Chapter

Network & Cyber Security in Hospitality and Tourism

Emmanuel Fragniere
University of Applied Sciences and Art Western, Switzerland

Kamil Yagci
Pamukkale University, Turkey

SUMMARY
The tourism sector was transformed early on by digitalization, which makes it a very innovative area of business. At the same time, this high level of digitalization maturity makes it a very vulnerable industry in terms of cyber security. As a tourism specialist, it is therefore crucial to have a good understanding of network and cybersecurity. In this chapter, we will address this topic in an accessible and popularized manner. The goal is to understand the challenges of cybersecurity and as a tourism professional to contribute with specialists in the field to protect your business, your network, and your customers. We will learn to understand the context of cybersecurity and to admit that hackers are always one step ahead. For this reason, we will see that international cybersecurity and safety standards are also very advanced and allow the sector to perform risk and crisis management to protect its business effectively.

Learning objectives:

After completing this chapter, the student will be able to:

- Become familiar with the technical terms of cybersecurity
- Understand the main cyber risks of tourism networks
- Know the main attack strategies of hackers
- Know the main cybersecurity and international standards
- Apply cybersecurity risk and crisis management techniques.
Introduction

The era of digital transformation has changed the way industries deliver their services to end consumers and other organizations. Tourism is certainly one of the economic sectors that has been most exposed to digitization over the last decade. Let's just mention companies like Easyjet, Ryanair, AirBnB and Uber that have contributed to a new form of tourism called e-tourism. E-tourism means that all Customer Journey (CJ) touchpoints are handled by global digital platforms.

Before talking about computer networks and cyber-risks, and to avoid confusion, we should not forget that tourism businesses are organized in networks. A network of tourism stakeholders is a living system and, as such, it has vulnerabilities, points of fragility. Secondly, the disadvantage of this increased dependence on computer systems is that exposure to cyber-attacks on these networks (physical and digital) increases. In addition, customers are demanding new online services and innovative products, forcing the sector to review its product portfolio and innovate by implementing new technologies. This digital transformation increases the surface area of attacks and makes tourist networks more vulnerable to cyber-attacks. In addition, regulators and governments are aware of these new threats and have increased demands on the cyber resilience of the organization and, as such, on the particular network structure of the tourism sector.

Cybersecurity is no longer an IT issue, but a major concern for the entire organization to protect its operations, assets and reputation. In this regard, best practices are outlined in international standards such as ISO/IEC 2700x and the NIST Cyber Security Framework. These guidelines, as well as other references in the field of business continuity management, can be combined to enhance the control environment. Nevertheless, many challenges remain, including the effective implementation of these frameworks throughout the organization and, in our case, in various networks of hospitality and tourism businesses. Cyber-risk is not exclusively an IT issue, as human and organizational factors are just as important as the implementation of the right applications and technologies (Theirm.org, 2014).

Why Cybersecurity is so Important to the Hospitality Management Industry?

The Marriott Hotel Group has received a significant fine for failing to protect the personal data of its customers. Indeed nearly 340 million of customer account were concerned by this cyber-attack. And even if the amount to be paid was finally lowered to about 20 million euros, let's not forget that the image damage is huge. Will the trust capital of these customers not be eroded? This shows that in the hospitality management sector network and cyber security must be taken very seriously.

British Airways has also been fined (22 million euros) for leaving vulnerabilities in its customer database of over 400,000 accounts vulnerable to cyber-attacks. The worst thing is that this BA network vulnerability remained "open" for almost 2 months without the company being aware of it. The image risk is important. But let's not forget that cyber-attacks could also affect critical facilities such as power plants, hospitals, air traffic control centers. If at the end of the day a player in the tourism sector like BA is not able to protect its computer network, can't the peace
of mind of the people who usually take the plane be damaged? This data breach problem does not only affect companies. We as individuals are unfortunately also all affected. To check if you yourself have suffered a data breach, you can enter the different email addresses you use on https://haveibeenpwned.com/

COVID has forced millions of people to work at home and in a totally improvised way. At the same time, the number of computer breaches has never been so high. Here we see that while serious companies are doing quality cyber resilience work, suddenly it's as if everyone working at home has let their guard down.

What are the most common cyber-attacks in the world? It is very difficult to make an inventory of these attacks on the computer networks of our companies. However, there are some "families" of typical attacks. We propose a business intelligence website that follows in a very precise way what are the main cyber-attacks at the moment: https://www.cisa.gov/cyber-resource-hub. At the end of this chapter there is a section titled “Key terms: a glimpse into the world of cyber-attacks” that will give more explanations and illustration of typical cyberattacks in the hospitality management sector.

