Guideline to implement cybersecurity in SMEs

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

Chapter 1

Outlines of Cybersecurity Fundamentals

ENGINE

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

SHORT SUMMARY

ENGINE

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

CHAPTER I: OUTLINES OF CYBERSECURITY FUNDAMENTALS

The first chapter aims to provide a general overview and basic knowledge about cybersecurity, describing and introducing basic concepts related to this field, with a clear focus on the most relevant information for SMEs.

This chapter is divided into five main thematic areas, including:

- A brief introduction to cybersecurity explaining what it is and why it is important;
- Cybersecurity for SMEs and the Cyber Security Culture (CSC);
- Definitions of concepts related to cybersecurity and possible threats;
- Web Application and Services and the main differences between them;
- Cybersecurity in the European context: funding programs, frameworks and legislation.

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

IMPORTANT ASPECTS OF CS
CHAPTER I

ENGINE

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

Most important aspects of CS:

Why is Cybersecurity important to SMEs and Managers

- As today's business has moved largely online, companies are required to adapt.
- The fast and continuous technological renewal causes difficulties especially to SMEs, requiring to protect themselves and protect their business from possible attacks.
- SMEs are most at risk with regards to cyber security threats; they have less security architecture and smaller IT teams being profitable and an easier target for hackers.

Reasons why SMEs need cyber security

- Small businesses are moving to the cloud
- Protecting business and valuable information
- Preventing spyware to maintain reputation and customer trust
- Protecting work safety and productivity
- Increasing remote working
- Protecting from cyber-attacks

Cyber Security Culture (CSC)

- CSC must be created ad hoc for every organization, matching the organization's mission and culture, but mainly employees' practices and needs.
- It is crucial to involve employees in developing a CSC to guarantee its full adoption.
- The lack of participation of employees and executives who ignore CSC are the main barriers in creating a CSC.

SET OF SKILL

ENGINE

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

Chapter 1 - set of skills

- General knowledge of main Cyber Security basic concepts
- How to create a Cyber Security Culture
- Basic Knowledge of The EU Strategy for Cybersecurity and related acts
- Basic knowledge of Cyber Security common taxonomy

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

ADDITIONAL MATERIAL

ENGINE

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

Web pages:

List of antivirus softwares: https://bestantivirus.com/antivirus-companies.html

DIgitalEU Prgram: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital

The EU 5G toolbox: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Learning and Classification of Malware Behavior https://link.springer.com/chapter/10.1007/978-3-540-70542-0_6

Wifi Alliance Discover Wi-Fi Security https://www.wi-fi.org/discover-wi-fi/security

HTTP vs HTTPS: Understand the differences https://www.copahost.com/blog/http-vs-https/

Cybersecurity for SMEs - Challenges and Recommendations https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Cybersecurity guide for SMEs - 12 steps to securing your business https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

A Systematic Literature Review on Phishing and Anti-Phishing Techniques https://arxiv.org/ftp/arxiv/papers/2104/2104.01255.pdf

Videos:

DigitalEU YT channel Introducing the DIGITAL Europe Programme: https://www.youtube.com/watch?v=_VkzyMgjD4E

Hardware and Software instructive Video: https://www.youtube.com/watch?v=vG_qmtdBPTU

ENGINE

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

Chapter 2

The NIST Framework

ENGINE

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

SUMMARY OF MODULE 2-ATLANTIS

ENGINE

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

Despite the fact that SMEs play a significant role in the economy of the European Union, the majority of them lack cybersecurity infrastructure. If we also combine the fact that six out of ten cyber-attacks target SMEs, it becomes easily understood why it is very hard for a small business to recover from such an attack.

A cyber-attack can come either from an external, i.e., a cyber-criminal, or an internal threat, i.e., an employee. There are a number of reasons why a cyber-criminal attacks an SME, such as profit, revenge or the thrill of creating a mess, just to name a few. On the other hand, the human error is what poses as an internal threat most commonly. Whatever the cause though, the effect on a company can be extremely huge and not only the information system but also productivity, their reputation and their credit worthiness can be affected.

