Cybersecurity Optimization and Training for Enhanced Resilience in Finance

D5.1 – Standardized system to security incidences handling and monitoring

[WP5 – Cybersecurity standard whitepaper for present and future threats in finance]

Contributors

Eliseo Venegas Mayoral (EVR)
Jose Manuel Panizo (FNMT)
Paul Rabel (University of Graz)
Robin Renwick (TRI IE)
Martin Griesbacher (RISE)
Nora Schreier (University of Graz)

Due Date	31.07.2021
Delivery Date	30.07.2021
Type	Report
Dissemination level	PU = Public

Keywords	SOTER, cybersecurity, security

Document History

Version	Date	Description	Reason for Change	Distribution
V01r00	26.02.2020	Draft	Initial draft	26.02.2020
V01r01	15.07.2020	Version	Inputs from all partners	15.07.2020
V01r02	25.09.2020	Version	Inputs from all partners	25.09.2020
V01r03	03.11.2020	Version	Inputs from all partners	03.11.2020
V01r04	05.01.2021	Version	Inputs from all partners	05.01.2021
V01r05	25.01.2020	Version	Inputs from all partners	25.01.2021
V01r06	02.02.2020	Version	Inputs from all partners	02.02.2021
V01r07	19.02.2021	Version	Inputs from all partners	19.02.2021
V01r08	10.03.2021	Version	Inputs from all partners	10.03.2021
V01r09	12.03.2021	Version	Input regarding NIS transposition	12.03.2021
V01r10	12.03.2021	Version	Restructuring	12.03.2021
V01r11	22.03.2021	Version	Input from UNIGRAZ	22.03.2021
V01r12	29.04.2021	Version	Input from UNIGRAZ	29.04.2021
V01r13	07.05.2021	Version	Revise Structure	07.05.2021
V01r14	11.05.2021	Version	Revise Structure post meeting	11.05.2021
V01r15	14.05.2021	Version	Revise Structure in meeting	14.05.2021
V01r16	14.05.2021	Version	Circulate new structure	14.05.2021
V01r17	26.05.2021	Version	New structure circulated by RISE	26.05.2021
V01r18	27.05.2021	Version	Input from UNIGRAZ	27.05.2021
V01r19	28.05.2021	Version	Input from TRI	28.05.2021
V01r20	10.06.2021	Version	Input from UNIGRAZ	10.06.2021
V01r21	25.06.2021	Version	Input from EVR	25.06.2021
V01r22	28.06.2021	Version	Input from EVR	28.06.2021
V01r23	30.06.2021	Version	Input from all partners	30.06.2021

V01r24	02.07.2021	Version	Input from UNIGRAZ	08.07.2021
V01r25	08.07.2021	Version	Final restructuring, input RISE	08.07.2021
V01r26	09.07.20251	Version	Input from UNIGRAZ	09.07.2021
v01r27	12.07.2021	Version	Input from RISE	12.07.2021
V01r28	15.07.2021	Version	Input from all partners	15.07.2021
v01r29	22.07.2021	Version	Input from TRI	22.07.2021
V01r30	23.07.2021	Version	Input from all partners	23.07.2021
V01r31	29.07.2021	Version	Finalize Executive Summary	29.07.2021
V02r00	30.07.2021	Version	Format review	30.07.2021

Abstract

SOTER is a European Commission H2020 funded project, entitled *'cyberSecurity Optimization and Training for Enhanced Resilience in finance'* (SOTER). This deliverable is part of WP5 and is entitled 'Cybersecurity standard whitepaper for present and future threats in finance'. In summary, the following deliverable provides an overview of standards, guidelines and best practice that exist currently within the financial services sector, with primary focus on the European landscape, but supplemented with best practice and standards from further afield. There is a focus on the human factor-based aspects of cybersecurity (esp. On training and awareness), as well as crucial components of best practice security incident managing and reporting within the European Union. The document also provides an overview of existing threat taxonomies and how they can be integrated into developing best practice, recommendations for threat mitigation and incidence response.

Table of Contents

Executive Summary

SOTER is a European Commission H2020 funded project, entitled *'cyberSecurity Optimization and Training for Enhanced Resilience in finance'* (SOTER), Grant Agreement No. 833923 This deliverable is contained within WP5 and is entitled *D5.1 - Cybersecurity standard whitepaper for present and future threats in finance*.

The objective of the deliverable is to identify and analyse current standards, guidelines, best practices and recommendations regarding cybersecurity in the finance sector. The document details the current landscape from mainly a European environment, supplemented with international best practice. The document focuses on technical aspects, and more specifically security governance and incident handling. This information is also supported by aspects related to the human factor elements of cybersecurity (esp. In regard to training and awareness). Following this, the deliverable aims to identify the predominant sector specific cybersecurity threats and incidents. This deliverable establish the basis on which deliverable *D5.2 - White Paper on Cybersecurity standards* is built.

The deliverable first presents an introduction chapter, which provides some detail on the SOTER project, and situates this deliverable in relation to related deliverables in the project. It explains that the core focus of the project relates to three core strands of cybersecurity:

- Governance
- Risk management
- Compliance

Chapter two provides an overview of existing European cybersecurity regulation. It outlines the cybersecurity regulatory framework that acts as the legislative base for the finance sector. It details the most relevant regulatory acts as:

- Directive on Security and Network and Information Systems (NIS Directive) – Directive (EU) 2016/1148
- Payments Services Directive (PSD 2) – Directive (EU) 2015/2366
- General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679
- eIDAS Regulation – Regulation (EU) 910/2014

Each of these regulatory acts oblige finance sector organizations to adhere to a set of rules or principles, which are viewed as integral to secure the critical sector of finance. In support of these regulatory acts are a number of European bodies. They act as sector regulators or

provide sector specific guidance aspects deemed integral to the proper functioning of the sector. These bodies are identified as:

- European Banking Authority
- European Central Bank
- European Union Agency for Cybersecurity

Chapter three provides an overview of the standards, guidelines, and recommendations for the finance sector, both mandatory and non-mandatory. There are three main sources:

- General requirements in the cybersecurity domain, which can include both mandatory and non-mandatory best-practice standards, certification processes, and solutions (e.g., ISO/IEC 27001).
- Requirements directly targeted at financial institutions, relevant for compliance in specific jurisdictions. (e.g., EBA Guidelines on ICT and security risk management).
- Recommendations from European (interdisciplinary) research for the development and implementation of trustworthy ICT products, services, and processes.

