HotelNewsNow
Vital information for hotel decision makers

Combating security breaches at hotels

19 Jul 2013

Data security breaches are a real and present danger, and privacy and data security must be a top priority for the hospitality industry.

Highlights

Wyndham and the FTC are in litigation from a security breach of over 600,000 Wyndham customers.
Forty-six states have security breach notification laws.
Executives and managers are key targets of social engineering.

By Peter Sloan and Deborah Juhnke
HNN columnists

Wyndham Worldwide Corporation is embroiled in litigation with the Federal Trade Commission arising from the alleged hacking and theft of payment card numbers for more than 600,000 Wyndham hotel customers. While this litigation involves novel and complicated legal issues, the underlying reality is both harsh and straightforward: Data security breaches are a real and present danger, and privacy and data security must be a top priority for the hospitality industry.

The case might ultimately resolve whether the FTC can sue non-financial institutions, such as hotel companies, regarding their privacy and data security programs. But regardless of this lawsuit's outcome, state laws already on the books unambiguously require hotels to protect their customers' and employees' personal information with painful repercussions if data security is breached.

Deborah Juhnke

Peter Sloan

Forty-six U.S. states have security breach notification laws compelling companies to notify state residents if there is a security breach regarding their protected personal information. Companies conducting business in Texas must provide breach notification for residents of states that do not have their own breach notification laws. Personal information generally includes the individual's name combined with other identifying information, such as Social Security numbers, driver's license numbers or financial account or card numbers with account access information. But some states add additional categories of combined information, such as birth dates (North Dakota and Texas); digital signatures (North Carolina, North Dakota and Texas); and electronic-identification numbers, email addresses and Internet account numbers or identification names (North Carolina).

A majority of states also have laws requiring companies possessing personal information to take reasonable measures to protect such information when it is disposed of or discarded, with some such states requiring companies to have a destruction policy and others specifying the means of personal information disposal. Arkansas; California; Maryland; Massachusetts; Nevada Oregon; Rhode Island; Texas; and Utah require companies with personal information of state residents to establish reasonable security procedures and practices to protect such information from unauthorized access, destruction, use, modification or disclosure. The Massachusetts regulatory scheme is particularly sweeping in the depth and detail of its requirements.

Wyndham's situation stands out because of the FTC's lawsuit. But the reality is that the Wyndham matter is one of "47,000+ incidents, 621 confirmed data disclosures, and at least 44 million compromised records" reported in 2012 across industries, according to the 2013 Verizon Data Breach Investigation Report. So, what must be done to avoid becoming a data breach statistic?

Improve detection: Organizations can work to shorten the time between a breach and identification of the breach. According to the Verizon Report, 62% of all breaches take months to discover. During that time, more data is compromised, more repositories can be breached and the damage—both to customer relationships and physical systems—becomes harder to repair. Unfortunately, many information technology personnel have a misplaced confidence that their detection mechanisms are better than they are. If not in place, consider implementing security information and event-management systems, including intrusion detection and protection.

Re-evaluate Payment Card Industry compliance: Compliance with the credit-card industry's PCI Data Security Standard is not just a good idea but it's also a contractual requirement with credit-card companies. Non-compliance may result in fines or expulsion from the credit-processing network. It is not enough simply to install PCI-compliant software. PCI DSS controls must be embedded into business processes. Among other matters, basic configuration settings should be adjusted to reset default passwords for point of sale, property-management and hotel-management systems. An annual PCI DSS audit is a good place to start. Consider, too, that payment applications have their own compliance standard, Payment Application DSS.

Address security risks from sources other than hacking: According to Verizon's report, barely half of the data breaches reported in 2013 involved some form of hacking. Other threats include social engineering (about one-third of incidents), insider threats and device vulnerabilities such as lost or stolen devices with unencrypted data. Social engineering—the art of manipulating people into performing actions or directly divulging confidential information—is particularly difficult to control, because it relies on people's conditioned desire to follow a link. Executives and managers are key targets, as they often have higher-level computing privileges and access to more confidential information. Training can play a key role in improving resistance to social-engineering threats.

Protect all personal information: Protected information includes not only customers' credit-card numbers but a wide range of other information that is commonly collected and stored for customer loyalty programs and other business purposes. Data security should cover repositories and data sources for all personal information, including that of employees.

Ensure your privacy policies accurately reflect the reality of your privacy and data security program: It might seem obvious, but boilerplate privacy and security policies can lead down a dangerous path. Ensure your published policies are legally valid and accurately reflect your privacy and data security practices.

It is impossible to secure against every possible data breach and adequate security is a moving target. Yet working toward that goal is important not only for compliance purposes but also as good business practice. Data protection and privacy must be viewed as an ongoing, daily process, not simply a "check-the-box" exercise to appease credit-card companies.

Peter Sloan is a Partner at Husch Blackwell LLP and a founding member of the firm's Information Governance group. His practice focuses exclusively on helping companies compliantly manage their records and information.

Deborah Juhnke is a Certified Records Manager and Director of Information Management Consulting at Husch Blackwell LLP. She assists clients with information governance initiatives, including risk assessments, records retention and e-mail system remediation.

The opinions expressed in this column do not necessarily reflect the opinions of Hotel News Now or its parent company, STR and its affiliated companies. Columnists published on this site are given the freedom to express views that may be controversial, but our goal is to provoke thought and constructive discussion within our reader community. Please feel free to comment or contact an editor with any questions or concerns.