Let's first talk about the ransomware which does not only create financial damage to the company but also psychological damage to the people who directly undergo this type of attack. Take for example the unfortunately well-known “WannaCry screen” that is presented in Figure 1. The employee directly impacted by this type of attack typically experienced a trauma that certainly continues to this day.

![Figure 1: Infamous Image Seen when Hacked by the WannaCry Ransomware](image)

Another attack that this time every reader has been confronted at least once is phishing. You receive for instance an email from (what you believe) your bank asking you to pay an unpaid invoice as soon as possible. In this case, the main danger would be that you enter the fake site and give your password. Ultimately you trust this email and enter your password, without
perhaps being aware of it, you have allowed the hacker to access your bank account and the 
hacker can then simply empty it!

It is as simple as that- When we say the hacker, beware, it is usually a computer program that 
represents the hacker (behind it, of course, there are men who perpetrate illegal activities called 
cybercrimes). So as shown for ransomware before, even if these attacks lead to impacts may 
be less for the company itself, this impact will be significant for you but also at the 
psychological level. Indeed, you find yourself completely alone without help. How many times 
your bank, which you try to contact to find a solution, gives you an end of no help!

The cyberattacks relies on pieces of software what we call algorithms, or a sequence of 
computer actions. These latter that we call malware execute themselves as soon as you have 
opened a file attached to an email for example and which is able to block your PC or making it 
less efficient because the pirate's goal is to use your PC for free to do mining (mathematical 
calculations required to establish blockchain operations that we will discuss later in this 
chapter).

Another acronym you may have heard is AI for artificial intelligence. How AI works is that it 
is computer programs, more precisely algorithms that literally learn by themselves how to detect 
new computer breaches in your corporate network. Of course, companies are preparing for it. 
But it's a wild race between enterprise security systems, the so-called cybersafety, and 
increasingly sophisticated hackers who rely more and more on AI to commit cybercrimes in 
your Cyberspace. So yes, as said before, never let your guard down. At the same time, it is 
important to remember that companies in the hospitality management sector are networking 
with many other companies, and this is the reality that compared to many other industry sectors. 
And typically, these cyber-attacks based on AI will tend to focus on the weak links which are 
the inter-company links and above all, as it is said in service the customer is also co-producer 
at the level of your clients!

Cyber awareness is therefore the major tool available. It is a question of continuously training 
your employees through in-house courses. Because as we will see in this chapter common sense 
approaches will often be the key to good cyber protection that ultimately leads to cyber 
resilience. It is also necessary to raise awareness among your customers. For example, today 
y any bank (which is necessarily part of your network), warns all customers, that never but then 
never will they ask you to enter your passwords in a link in an email!

For a long time, we have been accustomed to giving our username and then our password in 
relation to our internet interactions. Fortunately, the concept “two factor identification” is now 
widespread. For example, you enter your password and automatically receive a notification on 
your cell phone to get an additional confirmation. However, remember to design passwords 
with at least 14 characters and for each account to create different passwords. But then how to 
remember all these passwords? Remember to use a good password manager.

Use good antivirus software systematically. There are regular and updated studies that are 
generally based on three following criteria:

- The detection of infected files and their elimination.
• Protection against ransomware
• Protection against phishing.

Also, think about regularly updating these antiviruses and follow the instructions provided by your company. In the end, a good cyber hygiene as we all have a good health hygiene must nowadays be part of our daily life. As advised before, we recommend to regularly visit the following site of the CISA which is the Cybersecurity and Infrastructure Security Agency, and which gives very valuable and updated information on the theme of this chapter which is by nature in constant evolution: https://www.cisa.gov/cyber-resource-hub

ISO 2700x as a Reference Standard in Cyber and Network Security

The ISO/IEC 27000-series (often designed as 2700x) is certainly the most comprehensive and best-known standard for Information Security Management Systems (ISMS) in the world. It was originally published in 2005 by the International Organization for Standardization and the International Electrotechnical Commission. It has since undergone several revisions. Thus, today about fifty standards are available covering all aspects of information security management. In particular the standards IOE/IEC 27032 entitled "Guideline for Cybersecurity" and IOE/IEC 27033 (1-6) "Network security" are completely dedicated to the subject of this chapter.

