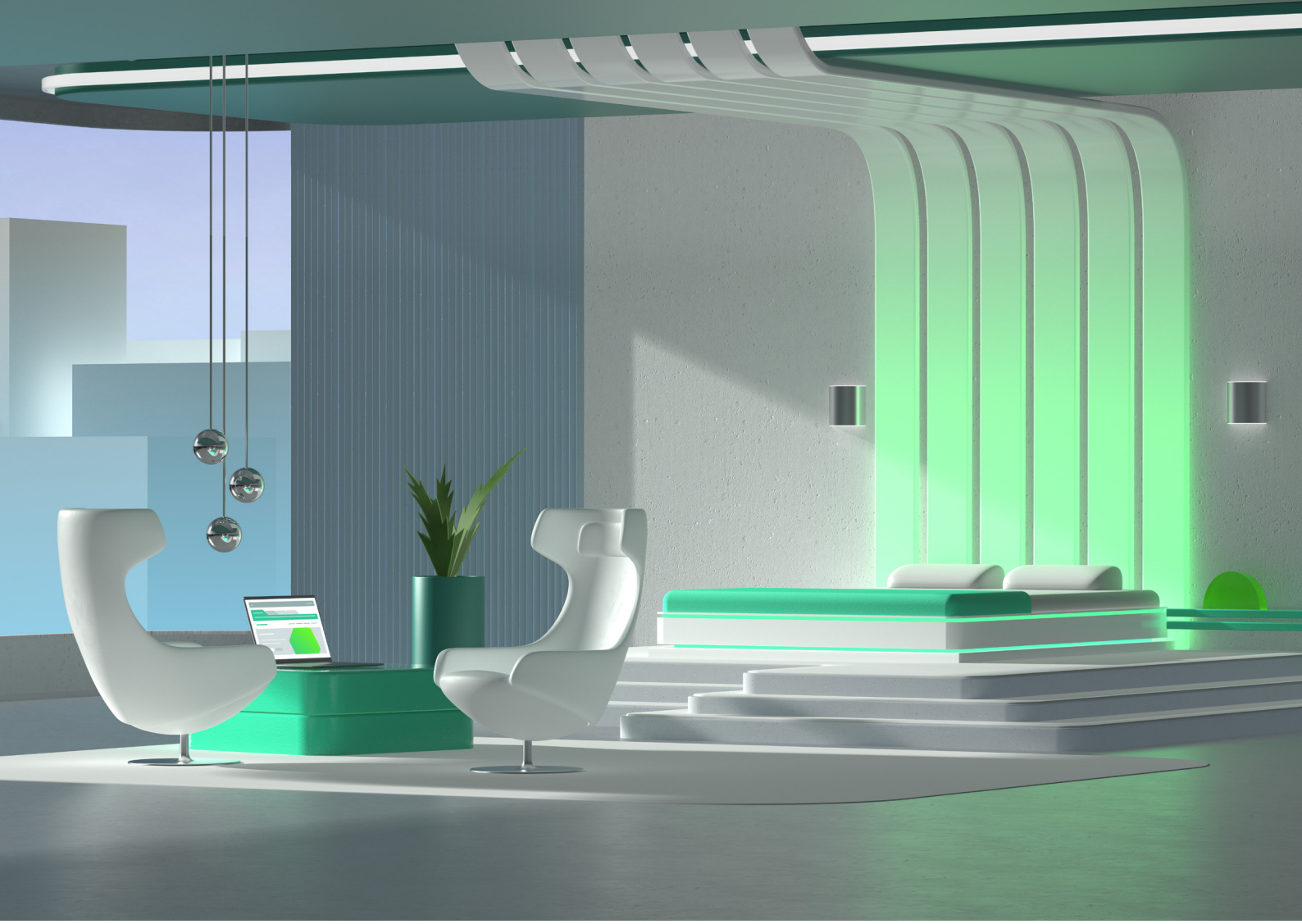


Building a safer future in Hospitality

kaspersky BRING ON THE FUTURE

go.kaspersky.com/hospitality

2021

Preventing threats from becoming guests

Before COVID-19, the hospitality industry was generating more than 10% of global GDP, with the World Travel and Tourism Council (WTTC) estimating a US$8.8 trillion contribution to the global economy in 2018.

