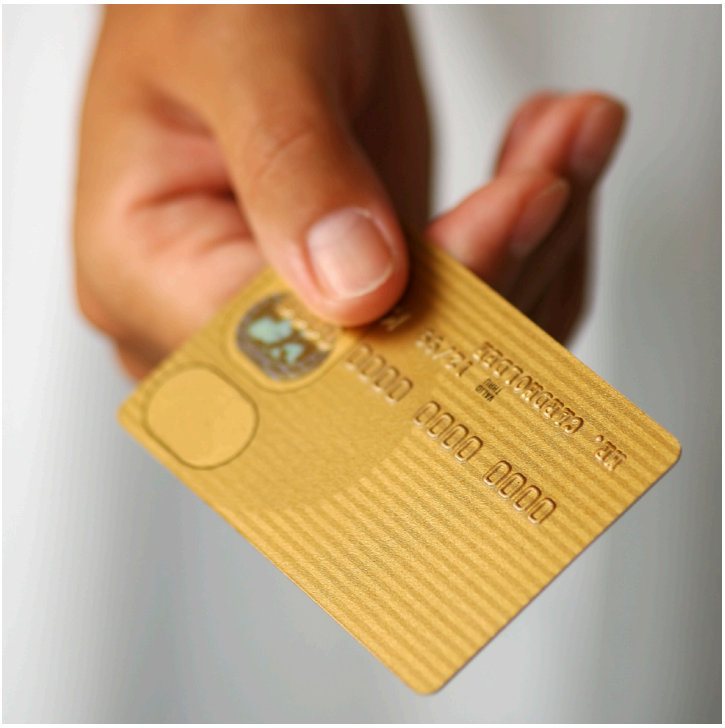
# HOTEL CYBER LIABILITY

## Managing Hospitality Risk



### WHAT'S AT RISK?

All businesses that use computer systems are vulnerable to some of the hazards of cyber liability, but hotels should be particularly mindful of the ongoing exposures and appropriate controls because they have access to a steady stream of their customers' personal information.

As recently as January of 2010, Wyndham Hotels and Resorts discovered that a hacker had penetrated the computer systems of one of the company's data centers. That system acted as a gateway, allowing the hacker to access information from separate computing environments at 37 properties. This exposed personal data such as guest names and credit card numbers, including expiration dates.

The hotel industry has become a prime target for hackers. A recent report from a unit of a data-security firm found that 38 percent of its data-breach investigations during 2009 occurred at hotels.

Hotels are like any other business that collects financial and personal information about customers—they face liability for theft of credit card or personal information. In 2008, the estimated average cost of an information breach to a company was $7.2 million, and of that sum, a third was attributed to lost business.

Even where there is no direct claim by a guest, a hotel will incur costs to inform its guests that there has been a breach. Forty-five separate states, as well as the District of Columbia, have enacted laws that require a company to inform clients and customers when their personal information—name, address, credit-card information, Social Security number, and other information—may have been compromised.

### WHAT ARE YOUR LEGAL OBLIGATIONS?

Because hotels deal with guests from many different jurisdictions, the hotel must analyze the notice requirements in every state that might be implicated to comply with the laws, which vary in the timing, content, and nature of the required notice.

In addition, many hotels may choose to assist their guests by providing free credit card monitoring and other services to help guests avoid potential problems. This also can be a significant expense, but it has become something of a standard response that may help in retaining guest loyalty.

### HOW CAN YOU BETTER PROTECT YOUR ORGANIZATION?

For some suggestions designed to assist you in developing sound policies and procedures for your organization, please turn this document over and review the attached checklist.

---

For more information about this and other hospitality risk management topics, please contact:

**National Specialty Underwriters, Inc.**
10900 NE 4th Street
Suite 1100
Bellevue, WA 98004
(425) 450-1090
**www.nsui.com**

NSU HOSPITALITY

# Checklist: Protecting Your Clients' Information

Data security should be ingrained as part of the property's culture. Here are some basic steps hotels can take to protect themselves and their customers:

- ❑ Limit the information you collect to the information you need, and do no hold on to it longer than you have to. Simply by following that rule, hotels will be able to limit their potential exposure.

- ❑ Get compliant. The Payment Card Industry Data Security Standards provide a comprehensive and proven set of guidelines to bolster data security, and their compliance is required by the five major card brands. Major brands usually provide the necessary IT support to ensure compliance, but smaller chains, portfolios or one-off properties likely will have to hire an outside consultant or security auditor to make sure the 12 guidelines are being met and then implement appropriate security measures.

- ❑ Conduct an informal audit: Gauge your employees' use of and ability to access information. Ask yourself: Who has access to what information? How are they getting it? Do they need that information to do their jobs? And if they do, make employees have their own usernames and passwords for tracking purposes.

- ❑ Make a concerted effort to track personal data throughout your entire information infrastructure. For example, you might know that you have a guest's credit card number stored on a paper file in your office (not that you should ever keep paper records of personal data), but did you know there might also be electronic copies in the hands of vendors or third parties if you outsource any booking services?

- ❑ Reset passwords. A good timeline is to reset passwords every 90 days, never using the same password more than once in a two-year span. Also, make sure you reset default passwords. Manufacturers often use the same keywords when they ship out and install their systems, making it easy for the savvy hacker to open what essentially amounts to an unlocked doorway.

- ❑ Shore up remote access. There are various types of authentication and encryption, and users should have their own unique usernames and strong passwords. Most importantly, the remote access channel should be cut off after each use.

- ❑ Create a network divide. There should be two sides to every hotel network: one side allows guests to access the Internet, and the other allows hotel associates to access the necessary programs and information to run that same property. The guest side should in no way be touching the hotel side, and vice versa.

- ❑ Enable wireless security. A Wi-Fi connection has become a must in hotel rooms throughout the world. But what about the security systems protecting it? It's an easy fix. Simply access your router, enable its encryption setting, enable password protection and have guests log on using the password. Hotel employees should first verify the guest is registered at the property before disclosing that network key.

- ❑ Invest in a robust set of firewalls. Firewalls should require authentication every time a user moves from one side of the network to another. Investing in these security systems can be expensive, but it's one of the best ways to isolate and contain breaches.

- ❑ Make information security a written workplace policy. Raise that level of awareness that this information represents a trust that your guests have placed in you—that you're going to use it appropriately, it's a value to the company, and it's an area that can get you in trouble if you misuse it or use it inappropriately.

- ❑ Finally, plan for a breach. This means having a protocol for addressing the breach, and most importantly, identifying, by name, a response team, including attorneys, security experts, C-level executives, public relations professionals, and others who can act immediately to identify the scope of a breach, the proper response, and make executive decisions to limit damage.