Unit 10: Cyber Security & Cyber Resilience in Tourism SMEs

DIGITOUR

Co-funded by the
Erasmus+ Programme
of the European Union

Project title: Building Digitalisation Readiness in the Tourism SME sector

Project acronym: DIGITOUR

Project number: 2021-2-IE01-KA220-VET-000048348

Module: Cyber Security & Cyber Resilience in Tourism SMEs

Primary Target Group: SMEs in the tourism sector

Secondary Target Groups: Expert VET providers, tourism representatives, and in-company trainers.

Estimated time: 120 to 150 minutes

Objectives: The objectives of this module are:

- To give learners an understanding of the challenges, risks and importance for cyber security systems.
- Learners become familiar with the basic, key concepts and technical terms related to the area that will help them strengthen the company's cyber security and cyber resilience;
- Learners can look to the future of the tourism industry with a developed skills set in cyber security and resilience.

Learning outcomes: By the end of this Bitesize the participants will:

- Describe the meaning of the term "cyber security" and "cyber resilience" and understand how these are imperative for any type of tourism provider;
- Demonstrate an understanding of the basics and essentials of cyber security and cyber resilience;
- Understand the main cyber risks and attacks of the tourism sector;
- Be aware of good practices for achieving cyber security and cyber resilience in business;
- Discuss the main pillars of effective, secure, and resilient cyber systems and know the main cyber security and cyber resilience standards.

Table of Contents

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

10.1 Introduction: Guiding Principles and Definitions

What is cyber security?

Definitions of cyber security vary, but in general, they all point to the security of cyberspace.

Cyber space is the dynamic and virtual space that connects different computer systems.

https://northafricapost.com/42416-morocco-is-not-a-cyber-jungle-defense-administration-tells-amnesty.html

Cyber security is made up of **2 key terms**:

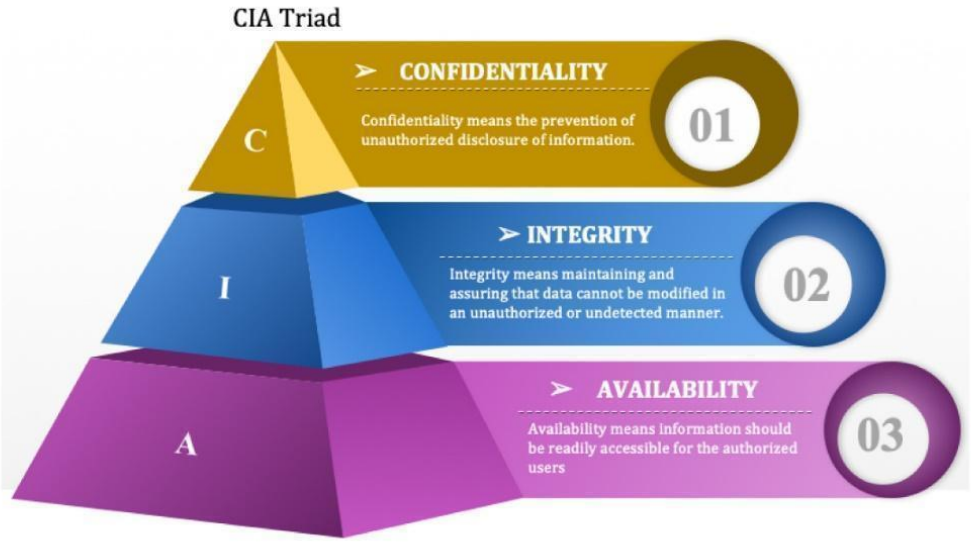
1. Cyber relates to the technology which contains systems, network and/or data.
2. Security relates to the protection which includes systems security, network security and application and information security.

The EU defines cyber security as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".

Confidentiality, integrity, and availability are known as the CIA triad, known as the 3 main principles of cyber security –

- ***Confidentiality:*** confidentiality measures prevent sensitive information from being disclosed to unauthorised access (e.g., data encryption, two-factor authentication).
- ***Integrity:*** integrity measures maintain the consistency, accuracy, and trustworthiness of data over the entire lifecycle by preventing data from being modified by unauthorised parties (e.g. data backups, using file permissions).
- ***Availability:*** availability measures ensure that information is consistently and readily accessible for the authorised parties in question and maintain the hardware and software systems that hold and display that information.

