Hospitality Industry Risks: Data Privacy and Security

PARKER | SMITH | FEEK

May 2012

By Nick Montera, Account Executive

Most hospitality businesses allocate time and capital to efficiently collect and process data in order to improve sales, customer service and loyalty, and operations efficiency. Technological advances have made it easier to manage a wide range of information about customers, vendors, and employees. Virtually all businesses that use computer systems are to some extent vulnerable to costly exposures associated with system breaches. Hotels and restaurants are no exception and, in fact, have much higher levels of exposure because they collect vast amounts of private data from customers as a part of their day-to-day operations through credit card transactions, online reservations, and rewards programs. Private data may be both personal (names, physical addresses, email addresses, social security numbers) and financial (credit card and banking). While technology helps your business run more efficiently, it also increases your risk for data privacy and security breaches, as well your liability to affected customers. Unfortunately, many hospitality companies have not upgraded their risk management plans to address the inherent exposures associated with today's sophisticated data management. A breach can severely impact the financial stability and continuing success of a company, and so it's important to understand the risks associated with data breaches and to develop plans to mitigate them.

Hospitality: A Targeted Industry

According to Nicholas J. Percoco, hospitality businesses often proves to be an easy target for criminals who are looking for high transaction volume, a large database of customer records, and low barriers to entry. In fact, organizations analyzing data breach trends consistently cite hospitality as the single most vulnerable industry:

- The accommodation and food service industries accounted for half of all breaches in the 2012 Verizon Communications Report.
- The food and beverage industry made up 44% of all 2011 data breach investigations by Trustwave Spider Labs.
- Hotels were the single most breached sector for credit card data theft in 2009, accounting for over a third of all major breaches.

Percoco, head of Trustwave Spider Labs, believes that the criminal element targets the food and beverage industry because of high transaction volume, which makes it possible to turn criminal activities into money very quickly. Trustwave Spider Labs found that food and beverage companies not only have systems that are vulnerable to infiltration, but often fail to detect a breach until long after it has occurred. Their study revealed that criminals stay undetected in a breached food and beverage system for an average of 173.5 days. The combination of high transaction volume and undetected breach time can prove devastating to a business.

A common misconception is that only large organizations need to worry about protecting against data breaches. In Verizon's 2012 Report, two-thirds of the 855 investigated incidents occurred at businesses with 11 to 100 employees, a common size for many hospitality enterprises. However, no hospitality company is immune. Smaller, independent enterprises are vulnerable because they are small and may have systems that are easily breached. On the other hand, franchise operations often share a regional, national, or international data system that, once breached, can affect all or most of the individual franchisees.

Most businesses today have data privacy and security exposures, which may include 1) a presence on the Internet, 2) data on servers connected to the Internet, 3) file maintenance that contains personal and/or financial information, and 4) transmission, storage, or processing of data such as credit card payments. Businesses in the hospitality industry need to be particularly cognizant of these exposures. It is important to develop programs to reduce the possibility of a breach and take steps to mitigate the impact of a breach before one occurs.

Costs of a Data Breach

A company that experiences a breach can incur a range of costs that quickly add up to a substantial loss. When private data is compromised, your expenses could include notification and claims processing, credit monitoring services for affected individuals (to lessen the potential for civil suits), and employment of a public relations team (to assist with damage control and preservation of your reputation). There may be additional costs associated with finding and fixing the root cause of the breach, and recovery of lost data. Finally, you may have liability claims for failure to have reasonable safeguards in place to protect personal and financial data.

In the event of a breach, you are responsible for notifying the affected individuals. In fact, 46 states have enacted broad privacy laws pertaining to notification whenever personal or financial information might have been compromised, lost, or stolen. Furthermore, if private data of individuals from other states is affected, you must comply with each applicable state's laws. For those in the hospitality industry, compliance can be costly and time consuming because it entails research into the privacy laws of the state of residency for every potential affected customer. Since many hotels and restaurants depend upon customers from all over the United States (as well as other countries), notification requirements and the related costs are of particular importance. The possibility of regulatory violations and fines can be drastically reduced if you have an adequate plan in place ahead of time.

Estimates of the average incurred cost for a breach vary between the studies, but one thing is evident: it's expensive. According to the Ponemon Institute's 2011 report, the average cost of a data breach in 2009 was $6.75 million per incident and $204 per individual record.

