Anatomy of a Hospitality Data Breach

By: Sandy B. Garfinkel and Lara A.H. Shortz

The Data Theft Reality

Hospitality security technology simply cannot keep up with hackers, who always seem to be one step ahead. 79% of all companies and organizations in the U.S. have had a data breach in the past two years. Per one industry source, there have been 696 breaches as of 12/1/14, as opposed to 552 last year (a 26.1% increase). Between 2008 and 2010, Wyndham Worldwide Hotels and Resorts suffered three separate attacks on its central property management and reservation systems—over 45 individual hotels were hit, with 800,000 credit card accounts stolen.

The retail industry has perhaps been hit the hardest by these cyber-attacks. Between April 17th and 19th, 2011, 77 million Sony Play Station accounts were stolen online, forcing Sony to turn off its Play Station Network—the outage lasted 23 days, and litigation is ongoing. In December 2013, Target experienced a pre-Christmas hack attack, when cyber-perpetrators stole the names, credit/debit card numbers, card expiration dates, PINS and magnetic strip data from 70 million customers. Additionally, the hackers retrieved non-payment card information, including phone numbers and email addresses. Since then, Home Depot, JP Morgan Chase and Kmart have all experienced similar cyber-breaches.

State Laws Generally Control Notification.

47 states and the District of Colombia have data/protection, notification laws. Pennsylvania was one of the first to lead the charge, passing the PA Breach of Personal Information Notification Act, 73 P.S. § 2301 et seq. in 2006. Recently, Congress has been considering multiple proposals for a federal data protection/notification law that could potentially preempt state laws. Regarding certain types of data, federal laws and regulations frequently control notification (e.g., HIPAA, HITECH).

Due to the increased rate of breaches, the landscape of state laws regarding data breach notifications is evolving. Iowa recently amended its notification law, and Florida implemented the rather strict 30-day deadline for notification where a breach, or reason to believe a breach, has occurred.

Typically Protected Data ("PII")

What constitutes typically protected data? Credit/Debit card, or Bank/Financial information containing account information (name of cardholder, account numbers, passwords), as well social security numbers and driver's license numbers are all considered PII. Certain information is only protected in certain states, including medical information, health insurance info, biometric data (fingerprints, voiceprints, retina images) electronic identification numbers, electronic mail names or addresses, Internet account numbers or identification names, digital signatures and parental legal surnames prior to marriage. Some information is never protected including publicly available information that has lawfully been made available to the general public from federal, state or local government records. Additionally, information that an individual has consented to have publicly disseminated or listed is not protected.

Paper Files are Not Immune

There is a general misconception that data theft is always a high-tech attack on electronically stored information. Paper files containing personal information can be just as vulnerable. Certain state laws are confined and limited by only addressing electronic breaches, while a few specify that personal data stored on paper is covered as well.

Employee Data

In addition to mass consumer concerns, employee data is another area where businesses are increasingly susceptible to cyber-attacks. In 2013, at Piedmont Healthcare, a system breach occurred where up to 10,000 employees were impacted by online fraud and identity theft. Later that year, at the University of Maryland, hackers stole names, social security numbers, and birth dates of over 300,000 individuals including student, faculty and staff. Types of protected employee information include both personnel and payroll files. Personnel data includes any information found on an employee application; name, address, social security number, email address, tax forms, driver's license information. Personnel files may contain employee benefit election forms, and medical information.

Payroll files frequently contain W-2 and W-4 tax forms, social security numbers, bank account information from direct deposit forms, and possibly credit/debit card information.

Significance of Social Security Numbers

Social security numbers are by far the most key piece of information exploited by identity thieves. Social security numbers can be used to: file false tax returns, apply for new credit cards, and access financial accounts.

Hospitality is Highly Vulnerable and Faces Unique Challenges

Hospitality is particularly a vulnerable industry, with the high volume of consumer traffic, domestic and international guests, high turnover rates of employees, and the need to tie into the computer systems of a myriad of other entities including franchisors and outside vendors.

