

Hospitality ICT Services

# 12 steps to take after a cyber attack



# Hotel data breaches

Life in the hospitality industry can be tough.

As global tourism starts to open up, hotels trying to get back on their feet after the pandemic are being advised to beware of an increase in hotel data breaches.

As a hotel manager, putting on a brave face and smiling assuredly while you take down a hotel guest's card details and handling their sensitive information can be onerous.

You want to know that you've put appropriate systems in place at your hotel chain that ensures you are safe from malware and hackers and even the occasional accidental data breach.

That way you can look your guests in the eye when they are making a guest reservation, confident in the knowledge that you and your company are doing your very best to protect their personal information.

Being obliging while handling a guest reservation is part of the job.

Nowadays it is common practice to compile a guest reservation database that preserves the valuable data of your guest, from their preferred room and meals to their long-standing travel arrangements.

The hospitality industry has become a soft target for cybercriminals due to the convenience of online booking systems. However, this convenience also comes with the risk of credit card number theft, website hacking, and internal network compromise.

**A cyber-attack on Marriott hotel led to the compromise of data belonging to up to 339 million guests.**



# What are hotel data breaches?

Simply put, a hotel data breach is when the sensitive information of a hotel's guests becomes compromised and ends up outside of the security system that the hotel has in place.

Increasingly, this happens due to concerted hacking attempts that target the treasure trove that is a database filled with passport numbers, home addresses, credit card details, phone numbers, and other valuable data.

Accidental exposure of personal information can happen due to software malfunctions or if the information is uploaded to the wrong cloud-based server.

Human error can play a part, and this is why all senior staff in the hotel industry needs to stay abreast of how to prevent hotel data breaches by educating themselves on employing better data security measures.

As soon as this hotel data is released, you have a breach.

Hackers can put the various pieces of the puzzle together quite easily by posing as a colleague and phoning or visiting reception, and enquiring about a guest's whereabouts.

Then, just by working with a name and credit card details, they can go on an unauthorized online spending spree.

Long-term brand damage, litigation, and costly fines for non-compliance are some of the consequences you'll be facing as you figure out how best to contain your breach incident.

It's therefore imperative that you have an organized network and software system that will protect you from the get-go.

# Types of hotel security breaches

In the same way, as you'd lock up your hotel guests' jewels in the hotel safe, you need to keep your customers' data safe. Once you recognize the value of your assets, you can start implementing the necessary technological and staffing systems to safeguard them.

## Denial of Service (DoS) attacks

The intention here is to oversaturate your work computer or website, rendering it incapable of carrying out any further requests.

In the hospitality industry, this often involves crashing a hotel's website through the use of botnet software so that the site cannot accept any new bookings.

By flooding the target website, network, or machine with traffic, the information overload will cause your IT system to crash.

This will result in extended 'front of house' downtime for your customer who relies on the expedience and functionality of your system to plan their travels.

## Hotel Malware

Short for 'malicious software', malware comes in all shapes and sizes.

If you've had a computer that has been connected to the internet, then the chances are that you've heard about viruses, ransomware, spyware, and Trojan horses.

The usual rules for protecting against malware regarding anti-virus software and software updates apply.



With hotels though, the vulnerability lies in the hotel WiFi or ‘internet hotspot’ whereby a guest might unwittingly download what they perceive to be an internet token or hospital passcode, only for it to sit on their laptop for months before announcing itself as malware and becoming active.

‘DarkHotel’ is a cyber-attack group known for targeting business executives in this manner.

Hotel ransomware will lock and encrypt your personal files, forcing you to pay the ransom in bitcoin if you wish to retrieve your personal information.

## Eavesdropping Attack

This form of cyber-attack is also commonly carried out over a network and can involve anything from a smartphone or printer that is temporarily connected to the company network.

Guests might let their guard down and click on an official-looking website while they are trying to access your hotel WiFi, and a nearby, remote machine can piggyback on their login and gain access to the company system.

Hotel WiFi networks provide the opportunity for a guest to reply to emails, make online payments, and transfer files all under the auspices of being able to let their hair down while they do this.

So the onus is on hotel management to ensure that the WiFi network is fully secure, and to explain to the guests exactly how they should go about logging into their network.

The strategic precision and sophistication with which eavesdropping hacker software can prey on the precise moment of opportunity that the trusting guest takes to conduct their business at your hotel are alarming, to say the least.