Overall, cyber security refers to every aspect of protecting an organisation and its employees and its assets against cyber threats or attacks.



https://thingscouplesdo.com/what-is-cia-triad-and-how-does-it-work/

What is cyber resilience?

In the business world, cyber resilience offers a more holistic way for digital business continuity. It is a new concept, referred to as digital fitness.

The EU defines cyber resilience as *"the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack".*

In the sophisticated threat environment, traditional security tactics focused on cyber security are failing. No organisation can simultaneously sift through alters, track vulnerabilities, apply security policies across various systems.

To manage these competing challenges, organisations must change their security posture from a defensive stance focused on malware to a more realist and resilient approach – a cyber resilience approach (Symantec, 2014).

The concept of cyber resilience can be thought as of framework with 5 main pillars –

1. **Prepare/Identify:** understanding the company's security and identifying potential risk postures to address security vulnerabilities;
2. **Protect:** understanding the company's threat landscape (e.g. its level of vulnerability and risk tolerance) ensures protective infrastructure;

3. **Detect:** once protective measures are in place, appropriate activities can be established to rapidly detect an attack, assess affected systems, and ensure a timely response;
4. **Respond:** this phase is crucial to provide guidance on which activities can help accelerate the time to respond and contain the impact of an attack once it is detected;
5. **Recover:** developing and implementing the appropriate systems for data recovery in the event of a cyber-attack, which is an essential component of any resilient security strategy.

https://www.amdhservicesltd.com/how-to-build-a-cyber-resilient-infrastructure

How are cyber security and cyber resilience linked?

Cyber security and cyber resilience may often appear interchangeable as they both relate to cyber safety, however, they are not the same thing:

- Whilst cyber security refers to an organisation limiting its threats by focusing on proactive dispositions against the growing proliferation of cyberattacks;

- Cyber resilience on the other hand refers to an organisation limiting as much as possible the potential damage and associated losses once an attack has already taken place while resuming business as usual.

10.2 Cyber Security and Cyber Resilience in Context

Cyber Security and Cyber Resilience in tourism

In the context of tourism and travel, digitalisation has become a strong enabler of business in today's digital world.

Cyber security and cyber resilience are important as the digital innovation they safeguard:

- Digital innovation redefined the tourist experience and has led to a heightened susceptibility of tourism to security risk.
- Cyber security and cyber resilience are tools that shape the sector and ensure a safer future for the tourism and travel SME sector.

Technology now plays an integral role in nearly every aspect of the travel and tourism experience:

- from inspiring tourists during the pre-purchase stage of the consumer journey,
- to leaving online reviews in the post-purchase stage.

This often involves online transactions, customer sensitive information, cloud integration, and digital payment technology, which as a result has increased the digital footprint of tourism businesses, rendering them exposed to cyber threats and attacks, some of which may constitute cybercrime (Paraskevas, 2020).

https://thecyberverdict.com/author/emmanuel/

Since 2010, several of cyber security breaches were reported, even by the biggest hotel chains in the world:

- Marriott International Hotel Group was responsible for a data breach in 2020 that failed to protect customers' personal data and disclosed names, mailing addresses, loyalty account numbers and various other sensitive information.
- An approximate 340 million guests were concerned by this attack. 2 years prior, in 2018, Marriott received an alert from an internal security tool regarding an unauthorised access attempt in their guest reservation database in the United States.
- Further investigation by cybersecurity experts revealed that unauthorised access to the hotel's reservation system had occurred as far back as 2014 (Secure Stay, 2020).

https://gritdaily.com/marriott-hit-by-second-data-breach-2020/

The repercussions of cyber threats and/or attacks can cause considerable harm to brand reputation and consumer trust, resulting in significant financial, legal, and regulatory consequences. Tourism providers can suffer from both direct and indirect financial losses (Paraskevas, 2020) –

- Direct financial losses: company expenses associated with IT recovery services, as well as legal fees and public relations services.
- Indirect financial losses: costs for hiring additional technical IT staff, providing staff training on cyber security and cyber resilience, upgrading cyber security infrastructures, etc.
- Reputational cost: if a data breach were to occur, there are also reputational costs to consider. Reputational costs can be staggering and lead to a decline in consumer confidence and bookings. Tourism providers must recognise their

responsibility to keep data and information safely secured to avoid substantial negative impacts on their business.

