Anatomy of a Hotel Breach

Written by Sandy B. Garfinkel

Monday, 09 June 2014 15:22

Data breach incidents have dominated the news in 2014, and they are only becoming more frequent and damaging. Every industry and every type of business has been a victim of cyber intruders or other types of data loss or theft. Information criminals take everything from sensitive corporate trade secrets to customer or employee personal information, including credit card account numbers, bank account codes, social security numbers, e-mail addresses and other items useful in carrying out identity theft. Security industry experts have estimated that 78% of all companies and organizations in the United States suffered some sort of data loss or theft within the past two years. The

prevailing view among most analysts is that data breaches are unavoidable, and that it is not a question of if companies will become victims, but when, and how prepared they will be to react when it happens.

Unfortunately, hotels and hotel companies have been, and continue to be, tempting and frequent targets for data thieves.

Why are hotels of such interest to information thieves? Several factors could be to blame. One may be that hotels do such a large amount of business through credit and debit card transactions, and payment card fraud is a favored type of identity theft crime among cyber criminals and those to whom they sell their stolen information. Another may be that hotels frequently must tie their data and computer systems together with the computer systems of others, such as the major hotel brands and, at times, outside vendors or contractors. High employee turnover and, in many cases, poor employee training in security practices may also contribute to the vulnerability of hotels to data thieves.

Wyndham's Data Incidents

Arguably the most notorious set of hotel data breach incidents happened to Wyndham Worldwide Corporation during the period of 2008-2009. Here's how those incidents unfolded:

In April of 2008, foreign hackers gained access to Wyndham's computer system through a single computer in one of Wyndham's franchised hotels that an employee at the property had connected to the internet. The internet connection permitted the hackers to intrude into the hotel computer. This computer was also connected to Wyndham's property management and reservation system (all Wyndham franchised hotels are required by contract to utilize Wyndham's management and reservations system). This pathway was used by the hackers to gain access to Wyndham's own servers at its data center in Phoenix, Arizona. Once inside Wyndham's system, the hackers obtained administrator passwords and access codes. At that point, the intruders had a ready pipeline to reach individual Wyndham franchised hotels that were connected to Wyndham's central servers.

Within approximately a month, the hackers had used Wyndham's computerized connections with its franchised hotels to compromise the computer systems of 41 different properties. Unfortunately, it took Wyndham a number of months to recognize that the intrusion had occurred.

Even more regrettably, the hackers returned twice more in 2009. Wyndham believed that the security vulnerabilities that had allowed the 2008 attack to occur had been

remedied, but they had not. The second cyber attack on Wyndham resulted in the compromise of information from 39 franchised hotels; the third, 28 hotels.

The hackers, believed to have been operating from Russia, stole guest credit and debit card account information. In total, over 600,000 accounts were compromised in this series of breaches. By no means do these incidents qualify to be among the largest data breaches on record, especially compared to a few of the more recent highly publicized incidents, such as the 2013 pre-Christmas cyber attack against Target, in which over 70 million individuals were affected, or the more recent EBay data breach, which is said to have impacted over 233 million people. Nonetheless, the potential for payment card fraud as a result of the Wyndham breach has been estimated to exceed $10 million.

The consequences to Wyndham have been serious and seemingly endless. Initially, just after the incidents occurred, Wyndham issued notifications to all affected individuals. Such notifications are required by the data breach notification statutes of 47 U.S. states. The notification process was extremely expensive, in part because Wyndham first had to obtain contact information for the affected people based only upon credit card account numbers. Wyndham also provided a year of credit monitoring to affected individuals, at the company's cost. In addition, Wyndham was required to spend time and resources attempting to satisfy a number of state consumer protection regulators and state attorneys general that it was adequately responding to the breaches.

As notifications were being processed, the franchised hotels began receiving notices from their credit card processors that the major credit card companies would be imposing assessments against the hotels, as merchants, for recovery of fraud costs associated with the breach incidents. The hotels turned to Wyndham and sought indemnification for these assessments. Ultimately, Wyndham bore the legal costs of challenging the majority of the credit card brand assessments and obtaining reductions in the fines.

Wyndham's woes over the breach incidents were only just beginning. In April of 2012, the Federal Trade Commission brought a lawsuit against Wyndham in federal court, alleging that Wyndham had failed to observe adequate security practices concerning personal consumer information, and that these failures amounted to unfair and deceptive trade practices. The Commission's complaint quoted the privacy policy which appears on Wyndham websites, which stated that Wyndham would use commercially reasonable efforts to protect the personal identifying information of its customers. The complaint then went on to allege that Wyndham had failed to employ reasonable industry practices to safeguard guests' data. Wyndham asked the court to dismiss the lawsuit, arguing that the Commission had overstepped its authority to regulate by

claiming to have the right to enforce unwritten, unspecified data security standards against companies. Over a year after it was filed, the court denied Wyndham's motion to dismiss in early 2014, and the litigation will soon begin in earnest.

