The Basics of Hotel Data Security

REVINATE

Table of Contents

01 Introduction

They say all press is good press but Yahoo, Marriott, eBay, Equifax, Facebook and Target likely disagree.

All these companies, and many more, have been in the news over the last few years because of security breaches that compromised their customers' data, including passwords, sensitive personal information and credit card numbers.

Given these high profile breaches, it's surprising that more than a third (36%) of hospitality business owners believe "data breaches are no big deal and are blown out of proportion." These executives may get a rude awakening if they experience a data breach.

As companies begin to rely on customer data to build better products and market them more effectively, they need to do everything in their power to keep the data from falling into the wrong hands. There's a tremendous amount of pressure on everyone within an enterprise that touches data to maintain security compliance.

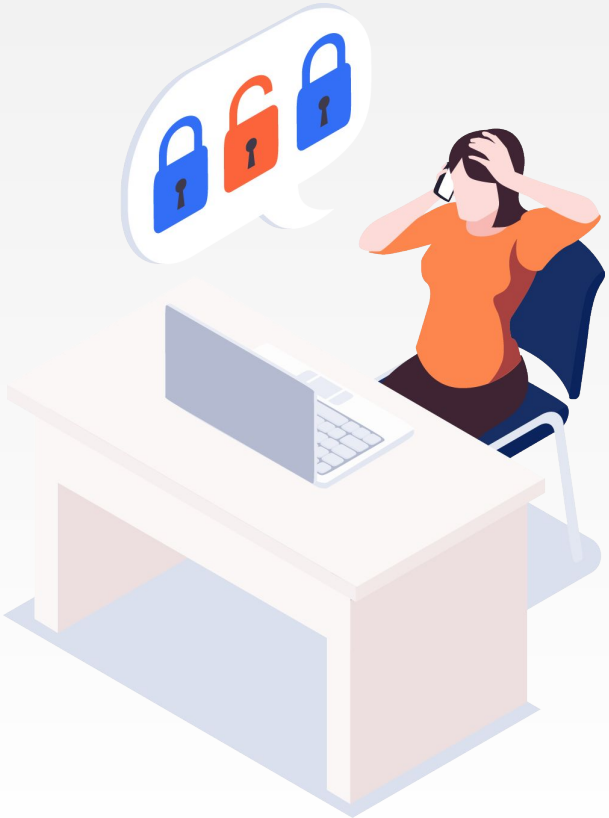
The global cyber security market is expected to more than double in the next five years.

Guest Trust is Critical

In the hospitality market, large quantities of personal data are being captured every minute. For example, hotels might use demographics, past spend data, reservations, preferences, reviews and much more to market their hotel or personalize the guest stay.

As a result, a hotel data breach can leave guests feeling uneasy and very exposed. Consumers trust hotels to keep them warm and safe when they're away from home and it goes without saying that they expect their personal data to be just as protected.

To help hoteliers navigate the ever-changing security landscape, we created this guide to provide best practices on how to secure guest data.



02 Government Regulations

To help set standards around security, governments and non-profit agencies have stepped in to dictate how companies need to store their customers' personal information.

The most expansive law is the EU's General Data Protection Regulation (GDPR). GDPR is a regulation in EU law that governs how companies safeguard the data of European consumers. But regardless of where your hotel is located, if you have European guests and mishandle their data, you can be held accountable by the GDPR. In fact, Marriott was recently fined $123M for a data breach that exposed 300 million customers' personal information.

In a statement of the regulator's intention to fine Marriott, UK Information Commissioner Elizabeth Denham explained, "The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected."

The Four Pillars of GDPR

PROOF OF CONSENT

- Explicit consent by all recipients is required
- Must use unticked opt-in boxes
- Double opt-in is a good way to be compliant

RIGHT TO DATA PORTABILITY

- Guests have a right to their data
- Controllers must be able to provide guests with their information
- Revinate data includes profile information, survey responses, and stay history

RIGHT TO ERASURE

- Guests have right to be forgotten
- Data processor must be able to delete guest entirely from its records
- Controller must work with all processors to ensure guest data is completely erased

RIGHT TO REFUSE PROFILING

- Guests can request not to be profiled
- Guests cannot receive marketing campaigns based on segmented data

Revinate covered GDPR in depth, prior to it going into effect in May 2018, sharing the four pillars that will have the biggest impact on hoteliers. To read more about the Four Pillars, visit the Revinate GDPR guide

More Regulations on the Way

GDPR is often referred to as the gold standard of privacy protection and many governments are using it as a template for their own regulations. While GDPR was the first far-reaching regulation to affect all hotels, it's clear that it was just the tip of the iceberg.

The California Consumer Privacy Act (CCPA), for example, goes into effect on January 1, 2020, and will have a similar impact. As part of CCPA, customers can request information on the data that businesses have about them and can demand that a business delete any personal information that the business collected from them. In addition, at any time, consumers can request that a business not sell their personal information to a third party.