IOE/IEC 27032 provides guidance for enhancing the state of cyber security defined as the "Preservation of confidentiality, integrity and availability of information in the Cyberspace". This is often described as the CIA or ACI triad (Availability, Confidentiality and Integrity).

Another ISACA definition of CIA triad that it "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability). We also mention that ISACA, or the Information Systems Audit and Control Association, is most certainly the one stop shop for obtaining professional cybersecurity accreditation(s).

Cyberspace is also defined by ISO/IEC 27032 as a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

Figure 2 explains this notion of the complexity of cyberspace and thus the challenges of cybersafety. Thus, cybersafety should make it possible to fight cybercrime as a whole.

For this purpose, the security application corresponds to systems to avoid any type of security threats within the network such as unauthorized access.

Network security represents the means to safeguard the usability and integrity of the corporate network and its data. Network security includes hardware, software and communication elements to face breaches in the network by managing all accesses in an appropriate way.

Internet security is an extension of network security and is related to the notion of information and communication technology systems.
Finally, it allows a good cybersecurity to ensure maximum cybersafety for the company, also called **cyber resilience**.

**Figure 2:** The Link Between Cybercrime and Cybersafety Through Cybersecurity as Defined by ISO/IEC 27032

Security Operation Center: a new approach to modern cybersecurity

ISO/IEC 27032 offers controls to deal with malware, hacking and social engineering. However, a new term has appeared compared to the diagram in Figure 2, called the Security Operation Center (SOC).

Here we give the definition of the well-known mcafee **anti-virus**:

"A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources."

As employees of the hospitality management sector, in recent years we have become more and more what could be called digital nomads. Today we are all used to go home after a day's work to have a last video conference session on the train or in the café, for example. The Covid has simply exacerbated this phenomenon and will most certainly upset our links with the company in the long term. The SOC then becomes crucial, since every employee who continues these work activities with his cell phone, with his PC at home exposes more and more his/her own company to network vulnerabilities regardless of the efforts made within the physical company. It then becomes important to be accompanied by experts and specialists who help integrate these new SOC-based cybersafety architectures. Otherwise, there is a risk of creating within the company what is called a **false sentiment of security**.

The SOC becomes a service that takes into account any type of device. Indeed, today's cyber risk is no longer limited to the inside of a company. It is also known as **intrusion testing** to identify and correct network vulnerabilities. But today, vulnerabilities are at the "**end of the"
line" when employees work from home or when they access corporate data directly from their smart phones. And let's not forget the proliferation of IoTs (Internet of Thing) that are now found in most types of electrical devices, such as refrigerators, and can also be the object of cyberattacks. Since it is said, that in the case of services, the customer is also a co-producer, so it is also a question of protecting the customer when they interact with the company through apps. It is even necessary to integrate in this SOC concept all the stakeholders of cyberspace. If a DDoS (Distributed Denial of Service, see Key terms end of the chapter) attacks a power plant, your network (i.e., in the hospitality sector) is also put at risk. The SOC therefore becomes an essential function in companies and must be staffed by specialists, often with a multidisciplinary background and not solely a technical expertise (especially programming).

In the case of the hospitality and tourism sectors, the notion of networks is very fragmented, complex and globalized. It is therefore a question of being able to follow the complete customer journey of its customers at all times. The Covid has also added an additional level of complexity with many employees in the sector being forced to telework without having been prepared for this situation. This adds many more vulnerabilities to the network as a whole. The increase in cyber-attacks in this period of Covid is quite impressive.

This brings us to the notion of social engineering. Any cybersecurity specialist will tell you that the weakest link is always human. So, a cybersecurity specialist will of course have to know how to program in python, Java or C/C++ to perform an intrusion test. This intrusion test is also called ethical hacking because it is the company itself that requires a test to identify and correct vulnerabilities of its own network. In terms of jargon, we speak to express this ethical hacking as white hacking when it is perpetrated by specialists mandated by the company as opposed to black hacking perpetrated by criminals.

But this technical skill is a necessary but not sufficient skill. In order to make the difference, the cyber security specialist must have competence in psychology and sociology. Indeed, social engineering is also called psychological fraud. The hacker will of course "program" his/her attack in the form of a computer code, but what he/she will primarily target is a human weakness. In practice, this can translate into naivety in the case of phishing. For example, a hacker may have stolen the identity of a customer you know well, and you respond directly to his/her request without checking and you fall for it. In the case of rootkits (see the Key terms section end of the chapter) for example, this type of malware will succeed in sending a distress email to one of your friends asking you if you can pay him/her a sum of money as soon as possible, not into his account, but into the hacker's!