Chapter 2 presents the tools and processes to be followed in order for small businesses to protect their information while reacting in a best possible manner should a cyber-attack occur. The chapter is grouped in five categories covering how to identify and be protected from a cyber-attack, how to detect one and finally how to appropriately respond and recover from the damage that the SME has suffered from.

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

IMPORTANT ASPECTS OF CYBERSECURITY

CHAPTER 2

ENGINE

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

Important aspects of Cyber security in our chapter:

- **The importance of adopting a framework in Cyber Security.** The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.
- What is NIST? NIST is a voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.
- **The Cybersecurity Framework consists of three main components**: the Core, Implementation Tiers, and Profiles.
- **Chapter 2 specifically explains the five high-level functions of the Core**: Identify, Protect, Detect, Respond, and Recover. These 5 functions are not only applicable to cybersecurity risk management, but also to risk management in general.

SKILLS AND COMPETENCES
ATLANTIS

ENGINE

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

Chapter 2 aims to transfer the following skills and competences:

Through the **Identify** function one will be able to:

- Become aware of the business context and relevant cybersecurity threats
- Identify which aspects are significant and in need of protection
- Develop a risk management strategy
- Focus and make priorities according to the risk management strategy

Through the **Protect** function one will be able to:

- Set the limits and the necessary precautions to deliver infrastructure services
- Limit the possible effect of a cybersecurity incident and protect the business
- Protect and maintain their resources through the implementation of the organisations' policies and procedures

Through the **Detect** function one will be able to:

- Define the measures and actions to be taken in order to identify a cybersecurity event in time
- Detect suspicious activity and relevant threats
- Analyse possible cyber incidents in order to prevent future ones
- Verify the effectiveness of protective measures

Through the **Respond** function one will be able to:

- Develop and implement a Response process plan
- Take actions to reduce both the risks and the impact of an incident
- Analyse the effectiveness of the Response process plan and update/improve if needed

Through the **Recover** function one will be able to:

- Restore capabilities, services or equipment after a cyber attack
- Implement improvements/reviews/updates on previous strategies and policies based on lessons learnt
- Prevent the occurrence of a similar incident
- Build a cybersecurity attitude on all levels of the organization

FUTHER READINGS
CHAPTER 2

ENGINE

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

Further Readings

Aderibole, A., Aljarwan, A., Rehman, M. U., Zeineldin, H. H., Mezher, T., Salah, K., . . . Svetinovic, D. (2020). Blockchain technology for smart grids: Decentralized NIST conceptual model. IEEE Access, 8, 43177-43190.

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. Computer Science & Information Technology, 7(3), 51-62.

Bohn, R. B., Messina, J., Liu, F., Tong, J., & Mao, J. (2011). NIST cloud computing reference architecture. IEEE World Congress on Services, 594-596. Retrieved from https://www.researchgate.net/profile/R-Bohn-2/publication/220985536_NIST_Cloud_Computing_Reference_Architecture/links/5525763f0cf25d66dc945a6c/NIST-Cloud-Computing-Reference-Architecture.pdf

Eckmaier, R., Fumy, W., Mouille, S., Quemard, J., Polemi, N., & Rumpel, R. (2022). Risk Management Standards - Analysis of standardisation requirements in support of cybersecurity policy. Athens: European Union Agency for Cybersecurity (ENISA).

European Commission. (2022, Jan. 09). The EU cybersecurity certification framework. Retrieved from European Commission - Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST Standard for Role-Based. ACM Transactions on Information and System Security (TISSEC), 4(3), 224-274. Retrieved from http://ce.sharif.edu/courses/93-94/2/ce678-1/resources/root/Reference%20Papers/08-RBACStandard-2000.pdf

Ferraiolo, D., Sandhu, R., & Kuhn, R. (2000). The NIST Model for Role Based Access Control. ACM workshop on Role-based access control, 10(344287.344301). Retrieved from https://www.researchgate.net/profile/David-Ferraiolo/publication/2624207_The_NIST_model_for_role-based_access_control/links/5411a7240cf264cee28b4b31/The-NIST-model-for-role-based-access-control.pdf