The chapter also provides detailed information on the human factor aspects of cybersecurity, detailing a number of recommendations drawn from both European and international bodies, as well as international accepted standards, such as those detailed by the International Standards Organization. This includes information on:

- European Banking Authority Guidelines
    - Information security policy
    - Information security training and awareness
- International Standards Organization
    - Education and determination of competence
    - Cybersecurity Awareness and training
    - Recruitment strategies
    - Management involvement
- European Union Agency for Cybersecurity
    - Cybersecurity skills development
    - Cybersecurity culture
    - Cybersecurity behaviours
- North Atlantic Treaty Organization

    - Human systems integration approach
- United States Department of Defence
    - Insider threat mitigation strategies

Chapter four aims to define a threat landscape focusing on major technical threats, main security incidents in the financial sector and relevant human factor threats, covering some relevant examples that give context to the threats identified as relevant for the financial sector. The predominant threats are summarised as:

- Malware: Web Application attacks and malicious code injection, local file inclusion and cross-site scripting.
- Intentional attacks: DDoS
- Vulnerability exploitation: Backdoors and supply-chain attacks, including vulnerabilities derived from emerging technologies.
- External party risk and external service providers.
- Global Operational Risks: Chances a company faces in the course of conducting its daily business activities, procedures, and systems.
- Social engineering, including insider threats and phishing.

The chapter also provides information on two of the most relevant threat taxonomies for the finance sector. The first developed by ENISA, and the second entitled the Common Attack Pattern Enumeration and Classification (CAPEC™). The discussion focusses also on how to identify human factor related threats in existing taxonomies (as they are important for general awareness and trainings) und which threats are currently dominant in the finance sector.

Chapter 5 summarizes the key points from all chapters and gives a conclusion and outlook on the current regulatory and best practice challenges for institutions in the finance sector. The interplay of regulations and standards is here a special concern, as relevant regulatory texts and guidelines from the EBA expect financial organisations to follow state of the art practices, which can normally be found in the leading standards (esp. ISO27000 family). Cybersecurity governance in the finance sector includes an extended information security management procedures and practices, incident prevention and mitigation and management of incidents (incl. Cataloguing and prioritization). Main activity aspects here are also IT operations management, identity and access management, IT asset monitoring and security information and event management, vendor and third-party management, data classification and retention, incident response procedures and continuity planning.

Additionally, regulation and standards require regular training and awareness programs, which should tackle human error, theft, fraud and misuse or loss on all levels of the organisation (incl. management, contractors and also to a limited extend customers). Competence of staff should be determined, improved and documented, according to leading standards. For this domain, the document suggests to continue the work on classification of human factor-related threats by reviewing and integrating elements from a broad range of leading threat taxonomies. Work on this will continue in D5.2.

List of Tables

List of Figures

List of Acronyms/Abbreviations

Abbreviation	Explanation
APIs	Application Programming Interfaces
APTs	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPEC	Common Attack Pattern Enumeration and Classification
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incidence Response Team
DDoS	Distributed Denial of Service
DOP	Digital Onboarding Platform
DPIA	Data Protection Impact Assessment
EBA	European Banking Authority
ECB	European Central Bank
eID	electronic identification
eIDAS	Regulation on electronic Identification, Authentication and trust Services
ENISA	European Union Agency for Cybersecurity
ENS	Esquema Nacional de Seguridad
eTS	electronic Trust Services
ETSI	European Telecommunications Standards Institute

EU	European Union
EVERIS	Everis Spain S.L.U.
FNMT	Fábrica Nacional de Moneda y Timbre
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Compliance
ICT	Information and Communications Technology
INCIBE	Instituto Nacional de CIBERseguridad
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NIS D	Directive on Security and Network and Information Systems
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services according to the NIS Directive
ÖNORM	Österreichische Norm
PCI DSS	Payment Card Industry Data Security Standard
PSD2	Payments Services Directive
PSP	Payment Service Providers
RISE	Research Industrial Systems Engineering GmbH
SANS	SysAdmin Audit, Networking and Security Institute
SOTER	Cybersecurity Optimization and Training for Enhanced Resilience in Finance
SP	Special Publication
TPP(s)	Third Party Provider(s) according to PSD2
TRI IE	Trilateral Research Limited
UNE	Una Norma Española
UNIGRAZ	University of Graz
WP	Work Package

Table 1. List of Acronyms/Abbreviations

1 Introduction

This deliverable is primarily focused on two main aspects of cybersecurity governance. It provides an overview of relevant regulations, standards, guidelines, and best practices for:

- Incident handling
- Human factor-related cybersecurity governance (esp. in regard to training and awareness).

The deliverable will discuss specific requirements of financial sector organizations and provide a grounding of the current landscape of legal requirements, standards and guidelines, ultimately providing the basis for good cybersecurity governance, risk mitigation and compliance in the sector.

1.1 Purpose of the deliverable

This report represents *D5.1 - Standardized system to security incidences handling and monitoring* [M25], of the SOTER project. It provides an overview of standardisation activities relevant to the SOTER project, as well as an overview of cybersecurity related threats that European companies in the finance sector face. The deliverable also provides a section on best practice regarding security incidence handling – a key consideration in the development of SOTER Digital Onboarding Platform (DOP).

The SOTER project, and also, this deliverable, is quite related to the cybersecurity area of GRC[1] (Governance, Risk Management and Compliance with regulations), which is a combined area focused on cover the organization's strategy to handle any interdependencies between the three components and to align IT with business objectives while effectively managing risk and meeting compliance and regulatory specific requirements that affect the organization and related systems.

Governance[2] is related to the organization strategy required to achieve its goals in a secure way by implementing guidelines, policies and procedures.

---

[1] https://www.researchgate.net/publication/220921351_A_Conceptual_Model_for_Integrated_Governance_Risk_and_Compliance, accessed 2021-07-26.

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, accessed 2021-07-26.

Risk management[3] is the procedure to identify, evaluate, analyse, treat, monitor and improve the risk related to an organization's system and activities.

Compliance[4] is the verification that the activities which the organisation are conducting in conformity with the regulations, directives and laws specifically applicable to its sector or are voluntary requirements that the organisation chooses to comply with.

1.2 Scope of this deliverable

The deliverable presented provides a guideline for security incident managing and reporting in EU, as well as standardisation work in cybersecurity focusing on the human aspects.