This notion of social engineering is crucial to integrate in any approach to cyber security. In the world of hospitality this notion is crucial to integrate you need to know the behavior of your customers, these cultural traits too in order to protect them and consequently to protect your own business.

The black hacker is often a very good programmer but also a very good connoisseur of human nature!
"Better Prevent Than Cure: Cybersecurity as a Component of Enterprise Risk Management"

According to Enterprise Risk Management (ERM), risk is what prevents the achievement of a business objective. The most famous ERM standards are COSO ERM and ISO 31000 and include all kinds of risk categories. Cyber risk is today and especially in the tourism industry an important category of ERM.

It is therefore crucial to prevent cyber risks and to integrate them into the “universe of your company” risks and especially not to see them as standalone. Indeed, as the traditional expression says, prevention is better than cure. This is particularly true in the case of cybersecurity. Indeed, the company can manage this prevention itself and often without too much cost and based on common sense. On the other hand, when the damage occurs it is very difficult to restore a cyberattack case for example (ransomware) and often, we are then forced to rely on external experts (firefighter, police, consultant), to incur substantial costs for often disappointing results, because the image damage will remain for a long time to come.

The ERM process can be summarized as shown in Figure 3. In step one, business objectives must be defined. For instance, a strategic business objective for an airline company can be to maintain an impeccable reputation of safety. Then risks that can prevent the achievement of the business objectives must be inventoried (i.e. step 2).

In our example, the inventory of risk could be a cyberattack, but not only. We could add other risks that would prevent the company from reaching this business objective such as: financial difficulties, bad quality of service, internal turmoil - We see here why cyberattacks cannot be considered as standalone risks. These risks are then evaluated by calculating their probability and impact (i.e. step 3). They are visualized through a risk map. We might evaluate here that the corresponding probability is small and the damage huge.

In step 4, treatments are in place to give an appropriate response to the significant risks by either mitigating, avoiding or transferring them.

Avoiding this cyber risk, would mean that basically, the company has to give up its activities. Transferring the cyber risk to a third party can create additional risks (e.g. image, reputation, loss of control). We are thus left with mitigation strategies that either lower the impact and/or the probability of occurrence. However mitigation the risk will not get rid of a residual risk (or net risk). At least it will make that the inherent risk will be reduced significantly.

Finally, step 5 or risks controls allow to monitor whether the treatment measures are effective. For the company, it requires the creation of an Internal Control System (ICS) made up of key risk controls. In our example, the ICS will contain typically several key risk controls related to our cyber risk. The ICS is mandatory in most countries and will be audited by external auditors. If the company is a public company, then any investor will be able to see if the company is sufficiently investing in cybersecurity. ERM is an iterative process. In general, in a large company, one or two full cycles are carried out per year.
Identification, Detection and Protection: On Dealing With Invisible Cyber Risks

In a case of "physical" risk, the critical incident when occurring is often visible, such as an explosion or fire. However, when the event that occurs corresponds to a cyber risk, there are often no easy indicators to detect it.

For example, during the period of COVID, many companies had to switch to teleworking mode overnight. Indeed, during the first wave and in light of the continuous spread of the coronavirus more and more cities and countries imposed a quarantine period or lockdown to their population with an access to the critical infrastructures, such as food shops, banks and hospitals. Governments around the world requested public and private companies to work from home as much as possible and on a very short period of time. For some of them, the switching was done in an improvised manner. For a lot of employees and students, a piece of the dining table became a desk for several months. To find an adequate computer or laptop and also a decent communication network to connect to the companies’ networks were a real challenge due to the rapid increase of demand in a very short period of time. Work productivity was definitely an issue for these companies as well cyber risks.

To monitor these stages, cause-and-effect analyses are sufficient for managers to properly rank risks and monitor the controls for each risk stage. Threats (upstream risk) should be handled...
with even more care as damages (downstream risk). As a matter of fact, the allocation of cyber risk resources should be changed to be more oriented toward the identification of threats and the implementation of detective controls to prevent any contagion of risks. Once the cyber risk propagates then it is usually too late.

Following the ERM approach, each significant cyber risk must be then supplemented with a control analysis that takes into account three following “states” of cyber risk: threat, event and propagation. Consequently, the appropriate control analysis involves three types of tests:

- Whether the threat is associated with a prevention system
- Whether the event (critical incident) is associated with a detection system
- Whether the ignorance of the problem is associated with a protection (or curative) system

The bow tie as a visual tool (see Figure 4) is interesting and practical, especially for setting up such controls, as we have seen above, to establish preventive, detective, and protective controls.

