ASSURED CYBER PROTECTION®

CYBERCRIME:

A Growing Threat to the Hospitality Industry

Protect your business from financial loss, operational disruption, and reputation damage.

CYBERCRIME:
A Growing Threat to the Hospitality Industry

Attracting the wrong kind of attention

Last year the hospitality industry accounted for 13% of the total cybersecurity incidents. Subpar cyber protections have bottom-line business ramifications.

The pressure to modernise and maintain pace with guest expectations has created exponential vulnerabilities for the hospitality industry. A ***recent report*** ranked the industry as the third highest risk of data breach and a prime target for network cyberattacks.

While hoteliers have been focussed on technology innovations such as biometric check-in, key card entry, AI voice assistants, smart HVAC systems, intelligent property management systems and more, to reduce costs and improve guest experiences, cyber criminals have been focussed on exploiting the risks. In simple terms, as more devices are connected to a network the risk increases and the ***more vulnerable it is to cyberattack***.

Therefore, it is essential that hoteliers fully understand what those risks are and how they can deal with them. They can then act responsibly to address the threats and safeguard their guests from cybersecurity compromise.

A cause for concern

Sophisticated attacks on the hospitality industry are becoming more frequent and more advanced and security breaches have become a common occurrence that are frequently featured in the media:

513,936,296 hospitality data records were stolen or lost in 2018 and in early 2020, **5.2 million guest records** were compromised in *one hotel chain breach* which resulted in a fine of **$124 million**

500 million travellers have been *victims of a cyberattack* through their business with hotels

Hundreds of hotels affected and taken off-line by the *Techotel ransomware attack*

According to ***Morphisec's 2019 Hospitality Guest Cybersecurity Threat Index*** every major hotelier has dealt with some form of data breach incident in recent years. Just as cybercriminals target financial institutions, hotels present a highly lucrative target where payment information of millions of customers can be harvested. With multiple attack entry points, hotels make an extremely easy mark for cyber criminals.

Hotels offer cyber criminals high-returns for what is often minimal effort. To put the size of the cyber-crime market opportunity in perspective, one major international hotel group provides for a minimum of 423.4 million guests every year.

Information collected by this group includes personally identifiable and financial information which includes names, addresses, credit card information, passport and identity documentation and much more.

Stealing personal and financial data reaps high rewards with information being sold easily on the dark web to facilitate identity theft and cardholder-not-present financial fraud.

What's the worst that could happen?

Threats are evolving all the time and hackers are constantly changing their attack MO. According to a *top hotel management publication* the top three threats affecting hotels are:

1 Phishing

Hackers target those in charge of areas like accounts with bogus emails, hoping to gain access to systems or convince them to approve money transfers.

2 Ransomware

Businesses are targeted by ransomware every 40 seconds. *More than 1 in 5* businesses that pay a ransom do not get their data back.

3 Distributed denial of service (DDoS) attacks

The hospitality industry has become a favourite target for DDoS attacks. Hotels use a wide array of *devices such as TVs and reservation systems* that can be leveraged to disrupt other systems.

While ransomware appears to be the most prevalent attack vector, cyberattacks of all kinds can cause a number of negative consequences for hospitality providers. The most common outcomes are:

- **Theft of guest personal or payment data**, leading to hefty fines and reputation damage.
- **Disruption of PMS or other critical systems**, halting operations and harming guest experience.
- **Critical systems or files held to ransom**, resulting in huge remediation costs (even if the ransom isn't paid)
- **High-profile guests targeted** for data theft, extortion, or surveillance. This creates a risk of regulatory fines and harms brand reputation.
- **Employee error or manipulation**, e.g., paying fraudulent invoices, clicking malicious links in emails, or exposing sensitive information on social media.

One hotel chain breach resulted in a fine of **$124 million**

Top cybersecurity threats for hospitality providers

According to Verizon's *2021 Data Breach Investigations Report*, 86% of cyberattacks against hospitality providers are financially motivated, while the remaining 14% are motivated by espionage. To protect their operations and to safeguard their guests, hospitality providers must understand the attack techniques they are likely to face within these categories. Some of the most common techniques include:

Insider threats
In its guide to Securing Property Management Systems, the National Institute for Standards and Technology (NIST) suggests up to 50% of security breaches in the hospitality industry are initiated by current or former employees. These are challenging to protect against, as insiders often have access to privileged accounts or information.