The immediate financial cost of a data breach is only part of the story. It can cause a loss of customer trust and a tarnished reputation, which can be extremely difficult and expensive to rehabilitate. This is especially true for hotels and restaurants, which usually have high public profiles.

Data Security and Risk Management Basics

There is no doubt that the risks associated with data retention and transfer are real and significant. For a hospitality organization, it is of paramount importance to identify areas of exposure and develop adequate risk management programs that address data privacy and security. To help you get started, here is a list of questions (from Cyber insurance specialist Swett & Crawford) with my added commentary:

- Is the corporation aware of all applicable state and federal privacy laws and notification requirements pertaining to customer data?
  - Due to the wide geographic dispersion of your clients, it is best to do this research upfront. If a breach occurs, you may not have adequate time to research and comply with state laws, which may be time sensitive. Missed deadlines could lead to costly regulatory fines and penalties.
  - Make sure that your organization is compliant with The Payment Card Industry Data Security Standards (PCI DSS) and any other standards that apply to your organization. Helpful information on PCI DSS can be found here.
- Is any personal identifiable information (PII) or client confidential information stored on computers or in paper files on premises? If so, where specifically is the data stored, how is it secured, who has access and how many PII data files are there?
  - PII is often defined as unique information that can be used to identify, contact or locate a single person. In Washington state, PII is defined as an individual's first name (or initial) and last name combined with one of the following: social security number, bank account number, credit or debit card number (including security code access code or password), driver's license number, or a

Washington identification card number.

  - Track personal data throughout your entire information infrastructure and identify all parties that have access to this data. Conduct an audit that gauges employee access to and use of personal data.
  - Make information security a written workplace policy.

- Are all of the companies laptops encrypted? Are portable media devices like thumb drives prohibited or at lease encrypted?
  - Devices such as laptops, smart phones, external hard drives and flash drives all present possible data security threats if lost, stolen, or hacked. While most people assume that system hackers are the greatest threat, recent studies show that lost or stolen portable devices are the most common cause of data breaches.
- Has the company implemented strong internal password controls and training to all employees?
  - Make sure passwords are strong. It is also a good practice to reset passwords periodically—90 days is a good timeline—and never duplicate passwords. It's also a good idea to reset default passwords.
- Are the company's firewalls current and all security patches regularly updated?
  - A firewall can be the best defense when trying to isolate and contain breaches. Despite the expense, it is beneficial to invest in a robust set of firewalls that require user authentication.
- Does the company outsource any services to third party vendors that may involve a client's information? If so, do these vendors provide hold harmless and indemnification agreements with regards to any data breach involving personal identifiable information?
  - It's a common misconception that outsourcing automatically transfers liability for data breaches to the vendor. It is vital that you have favorable hold harmless agreements and indemnification provisions in place with vendors, but even with these agreements in place, data owners can still be held responsible for compromised information.
- Does the company have in force a detailed plan in case of a data breach?
  - In addition to developing and implementing a risk management program for data breach, risk transfer via insurance can be a cost effective risk management mechanism.

Data Breach Insurance Coverage Basics

Over 30 insurance carriers provide coverage that is tailored to specifically address exposures related to data breach. Naming conventions vary by insurance carrier, but some of the more common ones are Data Security, Data and Privacy, Cyber Liability, and Data Breach insurance. Coverage may be written on a standalone basis or combined with your Professional Liability or Media policy.

A properly structured policy will provide both first and third party coverage. First party coverage pays for direct losses incurred as a result of a breach including (but not necessarily limited to) notification costs, recovery of lost and destroyed data, forensic investigation expenses, credit monitoring and call center services for affected customers, business interruption losses, extortion demands, and public relations expenses. Third-party coverage protects companies from liability suits filed by individual customers, credit card companies, regulators, and various other third parties. Coverage should extend to defense costs as well as damages. Depending upon the carrier and insurability from a legal standpoint, it may also cover regulatory defense, fines, and penalties.

As a hospitality business, your financial stability and continuing success depend upon a proactive approach to data security risk management. Lax security practices or a security gap could result in a breach that encompasses massive amounts of stolen data, creating financial loss for your customers, vendors, and employees, as well as your business. It's important to do all that you can to protect yourself from a breach. It's equally important to devise a solid risk management plan, including insurance coverage, to mitigate the severity of loss when one occurs. If you have not yet done so, consult with your insurance professional about your data exposure and risk management solutions.