The hospitality sector continues to be a major target for cyber-attacks. In 2012, the retail, food and beverage, and hotel industry made up the top three targeted industries for data breaches at 45%, 24% and 9% respectively. External attacks constitute the majority of data breaches, with 92% of them attributable to outsiders and 14 percent committed by insiders (employees). Hacking played a role in 52% of data breaches.

Hotel Wi-Fi networks pose a mammoth problem for guests. "Dark Hotel" poses a serious threat, by inviting hotel customers (frequently business executives) to download a program that masquerades as a legitimate and common software update. Through this process, the hackers obtain all of the hotel guest's private information including passwords and other data that should be protected. The malware can remain on the system undetected for several months before it even goes to work gathering the data.

Hospitality Liability Considerations

There are several myths that hotel and restaurant businesses adhered to, that can cost them substantial liability when cyber breaches occur. The first is that is a hotel uses a reservation system offered by its franchise, they will be covered if the system gets hacked. This is a major misconception, because often times this type of protection will be absent from the franchise agreement. Many of the contract provisions will actually state that the hotel will be responsible and indemnify the franchisor should there be a cyber-breach. Another myth is that if a hotel guest's credit card is stolen at the property level, the payment card processing company (PCP) will cover the hotel under its policy. Most PCP contracts are weighted favorably toward the PCP, and when a breach at the property level occurs, the PCP agreement will mandate that a hotel conduct a full forensic accounting of all its records—which can cost around $25,000 per location. Lastly, many hotels consider cyber liability coverage a waste of money when, a $1,000,000 cyber liability policy can often be obtained for as little as $7,000 annually; money well spent.

Response and Notification

Which state law applies? The law of the state where the affected individual resides is the law that governs notice, not the state where the merchant or employer is situated. As a result, some merchants or businesses may have to comply with many state laws when responding to a single breach.

What Constitutes a 'Breach'?

The aforementioned Pennsylvania Breach of Personal Information Notification Act defines breach as: *Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.*

Hawaii's Notification of Security Breaches Law is broken up into two sections: *(1) Unauthorized access to and acquisition of unencrypted or un-redacted records or data (computerized, paper or otherwise) where the illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person; OR (II) or unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key.*

When Breach Occurs, Who Must Issue Notification?

Under Pennsylvania's law, an entity that maintains stores or manages computerized data that includes personal information must issue notification. Further, a vendor that maintains, stores or manages computerized data on behalf of another entity must notify the entity on whose behalf the computerized data is maintained, stored or managed. The entity on whose behalf the computerized data is maintained, stored or managed must discharge the remaining notice duties.

Who Receives Notice?

The following people should receive notice when a breach has occurred: The individual (employee, cardholder, and consumer); the entity on whose behalf a vendor maintains, stores or manages the data; the nationwide credit reporting agencies must be notified; usually this is triggered if more than 1,000 individuals receive notice at one time.

Additionally, some statutes require a separate notice and/or copy of consumer notice to be sent to the state attorney general and/or a state consumer protection agency.

Consequences of Non-Compliance

In Pennsylvania, the Attorney General may bring an action for unfair or deceptive trade practices under the PA Unfair Trade Practice Act & Consumer Protection Law (no private right of action for affected individual). In California, there can be an individual cause of action "to recover damages," also civil penalty for willful or intentional violation of up to $3,000 per violation.

New Trends: Safe Destruction

On July 1, 2014 July 1, 2014: Delaware passed a law governing safe destruction of records containing a consumer's personally identifiable information. The law requires commercial entities to shred, erase, or to otherwise destroy or modify the records to make the personal information entirely unreadable or indecipherable through any means. Consumers actually harmed by violations of the law may file a civil action and seek treble damages.

Federal Data Breach Law

Many different federal data breach bills are pending before the U.S. Congress. Target and other recent high profile data breaches have put pressure on passing federal legislation. Passage of a federal data breach law may preempt state law and could result in a greater consistency in terms of types of data protected, pre-breach security standards and tightened response and notification requirements.

Incident Response Plan

Hotels must devise internal procedures—detection, analysis, recovery, and post-incident policies—to ensure they have a thorough response plan. Employers must also be proactively implementing policies and procedures to minimize/prevent data security breaches, including forming security incident response teams (SIRT).