Exploiting connected systems
Any 'smart' system connected to a network creates an entry point for hackers. In high profile examples, hackers have compromised businesses through their *HVAC systems* and even an *Internet-connected fish tank thermometer*.

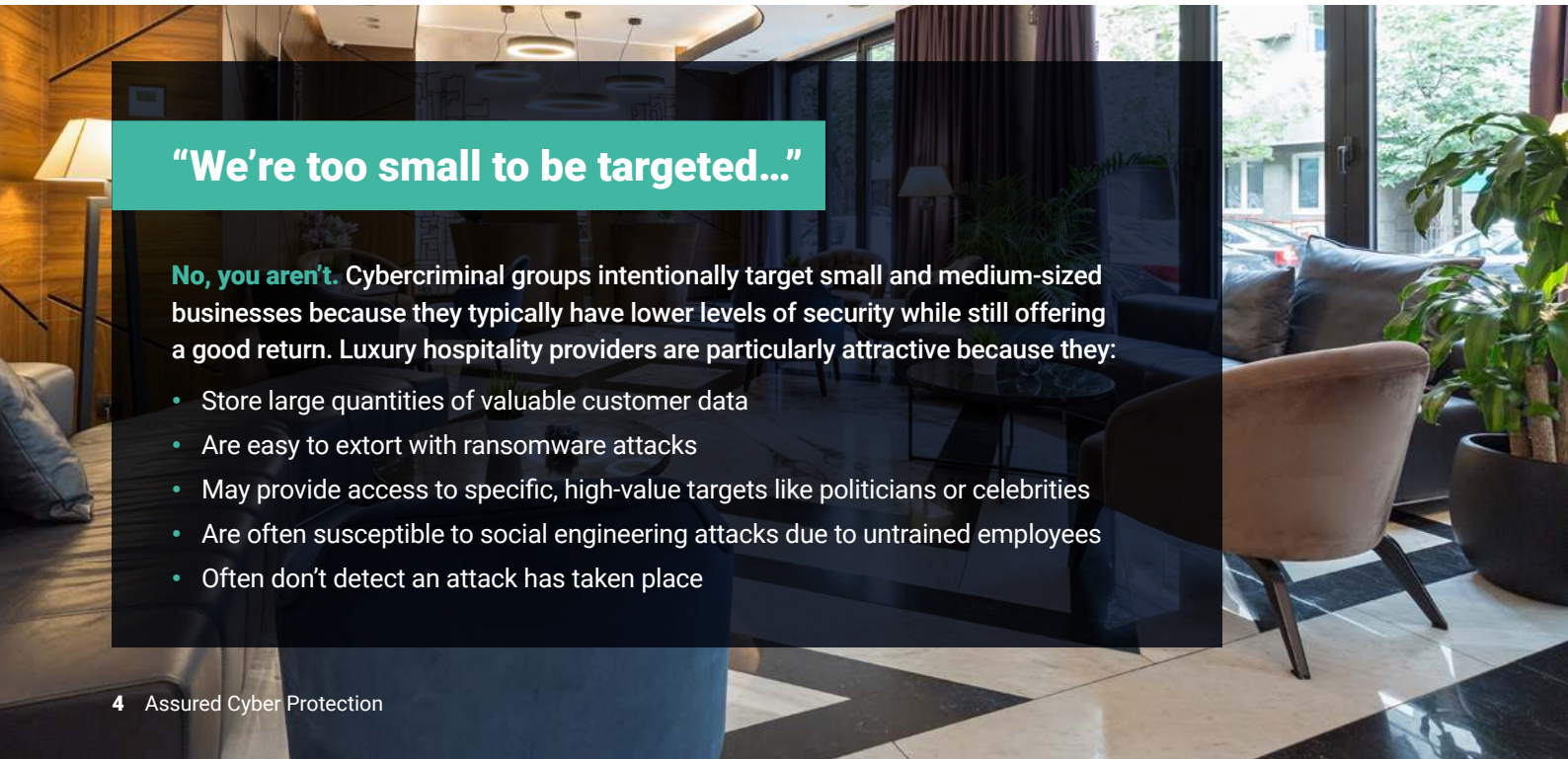
Phishing and social engineering
Phishing and social engineering aim to manipulate employees into undesirable actions. Business Email Compromise (BEC) scams are a common example, where payments or administrative employees are tricked into paying fraudulent supplier invoices.