ENGINE

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

FitzPatrick, G., & Wollman, D. (2010). NIST interoperability framework and action plans. IEEE PES General Meeting, 1-4. Retrieved from https://ieeexplore.ieee.org/abstract/document/5589699

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1). Retrieved from https://watermark.silverchair.com/tyaa005.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAtcwggLTBgkqhkiG9w0BBwagggLEMIICwAIBADCCArkGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMT_1cd_j7vhOj6I1aAgEQgIICii9reG4j7dGdJPEsfscIRjgr40v14cJdGnZxu2bhrJbLAoj

Greer, C., Wollman, D., Prochaska, D., Boynton, P., Mazer, J., Nguyen, C., . . . Pillitteri, V. (2014). Nist framework and roadmap for smart grid interoperability standards. Tratto il giorno Jan. 05, 2022 da https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30?pub_id=916755

Magonara, E., & Górniak, S. (2022). 5G cybersecurity standards-Analysis of standardisation requirements in support of cybersecurity policy. Athens: European Union Agency for Cybersecurity (ENISA).

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 1-3.

Scofield, M. (2016). Benefiting from the NIST cybersecurity framework. Information Management, 50(2), 25.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int' l L. J., 50, 305. Retrieved from https://spacesecurity.wse.jhu.edu/wp-content/uploads/2021/09/ssrn-id2446631.pdf

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4), 16. Retrieved from https://spacesecurity.wse.jhu.edu/wp-content/uploads/2021/09/ssrn-id2446631.pdf

Chapter 3

Secured Business Habits

ENGINE

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

SECURED BUSINESS HABITS
PHYSICAL & VIRTUAL SECURITY ASPECTS

ENGINE

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

Businesses need to protect themselves from damaging unpredictable cyberattacks, which often may threaten internal security. In order to do that they should strengthen and follow various prevention measures, starting from Physical Security Aspects.
Safety habits need to originate from individuals and controlled spaces, this means that Companies should train and educate employees to raise their awareness about risks and security such as keeping their devices secured or never leaving their desk without logging off from the device.
Then Companies should opt for better security, for examples use Cloud-Managed Camera System instead of IP Cameras, or authorize office-purpose devices only because regular security checks can easily be scheduled on those. Visitors Management Policy is also important to always identify visitors and to always keep track of employee position through badges.
In terms of Virtual Security Aspects, the place to start is the installation of Antivirus Softwares to prevent Endpoint attacks. There are several threats and consequences caused by attacks such as systems infected by viruses, downloaded malware or hackers installing malicious software.
Company should also have a well-organized and updated Backup Strategy to ensure no data losses and to have access to them whenever is necessary (3 copies of backup).
Then Disk Encryption is an useful security measure to protect Company sensitive information, passwords and encryption keys from hacking, together with Next-Generation Firewalls (NGFWs) which are designed to protect against more complex threats by adding additional layers of security and are capable of controlling applications at the application level, rather than simply static inspection as traditional firewalls do.
Similar to NGFWs there is DNS that is able to prevent malicious infection to the Company's devices.
URL Filtering is a common and successful method used by the organization to prevent their employees from visiting malicious, spammy or phishing pages.
Speaking of privacy protection there are numerous measures that Companies must adopt such as VPN which may prevent hackers from intercepting your internet traffic and stealing information protecting privacy with encryption methods, or Two Factor Authentication (2FA) which may help to notify of unauthorized presences, or DLP security tools to take control of emails, instant messages, applications downloaded and web browsing.
In addition, it is recommended to apply strong password criteria as well as changing password frequently, to secure remote access is to limit it to internal devices only and to secure business
Wi-Fi in a location where no one could have access the router physically.

SUMMARIES IN ITALIAN
RIASSUNTI IN ITALIANO

ENGINE

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

Sicurezza aziendale-Aspetti di sicurezza fisica e virtuale (The Hive)

Le aziende devono proteggersi dai cyber attacchi, imprevedibili e dannosi, che spesso minacciano la sicurezza interna. Per farlo è necessario seguire e rafforzare le misure di sicurezza, partendo proprio dalla Sicurezza Fisica.