Combining four distinct sectors — lodging, food and beverage, recreation, and travel and tourism — hospitality also accounted for one out of every ten employment opportunities in 2018, with 319 million people earning their living in the industry.

But when the pandemic struck, a combination of national lockdowns and restrictions on international travel left hospitality facing an existential crisis. With two-thirds of airlines grounded, international tourist arrivals plunged 93% in June 2020 compared to 2019; and 2020 was recognized as the worst year in tourism history, with one billion fewer international arrivals and just US$1.1 trillion in international tourism receipts. Meanwhile, at local level, many restaurants, bars, hotels and entertainment venues were forced into long-term closures.

Following this huge initial shock, government interventions throughout 2021 prompted by waves of new infections related to the Alpha, Beta, Delta and Omicron variants, resulted in continuing disruption, with bookings for meals, visits to theatres, cinemas and other entertainment venues, as well as holidays, flights and business trips being repeatedly cancelled, rebooked and re-cancelled.

Yet despite all this uncertainty, hospitality has responded to the pandemic by unleashing a wave of innovation across the industry. From bars, cafes and restaurants serving their former on-premises customers with carry-outs and takeaways, to hotel and holiday companies increasing their focus on aspects of the guest experience such as contactless transactions, hygiene and personal wellbeing, hospitality venues have been doing everything they can to attract customers back to their services in the 'new normal'.

Many of the innovations being introduced across the industry focus on digital transformation and increased use of technology — each of which inevitably creates new cyber-risks. Based on a combination of analysis by leading commentators such as Adobe, Deloitte and PWC, hospitality

513,936,296 hospitality data records were stolen or lost in 2018. In early 2020, 5.2 million guest records were compromised in one hotel chain breach. 423 million U.S. travelers have been victims of a cyberattack through their business with hotels. And 70% of guests believe hotels don't invest enough in cybersecurity protection.

With a wide variety of cyberthreats to defend against, from ransomware to fraud, retail and hospitality organizations need to prioritize tracking and mitigating risks associated with cyberthreats of greatest consequence to their environment.
Accenture

trade media, and our own experiences in working with hospitality companies around the world, there are five interrelated trends we believe need to be managed securely if organizations are to mitigate these cyber-risks, and maximize the benefits enabled by new technology.

These include:

Smart rooms, digital transformation and the Internet of Things (IoT)

Personalization, personally identifiable information (PII) and cloud adoption

Weaknesses in property management systems (PMS)

Guest Wi-Fi and the DarkHotel advanced persistent threat (APT)

The role of human actors

Trend #1: Smart rooms, digital transformation and the Internet of Things (IoT)

According to the 2021 report, 100 Hotel Trends You Need to Watch in 2021 & Beyond, smart rooms are #1 on a list of nine overarching themes.

As the authors note, 'The internet of things is spreading not only into homes, but also into hotel rooms. From access to streaming services to a room key on your smartphone, the essential hotel amenities in a guestroom are becoming increasingly digital. Guests want concierge services or temperature controls at the push of a button (or tap of a finger), and voice-activated controls are expanding beyond simply asking Alexa to play your favorite song. These trends might sound futuristic now, but in a few years, guests will expect them. Many of these innovations require only minimal changes to a modern guestroom, so a forward-thinking hotelier can implement them quickly and efficiently.'

Other smart room services and devices suggested in the media include everything from wireless device charging, voice search, facial recognition and tablet-based monitoring, to smart mirrors, concierge video chat and smart recognition technology.

65%

65% of the senior executives we surveyed agreed that buyer expectations are further ahead than organizations' current digital capabilities. As we emerge from the pandemic, the quality of customer experience is widely recognized as a key source of differentiation and driver of loyalty.