Ransomware and extortion
Ransomware is a type of malware that 'locks' files or computer systems, preventing a provider from regaining access unless it pays a ransom. There are other types of extortion attacks, but ransomware is by far the most common.

Data theft
Stealing customer data is a top priority for cybercriminals. These attacks usually rely on malicious software to identify and extract sensitive data, although there are several other approaches in common use.

Targeting high-profile guests
These attacks target high-profile guests such as business leaders and political delegations with malicious software to compromise devices, steal data, or conduct espionage.

Point of Sale (PoS) attacks
According to *one study*, around 18% of attacks on hospitality providers focus on PoS devices. These attacks aim to steal payment card data, which can be sold in bulk via online criminal marketplaces.



"We're too small to be targeted..."

No, you aren't. Cybercriminal groups intentionally target small and medium-sized businesses because they typically have lower levels of security while still offering a good return. Luxury hospitality providers are particularly attractive because they:

- Store large quantities of valuable customer data
- Are easy to extort with ransomware attacks
- May provide access to specific, high-value targets like politicians or celebrities
- Are often susceptible to social engineering attacks due to untrained employees
- Often don't detect an attack has taken place

The cost of a cyber breach

The impact of a successful cyberattack can be catastrophic for any business. According to IBM's 2021 Cost of a Data Breach Study, the average cost of containing a breach in the hospitality industry is $3.03 million, up from $1.72 million in 2020. This cost comes from four main areas:

1	**Detection and escalation**
	E.g., investigations, audits, crisis management, and communications to executives and boards.

2	**Notification**
	E.g., contacting customers, communicating with regulators, and engaging with outside experts.

3	**Lost business**
	E.g., revenue loss due to downtime, lost customers, and reputation damage.

4	**Post-breach response**
	E.g., help desk communications, legal expenditure, and regulatory fines.

Cybersecurity is a necessity, not a luxury

Cyberattacks aren't only a problem for hospitality providers. They're also an enormous concern for guests—particularly those that frequent luxury hotels and resorts.

An ***in-depth study of luxury travellers*** conducted by travel technology provider Amadeus, and validated by 200 business leaders from the luxury travel industry found that the security of information is a foundational requirement for all travellers.

Without it, guests are unable to enjoy luxury experiences because their basic needs aren't being met.

While the need to provide guests with this level of privacy and security is obvious, the necessity is for hospitality providers to have strong cybersecurity protection in place that can identify and prevent common cyberattacks.

70%

OF GUESTS BELIEVE HOTELS ***DON'T INVEST ENOUGH*** IN CYBERSECURITY PROTECTION

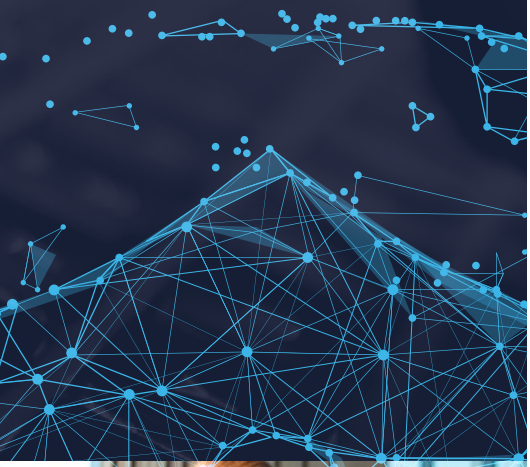
71%

OF CMOs BELIEVE THE MOST SIGNIFICANT COST OF A SECURITY INCIDENT IS BRAND VALUE WHICH CAN AFFECT COMPANIES FOR YEARS AFTER ANY CYBERSECURITY EVENT

40%

OF GUESTS BELIEVE THAT WIFI POSES THE GREATEST RISK AT THE HOTELS THEY STAY AT WITH POS ATTACKS REPRESENTING THE FEARS OF 22% OF GUESTS

The average cost of containing a breach in the hospitality industry is **$3.03 million**



Cybersecurity challenges for hospitality providers

Building and maintaining effective cybersecurity controls is never easy and several factors add to the challenge for most hospitality providers:

Large, complex networks
Hospitality computer networks are complicated and usually have many connected devices, including terminals, automated systems, mobile devices, servers, and smart hardware such as climate control and electronic minibars. Each of these devices is a potential entry point for a hacker.