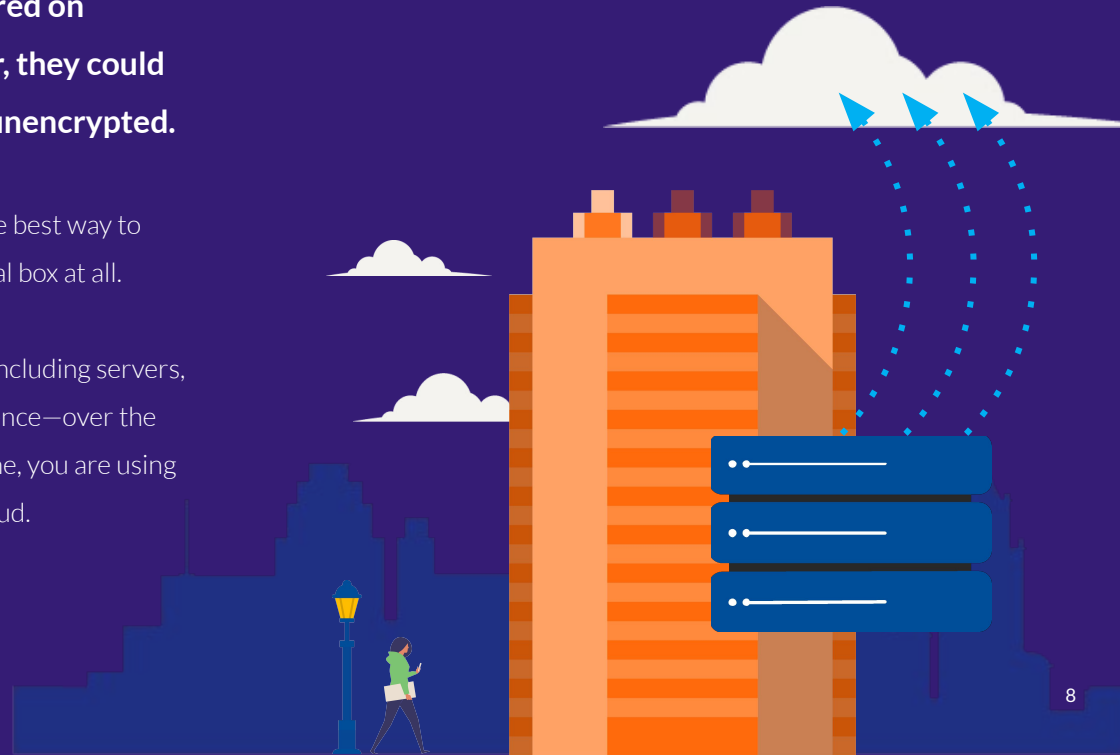
Also, the European Union will soon update its ePrivacy Regulation, which deals, in part, with consent for cookie use. The newest version will also address treatment for electronic communications. The current ePrivacy rules only apply to traditional telecommunications providers, meaning companies behind apps like WhatsApp and Messenger aren't included. However, proposed changes to the rules would make the regulation apply to Internet-based voice and messaging apps as well.

03 Why Hoteliers Should Embrace the Cloud

Prior to 2008 or so, a hotel's data was typically stored on premise. If someone gained access to the computer, they could potentially download data, which was most likely unencrypted.

With the advent of cloud computing, it became apparent that the best way to protect a physical box loaded with data was not to have a physical box at all.

Cloud computing is simply the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet. When you use a Google doc or pay your water bill online, you are using the cloud. There are four distinct advantages to being on the cloud.



Four Distinct Advantages to Being on the Cloud

1. YOU SPEND LESS AND GET MORE

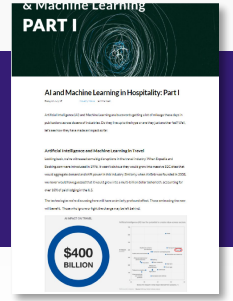
The cloud offers a higher level of service at a lower cost than managing equipment on-premise. Using the cloud doesn't require purchasing any hardware and it's easier and less costly than other solutions, which is why so many of the most advanced technology companies use the cloud.

The biggest cloud computing services run on a worldwide network of secure data centers, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This offers several benefits over a single corporate data center. First, your software services will run faster. Second, you benefit from greater economies of scale since a cloud provider is managing not just your assets, but those of thousands of other companies.

2. YOU CAN ACCESS THE DATA ANYWHERE

Since cloud data is accessible from anywhere with an internet connection, it also simplifies and greatly expands access to information and systems within your organization. Hoteliers can have accurate and detailed reporting and gain insight into their operations in real-time. The cloud is what enables your GM and your Director of Operations to log into Revinate to check the latest reviews at any time.