The main objective of the deliverable is to map formal and informal standards relevant to cybersecurity:

- Incident handling recommendations, according to European regulation.
- Standards and best practices in security industry to address risks.
- Analysis of the actions that should be taken reviewing past attacks.
- Recommendations developed from top risks that threaten European companies in the finance sector.

1.3 Structure of this deliverable

This deliverable contains five sections:

1. Introduction, including scope and structure of this deliverable.
2. A review of existing European regulations concerned with incidence handling and human factor related aspects (esp. awareness and training).
3. An analysis of best practices within the security industry.
4. An overview of known security incidents within the finance sector.
5. A conclusion section that summarises the document.

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, accessed 2021-07-26.

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf, accessed 2021-07-26.

2 Incident handling, awareness and training – existing European regulation

This chapter provides an overview of the existing security incidence handling regulatory framework, focusing on existing European frameworks, national bodies related to incident handling in Europe and analysing legal requirements for awareness and training.

2.1 Introduction

In the field of information security, security incident handling involves the monitoring and detection of security events on any IT infrastructure element, and the execution of proper responses to those events. Computer security incident handling is a specialized form of incident management, with the objective of development a well understood and predictable response to damaging events and other intrusions that may affect to an entity with economic, reputational, or operational consequences.[5]

An information security incident is any unplanned event, which can result in:

- Personal data breaches
- Physical security incidents
- Business continuity incidents

2.2 List of applicable regulatory acts regarding incident handling and monitoring

At the European Union level, regulatory acts relevant to security incident handling and monitoring have been issued both in the form of directly applicable Regulations[6] and in the form of Directives, which are addressed to the Member States and require transposition into national law.[7] Based on European Union secondary law, delegated or implementing acts may have been issued by the Commission, which further specify European Union secondary acts and are generally applicable in the Member States.[8]

[5] ISO 17799|ISO/IEC 17799:2005(E). Information technology - Security techniques - Code of practice for information security management. ISO copyright office. 2005-06-15. pp. 90–94.

[6] Art 288 (2) TFEU.

[7] Art 288 (3) TFEU.

[8] Craig, Delegated Acts, Implementing Acts and the New Comitology Regulation, European Law Review 2011, 671 (672).

In addition to these strictly legally binding acts, there are other relevant regulatory actions: Guidelines by the European Banking Authority (EBA), are not legally binding in the strict sense, but are effective due to their "comply-or-explain" methodology[9], and the guidelines' understanding of the respective subject matter may overtime feed into the development of legal practice and future regulatory efforts.[10] International, European and National Standards are very important in regard to determining the "state of the art" of certain incident handling schemes. They thus have certain legal implications in creating a presumption of conformity and facilitating the proof that incident handling procedures have been introduced in observance of the state of the art.[11] These guidelines, standards and recommendations will be discussed in chapter 3.

Regarding security incident handling and monitoring, European Union regulations and directives most relevant for the financial sector are:

- Directive on Security and Network and Information Systems (NIS Directive) – Directive (EU) 2016/1148
- Payments Services Directive (PSD 2) – Directive (EU) 2015/2366
- General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679
- eIDAS Regulation – Regulation (EU) 910/2014

2.2.1 European legislation

Regarding the regulatory efforts concerning cybersecurity incident reporting in the finance sector, there are both Regulations and Directives, the former being directly applicable in the Member States, the latter requiring transposing acts at Member State level.[12] Directives will be addressed with regard to existing provisions on security incident handling with direct relevance for the finance sector, although it is the respective national statutes implementing named Directives that are directly applicable in the Member States.

[9] Art 16 Regulation 1093/2010.

[10] Schwarze, Soft Law im Recht der Europäischen Union, European Law Journal 2011, 3 (10).

[11] Novotny, Stand der Technik von NIS-Maßnahmen – Auslegungshilfen zwischen IT, OT und IOT. In: Schweighofer, Kummer, Saarenpää (eds) Internet of Things. Tagungsband des 22. Internationalen Rechtsinformatik Symposions IRIS 2019, 565 (567–568).

[12] Art 288(2) TFEU.

2.2.1.1 Directive on Security of Network and Information Systems (NIS-Directive), Directive (EU) 2016/1148

One of the main objectives of the Directive on security of network and information systems, published in 2016, is to promote network and information security, deemed vital for the functioning of societies and economies within the European Union.[13] The Directive has been drafted in consideration of the increasing risk for information systems. These security incidents can be of varying character: "[…] [H]uman mistakes, natural events, technical failures or malicious attacks."[14]

The NIS Directive is considered the base of the EU's cybersecurity architecture. It provides implementing measures, directed at the Member State level in order to:

- Create a security culture in sectors deemed to form the critical infrastructure (regulating – among other sectors providing essential services – operators of essential services in the banking sector and regarding financial market infrastructures[15])
- Enhance national cybersecurity capabilities by requiring the Member States to develop or appoint:
    - A national strategy on the security of network and information systems[16]
    - Computer Security Incidence Response Teams (CSIRTs), also known as Computer Emergency Response Teams (CERTs)[17]
    - National competent authorities on the security of network and information systems[18]
    - A Single Point of Contact on the security of network and information systems[19]
- Improve cooperation and information exchange at EU level by establishing:

[13] COM (2013) 48 final 2.
[14] COM (2013) 48 final 2.
[15] Art 14 Directive (EU) 2016/1148.
[16] Art 7 Directive (EU) 2016/1148.
[17] Art 9 Directive (EU) 2016/1148.
[18] Art 8 Directive (EU) 2016/1148.
[19] Art 8 Directive (EU) 2016/1148.

- The Network of CSIRTs, a network comprising all the national Computer Emergency Response Teams[20]
- The Cooperation Group, comprising representatives of the Member States, the Commission and ENISA[21]

For Operators of Essential Services (OES), Art 14 NIS-Directive lays down security requirements and incident notification procedures, requiring that transposed statutes at the Member State level ensure that OES take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.[22]

On one hand, Member States shall ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of essential services.[23] On the other hand, Member States have to also lay down notification procedures for OES (Operators of Essential Services) to the competent authority or CSIRT, including a determination of the significance of the impact of an incident[24], which is relevant for follow-up cross-border reporting of the respective incident if there is a significant impact on the continuity of essential services in other Member States.[25]

The current status of transposition of the NIS Directive is found in the table below (Table 2).

