WHITE PAPER

BEYOND PCI — ARE HOTELS READY FOR THE NEW WORLD OF GUEST DATA PRIVACY AND SECURITY?

venza®

Better Visibility. Better Defense.

BEYOND PCI – ARE HOTELS READY FOR THE NEW WORLD OF GUEST DATA PRIVACY AND SECURITY?

DANIEL JOHNSON

Privacy concerns are paramount in virtually every industry, especially when it comes to personal information like Social Security numbers, credit card and banking data, and medical history. In the hospitality industry, which sees millions of visitors a year, the securing of data is a mounting concern with breaches making news headlines on a regular basis. As an industry estimated at over $177 billion in 2014, the hotel sector is among the most influential markets in the United States. With over 54,000 properties, more than five million rooms, and hundreds of millions of domestic and international guests each year, hospitality services are a key part of the American – and global – financial climate. In light of recent highly publicized breaches, the hospitality industry must broaden its scope of definition for security to go beyond minimal compliance.

"These companies and their employees forget even following PCI or filing the requisite paperwork, have no clue when they are handling your personally identifiable or financial information,"

PCI is just the beginning

The "Payment Card Industry Data Security Standard" (PCI DSS for short) was first officially introduced in 2001 and by late 2007 the first wave of a standard method for merchants to achieve PCI Compliance was in place. Since then, compliance standards have been at the forefront of precautionary measures, offering guidelines for keeping sensitive cardholder information related to guest payments safe from attack.

The landscape related to cybercrime, legal precedents, security practices, and privacy management continues to change. Subsequently, so do the ways in which hotels must handle data transmission and security, moving beyond the limited guidelines afforded by PCI DSS. With the level of personal interaction between hotel staff and the sensitive information of their guests, especially in this tech-centered era, privacy concerns have been developing in size and scale. In a telling Forbes article, the former director of security compliance at Wyndham Hotels expressed his concerns about how many operators are handling personal data. "These companies and their employees forget even following PCI or filing the requisite paperwork, have no clue when they are handling your personally identifiable or financial information," he said. "Our findings show that there is little to no training of employees on data privacy – insufficient or no policies in place for the protection of data."

PCI DSS updates are frequent enough. Version 3.2, for example, was published in May of 2016, roughly a year following the release of 3.1. Failure to comply to the standards can result in fines, lawsuits, scandals, extremely bad publicity and even bans from processing credit cards. It's critical for hotels and resorts to be up-to-date with the latest changes surrounding data security requirements. However, data security goes well beyond protecting cardholder information.

Privacy in the United States

While the U.S. Department of Commerce has continued to uphold the requirements under Safe Harbor, this grievous shortcoming has left many U.S. companies at risk.

Privacy is one area that's in the midst of a serious debate in 2016. Despite the seemingly unanimous agreement of the importance of privacy and the protection of personally identifiable information (PII) and payment data, the United States currently does not have adequate legislation regarding data surveillance and storage. While some policies exist on local or state levels related to privacy requirements, the lack of a coherent, unified national direction is quite startling. This is especially concerning in light of the European Union's (EU) strict policies regarding the minimum set of protections required by hospitality businesses operating across Europe. As such, the boundaries between the U.S. and the E.U. are widening, as domestic hotels struggle to keep up with required safeguards necessary to transfer information on European citizens.

Safe Harbor and Privacy Shield

In order to protect the well-being of the citizens of its member states, the EU implemented a set of directives necessary to keep personally identifiable information confidential. Within the Charter of Fundamental Rights of the European Union, under the heading "Protection of personal data", Article 8 stipulates:

- Everyone has the right to the protection of personal data concerning him or her.
- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- Compliance with these rules shall be subject to control by an independent authority.

Directive 95/46/EC was adopted to harmonize national provisions on protection of individuals in processing and free movement of personal data. The directive has been implemented in all EU countries.

U.S. companies wishing to deal internationally have historically been asked to meet a set of similar requirements, originally known as Safe Harbor. However, in October 2015, this Act was struck down as invalid, leaving over 4,500 U.S. operations without privacy guidelines for the transfer of data. This was a major blow to the hospitality market.

Hotels process vast quantities of data, much of it private information that goes beyond PCI. For example, in order to book a room, guests are required to input names, addresses, payment information, contact numbers, and email addresses – in short, the types of data necessary for criminals to steal an identity.

While the U.S. Department of Commerce has continued to uphold the requirements under Safe Harbor, this grievous shortcoming has left many U.S. companies at risk. In response to this invalidation, a new set of requirements known as Privacy Shield were designed to fix the gaps left in the aftermath of Safe Harbor's demise. However, this initiative, too, has been deemed to not be robust enough to meet international guidelines. Next steps are uncertain and hotels that are not monitoring this ongoing multinational discussion in anticipation of an eventual outcome may find themselves in hot water.

Hotel Corporate Responsibility and PII

With ever more data being generated, collected, harvested and processed, issues around data privacy and protection will continue to grow. This concept is at the forefront of doing business both in the United States and beyond, and should be a key factor in implementing best practices across any industry. There's consensus with the thinking that no business should be permitted to abuse, misuse, or otherwise, mishandle personally identifiable information (PII). However, there is no consensus on how to ensure the protection of PII. Nowhere is this more critically true than in the hospitality industry. The best practice for organizations that recognize the risk and challenges associated with compliance is to create environments that offer both operational efficiency and information security.

Hotels process vast quantities of data, much of it private information that goes beyond PCI. For example, in order to book a room, guests are required to input names, addresses, payment information, contact numbers, and email addresses – in short, the types of data necessary for criminals to steal an identity. While protecting payment information is a strong start, PII protection requires extra measures to ensure every piece of information provided by a guest is safeguarded to the highest possible level. This is a human issue and one that needs to be highly scrutinized. Establishing security protocols and implementing procedures to ensure that data is not stolen or used in an improper capacity is of paramount concern. In a world of cloud-based computing, data mining, high turnover and outsourcing, it only takes one wrong move to put your entire brand, and your reputation, in harm's way.

Regardless of the legal requirements in place, privacy and guest data security should be a fundamental focus of every hotel. It's not a matter of doing the right thing, it's a business imperative where investments today mitigate costs that may stem from legal action, audits and damaged reputation. Industry leaders must keep in mind that there is no silver bullet. As the landscape of privacy and security regulation continues to change, companies must be willing to evolve as well, least of which for the benefit of the safety and security of their guests. Those with intent to steal data are only getting bolder, which means that every hotel has a responsibility to be aware of the risks and prepared to respond. All must implement a layered approach using technologies, awareness programs and services. And, perhaps most importantly, hotels leverage their front-line staff to achieve security expectations and feel confident and confidently keep guests and their data safe.

CONTACT

Global Headquarters
10886 Crabapple Road, Suite 100
Roswell GA. 30075
+1 770.685.6500
Fax +1 770.685.6553
Toll Free 1.800.684.6132

EU Office
Prinses Margrietplantsoen 33,
2595 AM
The Hague, Netherlands
+1 404 432 4263

For more information, visit
www.VENZAgroup.com

guide@VENZAgroup.com

Drawing on decades of experience, VENZA can help you mitigate your data security vulnerabilities and ensure compliance, keeping your guests and their data safe from breaches. By delivering a security solution for readiness, reassurance and response, VENZA offers 360-degree visibility for proactive management of risks—so you can focus on guest service and building trust in your brand.

Employees are the first line of defense and VENZA arms them with prevention, protection and intelligence tools to help them become your strongest asset in fighting security and data fraud.

Better visibility means better defense. Know your risks, protect your enterprise with VENZA.