But smart rooms are just one of the many aspects of digital transformation being contemplated by today's hospitality entrepreneurs. As the same authors note, 'It's no surprise that a sizable section of our 100 hotel trends are technology-related. Innovation in the hotel technology sector has been blazing ahead at a rapid pace; previously expensive technologies like artificial intelligence and digital room keys are now more affordable than ever, and advances in payment systems and app capabilities mean that hoteliers and guests have exciting new options when it comes to booking, paying for, and actually experiencing a hotel stay. Though these may be "trends" now, they're only going to become more commonplace.'

Adobe came to similar conclusions: 'If there's one silver lining for travel and hospitality companies, it's that the pandemic has encouraged them to innovate. In the 2021 Travel & Hospitality Trends Report, 82% of businesses accelerated their digital transformation over the past six months and 87% plan to launch new digital offerings to boost engagement. This will place them in a much stronger position when the economy opens up again. For instance, touchless experiences have become more of a necessity and 34% of respondents are already using technology or apps to help manage guest experience.'

But while these innovations may be great news for guests, they will almost certainly prove a challenge for the hospitality industry's in-house IT teams tasked with keeping them secure.

How to manage smart rooms, digital transformation and IoT securely

As connected devices become increasingly integral to the hospitality experience, the security risks associated with them can be difficult to understand and mitigate. Hospitality venues providing staff with mobile devices to facilitate their work can also face serious issues due to a lack of centralized security management.

Connected devices face the risks of being a part of the corporate network, as well as those unique to the embedded systems on which they're based. Traditional antivirus solutions, however, cannot fully defend against the latest advanced, targeted and malware threats to embedded systems, including equipment such as point of sale (POS) devices and automated teller machines (ATMs). These therefore need more than antivirus — requiring specially designed, multi-layered intelligent protection based on a combination of Default Deny with Device Control.

In tandem with this, the poor security of the majority of IoT devices creates its own threats. These require the implementation of specialist security across the IoT ecosystem — minimizing risk and addressing cybersecurity threats to IoT systems and embedded devices through tools securing every software and hardware component of these interconnected systems — without overloading individual systems or devices or limiting overall flexibility.

Trend #2: Personalization, personally identifiable information (PII) and cloud adoption

Logistics and supply chain are a key part of the hospitality sector.

In late 2019, a French business-to-business (B2B) hotel booking firm was found to have exposed a client list of an unspecified number of the 600,000 global hotels they serve. The incident was one of many Elasticsearch misconfigurations reported in 2019 and underscores the dangers that arise when a single entity has data across the majority of the sector. This trend of supply chain incidents is likely to continue on as more companies move data to new virtualized environments, cloud and SaaS platforms.

In Adobe's 2021 Travel & Hospitality Trends Report, the five key trends identified as the industry opens up again following the pandemic are 'Prepare for a hyper-personalized future', 'Falling budgets are a barrier to personalization', 'Lack of data is making predictions difficult', 'Digital capabilities are a work in progress' and 'New demand requires new levels of agility'. This tells you all you need to know about the vital importance of data and the ability to harness it effectively to personalize the hospitality experience.

While estimates of the prevalence of cyberattacks and data breaches in different industries vary, it's fair to say that hospitality is among the top three targets globally. Hospitality companies store and process vast quantities of personally identifiable information (PII) and other valuable data that is meat and drink to cybercriminals and even state-sponsored cyberthreat groups. Breaches of this data have resulted from attacks targeting weaknesses in systems ranging from online booking and in-hotel Wi-Fi networks (see Trend #4) to a variety of other customer and B2B touchpoints.

An often-quoted IntSights report suggested that hotels are particularly vulnerable because of their widely distributed and highly connected nature, which means threats can come from many directions. Factors making them attractive to fraudsters also include the volume of financial transactions that hotels carry out, the sensitive and valuable personal data collected, the use of loyalty programs, and their national and international spread.