You can read about how we power Revinate with the most modern technologies in our engineering blog post, *Machine Learning and AI*. When you consider the new capabilities and business results that are possible with the cloud, the choice should be clear.



3. YOU DON'T HAVE TO BE AN EXPERT IN CYBER SECURITY

Having your hotel's resources hosted and managed in the cloud gives you better service and security than on-premise solutions. It frees up your technology personnel to focus on more guest-centric needs and services instead of becoming experts in a complex and otherwise unrelated field of cyber security and learning how to wire up cables, perform data backups, maintain hardware and conduct other time-intensive duties related to data center management.

4. YOU BENEFIT FROM THE LATEST TECHNOLOGY

Adopting the cloud isn't just a technical choice, it's a business strategy. Since most on-premise data centers have been built over time, they are a hodgepodge of aging legacy technology, making them a challenge to maintain and a nightmare to secure. Managing all of this means engineers don't have time to implement the latest and greatest technology. The top cloud companies are purpose-built to give their customers easy access to the newest cutting edge tools.

04 Cloud Security

As you can imagine, top cloud providers offer some of the most secure methods of hosting and networking available. However, you must do your due diligence. With the GDPR, for example, your hotel can be held liable for a security breach of outsourced technology services, so it is important to select a cloud provider with multiple layers of security to minimize exposure.

The big-named public cloud providers have made it their mission to give customers the cloud storage and services they need to function as a business. Their profitability and reputation depend on ensuring that customers' data remains secure within the cloud. As such, cloud providers may employ hundreds or thousands of developers and IT professionals to keep your data safe.

While companies are able to inherit their cloud provider's security protections, security and liability are ultimately the responsibility of each company building in the cloud. A recent breach at Capital One reminds us that with all the advanced features of cloud computing, security is still dependent on correct implementation.

Encryption

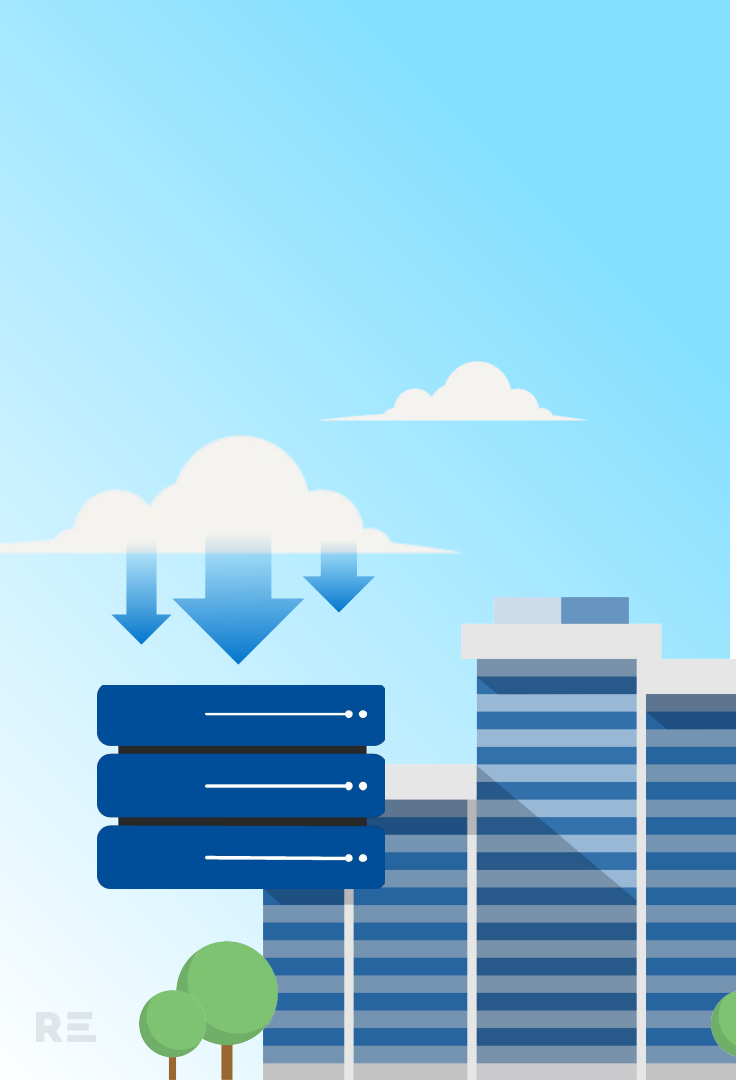
Although not all data is the same, virtually all data can be encrypted, which is one of the primary methods of data protection. You can encrypt data while it is “at rest,” which means it is stored in a static location, or you can also encrypt data “in motion,” such as when it is being transferred over the network.

