

Common Areas of Risk in the Hospitality Industry

DID YOU KNOW?
In 2017, more than 24,000 records were compromised in an average data breach.¹



With so many records at risk, businesses across North America must be aware of their areas of vulnerability.

At the Point-of-Sale (PoS) Terminal

The hospitality industry leads the way in terms of Point of Sale intrusions with 87% of PoS breaches.² Fraudsters have multiple points of entry since payment card data is widely distributed through the hotel, most hotels have multiple PoS terminal locations, and card information often arrives at the hotel long before a guest arrives.

Lack of Private Information Safeguards

Research has shown that 74% of hotels do not have breach protection. Less than half use end-to-end encryption, which protects cardholder data, and tokenization, which protects personal payment data at payment terminals.³

Data Interconnectivity Within Hotel

Due to the interconnection of hotel shops and services, such as restaurants, dry cleaning, spa, in-house business centers and more, a data breach can spread quickly across the one location, making it more complex and costly.

High Hotel Employee Turnover

Hospitality workers are on the front lines when it comes to customer service - and data security. But hospitality positions tend to have a high turnover rate which can affect real-time data security. Some studies show turnover rates among non-management hotel employees are close to 50%.⁴

Risks from Third-Party Vendors

The hotel industry shares a lot of confidential data with airlines, car rental companies, retail organizations and other third-party vendors. Studies have shown that approximately 60% of Chief Information Security Officers (CISOs) express some concern about third-party security practices and the risk of a data breach.⁵

Ransomware Attacks

While the theft of mobile devices, confidential information, and other valuables are always a concern, the interconnection of computerized systems means that a network breach with ransomware or other malware can affect structural parts of the hotel too. This includes door locks, heating and air, and electrical systems.

Lack of Mobile Security Management

Nearly one-third (32%) of organizations in a recent survey admitted to sacrificing mobile security to improve business performance. Mobile technology affects many systems in a hotel, including property-management systems, PoS systems, door locks, messaging systems and more.⁶

Outdated Equipment

As the hotel industry incorporates new technology, systems and software, stored or improperly-disposed of legacy assets can increase the risk of an attack.



3 Tips to Keep Your Business Secure



Identify All Potential Areas of Risk

Conduct a walk-through of your office. Point out and mitigate any risks that you see. This will allow you to discover your pain points and solidify an information security strategy to keep data secure.



Implement Secure Workplace Policies

By establishing comprehensive policies such as a *Shred-it All Policy* and Clean Desk Policy, you encourage people to think twice about their actions in the workplace. This will push them to comply and help protect your data.



Build a Total Security Culture

Using a top down approach and integrating information security throughout the workplace, you will be able to embed it into people's everyday behavior. This will encourage them to re-consider how to securely destroy any and all confidential information.

Sources:

1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. 2017 Data Breach Investigations Report, 10th Edition, Verizon
3. 2017 Lodging Technology Study, Hospitality Technology
4. Four Industries That Have High Turnover Rates, and What to Do About It, May 2017, Business.dailypay.com
5. What CISOs Worry About in 2018 Research Survey, Ponemon Institute and Opus, January 2018
6. Mobile Security Index Report 2018, Verizon

Learn more about information security in the hospitality industry:

877-227-5986 | shredit.com/hotel

Shred-it® is a Stericycle solution. © 2018 Shred-it International. All rights reserved.