Another rapidly growing and worrying trend, especially given increasing adoption of cloud storage by hospitality companies, is the misconfiguration of cloud, file sharing and software-as-as-service (SaaS) environments.

In 2018 alone, almost 514 million hotel data records were stolen or lost worldwide. The trend continued throughout 2020, with both Marriott and Prestige Software's Cloud Hospitality platform suffering massive breaches.

According to Accenture's 2020 Retail and hospitality threat trend report, 'Naturally, as usage of technology service providers, including cloud service providers (CSPs), has increased in recent years, so have the number of data breaches related to those environments. Threat groups are concentrating on critical nodes and technologies, leading to large-scale data theft and business interruptions. In particular, retailers and hospitality groups have disclosed breaches of customer personally identifiable information (PII) and loyalty program information due to misconfigurations. This is a concerning trend as more organizations execute against their journey to the cloud roadmaps. More data breaches are likely to arise, and as they do, they'll erode customer's trust in affected organizations and tarnish brand reputation.'

How to manage personalization, PII and cloud adoption securely

Unfortunately for hospitality companies, the financial value of the PII they collect and store mean they will continue to be a target for cybercriminal activity — as witnessed by the frequency with which major hotel chains such as Hilton, Marriott and IHG are discussed in dark web forums.

Breaches can result from everything from unpatched legacy systems to human error or deliberate fraud. But whatever the cause, breaches threaten guests' confidentiality and can damage an organization's reputation.

Endpoints — including servers, workstations and mobile devices — are the source of the majority of cybersecurity problems encountered by organizations. As a result, high quality endpoint protection **has** to be the first line of defense against attempted security breaches. And those planning to or already moving customers' or guests' data to public, private or hybrid cloud environments also need to invest in specialist cybersecurity specifically designed to secure these workloads.

Trend #3: Weaknesses in property management systems (PMS)

Data released in November 2021 from Cornell University's Center for Hospitality Research and FreedomPay revealed that while nearly all (96%) surveyed retail, restaurant and hospitality stakeholders are confident in their companies' internal risk assessment processes, their satisfaction (95%) in the security of their systems is misaligned with reality, as one-third of companies (31%) have experienced a data breach in their company's history. Of the companies that have been breached, 89% have been hit more than once in a year.

64%

64% of hospitality data breaches occur via corporate internal networks and 18% each via e-commerce and POS.

Retailers and hospitality companies have a particularly robust supplier network with high-dollar payments.

In some cases, this amplifies the opportunities for bad actors to misdirect large sum payments to accounts they control and have enough lead time to launder proceeds prior to law enforcement interdiction.

In March 2021, the US National Institute of Standards and Technology (NIST) issued a new practical cybersecurity guide to help hotel owners reduce the risks of what it called 'a highly vulnerable and attractive target for hackers' — the hotel property management system (PMS) which stores guests' personal information and credit card data.

As outlined in the three-part guide, hotel operators rely on a PMS for daily administrative tasks such as reservations, availability, pricing, occupancy management, check-in/out, guest profiles and preferences, report generation, planning and record keeping (including financials).

As a hotel's operations hub, the PMS controls on-site property activities for guests and colleagues, and interfaces with several services and components within its IT systems, such as POS and physical access control systems, Wi-Fi networks, and other guest service applications supporting availability, reservations and guest profile information.

On top of this, various interfaces create further links from the PMS to internal and external systems such as room-key systems, restaurant and banquet solutions, sales and catering applications, minibars, telephone and call centers, revenue management, on-site spas, online travel agents, guest Wi-Fi, loyalty solutions and payment providers.