The downloaded software needs access to just one connected device and it can then roam around your hotel network's entire root system.

From there it can distribute malware to other devices on the network, while simultaneously copying and updating files so that it doesn't even leave a digital trace.

It's now open season on the database of guest reservation details, as well as arrival and departure information – not to mention their credit card numbers.

## Phishing and Spam

When it comes to phishing and spam, the vulnerability lies mostly in human error. Sensitive data is obtained when someone poses as representing a legitimate institution.



They rely on the gullibility of the gatekeeper (for example, a hotel receptionist) to divulge that information.

Spam emails will use a 'spray and pray' tactic that can sometimes work if a hotel manager is fooled by the fake company letterhead, or a staff member blithely opens an attachment that seems official.

'Pop-up phishing' is ever more common. In this case, a browser window will alert you to a virus that has been detected on your computer.

The attacker will gain entry into your system (defined by cybersecurity experts as a 'beachhead') with something as seemingly innocuous as a file that you or your staff happen to have double-clicked on. Once 'ashore', they will start scanning your ports.

They are looking for host-naming conventions, ways to crack your company passwords, and a POS machine or server that the hackers can then control remotely.

This allows them time to extract credit card data (also known as RAM-scraping or memory scraping) without getting detected. And voila! Bad news, you now have a hotel data breach on your hands.

# How to protect against a hotel data breach

It's now time to roll up your sleeves as a hotel manager or hospitality business owner and figure out what you can do to protect yourself against a hotel data breach at your work address.

## Educate yourself on data security

Educate yourself. Educate your staff. Educate your hotel guests.

Your hotel's reputation is at stake, after all.

Especially when it comes to phishing attempts that prey on goodwill, you and your staff mustn't be bending over too far backward to accommodate a guest when it's actually part of an elaborate scam.

Likewise, your well-traveled hotel guest will expect a certain level of IT security and best practices when it comes to providing them with login credentials and asking for payment.

The more you read up on best industry practices, the more likely you are to remain vigilant, allowing you and your colleagues to spot a scam coming.

People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.

## Back up your hotel data

Keep your anti-virus software up to date, and back up your customers' personal information to a server that is separate from the one handling your day-to-day business affairs.

In the same way, as you would give your hotel kitchen, carpets, and rooms a 'deep clean' once a month, make backing up your data to your cloud or remote server a regularly scheduled monthly event.

Destroy all paper copies of receipts, invoices, and travel arrangements that have served their purpose.

If valuable data needs to be retained for tax purposes, store it off-site.

## Enhance password and network security

It's important that your passwords are varied and unique, and that they change regularly (ideally when you back up your data).

Password generators are making life easier for us to not have to think of a combination of the name of our first pet, our mother's maiden name, and the address where we grew up as answers to security questions for each and every email account that needs its own protection!

You can isolate the network that your guests use for their WiFi from that which is in use by the staff.

Setting up an appropriate firewall will restrict the type of person that would easily be able to gain access to your corporate network.

By compartmentalizing your networks you are also doing damage limitation should a data breach occur on one of the networks.

# A cyber attack in the hotel, what now?

Sjors Brul, founder and owner of Sbit, is only a few hours back from vacation when he receives an urgent phone call late at night.

An international hotel chain with more than twenty hotels has been the victim of a cyber attack.

A reconstruction of a more than radical operation.

The message popped up on all screens in the hotel organization that the cyber criminals were 'in', that the help desk had to be contacted and that an amount of Bitcoins had to be transferred to regain access to their own PCs.

Because all the PCs were held hostage.

'Ransomware' ensured that all PCs got encrypted, but also the servers could be held hostage.

"As a hotelier, you don't know that yet at that time," says Brul.

**"The first thing to do is not to panic, then you should turn off all access to the internet. In this case, it involved more than twenty branches spread over seven countries."**



# Powerless

PCs, cash registers, servers and workstations were all shut down.

The organization was put in a deadlock as an in-depth research was needed to figure out how the cyber criminals entered their systems. “What you absolutely must avoid is trying to fix it yourself, without the right knowledge.”

A cyber attack is a crime and should be carried out as such. A forensic team needs to investigate.

This team, called a ‘Red-Team’, is designated by the cybersecurity insurer. They start with two questions: what has been touched? How could this have happened?

