Unwanted Guests: How Hackers Are Targeting The Hospitality Industry

By: Imran Ahmad and Andra Enescu

In recent months, several large international hotel chains were the target of high-profile payment processing breaches. The hospitality industry will continue to be a high-value target for hackers who try to get access to hotel networks and steal guest and corporate information. According to the Annual Allianz Risk Barometer Survey, cybersecurity losses were among the top 10 global risks in 2014. Moreover, Verizon’s 2015 DBIR report indicated that in 70% of cases in the hospitality sector, incidents take months or longer to discover. To put things in perspective, on average cyber crime incidents are discovered in hours. In comparison to other industries, the hospitality industry typically is not aware of the breach until they are notified by an external party, such as a credit card provider or law enforcement - in fact, many cybersecurity breaches go undetected and unreported for months.

In an increasingly mobile and interconnected world, the hospitality sector has been keeping pace by delivering guests a unique experience through cutting edge apps, online access, and other services. These services are built on a digital network infrastructure which is vulnerable to cyber attacks. Moreover, from the moment guests reserve a room until they check-out, they will have used their credit card at the hotel bar, restaurant, spa and shops, unwittingly creating a digital footprint that, if accessed by cyber criminals, can be stolen and exploited on the dark net.

As the hospitality sector continues to provide guests with the best possible experience, it is confronted with the difficult task of balancing ease of access with appropriate security. Nevertheless, as cyber attacks increase in sophistication, frequency and magnitude, hospitality professionals need to be aware that these security breaches can cause irreparable harm to their brand from a reputational and financial standpoint and result in serious legal consequences. It is no longer a matter of whether the business will be attacked but when.

Given the growing rate of technological advances it is unrealistic for any organization to be completely impregnable to a cyber attack. However, hotel chains, can strategically allocate their resources to implement an incident response plan to help anticipate, withstand, recover from, and adapt to emerging cyber threats. Cybersecurity is not just an IT department issue but rather an enterprise-wide risk management issue. Cyber incidents frequently cross over multiple functional areas of a business and require oversight at the highest levels of the organization.

Here are a few quick wins that organizations can implement to mitigate their cyber exposure:

- **Defining leadership roles and responsibilities** – Organizations should establish a cyber monitoring team tasked with meeting regularly to assess threat levels, address gaps and make recommendations to management and the board of directors. The team should include key legal, business and c-suite executive stakeholders. To ensure effective risk management, Board members must be properly informed and should engage in Board-management discussions involving identification of which cyber risks the business is confronted with and determining what to disclose in the event an incident occurs.

---

1 Imran Ahmad leads Cassels Brock & Blackwell LLP’s cybersecurity law practice and can be reached at iahmad@casselsbrock.com. Andra Enescu is an associate and also a member of Cassels Brock & Blackwell LLP’s cybersecurity law practice.
• **Conduct regular risk assessments** – The hospitality sector should regularly conduct a 360-degree review of its network and assess its cyber vulnerabilities. This exercise can include evaluating current cyber incident protocols, conducting refresher employee training, indentifying data and asset vulnerabilities, etc. It is recommended that the organization consider retaining external counsel knowledgeable in cybersecurity matters to coordinate this exercise (counsel may retain a security audit firm for parts of the assessment, as appropriate) so as to ensure that the results are protected under solicitor-client privilege. The results and recommendations flowing from the assessment should be communicated to senior management and the Board who can then determine whether additional resources need to be allocated to cyber defences.

• **Train employees and ensure good hiring practices** – Hotel employees should be provided with training that will prepare them to quickly identify and report potential cyber issues. Employees are the first line of defence and providing practical and innovative ongoing staff training that focuses on fostering a culture of procedural compliance, a questioning attitude and having a depth of knowledge to identify potential threats, is critical. Additionally, to reduce internal threats, effective pre-employment background checks and employee screening measures should be implemented.

• **Have a cyber response plan** – From a risk management perspective, organizations should develop a cyber response plan that will map out key legal and business issues and will need to be addressed in the case of a successful cyber attack. A cyber response plan will limit damage, and reduces response costs and recovery time, increases the confidence of external stakeholders and reassures guests whose information may be compromised.

The annual global cost for cyber crime committed globally is estimated to be as high as $100 billion dollars. Cyber attacks can happen any day, at any time and if successful, a hacker can compromise the network infrastructure of any business in a blink of an eye. Cyber attacks are malicious, harsh, and pose a serious threat to the hotel industry in particular due to the high volume of credit card use by guests. As cyber attacks become more sophisticated, hotels should look to experts that can offer valuable tools and advice to help plan, design and implement effective cyber security defences. The bottom line is that the best way to defend against cyber attacks is to prepare and plan effective risk management procedures that can reduce the impact in the case of a cyber incident.

**Imran Ahmad**  
Direct: +1 416 860 6578 • Fax: +1 416 350 6934 • iahmad@casselsbrock.com  
2100 Scotia Plaza, 40 King Street West, Toronto, Ontario, M5H 3C2  
www.casselsbrock.com