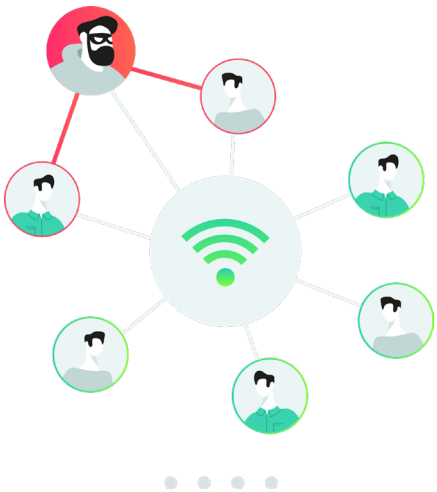
Because the PMS and its extended systems store, process and transmit a variety of sensitive guest information, including payment card information and PII, the value of the data held in a PMS and the number of connections to it create an attractive attack surface, and make the PMS a target for malicious actors wishing to exfiltrate sensitive data, deliver malware or profit from undetected fraud. An unsecured or poorly secured PMS can therefore expose a hotel — and the larger hospitality organization of which it is a part — to significant and costly data breaches.

As the guide notes, in recent years, criminals and other attackers have compromised the networks of several major hotel chains, exposing the information of hundreds of millions of guests. Breaches like these can result in huge financial loss, operational disruption and reputational harm, along with lengthy regulatory investigations and litigation.

How to operate property management systems more securely

To strengthen their PMS, NIST recommends hotels and other hospitality organizations to adopt security solutions creating a zero trust architecture that mitigates cybersecurity risk, through capabilities including role-based access control, privileged access management, network segmentation, moving target defense and data protection. Such an architecture helps to:

- Prevent unauthorized access via role-based authentication that controls and limits PMS access to those with a business need.
- Decrease breach potential and data exfiltration by protecting against unauthorized lateral movement and privilege escalation attacks.
- Prevent the theft of credit card and transaction data via data tokenization, explicitly allowing only identified entities access (allow listing) and enabling enforcement of access controls.
- Increase overall PMS security situational awareness via auditing, system activity logging and reporting, and limit exposure of the PMS to incidents in systems interfacing with it.
- Prevent unauthorized use of personal information, protecting guest privacy, and increasing consumer confidence and brand loyalty.