If, Despite Good Cyber-Risk Management, Damage Does Occur, it is a Matter of Crisis Management

A crisis is a situation where a tipping point is reached that prevents an organization from functioning properly. A crisis often results from the most unexpected events, such as the sudden loss of key employees, an unexpected lack of financial liquidity, damage to reputation, operational failure or the failure of strategic projects. In the sector of hospitality management, it could be a customer data breach sufficiently important to significantly damage the reputation of the company.

Lagadec (French crisis management expert, 2013) defines crisis as an event that puts strong destabilizing pressure on organizations that find themselves in critical situations and are subject to strong external and internal pressures. However, we must also take into account the fact that all these tensions and pressures go through a process that we could call a life cycle with an intensity of crisis stress, as shown in the Figure 5. In fact, the intensity of stress increases slightly after the event (or major incident). Then, when we are in the phase of effective crisis management, this stress intensity reaches its peak. And then it decreases significantly, to gradually decrease in the post-crisis phase. This shows that preparation is crucial. It is incomprehensible that important management issues can be addressed at the height of the crisis, such as the training of the crisis team.
It is therefore absolutely necessary to set up a monitoring system as early as the pre-crisis phase. This consists of rigorous and systematic identification of critical activities within the organization, as well as knowledge of its vulnerabilities (e.g., business risk mapping), crisis potentials, careful monitoring of adverse event reports, complaint and litigation management. It also means being attentive to weak signals such as rumors, monitoring all types of media (classic and social networks). Indeed, these crisis threats must be detected as early as possible. The company's management should not be afraid to clarify topics that would be taboo in the company.

In conclusion, it is important to mention that crisis management skills include (a) problem solving, (b) situational awareness, (c) resource utilization, (d) communication, and (e) leadership. These competencies are acquired and trained through exercises and drills that are often called tabletop, drills, or full-scale exercise depending on the expected level of realism. We will see in the next section how these crisis management skills are developed within the enterprise.

**Preparing for the worst: Business Continuity Planning, Business Continuity Management and Simulation Exercises**

How does the crisis management preparation take place in a critical incident resulting from the occurrence of a cyber risk? It all starts with the implementation of a BCP (Business Continuity Plan). “A BCP is a documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption” (ISO 22301, Business Continuity Management).

---

*Figure 5: Life Cycle of Crisis Stress Intensity*
BCM (Business Continuity Management) is a “holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities” (ISO 22301).

For a BCM to have a chance of success, it must be trained regularly and involve all stakeholders related to the company. This phase (see Phase 5 in Figure 6) is called "Exercising and Plan Maintenance" or "BCP Simulation Exercise".

A BCP simulation exercise is a form of practice, training and capability assessment involving the simulation of a major incident to which a prescribed or simulated response is provided. The purpose of the exercise is to allow participants to practice their day-to-day roles and functions while helping to develop, evaluate and test the functional capabilities of emergency systems, procedures and mechanisms to respond to the major incident. They are used to identify gaps and improve response preparedness before a real major incident occurs.

A fire drill is probably the best-known type of business continuity management, as everyone has already received this type of instruction on how to evacuate in the event of a fire, if not as employees, then at least as elementary school students. Sprinklers and fire extinguishers are available in most buildings to prevent the spread of a fire. Even if a fire never breaks out, most people are required to follow the building's evacuation plan in the event of an alarm. Regular drills should be conducted to ensure the chances of success in the event of an actual evacuation.

In the case of a cyber crisis simulation exercise, things are more complex as we will see. For example, BCPs must be put in place to deal with any significant risks accepted by the organization. This may seem like a lot of money and time spent on something that will hopefully never have to be used, but the cost of not having them in place at the time of risk would be even greater. Therefore, a cost-benefit analysis should be conducted on a regular basis to determine which BCPs should be maintained or which new BCPs should be established. In the case of
client data protection, and especially in Europe, this cost-benefit analysis must also take into account fines that can be huge (see Marriot and British Airways cases).