Le abitudini sulla sicurezza devono avere origine dalle persone e dalle aree sorvegliate, ciò significa che le aziende dovrebbero in primo luogo impartire una formazione per i propri impiegati per sensibilizzarli sulla sicurezza stessa e sugli eventuali rischi. Ad esempio non lasciare incustoditi i propri dispositivi o non lasciare la postazione senza prima aver effettuato il log out.

In secondo luogo le aziende dovrebbero adottare i dispositivi e le misure di sicurezza migliori come, ad esempio, l'utilizzo di telecamere che registrino nel Cloud anziché le telecamere a sistema IP o fornire ai propri dipendenti dispositivi aziendali così da poter effettuare verifiche di sicurezza frequenti. Per le aziende può essere importante anche un Regolamento per i visitatori così da poterli identificare e l'utilizzo dei badge per monitorare gli accessi dei propri dipendenti.

In quanto a Sicurezza Virtuale, il punto di partenza dovrebbe essere l'istallazione di Antivirus così da prevenire cyber attacchi di Endpoint. I cyber attacchi possono essere causa di molte minacce, ad esempio virus che infettano sistemi informatici, il download di malware o l'installazione, per mano degli hacker, di software dannosi.

Anche per questa ragione le imprese dovrebbero disporre di un sistema di Backup ben organizzato e frequentemente aggiornato, per scongiurare eventuali perdite di dati e per accedervi ogni qual volta ne sia necessario (sono consigliate 3 copie di backup).

Dovrebbero, inoltre, disporre di un Disco Crittografato in quanto può risultare utile alla protezione delle informazioni sensibili, delle password e delle chiavi di crittografia dell'azienda. In aggiunta sono funzionali i Firewall di Nuova Generazione (NGFWs), progettati per la protezione dei sistemi da minacce più consistenti attraverso la presenza di molteplici livelli di sicurezza e programmati per controllare le applicazioni dall'interno al contrario dei soli controlli statistici effettuati dai Firewall tradizionali.

In maniera analoga anche i Firewall DNS hanno la capacità di prevenire la diffusione di virus nei dispositivi aziendali. Mentre i filtri URL sono un metodo efficace per impedire ai dipendenti di visitare pagine infette.

Parlando di protezione della privacy, vi sono diverse misure di sicurezza che le aziende devono adottare, ad esempio la VPN, la rete virtuale privata, che può ostacolare gli hacker nell'intercettare il traffico internet e al furto di informazioni proteggendo così la privacy degli utenti.

Oltre a ciò è consigliabile l'Autenticazione a Due Fattori (2FA) per la notifica di utenti non autorizzati o la sicurezza DLP per il controllo di email, messaggi istantanei, download di applicazioni e dei browser. Infine è consigliabile rafforzare i criteri di generazione delle password così come un continuo cambio delle stesse; l'autorizzazione dell'accesso remoto solo ai dispositivi interni; o collocare il router del WiFi aziendale in un luogo protetto che ne evita l'accesso fisico.

Legge, politica e conformità informatica (Luigi Clerici)

Questo modulo copre i principali Standard in materia di Cyber Security, affrontando normative, standard, leggi e certificazioni applicabili a qualsiasi tipo di azienda, concentrandosi, ove applicabile, sulle Piccole e Medie Imprese (PMI).

Nella prima parte si concentra sulla famiglia di standard ISO/IEC 27000, ovvero una serie di best practices che mirano ad aiutare le organizzazioni a migliorare la sicurezza delle informazioni. Pubblicata da ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), la serie spiega come implementare le migliori pratiche di sicurezza delle informazioni: sono descritti i requisiti ISMS (sistema di gestione della sicurezza delle informazioni). Un ISMS è un approccio sistematico alla gestione del rischio, contenente misure che affrontano i tre pilastri della sicurezza delle informazioni: persone, processi e tecnologia. La serie è composta da 46 singoli standard; non c'è bisogno di conoscerli tutti, anche considerando che alcuni non saranno rilevanti per la tua organizzazione, ma ce ne sono alcuni di base che, in generale, le PMI dovrebbero conoscere e che saranno trattati in questo documento:

- ISO 27001
- ISO 27002
- ISO/IEC 27005:2018
- ISO 27017 e ISO 27018
- ISO 27701

Il modulo spiega anche il Regolamento generale sulla protezione dei dati (GDPR), che è una legge emanata dall'UE principalmente per proteggere la privacy dei dati e che è abbastanza importante per aziende di tutte le dimensioni poiché il regolamento si applica a tutte le organizzazioni che trattano i dati personali dei residenti nell'UE , siano essi ditte individuali, piccole imprese o conglomerati. Impone obblighi alle organizzazioni ovunque, a condizione che prendano di mira o raccolgano dati relativi a persone nell'UE. Il GDPR definisce una serie di termini legali e delinea sette principi di protezione e responsabilità che devono essere seguiti durante l'elaborazione dei dati. Inoltre, spiega come un'azienda può dimostrare di essere conforme al GDPR, come può garantire la sicurezza dei dati e quando un'azienda può elaborare i dati. Il GDPR illustra anche le nuove regole su ciò che costituisce il consenso di un interessato al trattamento delle proprie informazioni ed evidenzia le tre condizioni in base alle quali è necessario nominare un responsabile della protezione dei dati.
Altri framework presentati in questo modulo sono:

- Obiettivi di controllo per le tecnologie dell'informazione e correlate (COBIT), che è un framework per la governance e la gestione dell'IT.
- La IT Infrastructure Library (ITIL) mira a migliorare i controlli per la gestione dei servizi.
- Il Committee of Sponsoring Organizations of the Treadway Commission (COSO) è un framework che fornisce una serie di linee guida sulla gestione del rischio d'impresa, il controllo interno e la deterrenza contro le frodi.
- Gli orientamenti per la sicurezza delle reti e dell'informazione (NIS) sono finalizzati a rafforzare la sicurezza informatica in tutta l'UE.

Infine, questo modulo fornisce una panoramica sulle Certificazioni di sicurezza informatica (per privati) poiché al giorno d'oggi sono sempre più necessari professionisti con un forte background in sicurezza informatica.

LIST OF CYBERSECURITY ACTIONS

ENGINE

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

T.8 LIST OF CYBERSECURITY ACTIONS IN CASE OF AN ATTACK

- **Antivirus Software**: softwares to prevent End-Point Attacks
- **Disk encryption for Device Protection**: prevent hacking from getting access to company data
- **Frequent backups**: setup company strategy to avoid data losses
- **Next-Generation Firewall**: useful to detect and block sophisticated attacks by applying security policies at the application, port and protocol levels
- **Use DNS Servers**
- **Use of VPN**: it protects company navigation system and connection with encryption methods. Data that is sent over a WiFi connection is scrambled, making it impossible for hackers to intercept it.
- **URL filtering**: company policy to create a database of permitted websites; all sites that are out of the database are blocked to prevent employees from visiting malicious, scammy or phishing pages.
- **Two-Factor Authentication**: company IT system protection trough authentication methods that can be attached with employees' mobile number or email
- **Data Leak Protection (DLP)**
- **Safe password Enforcement**: establish a strategy to create strong passwords and planning periodical passwords changes
- **Securing remote access to internal devices**
- **Secure the wifi**: secure physical location and credentials protection strategy
- **Session timeouts**: technique used by businesses to set up a certain amount of time after which, without any activity, internal devices automatically log out

SKILL SET

ENGINE

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

T.5 SKILL-SET

●risks and security awareness: how to keep devices and workstations secured

●acquisition of competences on digital technology for cyber attack prevention: e.g. Cloud-Managed Camera System, Antivirus Softwares to prevent Endpoint attacks, DNS servers, VPN, URL filtering

●earning best practices to implement company security: e.g. planned backups, Visitors Management Policy, advanced password management, use of office-purpose devices only, Wi-fi protection

ADDITIONAL MATERIAL

ENGINE

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

PHYSICAL SECURITY

- **The importance of physical security in the workplace**: https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/

- **Ultimate Guide to Physical Security-A guide to getting started with access control; Kisi** (PDF)

- **Physical Security: Key Considerations for Remote and Office-Based Employees:** https://www.dhg.com/article/physical-security-key-considerations-for-remote-and-office-based-employees