Country	Implementing Status	Date published
Austria	transposed	28.12.2018
Belgium	transposed	03.05.2019/18.07.2019
Bulgaria	transposed	13.11.2018
Croatia	transposed	no information on publication date
Cyprus	transposed	05.04.2018
Czechia	transposed	09.03.2018/14.06.2018
Denmark	transposed	08.05.2018/09.05.2018/10.05.2018 and other dates

[20] Art 12 Directive (EU) 2016/1148.
[21] Art 11 Directive (EU) 2016/1148.
[22] Art 14 Directive (EU) 2016/1148.
[23] Art 14 (2) Directive (EU) 2016/1148.
[24] Art 14 (3) and (4) Directive (EU) 2016/1148.
[25] Art 14 (5) Directive (EU) 2016/1148.

Estonia	transposed	22.05.2018
Finland	transposed	30.12.2017/11.05.2018
France	transposed	27.02.2018/25.05.2018/26.06.2018/03.08.2018/ 29.09.2018
Germany	transposed	29.06.2017/02.05.2016/24.07.2015
Greece	transposed	03.12.2018/08.10.2019
Hungary	transposed	no information on publication date
Ireland	transposed	21.09.2018
Italy	transposed	09.06.2018
Latvia	transposed	18.01.2019 and other dates
Lithuania	transposed	10.12.2018 and other dates
Luxembourg	transposed	31.05.2019
Malta	transposed	06.07.2018
Netherlands	transposed	08.11.2018
Poland	transposed	13.08.2018/21.11.2018/30.10.2019
Portugal	transposed	13.08.2018
Romania	transposed	09.01.2019/17.07.2019/19.07.2019/24.07.2020
Slovakia	transposed	09.03.2018/14.06.2018
Slovenia	transposed	09.05.2018
Spain	transposed	08.09.2018
Sweden	transposed	10.11.2017/27.06.2018

Table 2. Implementation of the NIS-Directive in Member States[26]

2.2.1.2 Payment Services Directive (PSD2), Directive (EU) 2015/2366

The Payment Services Directive regulates payment services in the internal market (for example services enabling credit transfers[27], direct debits[28], card payments[29]) within European Bank institutions[30], with the aim of promoting security and transparency in payment services between customers and financial institutions.[31] It also requires payment

[26] Information compiled from https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive, accessed 2021-02-22 and https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L1148&qid=1613999354947, accessed 2021-07-08.

[27] Annex I (3) lit c Directive (EU) 2015/2366.

[28] Annex I (3) lit a Directive (EU) 2015/2366.

[29] Annex I (3) lit b Directive (EU) 2015/2366.

[30] Art 2 (2) Directive (EU) 2015/2366.

[31] Recital 7, 29, 33 Directive (EU) 2015/2366.

service providers to have access to payment systems in a non-discriminatory and proportionate way.[32] Payment Service Providers (PSPs) have to provide to the competent authority an updated and comprehensive assessment of the operational and security risks related to the payment services they provide, including the adequacy of the mitigation measures and control mechanisms implemented.[33]

To enable the operation of TPPs, financial institutions will be required to fulfil account information and payment initiation requests by providing TPPs with the necessary information via Application Programming Interfaces (APIs), given that they will be authorised by the payer. In this way, the Directive will allow payers to gain additional payment protection, as payments will need to be processed through "strong customer authentication".[34] This will provide a more robust and secure mechanism for payer authentication, to reduce the risk of payment fraud, or for data exchanged in a payment process to be leaked to an adversary.

PSD2 also requires TPPs to work as a payment institution with their local regulator and accept obligations to set up risk and control frameworks and comply with all relevant reporting obligations.

The incident reporting framework drawn up by PSD2 obliges the payment service provider to notify the competent authority in its home Member State, which then shall, without undue delay, provide details on the incident to the European Banking Authority (EBA) and to the European Central Bank (ECB).[35]

Art 96 of PSD2 includes the reporting obligations for payment services providers in the case of major operational or security incidents.[36] In order to further specify reporting requirements, EBA has issued guidelines[37] in close cooperation with the ECB and after

[32] Art 35, 36 Directive (EU) 2015/2366.
[33] Art 95 (2) Directive (EU) 2015/2366.
[34] Art 97 Directive (EU) 2015/2366.
[35] Art 96 Directive (EU) 2015/2366.
[36] Art 96 (1) Directive (EU) 2015/2366.
[37] EBA, EBA/GL/2017/17, Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2.eu, accessed 2021-07-08.

consultation of all relevant stakeholders on the classification of major incidents, the content, format (including standard notification templates) and the procedures for notifying such incidents (addressed to payment service providers).[38] Moreover, guidance is provided on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities and with the EBA and the ECB (addressed to competent authorities)[39].

2.2.1.3 General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

In 2012, the Commission proposed a new legal framework for the protection of personal data in the EU.[40] This strategy was supported primarily by the General Data Protection Regulation.[41] The General Data Protection Regulation was created in order to strengthen citizens' fundamental rights in the digital age, and facilitate business by simplifying rules for companies in the Digital Single Market. The GDPR includes a number of key changes for organisations that operate within the EU highlighting the following considerations:

- If the business is not in the EU, there is still an obligation to comply with the Regulation[42],
- The definition of personal data very broad in scope[43],
- The introduction of data protection impact assessments (DPIA), which are mandatory under certain circumstances[44],
- Amended data breach notification requirements[45],
- Inclusion of the right to erasure ('right to be forgotten')[46],

[38] EBA, EBA/GL/2017/17, Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366, Section 4, https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2.eu, accessed 2021-07-08.

[39] EBA/GL/2017/17, Sections 5 and 6.

[40] COM (2012) 11 final.

[41] COM (2012) 11 final 1.

[42] Art 3 (1) Regulation (EU) 2016/679.

[43] Art 4 (1) Regulation (EU) 2016/679.

[44] Art 35 Regulation (EU) 2016/679.

[45] Art 33 and 34 Regulation (EU) 2016/679.

[46] Art 17 Regulation (EU) 2016/679.