“And in the meantime, the organization was still flat on it’s back. It went back to pen and paper. In this case, the damage for the entire organization amounted to 100,000 euros per day.”

The ‘Red-Team’ (name for a investigative team appointed by the insurer) investigates how the criminals came in by checking the systems. “We, as an IT service provider, examine the quality of the backups.

We do that every day, to check that they are working, but also to make sure they are in a safe place. The backups are also often damaged by these hackers, but we have protection for that.”

What the criminals are mainly looking for is blackmailable information. That can be information about guests.

“But credit card details should no longer be found in the systems. They also focus on the PMS system, and on the online behavior of the employees.

Which websites were visited, which videos were viewed; that kind of information.

That is blackmailable information that you as an organization do not want to be exposed to the public.

# Communication

Of course, the criminals don't take a break when Red-Team starts the investigation. They see their activities and act accordingly.

They call and say that they are offering their services to Microsoft and that it is so annoying that your organization has been hacked. But they have the solution.

Another advice is: trust nobody and communicate with your own people.

As an organization you are extremely vulnerable when you are attacked.

It is like an army is standing at your door," says Brul.

To prevent cyber criminals from entering, it is wise to know how they get in.

This can be done in a number of ways.

"Phishing" is a common way of breaching a company's software system. Failure to carry out an update properly can also cause a breach. During the lockdowns, many employees used their private laptops for work which can make the system less secure.

"In this case, in which more than twenty hotels were the victims, it was an update that was not carried out properly.

The Red-Team found out that in this case, the criminals had been inside for four months.

That means any backups made in the meantime cannot be trusted."



Systems were reset to the last safe state, or in the worst case completely replaced.

From that point on, all data had to be examined and tested for reliability and safety.

Sjors Brul talks about ‘White Listing’; approving websites and systems one by one. “In this case, we worked in that ‘White Listing mode’ for four months.

Step by step, labeling every website and every link as safe before it could be used again.

We were lucky that this hotel chain works with the PMS system in a hosted environment and we were able to conclude fairly quickly that the PMS system was not attacked and therefore it was safe.”

# Awareness

According to Brul, you do this first of all by creating awareness in the organization about the dangers of cybercrime.

“The hotel industry is paying more and more attention to this, but there is still a lot of room for improvement.”

A cyber security threat is just one click away and employees often remain silent about this, also out of shame.

The sooner it is reported, the better the evil can be fought.

The danger lies in invisibility, but in many hotels, the digital door is ajar or even further.

Nothing can be seen on the surface, but a few months later the consequences could be disastrous.”



# Cyber attack checklist

A cyber attack on a hotel organization is often the result of months of preparation by cyber criminals. The criminals make their demands known if they have managed to collect enough sensitive information.

## **What steps should you take as a hotelier if you are faced with a cyber attack?**

1. Don't panic and don't investigate it yourself.
2. Turn off the internet connection.
3. Contact the cybersecurity insurance company.
4. Get forensics done.
5. Don't trust anyone.
6. Keep the team informed.
7. Inform the authorities within the legal deadline.
8. Check Backups.
9. Provide insight into when the criminals entered the system.
10. Distrust all information that is in system since the attack.
11. Restore the systems.
12. Take corrective action to reduce the chance of another attack.

# Find out how Sbit can help

Keep up to date with the hospitality industry's best practices by partnering with Sbit as your preferred security choice. We make sure that you and your staff have a high level of digital awareness that ensures that cybercriminals will have their work cut out trying to outsmart you.

We offer a free 'network detective scan' to assess any weaknesses in your hotel's IT network.

From there we have a great, easy-to-use online platform that will ensure that your hotel staff is the strongest link in your chain of hospitality.

In the event that you are already dealing with a server crash or ransomware, we have the technical skills to get your systems up and running again within one hour, thanks to our much-heralded 'back-up and discovery' solution, powered by Datto SIRIS 4.

We can assist with data backup setups and creating the right firewall so that you don't get locked out of your own system.

We are highly adept at providing the right camera surveillance solution for your hotel plan so that the right products and systems work together without intruding on your guests' privacy or hindering the functionality of your staff.

By being proactive it is easier to become that little more security conscious.

With Sbit, you're supported all the way.



## What more can we do:

WiFi

Digital signage

Television

Telephony

Office 365

ICT support

Office solutions

Remote management

Cloud

Monitoring



[www.sbit-hospitality.com](http://www.sbit-hospitality.com)