Therefore, it is crucial for businesses, and especially SMEs, in the travel and tourism sector to understand the importance of implementing cyber security and cyber resilience as priorities for their business, instead of as an afterthought.

Post Covid-19 Developments

In the wake of a global pandemic which forced the tourism industry to move online, the travel and tourism sector had to redefine their products, services, and consumer experiences to deal with the new reality.

In the post Covid-19 era, the number of cyber threats has never been so high.

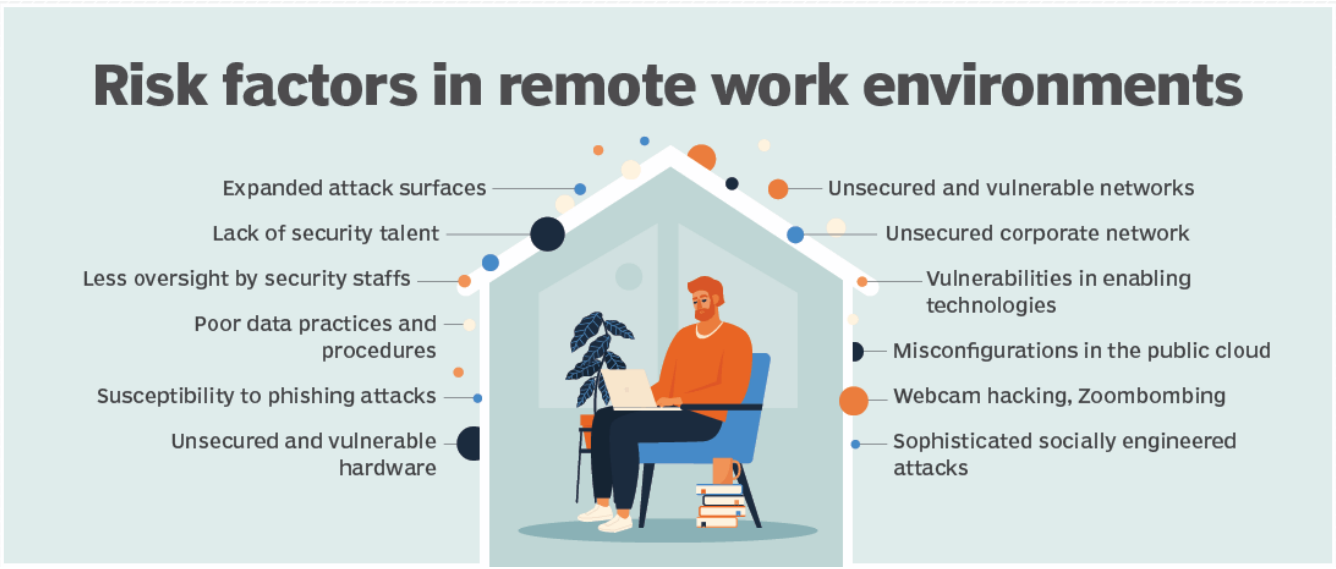
The World Travel & Tourism Council (WTTC) reports that accelerated growth in digital operations has left the industry more vulnerable and exposed to cyber risks (World Travel & Tourism Council and Microsoft, 2022).

This encouraged businesses to revisit their security posture to build a more cyber resilient enterprise and business owners are doing quality cyber security and cyber resilience work.

https://www.idealarticleswriter.com/2023/03/-Understanding-Digital-Forensics-Process-Techniques-and-Tools-.html

Cyber threat actors are agile and saw Covid-19 as an opportunity to exploit the vulnerabilities of tourism providers who were trying to facilitate travel while at the same time protecting public health. The continuous and inconsistent restrictions created room for cyber-attacks.