- Inclusion of aspects related to the transfer of data to third countries[47],
- Distinct responsibilities for the data processor[48],
- Inclusion of the right to data portability[49],
- Obligation to follow data-protection-by-design and data-protection-by-default methodologies.[50]

For the purpose of incident handling, GDPR contains in Articles 33 and 34 a requirement of notification and communication of personal data breaches to the supervisory authority, regulating also the procedure of handling a security incident involving personal data. At least the following information shall be contained in a personal data breach notification:

- Nature of personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,
- Name and contact details of the data protection officer or other contact point where more information can be obtained,
- Description of the likely consequences of the personal data breach,
- Description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[51]

2.2.1.4 Regulation on electronic identification and trust services for electronic transactions in the European Single Market (eIDAS), Regulation (EU) 910/2014

eIDAS is an EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. This regulation introduces eID (electronic identification) and eTS (electronic Trust Services), understanding these processes as the core for trusted electronic transactions and services in a digital market, deploying an additional security layer for any electronic document, telematics processes, certificates, authentication services and any electronic scheme, involving trust service providers. Since 2016, ENISA has been supporting Supervisory bodies for EU trust services with cybersecurity

[47] Art 44 et seqq Regulation (EU) 2016/679.
[48] Art 5, Art 12 et seqq Regulation (EU) 2016/679.
[49] Art 20 Regulation (EU) 2016/679.
[50] Art 25 Regulation (EU) 2016/679.
[51] Art 33 (3) Regulation (EU) 2016/679.

breach reporting under Article 19 of the eIDAS regulation. To this end, ENISA develops procedures and analysis, publishing these through their annual report every year.[52]

Additionally, according to Article 10 of the eIDAS regulation, security breaches of notified electronic identification schemes have to be suspended or revoked, without delay, by the notifying Member State and other Member States as well as the Commission have to be informed.[53] In order to regain availability of the cross-border authentication scheme, the authentication shall be re-established as soon as possible after the breach or compromise has been remedied and other Member States and the Commission shall be informed accordingly.[54] As a last resort, the electronic authentication scheme is to be withdrawn by the Member States, if the breach or compromise is not remedied within three months of suspension or revocation.[55]

2.2.2 European bodies related to incident handling

2.2.2.1 European Banking Authority

The European Banking Authority (EBA) is a European authority whose mandate is to ensure effective finance and banking sector regulation and supervision exists throughout the European Union.[56] The EBA provides regulatory guidelines and recommendations to the sector and provides input and guidance regarding the management of information technology risk, risk management, and risk mitigation strategies. One of the core pieces of regulation – as mentioned above – for the sector is the second Payment Services Directive. Alongside the Directive, a set of Regulatory Technical Standards on strong customer authentication and secure communication[57] have been developed, viewed as key to achieving the objectives of the Payment Services Directive.[58] The content of these Regulatory Technical

[52] The most recent report can be found at https://www.enisa.europa.eu/publications/trust-services-security-incidents-2019-annual-analysis-report/at_download/fullReport, accessed 2021-07-08.
[53] Art 10 (1) Regulation (EU) 910/2014.
[54] Art 10 (2) Regulation (EU) 910/2014.
[55] Art 10 (3) Regulation (EU) 910/2014.
[56] Art 1 (5) Regulation (EU) 1093/2010.
[57] EBA/RTS/2017/02.
[58] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2, accessed 2021-07-08.

Standards has fed into Commission Delegated Regulation (EU) 2018/389[59], thereby entering into binding effect and becoming directly applicable in the Member States.[60]

2.2.2.2 European Central Bank (ECB)

The European Central Bank (ECB) is the entity responsible for administrating the monetary policy of European Union member countries which have adopted the euro currency. The principal goal of the ECB is to maintain price stability in the euro area, thus preserving the purchasing power of the euro.[61]

The ECB works with the central banks of the EU member states to ensure the confidentiality, availability and integrity of their data. This helps to protect the national central banks as well as the whole EU banking system against cyberattacks, limiting the damage in case of data breaches and providing for the continuity of the work done in financial institutions and banks. The ECB cooperates with other EU institutions, such as the European Parliament, the Council and the Commission. The EU Computer Emergency Response Team – or CERT-EU for short – is the fulcrum for these joint efforts. CERT-EU warns its members about new threats and provides testing and offers advisory services. It also supports its members when responding to cyberattacks and exchanges information with Member States' national or government CERTs or CSIRTs on cybersecurity threats, vulnerabilities and incidents, possible counter-measures and for improving the protection of their ICT infrastructure, including through the CSIRT network according to Art 12 of the NIS-Directive.[62]. The response team is hosted by the Commission and financed by the participating institutions.[63]

"ECB Banking Supervision has implemented a cyber-incident reporting framework. All significant institutions from the euro area countries have to report significant cyber incidents as soon as they detect them. This enables our supervisors to identify and monitor trends in

[59] Commission Delegated Regulation (EU) 2018/389.

[60] Art 290 (1) TFEU.

[61] Art 127 (1), (2) and (5) TFEU.

[62] Art 4 (1) Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU), OJ C 12, 13.1.2018, p.1-11.

[63] European Central Bank, "What is cyber resilience?", available at: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, accessed 2021-07-08.

cyber incidents affecting significant institutions and to gain a deeper knowledge of the cyber threat landscape."[64]

According to the ECB cyber-incident reporting framework, relevant institutions are required to report cyber incidents to the ECB as soon as they are detected, covering various details of the incident.[65] The cyber incident reporting plan must contain a description of the categories of data subjects, a description of categories of personal data processed and the categories or recipients to whom the personal data have been or will be disclosed. Also, it is necessary to collect personal data of contact points within the institution.

2.2.2.3 European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity was established to contribute to the development of European Union policy in the field of network security.[66] The relevant subject matter ranges from risk management to incident reporting and information sharing.[67] According to this mandate, ENISA has issued an Incident Reporting Framework for the reporting of incidents under Article 19 eIDAS regulation, elaborating on – inter alia – incident reporting flows.[68] ENISA has also provided guidance and recommendation to the finance sector[69], amongst others, and continues to be the central research agency for the European Commission in regard to cybersecurity.[70]

[64] European Central Bank, "What is cyber resilience?", available at: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, accessed 2021-07-08.

[65] Calliess/Baumgarten, Cybersecurity in the EU. The Example of the Financial Sector: A Legal Perspective, German Law Journal 2020, 1149 (1168).

[66] https://www.enisa.europa.eu/about-enisa, accessed 2021-07-08.

[67] Art 5 (2) Regulation (EU) 2019/881.

[68] ENISA; Article 19 Incident Reporting. Incident reporting framework for eIDAS Article 19 2016, p. 18.

[69] https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector, accessed 2021-07-08.