On the development of new cyber risk scenarios more representative of the hospitality management sector. The development of new crisis management scenarios deserves special attention, especially in areas related to cyber risks. Indeed, the classical crisis scenarios used for training usually rarely include new threats such as cyberattacks. Consequently, the scenarios used to date to train crisis committees no longer necessarily correspond to reality. These scenarios are often linked to problems related to buildings such as an incident, a flood, a power outage, for example. Of course, it is important to train on logistical risks, but we must not forget the risks related to information systems or suppliers, thus related to information security.

A crisis linked to a cyber-attack regarding a DDoS with a key supplier is managed in a different way than a loss of a building. In the case of a cyber-attack, reaction times are very short, i.e. a few hours or even a few minutes. In a hospitality environment where companies are increasingly dependent on digital technologies and interconnected with other companies, the scenarios employed in simulation exercises must be adapted to their realities to be effective in the context of BCP simulation exercises.

These scenarios underpin any stress testing exercise. It is the chosen scenario that will allow the integration of all the precepts presented in this section. It shows the different dimensions that need to be integrated into a crisis management scenario. Thus, a good scenario integrates the following elements as shown in Figure 7:

- The actors ("Actor")
- The time dimension ("Time")
- A Threat type ("Threat type")
- An event ("Event")
- The resources to be used ("Asset/Resource")

![Figure 7: Cyber Risk Scenario Components (Risk IT framework, ISACA, 2009)](https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7)

DOI: https://www.doi.org/10.5038/9781732127593
The objective of the BCP simulation exercise is to assess the readiness, availability and response mechanisms of the technical operations and support units to resolve incidents related to service-oriented IT infrastructure. It is also to provide opportunities for testing and identification of improvement potentials. So, it is important that the scenario (even if extreme) is as close as possible to the reality.

When designing a scenario to “train” a given BCP, it may be useful to begin with a tabletop exercise to design or test the BCP to allow stakeholders to become familiar with roles, responsibilities, element of planning and objectives. Once all team members are comfortable with the new scenario, a functional (i.e., drill or full scale) exercise can be used as a practical test of the systems and response plan.

The tabletop exercise simulates an emergency situation in an informal, stress-free environment. To conclude, a scenario should be selected that is consistent with the problem statements that form a complete and realistic emergency situation. When the company has acquired more maturity in BCM, it is then relevant to conduct a drill or even a full scale exercise to train based on a situation closer to reality.

**Digital Trust and Blockchain Technology to Put an End to Cybercrime?**

**Blockchain technology** is considered by many to be a revolution in the business world. Theoretically, the blockchain could lead to a situation where no intermediary is needed for any economic transaction. Thanks to cryptographic algorithms and an almost infinite number of replications on computers around the world, a blockchain contract could never be altered, hidden or cancelled. As a result, trust in those acting as intermediaries would no longer be necessary. A new trust would therefore be created through blockchains. But these blockchain technologies have to prove their usefulness not at an abstract or conceptual level, but at the level of the business experience between a customer and a supplier. In particular, our traditional business models in the tourism sector, which are ultimately very linear, i.e., B2B and B2C, could possibly be complemented by a variety of new provider-user relationships thanks to the blockchain technology, with new models such as C2C and even C2B being addressed in the co-production and co-customer logic.

The blockchain technology makes central instances superfluous by transferring their functions to all participants of a system. It functions like a decentralized booking system that is managed collectively according to transparent rules via the computers of all participants. Each participant in the blockchain network can transmit new changes (transactions) to the database. However, they are only accepted if they are permissible or if they do not compromise the database. This means that no participant can change the entries of other participants. To control this, each participant in the blockchain system can view a copy of all transactions in the entire database at any time to track any transaction. So, there is no potential corrupt central instance that can be hacked or bribed. Precisely because the blockchain does not belong to anyone or belongs to everyone, anyone can trust it. Theoretically, it would mean that cyberattacks as they exist today would have no impact on digital platform relying on the blockchain technology.
Many applications are possible in the tourism industry: payment, hotel or transportation coordination and management, baggage management, rewards systems, identification management, rating systems, etc. For example, the Alastria project in Spain on digital ID aims to simplify in tourist operations the tasks requiring having all the information available on an individual in one place. Indeed, Blockchain technologies (should theoretically) make central instances superfluous by transferring their functions to all participants of a system. It would function like a decentralized booking system that is managed collectively according to transparent rules via the computers of all participants.

However, the Blockchain technology poses many challenges for its implementation, as there are still few large-scale applications that provide sufficient feedback to launch the adventure with confidence! Moreover, the Blockchain is still at a very technical level and is finally not very accessible for tourism professionals. Precisely because the Blockchain does not belong to anyone or belongs to everyone, anyone could trust it. However, today, this remains pure theory!

**The Digitalized Transformation of Hospitality Management and the Need for Adapted Cyber-Governance**

With the increase in information technology use, problems related to the security of digital technologies have become significant. Businesses are required to acquire information, use information technologies, and rely on the information they collected to continue their presence. The requirement of information technology use and related security problems cannot be ignored by both individuals and businesses. One of the industries with large data pools is the tourism industry. Thus, the protection of personal or corporate information, is a process that should be managed especially for businesses. In order for this management process to be successful, it is necessary for the corporations to have security policies, that are supported by the senior management, possible to implement and understand, and accepted at all corporate levels.

In order to ensure the corporate information security, technical measures, administrative measures (such as fines, regulations, etc.), certain standards (i.e., PCI-DSS, ISO 27001: Information Security Standard), and human factor should be considered. It would be possible to talk about information security when these factors are effectively managed. Because businesses have to create an environment where information security is ensured. Thus, the loss of confidence that may arise due to possible security problems may prevent the sustenance of the business and may lead to the loss of the partners, customers or even the market. Naturally, this also applies to tourism corporations, which occupy an important place in the service industry. Technology in hospitality industry is driven by the increasing transaction volumes, complex reporting requirement, and international communication needs. Information technology (IT) can improve almost all areas of hospitality industry, such as guest services, reservations, food and beverage management, sales, food service catering, maintenance, security, and hospitality accounting.

Depending on the business context and size, small and medium size organizations can be located in different physical locations, such as, on its own premises, on a building in a compound, on a floor of a building or in several offices of a business center. In any case, the organization needs to ensure that proper access control and security measures are taken at the
perimeter, building, and office levels at a minimum. Organization should also ensure that it provides its cyber assets with appropriate protection against physical threats such as fire, smoke, water leakages, air condition, etc.

Organizations are constantly dealing with threats emanating from hardened professionals in cyber-attacks. It is a sad reality that many intrusions are carried out by nation states, cyber terrorists, and powerful cybercriminal groups. There is an underground economy of hackers that facilitates the purchase or hiring of intrusion tools, techniques or personnel, and laundering of the monetary proceeds from successful attacks. It is often the case that attackers have far more technical expertise in cybersecurity than the average IT employee. Therefore, the attackers can leverage their advanced expertise to easily bypass many cyber defense tools set up by the IT departments in many organizations. This, therefore, calls for a redefinition of how organizations should deal with cyber threats and threat actors because leaving the task to the IT department is just not enough. While hardening systems and installing more security tools would have worked just fine a few years ago, today, organizations need a tactful cyber strategy to guide their cyber defense approaches.
Expert Insights

The Future of Digital Trust and Client Data Protection. Interview Realized with a Swiss Hotel Association Director

Moving towards a domination of online travel agents over the whole market of tourist offers, hotel establishments will cease to exist in their traditional forms. Forced to manage their assets via digital platforms, they will no longer be seen as hoteliers but as room renters who will subcontract other services such as breakfast.

Among companies, there is potential for improvement in terms of online presence and willingness to engage in online dialogue. It would therefore be necessary to carry out a pre-evaluation through a sector organization. In short, lessons should be learned from the past to accompany, also at the political level, this digital revolution which is already underway. Consequently, he stresses the need for legal regulations, for example with regard to the use of customer data. More generally, tourist destinations need a Master Plan in order to define a common and shared vision between the players. This Masterplan would also have the important task of visualising what the image of tomorrow would be for the destinations. Alas, the interconnectivity required to do this does not yet exist. For the interviewee, this means in concrete terms creating a system for aggregating all the data, which serves as a starting point for using the data for advertising and offer design.

The aim here is to achieve a higher security standard in the area of cybersecurity without incurring major costs. Since the interview partners are active in very different areas, the contractual relationships are correspondingly diverse. From the perspective of a service company, which supports tourism service providers in the areas of infrastructure, distribution and promotion, taking into account digitalization, contracts are processed on 4 levels, namely on the level of system manufacturer, destination, service provider (e.g., hotel) and guest. The company has contractual relationships with various system manufacturers, which also include maintenance. These are so-called Service Level Agreement contracts (SLA) with guaranteed reaction times in case of breakdowns. In addition, there are contracts with customers regarding the transfer of the service.