If that were not enough, in May of 2014, a Wyndham shareholder brought a derivative action lawsuit against Wyndham. The claims in that lawsuit focus on the fiduciary liability of Wyndham's board of directors for the data breaches themselves as well as the ensuing Federal Trade Commission lawsuit. The complaint alleges, among other things, that Wyndham failed to disclose the incident to shareholders in its financial filings in a timely manner. Wyndham has already filed a motion to dismiss the shareholder complaint, but no decision has been issued on that motion as of the time of the writing
of this article.

The fallout and consequences to Wyndham from these events have been dire. Adverse impacts to Wyndham include harm to its image and reputation, the cost of notification of consumers and credit monitoring, legal fees and loss of goodwill among consumers, among other things.

What Can Be Learned From the Wyndham Breach Incidents?

Security experts and analysts are becoming more vocal in warning consumers and corporate America that data intrusions are unavoidable. It is becoming the accepted industry wisdom that a determined hacker can get into virtually any system, regardless of how well it is protected. Therefore, it is difficult to say that a good lesson to take away from the Wyndham data incidents is that hotel companies should attempt to make themselves invincible against cyber attacks. Moreover, hotels often have certain inherent vulnerabilities to data theft, including the requirement that their computer systems must often be tied to those of entities which they do not control. There is no easy solution to this circumstance.

Rather, industry experts, as well as lawmakers, are beginning to call for faster and better intrusion response as a defense – through implementing closer monitoring and tighter protocols to detect breaches earlier, and having detailed and rehearsed cyber incident response plans, to name a few. Data breach response plans should include, among other things: creation of an incident response team (company officers, general counsel, outside data breach response counsel, information technology
personnel, communications personnel, risk management personnel, etc.); a game plan for analyzing and containing a breach incident, including identification of forensic assessment and response firm; and, a plan for notifying affected individuals and

government agencies where required. Speed in responding to an exposure or theft of information is a key component to reducing a company's exposure after a breach. The Wyndham incidents underscore that delays in identifying breaches and shutting down exploited system vulnerabilities, in notifying affected people and consumer protection agencies, and in
notifying shareholders, can all lead to higher levels of exposure.

One way to mitigate some of the breach-related costs similar to those incurred by Wyndham is to carry cyber protection insurance. The use of cyber insurance is widely increasing as data breach incidents become more frequent and more broadly reported through the media. Cyber policies come in a wide variety of forms and costs. The scope of coverage and exclusions from coverage must be carefully assessed to make sure a company has reasonable protection in exchange for its premium payments.

In the end, hotel owners, management companies and brands may not be able to avoid becoming the victims of cyber attacks, much in the same way that Wyndham and its franchised hotels became victims. What hotel companies can control, and should strive to prepare for, is their readiness to respond.

Last modified on Monday, 09 June 2014 17:40

Sandy B. Garfinkel

Website: www.eckertseamans.com/directory.aspx?View=Detail&DirectoryID=415

Sandy Garfinkel has a diverse litigation practice, which focuses primarily on business litigation, with a particular emphasis in the hospitality industry.

Hospitality

- Represents hotel management companies, hotel owners, hotel developers and major hotel brands in commercial disputes and a vast array of other issues;
- Substantial experience and expertise in advising and representing hospitality industry clients with regard to dealings and disputes between and among hotel owners, managers, franchisors, vendors and guests;
- Provides legal services relating to compliance with electronic data security laws and industry standards, and in responding to breaches of data security.

Business Litigation

- Representation of manufacturing enterprises, commercial and residential builders and developers, oil and gas production companies, creative and computer design companies, professional athletes, insurance companies, professional associations, architectural firms, management companies and communications companies in various types of tort and contract disputes;
- Registered with the United States Council for International Business as both an arbitrator and a mediator for international commercial disputes, including disputes filed with the International Chamber of Commerce;
- Represents commercial and public sector clients in trial, arbitration and appellate court practice as well as practice before governmental and administrative tribunals;
- Has tried numerous jury and non-jury trials in federal and state courts in various jurisdictions;
- Has argued before all Pennsylvania appellate courts and the U.S. Court of Appeals for the Third Circuit.

Data Security and Responding to Data Theft

- Substantial experience and expertise in responding to thefts of personal information and electronic data security breaches;
- Expertise in the application of state laws requiring notification to state agencies and affected individuals, in required forensic investigation, including security assessments and certification, in compliance with PCI-DSS (Payment Card Industry Data Security Standards), and in addressing fines issued by credit card brands.

Oil and Gas / Marcellus Shale

- Represents oil and gas producers and developers for issues relating to property and mineral title, acquisition of land and easements, land use and zoning issues.

Real Estate and Land Use

- Represents real estate development companies, municipalities and public authorities in litigation matters arising from construction and real property disputes;
- Represents public transit authorities, public sewer authorities, townships and private land owners in eminent domain proceedings;
- Handles real estate related litigation matters including the areas of zoning, land use, and real property taxation.