[70] https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector, p. 3, accessed 2021-07-08.

2.3 National bodies related to incident handling

The following subsections will provide information on national bodes most relevant to the SOTER project. This is primarily due to the location of the organisations that form the consortium.

2.3.1 German supervisory authority (BaFIN)

BaFIN is the acronym for the Federal Financial Supervisory Authority in Germany. In November 2017, the BaFIN published the Circular on Supervisory Requirements for IT in Financial Institutions.[71] This document elaborates on the supervisory requirements for IT in financial institutions, addressing the requirements that will lead to the secure design of IT systems and processes, as well as to the relevant requirements related to IT governance, taking into account appropriate technical and organisational equipment of IT systems with respect to information security and adequate contingency planning. Furthermore, requirements on outsourcing and IT services supplied by third parties are covered in a dedicated module.

Specifically, this local circular focuses on:

- IT Strategy,
- IT Governance,
- Information Risk Management,
- Information Security Management,
- User Access Management,
- Application Development,
- IT Operations,
- Outsourcing and third parties and

[71] Circular 10/2017 (BA): Supervisory Requirements for IT in Financial Institutions, published on 6th November 2017 (in the version of 14th September 2018), https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html, accessed 2021-07-08.

- Critical infrastructure operator.[72]

2.3.2 Spanish supervisory authority

The INCIBE is the Spanish National Cybersecurity Institute[73], a body responsible for the development of cybersecurity and digital trust. Its activity is based on research, the provision of services and coordination with the agents with competences in the field, contributing to building cybersecurity at a national and international level.
INCIBE's activity is founded on three fundamental pillars[74]:

- Services: INCIBE works for the user's protection and privacy, promoting mechanisms for the prevention of and reaction to data security incidents, minimising their impact where they occur, and promoting training and raising awareness.
- Research: INCIBE has at its disposal a great ability to address a range of complex projects of an innovative nature, guiding this approach as a research approach.
- Coordination: INCIBE participates in partnership networks, and therefore the coordination and collaboration with other national and international entities is an essential element of INCIBE's activity.

INCIBE-CERT[75] is the security incident response centre of reference for citizens and private law entities in Spain. It is one of the reference incident response teams that coordinates with other national and international teams to improve the effectiveness of the response to crimes involving networks and information systems, reducing their impact on public security.

2.3.3 Irish supervisory authority

The National Cyber Security Centre (IE-NCSC) of Ireland [76] was formed in 2011, and is the main governmental body responsible for the execution of Ireland's National Cyber Security Strategy (2019-2024)[77]. The NCSC is given the responsibility of the government to:

[72] https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html, accessed 2021-07-08.
[73] https://www.incibe.es/en/what-is-incibe, accessed 2021-07-08.
[74] https://www.incibe.es/en/what-is-incibe/what-we-do, accessed 2021-07-08.
[75] https://www.incibe-cert.es/en/what-incibe-cert, accessed 2021-07-08.
[76] https://www.ncsc.gov.ie/, accessed 2021-07-08.
[77] https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf, accessed 2021-07-08.

- Advise and inform relevant bodies, government departments, and the sector in general
- Ensure that national and critical infrastructure are suitably protected and informed
- Understand and communicate the current cybersecurity climate.

2.3.4 United Kingdom supervisory authority

In a similar fashion to Ireland, the United Kingdom also has a National Cyber Security Centre[78] (UK-NCSC), whose role is to:

- Provide guidance on cybersecurity topics available to all
- Respond to formal cyber security incidents within the United Kingdom
- Nurture the UK's cyber security capability through specific events, guidance, and training
- Actively secure public and private sector networks

2.4 Legal Requirements for Awareness and Training

Since the human factor in cybersecurity is widely recognized as a main concern for incidents, measures related to improve the cybersecurity awareness and behaviour of general employees are increasingly addressed in regulatory considerations. The main elements are awareness and training. Currently, legal requirements are yet just addressing basic elements for human factor related aspects of cybersecurity. A main challenge for compliance considerations is the indirect obligation to follow state-of-the-art cybersecurity procedures which are defined not in the regulatory texts but through standards of the cybersecurity industry.

The Payment Services Directive and the respective national implementing law requires an information security policy be implemented in the process of application for authorisation as a payment institution[79], which shall take into account the guidelines issued by the EBA on ICT and security risk management.[80] These will be discussed in section 3.4.1.

[78] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, accessed 2021-07-08.

[79] Art 5 (1) lit j Directive (EU) 2015/2366.

[80] Art 5 (1) subparagraph 2 Directive (EU) 2015/2366; EBA/GL/2019/04.

While PSD2 does not explicitly contain requirements in regard to **training** and the NIS Directive only requires Member States to ensure that operators of essential services take appropriate and proportionate technical and organisation measures to manage the risks posed to the security of network and information systems[81], the EBA considers "security training and awareness, and monitoring of emerging risks, to be reasonable and plausible security measures designed to mitigate security and operational risks"[82] in their corresponding guideline. Therefore, information security policies, training and awareness can be considered as important domains for cybersecurity measures in the finance sector. More details of the respective guideline's content will be discussed in section 3.4.1.

[81] Art 14 Directive (EU) 2016/1148.

[82] EBA/GL/2017/17, p. 12, which has now been repealed by EBA/GL/2019/04, but the importance of training and awareness is still stressed, EBA/GL/2019/04, p. 22.

3 Standards, Guidelines and Recommendations

In regard to relevant standards, guidelines, and recommendations within the finance sector it is possible to differentiate between three main sources:

1. General requirements in the cybersecurity domain, which can include both mandatory and non-mandatory best-practice standards and solutions (e.g. ISO/IEC 27001[83]). But as regulations and sectoral guidelines can call for the following of best practices the "non-mandatory" aspect of standards should be considered very carefully. At least when not following the leading standards and best practices it can be challenging to argue for the use of alternative not so well established standards.
2. Requirements directly targeted at financial institutions and which are relevant for compliance in specific jurisdictions.
3. Recommendations from European (interdisciplinary) research for the development and implementation of trustworthy ICT products, services and processes. These are relevant for European research & innovation projects in regard to the inclusion of European values and fundamental rights.

