



Posted On: 9/1/2009

Experts Respond to Radisson's Breach and How Hotels Can Bounce Back

Christina Volpe, Associate Editor

According to data released from an international survey conducted by [Secure POS Vendor Alliance](#), 46 percent of consumers in the U.S., France and Great Britain are concerned about the potential for a data security breach to occur when paying with their credit or PIN-based cards. If you have read the headlines for the past year, this is not a surprising statistic as more and more instances of security breaches come to light. The past few weeks, in particular, have been a hotbed of such activity. The arrest of accused hacker Albert Gonzalez may have dominated national headlines, but for hospitality, the biggest news on the data security front came from an open letter released by [Radisson Hotels & Resorts](#) informing guests that the hotel chain had suffered a data security breach between November of 2008 and May 2009. *Hospitality Technology* sits down with security experts Dr. Larry Ponemon, chairman and founder of the [Ponemon Institute](#), and Ed Goodman, chief privacy officer of [Identity Theft 911](#) to discuss Radisson's breach and what strategies hotels need to take to rebuild customer confidence.

What we know about the breach so far

Radisson Hotels & Resorts issued an [open letter](#) to customers on August 19, 2009 informing them that the computer systems of some Radisson hotels in the U.S. and Canada were accessed without authorization between November 2008 and May 2009. This unauthorized access was a violation of both civil and criminal laws. Radisson is coordinating with law enforcement officials to assist in the investigation of this incident. While the number of potentially affected hotels involved in this incident is limited, the data accessed may have included guest information such as the name printed on a guest's credit card or debit card, a credit or debit card number, and/or a card expiration date.



At this time Radisson does not know how many properties and/or guests were affected. The company was alerted of the breach through information provided by payment card companies (Visa, MasterCard, etc), and Radisson's payment card processors. In addition to working with law enforcement and forensic investigators, Radisson has conducted a review of potentially affected computer systems and has also implemented additional security measures designed to prevent a recurrence of such an attack and to protect guest privacy. Radisson also placed ads in the Wall Street Journal and USA Today (Aug. 19), and established a Website and call center to address customer concerns. The hotel chain also arranged for guests to receive free credit monitoring for one year if they stayed at Radisson properties in the U.S. and Canada between November 1, 2008 and May 31, 2009.

Asking the experts

HT: One of the most surprising details of this event is that the breach occurred for nearly six months before the company was alerted to it by its payment card

companies. Is it common that a breach can go on for this long before being noticed?

Dr. Larry Ponemon: I'm not sure that I can tell you with great precision what a security breach looks like, but I will say that there are many cases where the organization reporting the breach, reported the breach for some time close to a year before the breach was detected. The fact that Radisson's occurred for several months is not unusual.

Ed Goodman: It is common in general, not just for hotels. Hartland, for example, had a similar window. If someone got in and no one noticed -- from that perspective it is not uncommon for these windows to be there. The reality is that it is still not even clear they [Radisson] know what has happened.

HT: For hotels that have suffered breaches, is it common for them to be alerted of the breach by their credit card processors as opposed to finding the breach themselves?

LP: Basically in some cases and in the case of Radisson, there is an invisible connection to payment processors so when you stay at a Radisson property and pay with credit card, a third party is involved in capturing your credit card detail to make sure the card is valid and to allow them to clear that transaction to the bank. Processors are an important part because every hotel chain uses a third party chain to process. The question that you ask is that it is usual for a hotel to not detect, actually that is kind of a hit and miss and what I find is that some processors are in fact actually better at detecting criminal activity. In the case of Radisson, their processor is a very capable organization. You cannot say that all third parties are bad, some are the source of the breach in this case they are the source of the solution.

In many cases the hotel industry is an IT infrastructure composed of a lot of decentralized security structures is hard to maintain. There is not one central IT structure to maintain and that is not necessarily true in all cases. Starwood has a more centralized IT structure and it has more state of the art security than any hotel chain. But not all hotels have that infrastructure. The credit cards, because they are about securing the process, have more security measure and more of these organizations have to comply with PCI DSS. You can conclude that the processor is better than the hotel but I have experienced some are that pretty good at detecting fraudulent activity.