Digital transformation
Hospitality providers are constantly adding new technologies and features to their networks in response to guest requirements. For example, COVID-19 led to guests demanding contactless check-in. New technologies and connections to the network may present additional security risks that need to be considered.

Customers (and attackers) are on site
Direct physical access to a target network is a massive advantage for a hacker. Hospitality providers typically have networked devices in publicly accessible locations and must take extra precautions to protect these devices and other vulnerable systems such as guest WiFi networks.

Employee churn
Humans are often the weakest link in a network. A combination of high churn and low cyber awareness among employees (many of whom are young and active on social media) creates a significant risk, because it makes it difficult to ensure employees are properly trained to spot attacks and avoid accidentally endangering the organisation.

Third-party risk
Most hospitality providers have large supplier ecosystems and rely on technology sold by many different companies. Each relationship and dependency are a potential weakness, however, keeping track of them and ensuring all software and integrations remain up-to-date is a significant challenge.

While these characteristics can make cybersecurity a challenge, they are far from insurmountable. To overcome them, hospitality providers should take a ground-up approach to cybersecurity that starts with a solid foundation and then expands to address company-specific risks.

Seven steps to protect against cyberattacks

STEP 1

Secure network design, setup, and maintenance

Hospitality networks must be designed and built with security in mind. This includes:

- Segmenting the network to keep guest services separate from business functions.
- Ensuring all data is stored securely and in line with regulations like PCI-DSS and GDPR.
- Maintaining secure offsite backups that allow prompt recovery in the event of a breach.
- Ongoing patching of all systems to ensure they are protected against known vulnerabilities.

STEP 2

Restrict user access

Current and former employees pose a risk – usually by accident, but sometimes through malicious intent. Controlling user access is a simple way to minimize this risk. Standard procedures include:

- Restricting all user access to the minimum level needed to perform a job role.
- Ensuring access is revoked immediately for employees that leave the business.
- Enforcing strong passwords and using multi-factor authentication (MFA) solutions.

STEP 3

Employee training

Employees should be assessed to determine how much risk they pose to the organisation and provided with training appropriate to their role and level of cyber awareness, e.g., payments employees should be able to spot fraudulent invoice scams, and younger employees should know not to discuss business matters over social media.

STEP 4

Create defence in depth

Basic cybersecurity tools like firewalls, antivirus, and logging tools are essential. However, some attackers will evade these security controls, and you must have the means to detect this activity so you can investigate and prevent it. Typically, this can take the form of sensors throughout your network that pick up unexpected activity and report it to a human security practitioner.

STEP 5

Never stop thinking about cybersecurity

Whenever you add to your technology profile, consider cybersecurity. Choosing tools and systems with a strong security profile will dramatically reduce the risk of introducing new technologies.

STEP 6

Incident investigation and response

Tools can alert on possible issues, but most cybersecurity incidents need to be investigated by a human. This process must happen promptly, as incidents can escalate quickly if they aren't addressed. This can be done internally or outsourced to a security service provider.

STEP 7

Understand cyber risk

Never allocate your cybersecurity budget based on media or marketing hype. Instead, build an understanding of what poses the greatest risk to your operations and allocate resources accordingly. Data-backed cyber risk management tools can be highly valuable for this process.

Tailor your cyber security program with Assured Cyber Protection

Assured Cyber Protection is a global technology partner that empowers hospitality providers to design, implement, and maintain secure networks that ensure guests can enjoy their experience with peace of mind and protect the business against cyberattacks.

Give your guests the VIP privacy and security they demand without overspending or worrying you've invested in the wrong areas. We'll design a cybersecurity solution that fits your needs and supports existing IT management or maintenance contracts.

Working with Assured Cyber Protection, your hospitality business can:

- Protect against financial losses, operational disruption, and reputation damage
- Ensure guest experience is unharmed by system damage or security incidents
- Allocate cybersecurity budgets with confidence informed by a data-backed risk dashboard
- Prepare employees to support security objectives and avoid accidental compromises
- Reliably deliver VIP security and privacy for all guests
- Safeguard your reputation and customer loyalty

Get in touch today...

...to discuss your needs with one of our cybersecurity experts.

enquiries@assuredcyberprotection.com
www.assuredcyberprotection.com

ASSURED CYBER PROTECTION®