Encryption is the process of converting data into a complex series of characters that can only be deciphered with a private key. As a result, even if malicious users gets access to your data, they will not be able to decipher the data unless they have the key as well. Only authorized personnel will have access to these files, thus ensuring that your data stays secure.

REVINATE: *By making the investment in the leading cloud computing platform, Amazon Web Services (AWS), Revinate is able to provide customers with peace of mind that their data is being stored on a highly secure and scalable platform.*

High Availability

Cloud providers often have their physical resources spread all over the world. Data may be spread across tens or hundreds of machines, all in different locations. This decentralized structure protects users from data loss due to hardware crashes or natural disasters.



Disaster Recovery

Part of cybersecurity is ensuring that data is available and protected as much as possible, even against natural disasters such as floods, hurricanes and tornadoes. Data can be fragile when backed up on-premise. Keeping information in a nearby physical location means that backups are much less effective, if not entirely useless in a disaster.

Using a public cloud provider to backup your information makes it much more likely that you can rebound from unexpected catastrophes, as long as your backups are kept in a different geographic location than the primary data store.

Point-in-Time Recovery (PITR)

In the event your data does get corrupted, whether it is from a hardware or software issue or the result of malicious activity, PITR ensures that you can restore your data to a specific point in time before the incident. If there is ever a data corruption problem, many cloud providers allow customers to restore to the exact second in time they want the data to reflect, ensuring that not even a single transaction is lost.

Firewalls and Intrusion Protection Systems

Hosting providers use firewalls, which prevent unauthorized internet users from accessing private networks connected to the internet. With a firewall, a hotel can control how employees connect to websites, whether files can be sent to people outside the network, and so on. A firewall gives a company tremendous control over how people use the network.

Intrusion protection systems are another proactive way that data remains safe in the cloud. Most internet accessible data storage systems are under constant attack from malicious users and bots looking for a weak spot or way in. Intrusion prevention is a preemptive approach to network security which is used to identify potential threats and respond to them before data is compromised. Intrusion detection systems (IDS) and intrusion protection systems (IPS) monitor and protect resources from malicious activity.

Security Automation

Leading cloud providers will also use artificial intelligence (AI) and machine learning (ML) to identify malicious traffic and shut it down immediately. Machine learning, for example, can mimic and automate the behavior of security specialists to search and identify weak spots in the network. Even incident response can be automated, using the power of the cloud, enabling organizations to leverage machine learning in order to keep up with the latest security threats.

Security as Code

Companies that have fully adopted the cloud also treat security as any other code. Security tools and infrastructure should be tested and deployed, like any software, to help security teams rapidly scale and protect changing environments.

REVINATE: *In our dedication to providing the highest levels of data protection, Revinate has retained a leading auditor to achieve SOC 2 Compliance, along with a full-time team of in-house data security experts.*

05 Certifications

By now, you hopefully agree that data in the cloud is safer than data stored on-premise. But security is just one factor to consider. In addition to your specific business requirements and goals, look for these non-functional requirements when vetting vendors:

SOC 2 COMPLIANCE

As we mentioned previously, you must remain vigilant about your data, even if it is stored with a reputable cloud provider. To help companies ensure data compliance, auditing solutions have been developed. SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your hotel and the privacy of your clients. SOC 2 was developed by the American Institute of CPAs (AICPA), and it defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy.

While SOC 2 is not legally required for cloud providers, your hotel should consider it a requirement for any cloud provider you are considering or currently using. Revinate, for example, has engaged a leading auditor to review its controls and issue an independent accountants Type II SOC2 Report.

Training and Cloud Adoption

There is no doubt that the cloud can dramatically change the technology landscape and business results of a company. We have reviewed the business drivers, technical best practices for securing your data, and some high level considerations when choosing cloud providers, but what about your employees?

The impact that cloud adoption can have on day to day business operations is often overlooked. Hotels must think about how business processes will need to change to make best use of the cloud. For example, what type of training will you need to provide your back of house IT staff to make sure the cloud implementation is really secure? Like with GDPR, what awareness and training will front of house guest services need to know when rolling out a new cloud implementation?

06 Conclusion

The hospitality market's reliance on large amounts of guest data presents both a liability that can be mitigated by advances in cloud security, and a business opportunity to benefit from innovative cloud capabilities.

Savvy hoteliers in 2020 and beyond will ensure their data is protected by best-in-class security services, establish compliance with all privacy laws, and avoid any negative press, fines, or loss of consumer trust that will result from lax security.

Get a Demo of Revinate and Start Making the Most of Every Guest.

Revinate's distinctive approach to data security helps protect hotels around the globe against data breaches and other security risks associated with CRM and database marketing. Revinate is the most complete and robust solution to help keep hotel guest data secure.

To learn more about how Revinate can provide a secure and scalable solution for your hotel, sign up for a demo today.

GET A DEMO

LEARN MORE