The adoption of remote work, which has led to a greater reliance on personal and mobile devices, has increasingly placed responsibility for company cyber security on employees.



https://www.techtarget.com/searchitoperations/news/365534899/Securing-remote-access-grows-crucial-for-DevSecOps

While companies' on-site cyber ecosystems tend to be secure, this security had previously not been extended to employee homes. As a result, attackers who gained access to home or public Wi-Fi networks could easily breach company systems, emphasising the need for a more comprehensive approach to cyber security – one that emphasises cyber resilience.

Although organisations cannot guarantee the security of home or public Wi-Fi networks, staff training can help safeguard employees against threats when using IoT (Internet of Things) devices.

Cyber threats resulting from COVID-19 should not be treated as separate to organisational risk, including cyber risks associated with hybrid work models.

As such, to ensure cyber resilience, organisations must broaden their threat monitoring efforts to encompass possible entry points for attacks through home and public Wi-Fi systems (World Travel & Tourism Council and Microsoft, 2022).

10.3 Cyber Vulnerability of tourism SMEs

How are tourism SMEs vulnerable?

The WTTC reports that more than 7 in 10 (72%) SMEs in the UK, US and Europe have fallen victim to at least 1 cyber-attack (World Travel & Tourism Council and Microsoft, 2022).

Among the travel and tourism industry, which comprises mostly SMEs such as agencies and tour operators, the percentage is even higher, with SMEs accounting for about 80% of all businesses.

"Did you know that a cyber-attack happens every 39 seconds and 291 data records are stolen every second?"

https://wisedistribution.co.uk/deception-technology/

Tourism SMEs have become an attractive target for cybercriminals in the last few years:

- The high level of digitalisation maturity makes tourism SMEs a very vulnerable industry in terms of cyber security and cyber resilience, especially due to poor defences in IT and point-of-sale (POS) systems (Fragniere & Yagci, 2021). According to Hussain (2023), hackers have realised that SMEs are easier targets as compared to larger companies with inadequate cyber safety, either due to lack of qualified and skilled personnel (i.e. human error) or insufficient budgets.
- Tourism SMEs are especially vulnerable to cyber threats because of the highly sensitive data and analytics they store on the cyber space, making it valuable

information for cyber criminals that attempt to access and breach such data, leading to identity and financial theft, threatening data governance and customer and employee privacy protection (customers' e-mail addresses, passport numbers, credit card details etc).

- The tourism SME industry is particularly susceptible to cyber threats, as it is fragmented in its nature, with the entire supply chain (which involves numerous agents and third-party service providers) being a potential area of entry for threat actors. Proactive cyber security measures to ensure cyber resilience and maintain effective business operations are necessary.

The European Union Agency for Cyber Security (ENISA) found that 90% of the SMEs stated that cybersecurity issues would have serious negative impacts on their business within a week of the issues happening, with 57% saying they would most likely become bankrupt or go out of business.

https://www.enisa.europa.eu/

How should the SME respond in case of a data breach?

In case of a data breach the SME is advised to notify this breach to the information and data protection commissioner and attach this online notification form not later than 72 hours of becoming aware of such a breach.

If the breach poses risk to the data subject, the supervisory Authority needs to be notified.

These are 5 concrete actions that can be taken by an SME, following a data breach.

1. Identify the source and extent of the breach.
2. Alert your breach task force and address the breach as soon as possible.
3. Test your security fix.
4. Inform the authorities and all affected customers.
5. Prepare for post-breach clean-up and damage control.

10.4 Cyber Threats in tourism SMEs

What are cyber threats?

Any circumstance or event with the potential to adversely impact business operations, assets, employees, and/or other organisations, or a nation through a system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.

There are 3 main types of cyber threats:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.
2. Cyber-attack often involves politically motivated information gathering.
3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

What are the main types of cyber threats in tourism SMEs?

