Hospitality

Effective data breach protection for the hospitality industry.

Essentially, a data privacy breach is not a question of "if". The only question is "when?"

Information exposures within the hospitality industry have many causes and are difficult to control. And even with the best systems, controls, personnel and procedures, no hospitality provider is immune to the risk. It only takes one small human error, a simple property crime, or one clever hacker, to compromise millions of records, or otherwise wreak havoc on your organisation.

Significant exposure

Hospitality providers present extremely tempting targets for identity thieves. Publicly available wireless networks, physical point of sale devices within hotel restaurants and bars, and a multitude of employees with access to guest information, all increase the risk. Smaller, independent organisations may be challenged to allocate sufficient resources to network security in a world in which hacking and malware threats evolve very rapidly. For larger franchise operations the biggest risk may be interconnectivity: if franchisees and the franchisor share a single hospitality management system, one small mistake or vulnerability can lead to a breach that results in significant and lasting reputational damage.

Payment Card Industry (PCI)

Commerce without credit and debit card payments has become virtually unimaginable. Whether at the point-of-sale, online, or through a call center, the hospitality industry processes a staggering amount of credit card transactions. A breach of credit card information, which the card brands frequently detect before the organisation even suspects any foul play, can result in fines, penalties, mandated computer forensic costs, legal fees, and worst of all, the inability to process payments.

Hospitality

Regulatory investigations and penalties

Compliance with the UK's Data Protection Act (DPA) is not just about the confidentiality of personal data, it is also about information security and ensuring that data is securely stored and managed.

The Information Commissioner's Office (ICO) has several options when it finds that an organisation has breached the UK Data Protection Act. A significant breach of personal data could result in actions including issuing monetary penalties, enforcement notices, auditing and prosecutions.

In February 2015, an online company was fined £175,000 by the ICO after IT security failings led to hackers accessing customer records, including credit card details. As a result of the breach, 5,000 customers were victims of credit card fraud.*

No matter the industry sector or size, if an organisation fails to comply with data protection regulation the consequences can be severe, from reputational and share price damage, to hefty fines up to £500,000 and even criminal charges.

*Source: www.ico.org.uk

Why Beazley

Beazley, a leading insurer of technology and information security risks, has developed Beazley Breach Response (BBR), a solution to privacy breaches and information security exposures tailored to the needs of the hospitality industry.

BBR is a complete privacy breach response management and information security insurance solution which includes a range of services designed to help you respond to an actual or suspected data breach incident effectively, efficiently, and in compliance with the law.

Third party coverage

- Third party information security and privacy coverage with up to €25m/£15m in limits in addition to the breach response coverage
- Regulatory defense and penalties
- Website and offline media liability
- PCI fines, penalties and assessments*
- Cyber extortion
- First party business interruption and data protection with limits up to €25m/£15m.

* Where insurable by law

Top 3

1 of the top 3 industries targeted for data breach attacks

Source: 2014 Global Security Report

beazley

Data breaches take many forms. External hackers and malicious insiders cause many breaches, but did you know that simple carelessness is responsible for a surprisingly large number of breaches?

Every breach is different. It is important to work with a partner who has been there before.

BBR Services

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage data breaches successfully. In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

BBR Services is a dedicated team of data breach professionals who assist BBR policyholders at every stage of incident investigation and breach response.

They coordinate the carefully vetted forensics experts and specialized lawyers to help you establish what's been compromised; assess your responsibility; and notify those you have to. In addition, BBR Services coordinates credit or identity monitoring for your customers and PR advice to help you safeguard your reputation.

Hacking and malware

- A property management company that operates several spa hotels contacted Beazley. One of their spa resort locations was believed to be infected with malware. Over the weekend, the BBR Services team coordinated with an external forensic team to be onsite to investigate that Monday. After an extensive investigation, it was discovered that their organisation's central processing centre, which was housed in a separate state, was infected. After additional investigation, the external forensic team was able to conclude, based on available logs, that the malware had not accessed any personally identifiable information of the patrons or employees. With counsel from an experienced privacy attorney, the company was able to conclude that the incident was not a reportable breach.

- A hotel discovered that malware infected its central processing centre and, as a result, it was not able to determine whether the malware originated from the hotel's central processing center or from one specific property. BBR Services connected the hotel with legal counsel and a forensic firm. The forensic investigation revealed that no personally identifiable information (PII) was accessed, and the hotel was not required to notify.

Hospitality

Learn more:
www.beazley.com/bbr

Unintended disclosure

- A hotel chain franchisee had a computer error where guests' credit card numbers, passport numbers, or driver's license numbers were entered into a field intended to house residential address information, which was then shared with marketing partners for potential mailings. BBR Services connected the hotel with a law firm as well as a forensic firm, who together determined that approximately 30,000 individuals needed to be notified. BBR Services also coordinated the notification and call centre services vendor.

Physical loss/non-electronic records

- A hotel received complaints of credit card fraud from approximately 50 guests. BBR Services connected the hotel with legal and forensic firms to investigate. Soon after, each hotel property received notification that an issuer had identified the property as a common point of purchase (CPP) for cards that subsequently experienced counterfeit fraud. This resulted in a payment card industry (PCI) investigation. The forensic provider located malware on a backup payment system. Ultimately, the hotel had to post substitute notice on its website and issue a press release. BBR Services also coordinated call centre services for the hotel.

"The response from the Beazley Group after discovering a potential data breach was an amazing demonstration of customer service and professional guidance. The response time was fast, less than an hour before the team was pulled together for a teleconference with our representative and we were issued next steps within an hour after that. Having Beazley in our back pockets has already paid for itself three-fold and in my opinion is essential for any business continuity and disaster recovery plan."

Sonya Lynn, EVP, Chief Operating Officer
Craft3

beazley