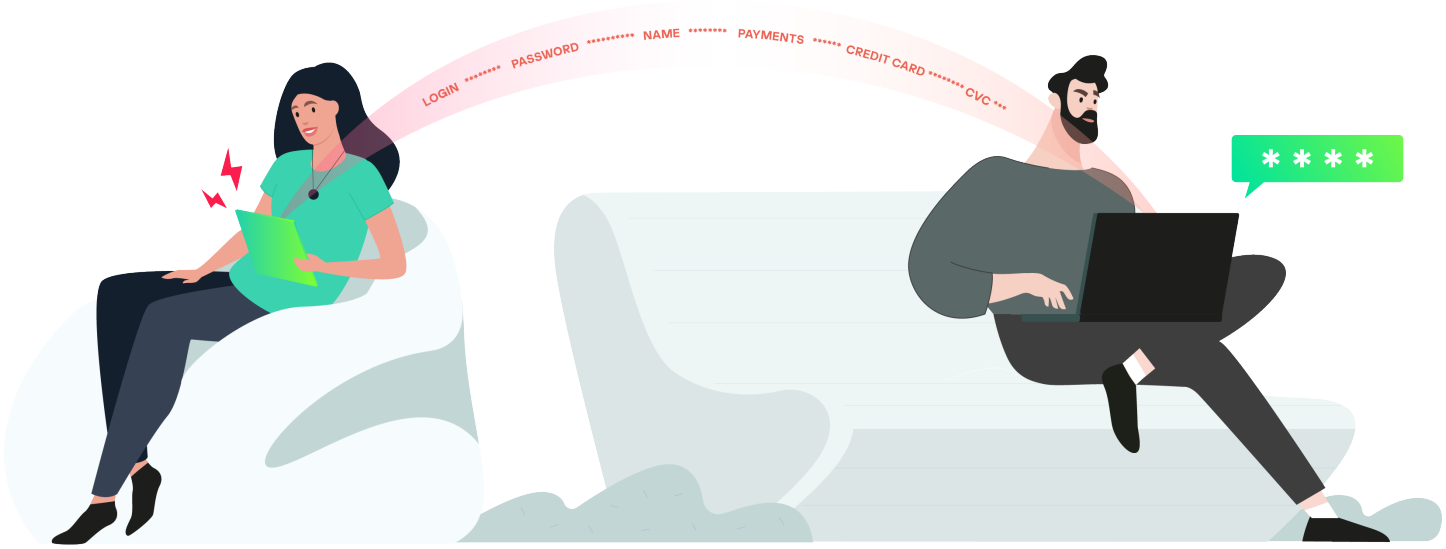


Trend #4: Guest Wi-Fi and the DarkHotel advanced persistent threat (APT)

Although there are hospitality companies which promote their facilities as providing an opportunity for a 'digital detox' by specifically excluding Wi-Fi from their premises, for the vast majority of guests, being given the hotel's Wi-Fi access code is a top priority on arrival at the check-in desk.

Wi-Fi has something of a checkered history in the hospitality industry. Having built up a reputation for being slow, unreliable and often almost impossible to connect to, as the digital transformation and smart room developments outlined in Trend #1 continue to gather pace, a fast, dependable and secure Wi-Fi network will be fundamental to commercial success.

There is, however, another aspect to guest Wi-Fi access that all hoteliers and hospitality companies need to be aware of, and that's the DarkHotel advanced persistent threat (APT).



90%

The cybercriminals behind DarkHotel have been operating for over a decade, targeting thousands of victims across the globe. 90% of the DarkHotel infections seen by Kaspersky have been in Japan, Taiwan, China, Russia and Korea, but we've also seen infections in Germany, the USA, Indonesia, India and Ireland.

- DarkHotel has been known to compromise luxury hotel networks and then stage attacks from those networks on selected high-profile victims using a combination of spear phishing, dangerous malware and botnet automation designed to capture confidential data.
- Hotel Wi-Fi exploits are used against targets as a means of spear phishing. By tracing unsuspecting executives who are traveling overseas, they can preemptively infect the Wi-Fi network of their hotel by planting an infection on the hotel's server.
- This infection spreads a rare Trojan masquerading as one of several major software releases including Google Toolbar, Adobe Flash and Windows Messenger. This first stage infection is used by the attackers to qualify their victims. Then, once the intended targets have been identified, DarkHotel attackers download further malware to their computers to steal confidential data.

How to defend against threats such as DarkHotel more effectively

DarkHotel's attack developers use surgically precise attack methods to execute and clean up after their attacks. Their demonstrated high level of coding skill and planning makes their attacks extremely difficult to trace, much less spot amid an attack. And their coordination in hotel attacks specifically suggests they may have insider assistance at hotels.

The scale of targeting suggests nation-state actors or nation-state support for the attacks. And, with their history of targeting political, nuclear and economic forces, DarkHotel poses a threat to national security across many countries, while their spear phishing and botnet methods are still an ongoing threat for users.

Because of this, it is important to protect hotel servers by installing high quality internet security software including proactive defense against new threats, rather than just basic antivirus scanning and malware removal. Web protection capabilities such as link threat-scanning and phishing filters can also help to combat threats such as those used by DarkHotel.

Trend #5: The role of human actors

As if the external threats to hospitality companies weren't challenging enough to deal with, the industry also struggles when it comes to insider threats.

In many industries, security efforts often focus on the network perimeter and implementing measures to block external threats, but insider threats can be just as damaging if not more so. Insiders can steal sensitive information for financial gain, take information to provide to their next employer, or abuse their privileged access to cause significant harm.

Insider breaches can also have major consequences for organizations, including reputational damage, loss of revenue, the theft of intellectual property and reduced market share.