When it comes to cyber threat attempts, travel and tourism SMEs are one of the most impacted industries globally.

Cyber-attacks in the travel sector mainly target credit cards, personal identifiable information, hospitality reward programmes and publicly available internet (Walson, 2022).

A PwC Hotel Outlook Report from 2018 to 2022 stated that the hotel industry had the maximum number of data breaches after the retail sector.

According to the WTTC, phishing, malware, and ransomware threats remain constant, with ransomware accounting for 23% of cyber-attacks in 2021, and phishing used in 33% of cyber-attacks. Cyber criminals largely gain access to cyber environments through phishing, credential theft, or remote desktop control (World Travel & Tourism Council and Microsoft, 2022).

https://motyl-szary.com/2023/03/31/top-cybersecurity-threats-and-proactive-measures-to-protect-personal-and-business-data/

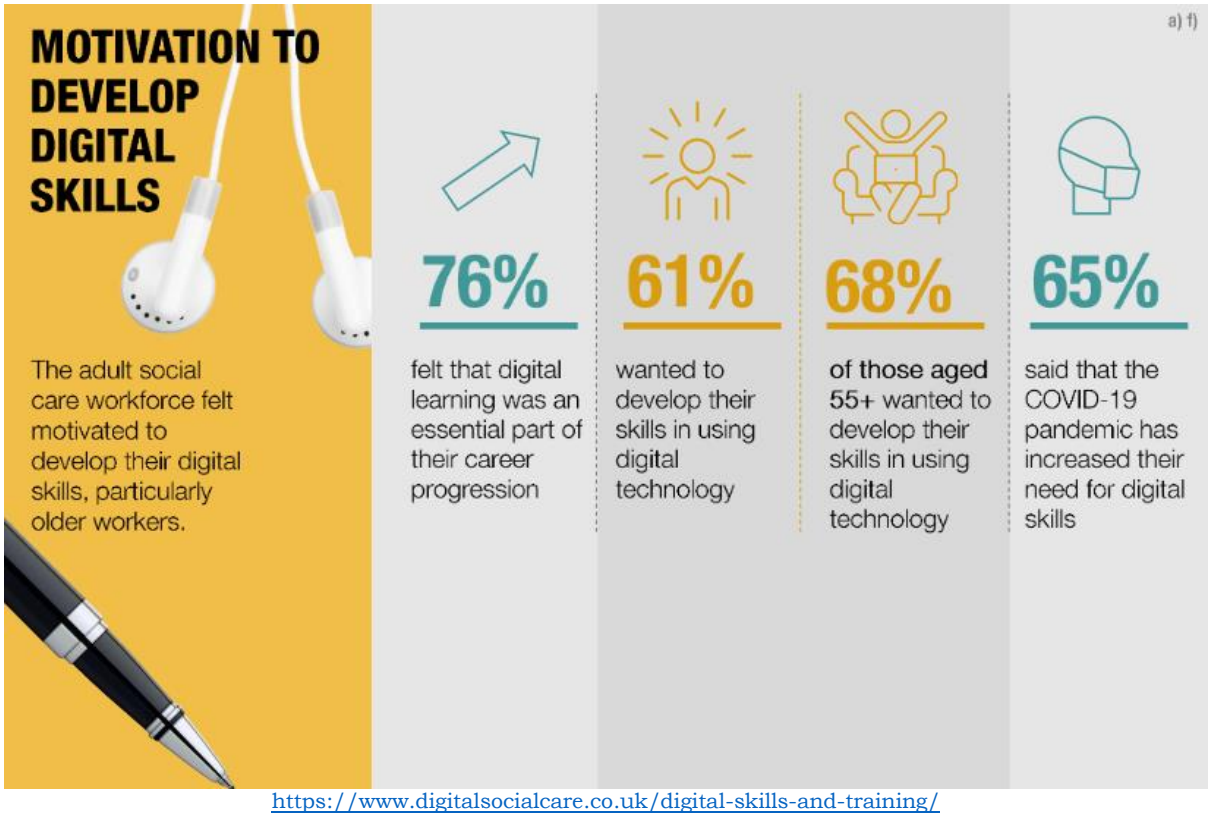
The most common methods used by malicious actors when trying to threaten the cyber security and cyber resilience of a tourism business –

