International Journal of Safety
and Security in Tourism/Hospitality

The Human Side of Cyber Security Breaches

Doctor Peter Tarlow

Facultad de Ciencias Económicas

The Human Side of Cyber Security Breaches

Dr. Peter Tarlow[1]

Years ago, tourism security experts worried about such micro-aggressions as: room invasions, acts of personal robbery, or tourist victimization due to acts of pick pocketing. These problems should not be minimized and in many parts of the world are still major issues. Nevertheless, these micro-aggressions have now morphed into macro-aggressions and their consequences vibrate throughout the world of tourism.

The recent unfortunate hacking of the Marriott hotel Starwood brand database resulting in the loss of personal information by approximately half a billion people serves as another example that the world of tourism security is fast changing. According to news reports unauthorized access to customers' personal information may well have been occurring since 2014. To make matters worse, it is only four years later that we know the full extent of this hacking or unauthorized taking of personal information.

Although no one can be entirely certain as to who has what personal information, it would appears that millions of patrons' personal information such as: passport and credit card numbers, dates of birth, addresses, gender times of arrival and departure from and emails may now be in unauthorized hands; meaning that these victims may now be open to multiple forms of identity theft.

Tourism is data dependent. Hotels, airlines and other parts of the tourism industry as a convenience to customers and as a way of being more efficient keep their clients' credit card numbers on file. Passports and driver licenses are used as proof of personal identity and agencies such as TSA in the United States must assume that identification documents are not only valid but also not falsified.

The Marriott-Starwood data breach then serves as a warning for the entire tourism industry. If customers cease to be confident that their personal information will be secure and open only to those who have proper access to it, then the long-term consequences to the travel and tourism industry might

[1] President of Tourism & More Inc.

become catastrophic. To make matters more difficult, although the tourism and travel industry has invested great amounts in time and money in cyber security there is currently no one who can guarantee 100% data privacy. Just as there is no such thing as total security in the physical world, the same reality holds true of the cyber world. There will always be those who seek new ways to harm others. For example over the last few years there have been a number of spectacular cyber attacks including:

- The hacking of the Democratic Party's 2016 election data
- The data breach, commonly called the *Panama Papers* at the Panama law firm: Mossack Fonesca,
- The hacking of half a billion Yahoo accounts in 2016
- The introduction of ransom-ware into the tourism industry creating a myriad of new problems for the travel industry

Realizing this fact there are two key issues in the world of cyber security. The first issue is: the maintaining of privacy for personal data. The problem is that no matter what new measures the tourism and travel industry might take to protect personal data there is always the potential that some attacks will break through our cyber security's protective walls. Just as in the physical world, there can never be a total guarantee of personal data safety. The second issue is what does the travel and tourism industry do when a tourism breach occurs. The issues of cyber crisis management are as important as the issue of cyber security. From the perspective of the tourism industry good cyber crisis management is essential in maintaining not only customer confidence but also customer loyalty.

Most customers might well assume that major tourism companies are doing everything possible to safeguard their clients' privacy. As customers have already factored this assumption into their business relationship the real issue becomes: when there is a successful attack how do tourism industry business regain customer trust. Below are a few suggestions on cyber crisis management.

-Have a plan. It is essential that every tourism entity assume that at some point it will suffer some form of cyber attack. Do not wait for the attack to occur to begin to figure out how damage mitigation will occur. Remember a cyber attack results in not only damage to the client but also in the client's customer of the tourism entity. It is essential to realize that the media may not always reflect an accurate picture of the data breech. Thus a post-cyber attack plan should include not only caring for impacted clients but also careful working with media outlets so that they have full access to and report accurate information concerning the cyber breech.

-Tell the truth. As bad as the crime may be, tourism disasters occur when a business does not tell the truth. Once it becomes clear that there is a cover –up the victimized business has managed to lose customer confidence twice: once due to the data breachand then due to an unwillingness to tall the truth.

-Work to rebuild confidence. Nothing hurts a tourism industry more than lack of timely and accurate information. After a tourism cyber attack customers are rightly upset and feeling vulnerable. Make sure to publicize in as many ways as possible how your business is helping cyber attacks victims. Let the attack's victims know that they are not alone and that you have developed a plan to aid them in whatever way possible. Be sure to allow victims to know that you are continuing to monitor the situation and both security and legal experts provide advice as to what people can do to protect themselves after a data breech.

-Tell the public what your company is doing to help. Send out notifications as to what the public should look for or what signs may indicate personal issues. Then consider step such as: free access to one of the credit and data protection businesses, contacting lawyers who are prepared to help with issues of Identity theft, changing passwords, regularly monitoring of accounts for issues of fraud

-Provide information as to what travelers can do to protect themselves when traveling. In a world based on information it is almost impossible for every traveler to know what to do and what not to do. Hotels, airlines and airports can help by reminding their guests to be careful not to:

- Use public access locations to transmit personal or financial data
- Use Bluetooth sparingly and make travelers aware that Bluetooth communications may be susceptible to interceptions
- Remind visitors that public Wi-Fi networks are also vulnerable
- The use of a smartphone can create less vulnerable hotspots.

-In an age of both phusical and cyber insecurity tourism officials make sure that their security agents are not only well trained in every aspect of security including the customs and cultural habits of their customers, but also well paid. In a business security climate as unstable our current climate, it is essential that security personnel and top business executives work together, receive regular news updates, and be able to act not only quickly, but in a caring and professional manner with travelers. It does no good to have people well trained in the technical aspects of security if they forget that their clients are real feeling people who are fearful in a world of the unknown.

Dr. Tarlow can be reached at ptarlow@tourismandmore.com