Reflecting the scale of the threat posed by insiders including current and former employers, contractors, or other individuals with inside knowledge about an organization, in October 2021 the US Government's Cybersecurity and Infrastructure Security Agency introduced a new

Even as organizations employ robust security policies and increase the efficiency and effectiveness of their cybersecurity tools, the human element of cyberthreats, notably insider threats, remain a challenge. Malicious insiders in the retail and hospitality industries can go unnoticed due to factors such as high in-store employee turnover and seasonal staff.
Accenture

91%

91% of companies believe their customers deeply care about cybersecurity, while 86% believe it increases customer loyalty.

Companies fear internal threats, with hospitality companies most frequently citing human error (86%) and lack of employee education (81%) as negatively impacting cybersecurity systems.
Hotelbusiness

Insider Threat Risk Mitigation Self-Assessment Tool to help public and private sector organizations further their understanding of insider threats and develop prevention and mitigation programs.

While large organizations are likely to have conducted risk assessments and put measures in place to mitigate insider threats, small- and medium-sized businesses tend to have limited resources and may not have assessed their risk level. The tool therefore consists of a series of questions to establish the level of vulnerability to insider threats, and provide feedback to help users develop appropriate mitigations to guard against insider threats and reduce risk to a low and acceptable level.

How to manage insider threats securely

Effective cybersecurity mandates removing practices that are inherently risky, such as:

- Continued use of software that has reached its end-of-life and is no longer supported by the software developer — as without support, patches are no longer issued to correct vulnerabilities, which can be easily exploited by cyber actors to gain access to internal networks.
- Failure to change default credentials and passwords that are known to have been compromised in data breaches or have otherwise been disclosed.
- Using single factor authentication for remote or administrative access to systems — which, while this provides a degree of security, is not sufficient to resist the brute force tactics of hackers.

To reduce the risks posed by insider threats, putting policies in place to immediately prevent access to corporate systems by former employees should unquestionably be added to this list.

Also, given that in any environment people can still make honest mistakes, interactive and compelling cybersecurity awareness training that helps to reduce these errors is another vital investment.

Summary

When it comes to cybersecurity, hospitality is unusual in that even though the industry faces significant cyberthreats, the level of protection implemented by many companies can be relatively low.

- For those companies experiencing what we class as 'commodity' threats, there is much to be gained by implementing basic security practices such as keeping operating systems and applications regularly updated, ensuring devices and internet access are properly secured, and investing in an endpoint solution delivering automated protection against the vast majority of these commodity threats.

- As we've seen throughout this document, many hospitality businesses suffer from weaknesses in their property management systems, and/or are involved in digital transformation exposing them to new classes of potential threats related to technologies such as cloud computing and IoT, for which they need more specialized protection capable of dealing with these threats.

- All hospitality businesses face ongoing issues resulting from innocent staff mistakes and other insider threats, for which effective cybersecurity awareness training is another vital defense.

Kaspersky is a pioneer in helping hospitality companies protect data and business continuity 24/7 against cyberthreats ranging from commodity, advanced and evasive threats to targeted attacks — mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Our **stage-by-stage cybersecurity approach** is designed to clarify which level of security as well as which specific solutions best suit your organization. The stages provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring a smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations — essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security — for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing ...

3

Kaspersky Expert Security — for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▪ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▪ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▪ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▪ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▪ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▪ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▪ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▪ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum **and** Kaspersky Managed Detection and Response Optimum ▪ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

Targeted Solutions

What	How
 **Kaspersky Fraud Prevention**	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any business, ensuring safety and protection for clients.
 **Kaspersky DDoS Protection**	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according the nature of each DDoS attack.
 **Kaspersky Embedded Systems Security**	A multi-layered solution delivering unequalled protection to Windows-based embedded devices — even those with limited system resources and running discontinued OSs. Opt-in security layers including application and device controls, exploit prevention and anti-malware mean protection can be optimized for lower-powered devices — including vulnerable older PCs running unsupported OSs such as Windows XP.

Cyberthreats News: www.securelist.com
IT Security News: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Technologies at a glance: www.kaspersky.com/TechnoWiki
Awards and recognitions: media.kaspersky.com/en/awards
Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE