Mr. Bolger

Insurance

With Cyberattacks on the Rise, Is Your Hotel Protected?

By Christopher Bolger, Senior Risk Manager, Venture Insurance Programs

When Target Corp. was hacked last holiday season, the size and scope of this incident brought national attention to the growing threat of large-scale, financially motivated cybercrimes. In this case, hackers stole credit and debit card records and other personal information from an estimated 70 million people.

It is believed thieves gained entry to the systems by infiltrating computers owned by one of its third-party vendors and then used "memory-parsing" malware that captures information at the point of sale before it is encrypted.

While the attack on the retail giant was one of the largest cybercrimes ever, it is only one of many ways computer systems can be breached. And retail stores are only one type of business that can be targeted.

Consider the hotel industry. With the volume of credit card swipes at check-in, as well as at their bars, restaurants and shops, hotels offer ample opportunities for cyberattacks. In fact, a credit card breach was detected earlier this year at food and beverage outlets at more than two dozens hotels belonging to some of the country's largest hotel chains.

Every hotel executive should take seriously the threat of computer security breaches, implementing the most up-to-date prevention and risk management practices, creating an emergency response plan and securing sufficient insurance coverage.

Evaluating the Threats

As mentioned above, the extensive use of credit cards in daily operations is a primary way hotels are susceptible to cyberattacks. Not only do hotels transact business through credit cards, but those cards are kept on file and often accessed multiple times during a guest's stay. Each charge made at a spa, gift shop, bar or restaurant during the course of a stay is another opportunity for cybertheft.

You should also consider intentional acts of theft by employees. For example, food and beverage servers can use small devices, easily hidden in a pocket, to swipe customer credit cards over an extended period of time and then sell the data.

Another area of entry is through public Wi-Fi access, which is usually unsecured. Naturally, hotels want to provide guests with the best possible lodging experience and many favor ease of access over security. That can be a mistake. Wi-Fi access needs to be secured. Ironically, Computer Weekly reported a government conference on cybersecurity in a London hotel came under attack through the hotel's free Wi-Fi network.

While these are three areas where hotels may be vulnerable to data breaches, there are many possibilities. An employee's laptop may be stolen, or access to hotel data may be gained through third party vendors who have access to hotel systems. As we will discuss

HBR Feature Focus

Discussions on Emerging Growth Markets

JUNE: Hotel Design: Creating an Experience

Do Spas Need to Be Healthy?

By Mark Wuttke, Principal, The Wuttke Group

The spa industry delivers a menu of services ranging from natural and organic products to procedures that promise immediate results but may be inherently unhealthy. Does it matter? The answer depends upon a spa's positioning. Over the past decade, "wellness" has become the buzzword in many spas and appealing to many spa-goers. Prognosticators have dubbed wellness the next trillion-dollar industry. But not every product and process on the wellness bandwagon is healthy. This article examines the meaning of the word and provides a guideline to help the operator determine what services align with one's brand, guest expectations, and financial projections. READ MORE

Next Generation Wellness Movement: Spa Hotels vs. Hotel Spas

By John Morris, Director of WELL Spa and Salon at Grand Geneva Resort & Spa, Grand Geneva Resort & Spa

Wellness is in – digital detoxes, spirituality concierges and vegan restaurants are trending in the hospitality and travel industries because of a growing segment of travelers either seeking to maintain a healthy lifestyle on the road or looking to improve their wellness through retreats and education. Some resorts have gone above merely draping their brand in wellness terminology and instead have integrated these health-conscious components into their design and programming. Evolving with the wellness movement means adapting to the rising demand for physical fitness centers, beauty treatments, weight management regimes, relaxation and stress relief, and health-related education while traveling. READ MORE

below, a thorough vulnerability analysis is necessary to determine risk.

The Impact

There is a financial impact when any type of computer security breach occurs. It is estimated Target will lose half a billion dollars from its well-publicized attack. Costs range from computer forensic investigations and customer notifications to legal defense of potentially costly lawsuits.

But the impact goes further than the corporate bottom line. You can face a public relations setback that has the potential to jeopardize the trust and patronage of even your most loyal guests. Many people affected by breaches promise never to do business with the involved company again, resulting in a loss of market share.

Data breaches can also carry personal risk for hotel executives and board members. Attacks are drawing increased scrutiny from government regulators, including the U.S. Securities and Exchange Commission (SEC), who want to ensure directors and officers are taking necessary steps to prevent breaches.

Prevention and Risk Management

Of course the best way to deal with a data breach is to prevent it from happening in the first place. Here are some key areas to consider when seeking to improve the security of a hotel's data systems.

Define roles, responsibilities and oversight. Responsibility for data security may fall to a Chief Information officer, Chief Security Officer or a new position being created called Chief Privacy Officer. Whoever is responsible, the person's role should be clearly defined, including interactions with other departments and relevant outside vendors. Also consider board oversight. Is there a board member or audit committee with the technical expertise to adequately review cybersecurity issues?

Conduct a risk assessment. This assessment should be specific to guest privacy policies and data security. You need to know how, why and where your data is vulnerable and what safeguards are applied to each computer and device. You should see a network map that shows where data is stored and who controls it.

Get expert help. The technical aspects of cybersecurity should be undertaken with specialized consultants. These experts can offer valuable tools to help build necessary firewalls, data encryption and other safeguards. Some of these services are made available through your insurance partner.

Bolster your safeguards. Each hotel will have unique security requirements based on its specific systems and operating environments, but there are considerations that apply to all hotels.

- Limit the number of computers and devices that store sensitive information.
- When using a Wi-Fi network, use a secure wireless connection and an effective firewall.
- Use encryption for storing, receiving and transmitting data.
- Have all employees use strong passwords, which are changed regularly.
- Check security practices of any vendors that interface with your computers or who serve your guests.

Create effective and realistic policies and procedures. Make sure you have an effective and accurate privacy policy in place, detailing measures you take to secure guest data and the real risks involved. These cybersecurity policies and procedures should be written, implemented and incorporated into the overall written safety and emergency planning program, including assigned responsibilities.

It's important to note in 2012, the Federal Trade Commission filed suit against Wyndham Worldwide Corporation and three of its subsidiaries claiming the hotel did not take common and well-known security measures to prevent a series of cyber attacks that began in 2008. The suit also claimed the company's privacy policy misrepresented the security measures it put in place.

Consider mobile and social. Extend your policies across social media and mobile devices, and create enforceable employee policies. According to recent market research, nearly half of all global Internet consumers employ mobile devices as their primary means of accessing the Web. Due to this rise of "anywhere" access to the Internet and the volume and type of information shared across social media platforms, security policies must factor these elements into privacy and security policies to properly mitigate risk.

Create a specific crisis response plan. In the event of a breach, you will need crisis response services that will take the necessary steps related to ensure business continuity, notification of guests, suppliers, employees, law enforcement and regulatory bodies, and communicate effectively with the media.

Ensure good hiring practices. While there are unknown hackers located in other countries, you can reduce the threat of internal attacks by making sure you have effective pre-employment background checks and other screening for employees, especially those with access to computer systems and guest credit cards.

The Ancient Healing Powers of Natural Hot Springs

By Susan Hartzler, Public Relations Executive, Mental Marketing

For centuries, Native Americans, early European explorers, and visitors from around the world have flocked to natural hot springs to bathe in the healing waters. "Taking the waters" through a soak or a sip, was believed to cure almost any ailment. But over time, the popularity of this practice lost its resilience…until now. In both Europe and Japan, hot spring therapy has been an accepted and popular treatment for musculoskeletal problems for some time now, believed to help those with high blood pressure, eczema and a variety of other complaints. The recent resurgence of wellness resorts and destination spas is bringing these ancient healing bathing rituals back in vogue here in the United States. READ MORE

Spa Services for Families: A Growing Trend

By Lucia Rodriguez Amasio, Laniwai Spa Director, Aulani, A Disney Resort & Spa, Hawaii

Traditionally, spas have been retreats for adults to relax and revitalize, far away from children. But with the rise of wellness in spas, another trend has taken rise – incorporating children and teens into a complete family wellness experience. Teens, children, and even tots are now going along for the 'spa-ride,' creating a unique activity for families to do together. With the rise of spas broadly associating with wellness, the total approach and commitment to improving one's health, far more families want to get there spa-on together. Today, whole families are enjoying the spa together, and more spas are finding creative ways to welcome the entire clan. READ MORE

Insurance

While effective safeguards can protect a hotel from many threats, hackers are becoming more sophisticated and often operate overseas. This makes it more difficult to investigate and prosecute suspected attacks – and essential to have privacy and data breach insurance coverage.

These insurance policies were initially very costly, but have become increasingly affordable as more insurance carriers have entered the market. Today, robust coverage is available for hotels, including policies for first-party (the hotel) costs and third-party (guests and others affected) liability.

These policies should cover a hotel's costs to respond to the data breach, including:

- Forensic computer investigations to confirm the breach and identify whose information has been put at risk. This can be a costly endeavor.
- Costs to draft and deliver notifications to individuals, the payment card industry or a regulator. This coverage should include costs to set up a call center.
- Credit or identity protection services for affected individuals.
- Crisis management and public relations specialists to help mitigate the potential fallout from a breach event.

Privacy protection is necessary to cover the costs to defend claims related to handling personally identifiable or confidential corporate information, including:

- Violations of privacy or consumer data protection laws.
- Negligence or breach of contract.
- Negligent network security resulting from events such as the transmission of malicious software or a denial of service attack (when the hotel's systems or website are not available to guests or other intended users).
- Regulatory actions, which can be costly to defend and include defense costs, civil penalties and compensatory awards.

Other coverage can be added, including:

- Cyber extortion: when a hacker threatens to hack into and damage websites or data in an attempt to extort money.
- Hacker damage to your digital assets, including websites and other electronic data.
- Cyber Business Interruption that compensates hotels for loss of revenue due to a cyberattack.

When considering insurance, it's important to make sure you have sufficient limits to cover each of the costs and liabilities you potentially face. There have been breaches that have taken up to two years to discover. A continuous evaluation of your policies and procedures is crucial to a successful program. And ask if your insurer provides pre-breach risk management services and post-breach response services to help manage an incident as it unfolds.

Cybercrime is evolving and escalating, and the potential damage to a hotel's bottom line and reputation cannot be ignored or understated. A hotel's data systems, risk management and crisis response plans, privacy policies and governance all need to be updated regularly to ensure they continue to keep pace with emerging threats. The same is true with insurance. Policies continue to improve so review your cyber coverage annually to be sure your coverage and limits are adequate.

Senior Risk Manager for Venture Insurance Programs. Mr. Bolger has specialized in hospitality risk management since 2007 and is responsible for improving the risk performance of Venture's hospitality clients by reducing the frequency and severity of claims, analyzing loss reports to identify trends by industry or location, and improving loss ratios in order to improve pricing for the hotel and profitability for the insurer. Overseeing all risk management operations, including the claims adjusting teams, Mr. Bolger ensures proper proactive claim management and loss control procedures are in place with the overall goal of minimizing the overall cost of risk. Mr. Bolger can be contacted at 800-282-6247 ext. 242 or Cbolger@ventureprograms.com ***Extended Bio...***