A company operating in the field of hotel management solutions refers to licensing and purchase contracts for software use, usage and service contracts. It also, of course, has contracts with hotels. Further contracts arise with regard to the GDPR (data protection basic regulation). With regard to the gastronomy/hotel industry, it means table and room reservations. Cyber safety in the hospitality industry requires a radical change of mindset. Even today, most of our business is still done mainly with a handshake!
Key Terms: a Glimpse Into the World of Cyber-Attacks

Cyber-attacks are costing the hospitality management industry a fortune. Some people even talk about cyberwar rather than cyberattacks, as the phenomenon has taken on a worrying scale and is unlikely to be curbed in the future.

Adware is a software that once on your computer presents pop-up ads you know it is already installed. It is often difficult to establish a boundary between malware and adware. Be also aware that if you accept cookies from a notification it is not only a question of compliance with the European law GDPR, for example, but also of the possibility to take possession of your PC without having to go into the technical details. Even if most of the companies that let an adware notification acceptance are honest some hackers will on the contrary exploit your trust and naivety.

Botnet is the contraction of the words robot and network. They are robots that communicate between computers. Although there is nothing negative about botnets is that malware very often places them on your computer, which allows hackers to ensure that as soon as your computer is connected to the Internet its own botnets enter into communication with your botnet-infested computer and can execute malicious commands. It is also very difficult to detect them on your computer even if it is equipped with a good antivirus.

Rootkits are malware that try to hide as much as possible, not to leave any traces. They thus try to place themselves at a higher level of user rights (root administrator!) and to be able to raise security levels, to disable anti-virus software. The malware that carries them is often called Trojan horses, referring to mythology, where typically, a rootkit can hide in a quite banal and conventional file exchange and stealthily install itself in critical places of the operating system. Even if they seem harmless, they have the ability to stay dormant for a very long time and be activated for specific tasks, such as using your computer to launch an astronomical amount of spam in a very short period of time.

Spyware is malware that collects confidential data from your computer system and extracts them without any apparent breach in your data servers.

In a general manner, a computer virus is a malware that reproduces itself as a result of the infection of legitimate software called host. It is also a generic term for all types of malware. In fact, we usually buy a maximum spectrum antivirus to cover all cases. Be careful, anti-virus can also be malware. So avoid free anti-virus. Ask an expert to find the most effective anti-virus or antivirus even if it means paying a considerable amount of money. As we often say “it is better to pay now than later”.

DDOS (Distributed Denial of Service) is an attack in good form that starts from a computer army and will literally bomb a site for example. Thus the usual users of the site will be denied access to the site because it is totally clogged by the DDOS attack. Typically, the firewall and IPS (Intrusion prevention system) of the attacked company are very quickly put out of order and the company is cornered. DDOS is often the business of a well-organized activist group. But in the tourism sector, one could imagine such attacks on airline companies, relying on the Flygskam ideal on for example.
**Worms** are also malware, but unlike viruses, they do not reproduce themselves by infecting an executable program, but can directly duplicate themselves once they are executed from the Internet.

**Identity fraud**, also known as identity theft enables the hacker, under the cover of a stolen identity, to commit serious crimes and also to put the person who has been cheated in legal risks or even important image risks. For this reason, never place yourself in this category of people who pretend not to care about protecting themselves from cyber-attacks because they have nothing to hide. Many of these people, extremely vulnerable, have thus suffered damage that could have been easily avoided by applying the basic rules of cyber hygiene. Just from a more technical standpoint and related to this notion of identity fraud, you will often see the acronym **IP** which means Internet Protocol address, and which corresponds to the address of your computer or the address of a corporate computer network for example.

**Email External Fraud and USB Key as a Gift!**

Finally, let’s talk about our old friends cyber email that seems quite harmless. Beware and be very careful when a file is attached to your email. Today in most companies today firewall systems block files that could be infected. Nevertheless, be very careful. Do not open them unless you are sure of their origin! Also be careful with USB keys. Some companies claim that their internal network is not connected to the outside company. So theoretically, they are immune to cyberattacks but don not be mistaken. Do you know one of the most effective intrusion techniques that costs nothing realized by cyber security auditors. Outside the company, usually at the place where employees meet to smoke their cigarettes, they leave a USB key on the floor. What happens, you bet, one of the employees takes this USB key and is so curious to consult its contents, that as soon as the cigarette break is over, the employee plugs the USB key into his/her computer, with inside a test software that will allow to check if the intrusion has been successful.

**References**


https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7
DOI: https://www.doi.org/10.5038/9781732127593