- Malware: this is one of the most common cyber threats which is spread via an unsolicited email attachment or legitimate-looking download. Malware attack compromises an organisation's sensitive systems and data by infecting them with malicious software such as viruses, worms, Trojan horses, and other spyware (Paraskevas, 2020).
- Phishing: this has always been the most common type of cyber-attack and often occurs through emails. It takes place when cyber criminals send emails to victims which seem to be from a legitimate company (e.g. a bank) and ask for sensitive information (e.g. bank account details, passwords).
- Point-of-sale (POS) attacks: also very common in the travel and tourism sector and gives threat actors valuable data including credit card information such as card numbers and personal identification numbers (PINs).
- Man-in-the-middle: this type of cyber-attack occurs on an unsecure WiFi network where an threat actor could intercept data being passed from the victim's device and the network.
- Ransomware: the goal of this threat is not to steal data but to deny its owner access to it and make the target pay the attacker directly. Ransomware is programmed to identify the company's most sensitive or valuable data.
- Botnet attacks: use of large networks, often comprised of numerous computers, smartphones, or intelligent devices (aka. 'zombie armies') for carrying out malicious activities such as login attempts, spam attacks, or the takedown of networks, network devices, websites or an organisation's IT environment.

- Attacks on third-party Service Providers: threat actors also target members of the organisation's 'DexteR' (digital partners and third-party service providers) – these often considered the weaker links in the network and represent attractive aggregation points for sensitive company data (IBM 2018 as cited in Paraskevas, 2020).

10.5 Good Cyber Practices for tourism SMEs

One crucial element of cyber security and cyber resilience is **providing staff education and digital skills training**. Employees who are properly trained on how to prevent falling victim to cyber-attacks and know what to report, can enhance a tourism SME's security systems and reduce the risk of cyber threats, such as unauthorised access to the company's cyber systems.



https://www.digitalsocialcare.co.uk/digital-skills-and-training/

The WTTC identifies 7 good practices that can be taken in order to further enhance cyber resilience:

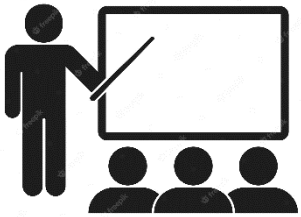
1. Integrate cyber risk management into organisational risk management

Cyber risks should be prioritised and managed along with other business and operational risks. Businesses should regularly review and update their risk management processes and allocate a budget according to the risk level and mitigation measures required. Skilled employees are necessary to create and inform cyber risk policies, implement best practices, and manage risks proactively and continuously.

2. Educate and train all staff

Training is crucial for introducing new staff and for educating current staff to ensure the effective use of digital systems and processes and safety. While not all employees

require the same level of training, it is important for staff to have a fundamental understanding of cyber security principles. This reduces the likelihood of cyber-attacks resulting from insiders.



https://www.freepik.com/premium-vector/training-icon-vector-training-education-icon-blackboard

3. Expand risk protections beyond the physical workplace

With the move to remote and hybrid working, cyber controls should be applied more broadly. It is crucial to consider how hybrid working models could affect security and heighten vulnerabilities, including home Wi-Fi security, employee cyber hygiene on their own devices, etc.

4. Employ a zero-trust approach to cyber security

The zero-trust approach moves away from previous methods that relied on higher levels of trust within the organisation. It relies on explicit verification of access requests, least privilege access, and assumes a breach or compromise. This enables more flexibility in access while limiting exposure to core systems.

https://pbosecure.com/blogs/apply-zero-trust-information-security-framework-to-icsot-environment

5. Employ ongoing threat assessments

This includes enhancing resilience against cyber threats by building relationships with experts in the field, using analytics to refine protection measures, conducting penetration tests to identify vulnerabilities, segmenting systems to limit the impact of breaches, and prioritising the protection of systems.

https://www.clipartmax.com/middle/m2H7i8G6K9m2A0Z5_a-checklist-with-a-warning-sign-to-depict-risk-identification-risk-assessment/

6. Be transparent

It is key to communicate implemented security measures and the reasons for data collection, data usage, and data storage periods. Tourism SMEs should collect only the least amount of personal data and payment information needed and offer the

highest levels of protection to foster trust. Compliance with legislation and standards (e.g. GDPR) should be highlighted. If a breach occurs, affected parties and regulatory bodies should be immediately notified, and measures should be taken to mitigate the impact of the breach.