- **Security in the Workplace - Informational Material:** https://www.dm.usda.gov/physicalsecurity/workplace.htm

- **What is physical security? Understanding workplace safety:** https://www.sine.co/blog/what-is-physical-security-understanding-workplace-safety/

- **Guide to Physical Security in the Workplace, Openpath; 2020** (PDF)

- **7 Office Security Measures to Keep Your Workplace Safe:** https://attorneyatlawmagazine.com/7-office-security-measures-to-keep-your-workplace-safe

- **Protect Your Workplace; Homeland Security** (PDF)

- **Workplace Physical Security Is an Essential Component of Cybersecurity: 11 Ways to Better Protect People, Devices, and Data:** https://www.idwatchdog.com/physical-security-leads-to-cybersecurity/

- **Top 5 Physical Security Risks - And How to Protect Your Business:** https://blog.usecure.io/physical-security-risks

- **What is physical security? How to keep your facilities and devices safe from on-site attackers:** https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html

- **10 Surprising Security Risks Inside Your Office:** https://www.softwareone.com/en/blog/all-articles/2021/02/08/10-security-risks-in-your-office

- **Physical security; Homeland Security** (PDF)

- **Why Cybersecurity In The Workplace Is Everyone's Responsibility:** https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility

- **Information security Manual; Australian Cyber Security Centre; 2022** (PDF)

VIRTUAL SECURITY

- **5 tips to strengthen the cybersecurity of your virtual office:** https://blog.hushmail.com/blog/5-tips-to-strengthen-the-cybersecurity-of-your-virtual-office

- **Cybersecurity Guidelines; IBA's Presidential Task Force on Cybersecurity; 2018** (PDF)

- **Cybersecurity 101-A guide for SMBs; IT GOVERNANCE USA GREEN PAPER; 2021** (PDF)

- Cybersecurity Management Guidelines Ver. 2.0; Ministry of Economy, Trade and Industry (METI) and Information-technology Promotion Agency, Japan (IPA) (PDF)

- **Cyber Security Guidelines:** https://www.cyber.gov.au/acsc/view-all-content/ism/cyber-security-guidelines

Chapter 4

Cyber Law, Policy and Compliance

ENGINE

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

SUMMARY
CHAPTER 4

ENGINE

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

Cyber Law, Policy and Compliance

This module covers the major Standards concerning Cyber Security, dealing with applicable regulations, standards, laws and certifications that are relevant to any kind of Company, focusing, where applicable, on Small and Medium Enterprises (SMEs).

It focuses in the first part on the ISO/IEC 27000 family of standards which is a series of best practices that aims at helping organizations improve their information security. Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices: ISMS (information security management system) requirements are described. An ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology. The series consists of 46 individual standards; there is no need to know all of them, also considering that some won't be relevant to your organization, but there are a few core ones that, in general, SMEs should be familiar with and that will be covered in this document:

- ISO 27001
- ISO 27002
- ISO/IEC 27005:2018
- ISO 27017 and ISO 27018
- ISO 27701

The Module also explains the General Data Protection Regulation (GDPR), which is a law made by EU mainly to protect data privacy and which is quite important for all sizes of companies due to the fact that the Regulation applies to all organisations that process EU residents' personal data, whether they are sole traders, small businesses or conglomerates. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The GDPR defines an array of legal terms and outlines seven protection and accountability principles which need to be followed when processing data. Moreover, it explains how a company can demonstrate to be GDPR compliant, how it can ensure data security and when a company is allowed to process data. The GDPR also demonstrates the new rules about what constitutes consent from a data subject to process their information and highlights the three

conditions under which it is required to appoint a Data Protection Officer.

Other frameworks presented in this module are:

- Control Objectives for Information and Related Technology (COBIT) which is a framework for IT governance and management.
- The IT Infrastructure Library (ITIL) aims to improve controls for service management.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a framework that provides set of guidance on enterprise risk management, internal control and fraud deterrence.
- Network and Information Security (NIS) guidelines are finalized to enhance cybersecurity across the EU.

Finally, this module provides an overview on IT security Certifications (for individuals) due to the fact that professionals with a strong background in IT Security are more and more needed nowadays.

