develop the confidence to be a leading player in the new, expanded digital trust ecosystem. They need to focus on key priorities:

- **Get the right attention in the boardroom** – With digital opportunities and risks becoming so central to business strategy, boards and audit committees must have the digital expertise to set the level of risk that they are willing to accept.
- **Rethink your approach to technology risk** – Managing the risk in this ever changing world needs new and more dynamic approaches based on up-to-date understanding of the situation.
- **Develop a business strategy for the digital age** – What’s certain is that you will need a business strategy for the digital age – not a digital strategy.
4. The legal risks are significant

On the 14th April 2016 the EU Parliament approved the General Data Protection Regulation (GDPR), and organisations now have until 25 May 2018 to comply. This new regulation is the biggest change in data protection law for 20 years, but what does it mean?

This is a landmark piece of legislation that has radically changed our perceptions on how personal data should be handled in business. The GDPR covers every processing operation that can be done on personal data, irrespective of whether it is undertaken by automated or non-automated means or whether done actively or passively (e.g. collection, recording, storing, using, adapting, amending, sharing, transmitting, archiving and erasing the data).

The threat is real. Data breaches are happening in all sectors and industries. Companies, customers, vendors and stakeholders need assurance that personal data is being safeguarded in a secure manner, but also that robust processes are in place for ensuring the processing of such data is fair and legal in the first place.

The General Data Protection Regulation (“GDPR”) is the modern age answer to ensuring all organisations processing personal data are held accountable for ensuring our fundamental right to the protection of personal data is upheld. Serious contraventions of the law will be punishable by fines of up to either €20 million or 4% of total annual worldwide turnover.

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 recognized 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.

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.
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?

How compliance are you with the new EU General Data Protection Regulation?
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?
What’s your RoI?
How do you compare to peers and best practice? What looks good?
Innovation in a Digital era?

How PwC can help

As a multi-disciplinary practice, we are uniquely placed to help our clients adjust to the new environment. We provide a comprehensive range of integrated cyber security and data privacy services that help you assess, build and manage your cyber security and data privacy capabilities, and respond to incidents and crises. Our services are designed to help you build confidence, understand your threats and vulnerabilities, and secure your environment. Our cyber security services and data privacy delivery teams include security consultants, compliance, lawyers, risk specialists, forensic experts, incident response, technology and change management specialists. Our team is truly global with on the ground experience in all the major economies.

Contact us

Tassos Procopiou
Partner
Advisory
T: +357 - 22 555 750
tassos.procopiou@cy.pwc.com

Efthyvoulos Efthyvoulou
Senior Manager
Advisory
T: +357 - 22 555 460
efthyvoulos.efthyvoulou@cy.pwc.com

Philippos C Soseilos
Partner
In charge of Hospitality & Leisure Group
T: +357 - 25 555 606
philippos.soseilos@cy.pwc.com

Demos Demou
Manager
Advisory
T: +357 22 555 056
demos.demou@cy.pwc.com

PricewaterhouseCoopers Ltd
PwC Central, 43 Demostheni Severi Avenue
CY-1080 Nicosia, Cyprus
P O Box 21612, CY-1391 Nicosia, Cyprus
Tel: +357-22 555 000
Fax: +357-22 555 001

City House, 6 Karaiskakis Street,
CY-3032 Limassol, Cyprus
P O Box 53034, CY-3300 Limassol, Cyprus
Tel: +357-25555000
Fax: +357-25555001

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.
© 2018 PricewaterhouseCoopers Ltd. All rights reserved. PwC refers to the Cyprus member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.