Hospitality

Effective cyber breach protection for the hospitality industry.

Essentially, a cyber 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 centre, 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.

Top 3

1 of the top 3 industries targeted for data breach attacks

Source: 2018 Global Security Report

Regulatory landscape

The European General Data Protection Regulation (GDPR) is one of several recent global, legal and regulatory developments that impose significant new data privacy compliance and reporting obligations on organisations that manage personal data.

The GDPR introduced mandatory data breach notification obligations and expanded the regulators' authority and control, including the ability to levy significant fines. The GDPR also opens up the potential for class action style privacy claims throughout Europe, not just for financial losses but also for mental distress. Countries such as Australia, Brazil, Israel, Mexico, the Philippines, South Africa and South Korea are following Europe's lead and are implementing data privacy laws that are more robust.

These new laws and regulations present complex challenges to organisations in terms of what measures they need to implement in order to protect information over which they have custody. Responding effectively to incidents that affect this data and mitigating the potential costs and impacts of the incident is now a critical concern.

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 cyber breach incident effectively, efficiently, and in compliance with the law.

Coverage

Breach response
- Legal services
- Computer forensic services
- Notification services for up to five million affected individuals
- Call centre services
- Credit monitoring, identity monitoring or other personal fraud or loss prevention solutions
- Public relations and crisis management expenses
- All of the policy's multiple limits will be available for breach response.

First-party
- Business interruption loss from security breach or system failure
- Dependent business interruption loss from security breach or system failure
- Cyber extortion loss
- Data recovery loss
- Data and network liability.

Third-party
- Third-party information security and privacy coverage up to £15 million
- Full media liability
- Regulatory defence and penalties
- Payment card liability and costs.

eCrime
- Fraudulent instruction
- Funds transfer
- Telephone fraud.

Criminal reward

Cyber 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 cyber 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 specialised 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 offers PR advice to help you safeguard your reputation.

BBR Services also provides a full range of resources to help mitigate risks before an incident occurs. On our Beazley owned and managed risk management portal, beazleybreachsolutions.com, you will find resources for incident response planning, employee training, compliance, and security best practices. Newsletters and expert webinars educate you about the latest threats, preventive steps, and regulatory developments. BBR Services also coordinates a variety of pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops, so you can improve the robustness of your cybersecurity.

Case studies

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 on site to investigate that Monday. After an extensive investigation, it was discovered that the 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 centre 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.

Case studies

Unintended disclosure

- A hotel chain franchisee had a computer error where guests' credit card numbers, passport numbers or driver's licence 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 back-up payment system. Ultimately, the hotel had to post a 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

The descriptions contained in this communication are for broker preliminary informational purposes only. Coverages are underwritten by Beazley syndicates at Lloyd's and will vary depending on individual country law requirements and may be unavailable in some countries. The exact coverage afforded by the products described in this communication is subject to and governed by the terms and conditions of each policy issued. Beazley Solutions Limited is a service company that is part of the Beazley group of companies. Beazley Solutions Limited has authority to enter into contracts of insurance on behalf of the Lloyd's underwriting members of Lloyd's syndicates 623 and 2623 which are managed by Beazley Furlonge Limited. Beazley Solutions Limited is an appointed representative of Beazley Furlonge Limited which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the UK (ref 204896) in its capacity as insurer. BZCER001_UK_02/19