CYBERSECURITY ACTIONS
CHAPTER 4

ENGINE

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

List of cybersecurity actions to prevent an attack/necessary in case of an attack

- **Integration of cybersecurity into the organization's strategic objectives and ensuring that cyber security roles are defined within the organizational structure.**
- **Familiarization with ISO/IEC 27000 family of standards which is a series of best practices which aims at helping organizations improve their information security. Especially:**
  - ISO 27001
  - ISO 27002
  - ISO/IEC 27005:2018
  - ISO 27017 and ISO 27018
  - ISO 27701
- **Implementation of a management system compliant with ISO/IEC 27701 and ISO/IEC 27001 in order to meet the privacy and information security requirements set forth in GDPR as well as other data protection regulations.**
- **Consultation of Annex A of ISO 27001 because it provides an essential tool for managing information security risks**
  - Information security policies – controls on how the policies are written and reviewed
  - Organization of information security – controls on how the responsibilities are assigned; includes the controls for mobile devices and teleworking
  - Human resources security – controls prior, during and after employment
  - Asset management – controls related to inventory of assets and acceptable use
  - Access control – controls for the management of access rights of users, systems and applications, and for the management of user responsibilities
  - Cryptography – controls related to encryption and key management
  - Physical and environmental security – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.
  - Operational security –controls related to the management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
  - Communications security – controls related to network **security,** segregation, network services, transfer of information, messaging, etc.
  - System acquisition, development and maintenance – controls defining security requirements, and security in development and support processes
  - Supplier relationships – controls on what to include in agreements, and how to monitor the suppliers

- Information security incident management – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- Information security aspects of business continuity management – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- Compliance – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

- **Making sure to be GDPR compliant: protection principles must be implemented in the design of any new product or activity.**
  - Requirement to handle data securely by implementing "appropriate technical and organizational measures as stated in the GDPR regulations.
  - Requirement to have in place organizational measures like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.
  - Processing of data only when having the legal basis to do so and by documenting this basis and notifying the data subject (transparency!)
  - Following of the consent rules.
  - Checking if there is a need for data protection officer
  - Important: Every company has to comply with GDPR, as it is managing employee's personal data.
  - Keeping records of data processing
  - In case of a data breach, there are 72 hours to tell the data subjects or face penalties.

SET OF COMPETENCES
CHAPTER 4

ENGINE

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

SET of Competences for Chapter 4

- Basic knowledge on the most important ISO 27000 series Standards: ISO 27001, ISO 27002, ISO/IEC 27005:2018, ISO 27017 and ISO 27018, ISO 27701
- Basic knowledge on the legal terms of General Data Protection Regulation (GDPR)
- Basic knowledge on the different requirements of GDPR
- Basic knowledge on the application of measures to meet data privacy compliance requirements
- Basic understanding the COBIT Framework
- Basic understanding of the ITIL Framework
- Basic understanding of the COSO Framework
- Basic Understanding the NIS Framework
- Knowledge on the most common ICT Certifications

ADDITIONAL MATERIAL
CHAPTER 4

ENGINE

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

- 10 Critical Steps to GDPR for SMEs
  https://www.ecomply.io/blog-en/10-critical-steps-to-general-data-protection-regulation-gdpr-for-smes#:~:text=GDPR%20requires%20you%20to%20maintain,refers%20to%20an%20identifiable%20person.

- Rules for the protection of personal data inside and outside the EU.
  https://ec.europa.eu/info/law/law-topic/data-protection_en

- SUPPORT SMALL AND MEDIUM ENTERPRISE Report on the SME experience of the GDPR
  https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

- Martin Brodin A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises

- GDPR Information material for SMEs
  https://www.consumerlawready.eu/sites/default/files/2021-06/GDPR%20-%20Information%20Material%20for%20SMEs.pdf

- ISO/IEC STANDARD 27001
  https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001

- Cybersecurity Standards and Certification
  https://www.enisa.europa.eu/topics/standards

- COBIT adoption in Europe
  https://www.itgovernance.eu/it-it/cobit-adoption-in-europe-it