7. Implement an organisational standard

Business leaders should comply with legislation in the regions where their organisations operate. The EU's mission to foster a standardised approach to cyber security and resilience and data protection has led to the development of:

- The EU Cyber Resilience Act seeks to establish common cybersecurity rules for digital products and associated services that are placed on the EU market.
- The EU Cybersecurity Act strengthens the ENISA and establishes a cybersecurity certification framework for products and services.
- The evolving cyber landscape necessitates specific cyber laws to enhance civil protections; this is where the EU's General Data Protection Regulation (GDPR) comes in. ENISA's current priority is to encourage data protection measures to show how cyber security technologies can support the fulfilment of the GDPR's data protection principles (see steps regarding data breach response in Section 10.3).
- As part of the 2023 European Year of Skills, the Commission adopted a Communication on a Cybersecurity Skills Academy on 18 April 2023.

  Such regulations and policy initiatives must be considered by tourism SMEs when they are developing and implementing an organisation standard, which should also be informed by cyber security, privacy, and legal experts.

The ENISA developed a cybersecurity guide for SMEs which highlights 12 steps in which SMEs can secure their businesses.

The steps are:

1. Develop good cyber security culture;
2. Provide appropriate training;
3. Ensure effective third-party management;
4. Develop an incident response plan;
5. Secure access to systems;
6. Secure devices;
7. Secure the network;

8. Improve physical security;
9. Secure backups;
10. Engage with the cloud;
11. Secure online sites;
12. Seek and share information;

https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/

10.6 Conclusion

- This module looked into the ways cyber security and cyber resilience play a key role in tourism business operations, the issues and risks posed by cyber-attacks, and good practices.
- Digital skills can serve as a tool for the tourism sector to better understand how cyber security and cyber resilience are shaping the sector and plan for a safer future.
- Embracing security and resilience as a normal way of the business's cyber lives is in the common interest.

10.7 Reading & Additional Materials

Reading materials

https://link.springer.com/chapter/10.1007/978-3-319-16486-1_31

https://www.ttgmedia.com/news/news/smes-at-greatest-risk-of-cyber-attacks-says-wttc-33908

https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/

https://link.springer.com/referenceworkentry/10.1007/978-3-030-05324-6_100-1

https://securestay.medium.com/the-history-of-hotels-cyber-attacks-4b6a09c8bf30

https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf

https://wttc.org/Portals/0/Documents/Reports/2022/WTTC_x_Microsoft-Codes_To_Resilience.pdf

https://idpc.org.mt/report-a-breach/

https://www.whoa.com/5-steps-to-take-after-a-small-business-data-breach/

Websites

https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity

https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport

https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection

https://www.eurotechconseil.com/en/blog/difference-between-cyber-security-and-cyber-resilience/

https://www.goallsecure.com/cyber-security-in-travel/

https://www.i-scoop.eu/cybersecurity/cyber-resilience/
https://mbb.org.mt/wp-content/uploads/2022/12/CRA-Brief-.pdf
https://www.omnicybersecurity.com/cyber-attacks-travel-tourism-industry/
https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
https://www.wcrcentre.co.uk/post/why-should-cyber-security-matter-to-an-sme-in-the-tourism-and-hospitality-industry

YouTube Videos

https://www.youtube.com/watch?v=z5nc9MDbvkw

https://www.youtube.com/watch?v=JbEPJv7Ybcs

https://www.youtube.com/watch?v=inWWhr5tnEA