EG: It does happen on quite a few occasions, but in situations like this where they [hackers] are going after payment card data all of the fraud is going to original. Internal fraud departments at banks will be looking at the source of where the fraud is coming from and they will find a commonality. In this case it was Radisson. Hotels are in a weird situation when it comes to following PCI because typically they are given a credit card to hold a room for guests and those charges do not even run through. Because of the nature of the hotel industry, I am surprised that more of these haven't happened. They are a treasure trove when it comes to data and it all goes back, and is charged to a credit card. They are holding onto that data. and in many cases they do not even notice that fraud.

We also do not know about how the hack occurred. Some properties may have been using wireless technology that would allow them to gain access. My theory, and this is speculation, is that it was some sort of inside job or someone gained potential access through wireless networking. Most hotels provide it [WiFi] in lobbies or in rooms, and those networks in theory should be segregated from hotel networks. BJ's for example was accessed in this way. Often the network is set up so that guests are billed for it, so there is a connection to a payment system. A lot of hotels offer it to guests as an added benefit but it should be a no no to have it hooked up to anything that has a payment system.

HT: Radisson has taken a number of steps since the release of the open letter. Is this the right strategy that a hotel should follow should they suffer a breach?

LP: I think that the procedure that Radisson rolled out is very sensible and I believe that most

companies that have a breach do not realize that this event is unlike other events. A guest can slip and fall in your hotel and it can make it to the front page of the paper. People will care about, it but they don't care about it as much. But a data breach changes perceptions and behavior of customers and that is dangerous. Hotels are expected to be trusted and you don't want a hotel to have willy nilly behavior.

I think that what it means to the consumer is that the hotel has to be very careful by reporting to the people who need to know and not over reporting. In reality people who do not need to know should not be told. You don't want to go through the pains but those people who are victims need good communication. I think what Radisson did was good practice. They had an outside public relations firm but they did a good job of being clear and concise and really getting the message across.

The other issue is the point of how long can we not report the breach there is a balancing act. On one hand we have the breach victim and on the side of the equation if you let the information out to early, it gives the bad guys more. What we find is that a good practice is not to talk about the actual incident until the actual investment is completed. It is a normal operating practice.

EG: My attitude has always been in working in this industry to be as forthcoming as possible. In the privacy community that makes hotels less of a target. They want to says, "listen we are going above and beyond to make sure that you haven't suffered any fraud." It tends to go a long way and it is all about how you approach a notification letter. Being evasive and appearing that way is always a negative. Radisson took a nationalized approach -- each one of them has its own disclosure of breaches so national groups that feature breaches will take a standardized approach. That said, Massachusetts has a unique law that requires that you do not disclose the actual facts of the breach. That could be why they are trying to cover their butts. Consumer are savvy now a days and they can smell something that isn't right, and if they feel that a company is not being truthful they can take their business to other places. From that perspective, hopefully not just Radisson, but the hotel industry as a whole will build their defenses.

HT: No hotel guest would be happy to hear that their (or other guests') information has been stolen. What is the likelihood that news of a breach will lead guests to book with other hotels as opposed to yours and how do hotels rebuild consumer confidence?

LP: We do a cost of data breach study year and what's interesting about the study is that the abnormal churn rate, which is where people will chose another hotel, can be up to 8 or 9 percent. If you have one million customers that means eight percent may think seriously about going to another hotel. Now it is very likely that it will be less than that one for Radisson, The reasons why people lose confidence is because a company does a lousy job of getting the message out.

The first thing you do it show real remorse and concern and you provide them with the appropriate tools. And an organization that provides identity theft monitoring is doing a good job. The other thing that you do is that you do not burry the information, you provide the customer with the ability to ask questions even if they are weird questions. Take each and every one of these calls seriously. The most important thing for Radisson is not to let it happen again, be careful in the terms of systems that you have in place and have some basic common sense control.

EG: There becomes a huge loss of consumer confidence. Hotels are like airlines in that customers pick one that they are comfortable with and get reward points, and there is a high level of customers being tied to one chain over another. It might result in the loss of long term customers. Consumer confidence is shaken and doing things that they have done, and taking some extra steps that aren't mandated by law is a good step. Their marketing folks are going to have they work cut out for them.

I think that offering up the tools to at last provide mediation of the loss is a good step, but really going the extra mile will cost money but will pay off. Groups can make it up to them in other ways, this is the approach that TJX offered. Maybe we will give you 50 percent off of you hotel stay or offer a buy one night get the second free promotion as an easy way to sway guests. You are not admitting any guilt but you are saying, "listen we value you as a customer, and we are sorry, and we want to make it up to you by giving you x or y." It can really go a long way.

- - -