- Iso 2019 IEC, ISO and information communication technology (PDF)

Video

- GDPR 3 years on: Experiences and challenges of the European SMEs. Awareness raising campaign for SMEs
  https://www.youtube.com/watch?v=G7aIsgJjJI8

Chapter 5

Blockchain and Cryptocurrency Technologies

ENGINE

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

SHORT SUMMARY
CHAPTER 5

ENGINE

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

Chapter 5: Blockchain and Cryptocurrency Technologies

This chapter gives a gentle, conceptual and honest introduction to blockchain technology. Gentle means that the seminar is targeted to non experts. Conceptual means the focus will be on key concepts instead of technicalities or one specific blockchain platform. Honest refers to the fact that the chapter is not the (usual) enthusiastic business presentation about blockchain, but it also highlights misconceptions and dispel some common myths about blockchain. The main objective is to provide a high-level understanding of blockchain technology and explore its role in the foundation of modern cryptocurrencies.

In the first part of the chapter, we will introduce some cryptographic primitives and their security properties that are necessary for building cryptocurrencies. In particular, we will discuss the essential concepts of cryptographic hash functions, blockchain data structures, and digital signatures.

The second part shows how the cryptographic primitives, such as hash functions and digital signatures, can be combined to construct very simple cryptocurrencies. To this end, we present the steps for designing two simple digital cash: GoofyCoin and ScroogeCoin.

The third part of the chapter addresses some fundamental aspects of Bitcoin, such as decentralization, distributed consensus models, and security considerations. In addition, we provide a broad overview of blockchain architectures highlighting the characteristics and challenges of both permissioned and permissionless blockchains.

The chapter concludes with a list of limitations and misconceptions about blockchain, separating myth from reality.

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

IMPORTANT ASPECTS OF CS
CHAPTER 5

ENGINE

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

- **Data integrity:** *Blockchain provides a secure and efficient way to create a tamper-proof log, storing immutable and permanent transactions which cannot be altered or deleted. In blockchain, changes made to the already recorded data are processed as new transactions. In this way, the immutability of blockchain guarantees the integrity of data stored in blockchain transactions.*

- **Data transparency and traceability:** *All the historical transactions stored in the blockchain are digitally signed and time-stamped, so network users can easily trace the history of transactions and track accounts at any historical moment.*

- **Availability:** *The large number of nodes ensures the blockchain resilience even when some nodes are unavailable. In addition, each node in the network has a copy of the distributed ledger. Thus, the correct blockchain remains accessible to other peers even when a node gets compromised.*

- **User confidentiality:** *User keys are the only link between a user and their data in the blockchain. User keys, on the other hand, are simple to anonymize. Some networks, such as zk-SNARK and zk-STARK, use zero-knowledge proofs to maximize user confidentiality. As a result, users can preserve their anonymity with blockchain.*

SET OF SKILLS
CHAPTER 5

ENGINE

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

- **Blockchain technology:** You will learn about the essential concepts of blockchain technology starting from basic components of a blockchain such as transaction, block, block header, and the chain. In addition, you will get a broad overview of the decentralized peer-to-peer network, blockchain architectures and the underlying consensus algorithms.

- **Cryptographic primitives:** You will be introduced to the basic concepts of cryptographic hash functions, blockchain data structures, and digital signatures.

- **Cryptocurrency principles*:*** You will be prepared to design very simple cryptocurrencies, namely, GoofyCoin and ScroogeCoin.

- **Bitcoin:** You will discover the aspects of decentralization in Bitcoin and Bitcoin consensus algorithm.

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

ADDITIONAL MATERIALS
CHAPTER 5

ENGINE

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

- Website blockchain.info
- Blockchain Technology Overview - NISTIR 8202 https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
- Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction-A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, Princeton University Press, 2016
- Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
- Paxos Made Simple, Leslie Lamport https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/paxos-simple-Copy.pdf

ENGINE

Guideline to implement cybersecurity in SMEs

Funded by the Erasmus+ Programme of the European Union

This project is funded by the European Union ERASMUS+ Program
Key Action 2 Cooperation for innovation and the exchange of good practices.
Project Reference: 2020-1-DK01-KA202-075161