3.1 List of sector specific guidelines

The European Banking Authority considers information security reviews, assessment and testing as key mechanisms to mitigate ICT security risk in the finance services sector.[84] These assessments are recommended to be conducted at least annually.[85] Furthermore, within Europe, Member States' implementations of the Payment Services Directive requires payment service providers to provide updated and comprehensive assessments of both the operational and security risks relating to the payment services they provide, as well as on the adequacy of mitigation measures and control mechanisms implemented in response to those risks.[86] As assessments in the sector are often based on the current cybersecurity standards (e.g. ISO 27001 or BSI standards in Germany), non-sector specific cybersecurity standards can also be relevant for the extended finance sector, as information security best practice is often maintained regardless of sector.

[83] International Standards Organisation, ISO/IEC 27001, https://www.iso.org/isoiec-27001-information-security.html, accessed 2021-07-08.

[84] EBA/GL/2019/04, p. 18.

[85] EBA/GL/2019/04, p. 21.

[86] Art 95 (2) Directive (EU) 2015/2366.

3.1.1 International Guidelines

- SANS Security Assessment Guidelines for Financial Institutions[87]
- Financial Stability Board: Effective Practices for Cyber Incident Response and Recovery, Final Report[88]

3.1.2 European Guidelines

- EBA Guidelines on ICT and security risk management[89]
- EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)[90]. These have been repealed by the EBA Guidelines EBA/GL/2019/04 on ICT and security risk management.[91]
- Reference document on security measures for operators of essential services (CG Publication 01/2018)
- Guidelines on the assessment of the Information and Communication Technology (ICT) risk in the context of the Supervisory Review and Evaluation Process (SREP), EBA/GL/2017/05[92]
- ENISA Article 19 Incident reporting – incident reporting framework for eIDAS Article 19 (December 2016)[93]

[87] https://www.sans.org/reading-room/whitepapers/auditing/security-assessment-guidelines-financial-institutions-993, accessed 2021-07-08.

[88] https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/, accessed 2021-07-26.

[89] EBA, Guidelines on ICT and security risk management, EBA/GL/2019/04, https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management, accessed 2021-07-08.

[90] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2, accessed 2021-04-09.

[91] EBA, Guidelines on ICT and security risk management, EBA/GL/2019/04, https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management, p. 18, accessed 2021-07-08.

[92] https://www.eba.europa.eu/eba-publishes-final-guidelines-to-assess-ict-risk, accessed 2021-07-08.

[93] https://www.enisa.europa.eu/publications/article19-incident-reporting-framework, accessed 2021-07-08.

3.1.2.1 EBA Guidelines on ICT and security risk management

Important contents of the EBA Guidelines on ICT and security risk management are recommendations in regard to:

- Information security policy
- ICT incident and problem management
- Business continuity management

3.1.2.2 Compliance announced by national supervisory authorities

3.1.2.2.1 Austria

The FMA (Austrian Financial Market Authority) has declared intent to comply with the EBA Guidelines on ICT and security risk management as of the notification date, which was 3rd March 2021.[94] In regard to EBA/GL/2017/05, the FMA has also declared compliance.[95]

3.1.2.2.2 Ireland

The Central Bank of Ireland has announced compliance with the EBA Guidelines on ICT and security risk management as of the notification date.[96]

3.1.2.2.3 Spain

The Banco de España has announced compliance with the EBA Guidelines on ICT and security risk management as of the notification date.[97]

---

[94] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/896720/EBA%20GL%202019%2004%20-%20CT%20GLs%20on%20ICT%20and%20security%20risk%20management.pdf, accessed 2021-07-08.

[95] https://www.fma.gv.at/eu/eba-leitlinien-und-andere-konvergenzinstrumente/, accessed 2021-07-08.

[96] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/896720/EBA%20GL%202019%2004%20-%20CT%20GLs%20on%20ICT%20and%20security%20risk%20management.pdf, accessed 2021-07-08.

[97] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/896720/EBA%20GL%202019%2004%20-%20CT%20GLs%20on%20ICT%20and%20security%20risk%20management.pdf, accessed 2021-07-08.

3.1.2.2.4 United Kingdom

The Bank of England has produced a report entitled "Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU".[98]

3.1.3 National Guidelines

- BSI Guide to Basic Protection based on IT-Grundschutz (October 2018)[99], establishing a holistic approach to information security management, while complying with BSI Standard 100-2 and ISO Standard 27001.[100]
- Spanish security scheme[101] (ENS) defined in October 2015 set out to way relative to the protection of personal data, and in particular the security and confidentiality of the data included in the files, systems and applications of the public administrations and indicates the common way to act in specific areas, like the response to security incidents.[102]

3.2 List of general cybersecurity standards

This section will outline the core standards within the general domain of cybersecurity. It will include international, European, and relevant national standards and functions as a comprehensive reference for standards relevant in the SOTER project.

---

[98] https://www.bankofengland.co.uk/-/media/boe/files/paper/2019/interpretation-of-eu-guidelines-and-recommendations-boe-and-pra-approach-sop.pdf, accessed 2021-07-08.

[99] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html;jsessionid=1C212ABCFF29BA7D86B1326EF9E593D3.internet471?nn=128634, accessed 2021-07-08.

[100] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html, accessed 2021-07-08.

[101] https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001, accessed 2021-07-08.

[102] https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html?idioma=en, accessed 2021-07-12

3.2.1 International Standards

- ISO/IEC 27001:2013 Information technology – security techniques – information security management systems – requirements[103]
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls[104]
- ISO/IEC 27004:2016 Information technology – security techniques – information security management – monitoring, measurement, analysis and evaluation[105]
- ISO/IEC 27005:2018 Information technology – security techniques – information security risk management[106]
- ISO/IEC TR 27006:2015/AMD 1:2020: Information technology – security techniques – requirements for bodies providing audit and certification of information security management systems – Amendment 1[107]
- ISO/IEC 27009:2020 Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements[108]
- ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security[109]
- ISO/IEC 27016:2014 03 01 Information technology -- Security techniques -- Information security management -- Organizational economics[110]
- ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management[111]

[103] https://www.iso.org/standard/54534.html, accessed 2021-07-26.
[104] https://www.iso.org/standard/54533.html, accessed 2021-07-26.
[105] https://www.iso.org/standard/64120.html, accessed 2021-07-26.
[106] https://www.iso.org/standard/75281.html, accessed 2021-07-26.
[107] https://www.iso.org/standard/77722.html, accessed 2021-07-26.
[108] https://www.iso.org/standard/73907.html, accessed 2021-07-26.
[109] https://www.iso.org/standard/74046.html, accessed 2021-07-26.
[110] https://www.iso.org/standard/43756.html, accessed 2021-07-26.
[111] https://www.iso.org/standard/67851.html, accessed 2021-07-26.

3.2.2 European Standards

- ETSI TR 103 456: CYBER; Implementation of the Network and Information Security (NIS) Directive[112]
- ETSI TR 103 331: CYBER; Structured threat information sharing[113]
- ETSI TR 103 306: CYBER; Global Cyber Security Ecosystem[114]

3.2.3 National Standards

3.2.3.1 German Standards

- BSI-Standard 200-1: Information Security Management Systems (ISMS)
- BSI-Standard 200-2: IT-Grundschutz-Methodology
- BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz

3.2.3.2 Spanish Standards

- UNE-ISO 22320:2013 Societal security. Emergency management. Requirements for incident response[115]
- UNE-EN 16352:2013 Logistics - Specifications for reporting crime incidents[116]
- UNE-EN ISO/IEC 27000:2019 Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016)[117]

[112] https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf, accessed 2021-07-26.
[113] https://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.02.01_60/tr_103331v010201p.pdf, accessed 2021-07-26.
[114] https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.04.01_60/tr_103306v010401p.pdf, accessed 2021-07-26.
[115] https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0052363, accessed 2021-07-26.
[116] https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0051918, accessed 2021-07-26.
[117] https://www.aenor.com/normas-y-libros/buscador-de-normas/une/?c=N0061478, accessed 2021-07-26.

3.2.3.3 Austrian Standards

These standards apply to web applications and were developed for banks, industrial companies, administrative bodies and insurance companies.[118] The series of standards consists of the following parts:

- ÖNORM A 7700-1: Definition of relevant terms
- ÖNORM A 7700-2: Data protection requirements
- ÖNORM A 7700-3: IT security requirements
- ÖNORM A 7700-4: Requirements regarding the secure operation of web applications

3.2.3.4 United Kingdom Standards

The United Kingdom standards body, the British Standards Institute (BSI) has adopted relevant ISO Information Security standards as their national standards. These include the following:

- BS EN ISO/IEC 27001:2017 - Information technology. Security techniques. Information security management systems. Requirements
- BS ISO/IEC 27003:2017 - Information technology. Security techniques. Information security management systems. Guidance

They also provide their own national standard on:

- BS 7799-3:2017 - Information security management systems. Guidelines for information security risk management

3.3 Best practice for cybersecurity governance and incident management

Strengthening cybersecurity, and consequently, incident handling, is an important objective for any organisation. There exist a number of specific technical and organisational solutions to promote cybersecurity best practice in Europe. This chapter will outline some of the core methodologies, centring on three dimensions: confidentiality, availability, and integrity.

[118] https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards/OENORM-A7700-Sichere-Webapplikationen.html, accessed 2021-07-08.

3.3.1 List of best practices

The following standards and methodologies may be viewed as a set of best practices and procedures regarding incidence handling:

- ISO/IEC 27035:2016 (Incident Management)[119]
- NIST SP 800-61 Incident Management[120]
- Digital Single Market Strategy (DSM)[121]
- ENISA (European Network and Information Security Agency) Incident Management Guide[122]
- Payment Card Industry Data Security Standard (PCI DSS)[123]
- EU Cybersecurity Act (Regulation (EU) 2019/881)[124]
- EU Blueprint[125]

3.3.2 Description of best practices

3.3.2.1 ISO 27035:2016

Managing incidents effectively involves detective and corrective controls designed to recognize and respond to security events and incidents, minimize adverse impacts, gather forensic evidence (where applicable) and in due course 'learn the lessons' in terms of prompting improvements to the ISMS, typically by improving the detection mechanisms, preventive controls or other risk treatments[126].

Information security incidents commonly involve the exploitation of previously unrecognised and/or uncontrolled vulnerabilities, hence vulnerability management (*e.g.,* applying relevant

[119] https://www.iso.org/standard/60803.html, accessed 2021-07-08.
[120] https://www.nist.gov/privacy-framework/nist-sp-800-61, accessed 2021-07-08.
[121] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, accessed 2021-07-08.
[122] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management, accessed 2021-07-08.
[123] https://www.pcisecuritystandards.org/document_library, accessed 2021-07-08.
[124] https://eur-lex.europa.eu/eli/reg/2019/881/oj, accessed 2021-07-08.
[125] https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf, accessed 2021-07-08.
[126] ISO 27035:2012, p.2

security patches to IT systems and addressing various control weaknesses in operational and management procedures) is part preventive and part corrective action[127].

This standard covers the processes for managing information security events, incidents and vulnerabilities.

The standard expands on the information security incident management section of ISO/IEC 27002[128]. It cross-references that section and explain its relationship to the ISO27k eForensics[129] standards, with 5 key stages[130]:

1. Define a plan and prepare to deal with incidents *e.g.* prepare an incident management policy, and establish a competent team to deal with incidents;
2. Identify and report information security incidents;
3. Analyse incidents and make decisions about how they are to be addressed *e.g.* patch things up and get back to business quickly, or collect forensic evidence even if it delays resolving the issues;
4. Respond to incidents *i.e.* contain them, investigate them and resolve them;
5. Learn the lessons - more than simply identifying the things that might have been done better, this stage involves actually making changes that improve the processes.

The standard provides template reporting forms for information security events, incidents, and vulnerabilities.

3.3.2.2 NIST SP 800-61 Incident Management

Other relevant standard, not necessarily within EU, but currently used as a baseline for best practices, NIST Special Publication 800-61 focused in security incident handling. This standard provides a methodology on how to manage security incidents for all U.S. federal information systems except those related to national security.

[127] ISO 27035:2012, p.3
[128] https://www.iso.org/standard/54533.html, accessed on 2021-07-26.
[129] https://www.iso.org/standard/78647.html, accessed on 2021-07-26.
[130] ISO 27035:2012, p.7

In order to prevent, detect and handle security incidents, this standard define several functions. According to NIST SP 800-61, these functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk[131]:

- **Preparation** – The first step when facing security incidents is to establish incident response capabilities and to prevent security incidents by securing the systems. The organization should define some mechanism for preparing against security incidents, like communication procedures, security in the facilities, analysis of hardware and software, analysis of resources and mitigation software. Also, the organization should deploy some preventing measures, like periodic risk assessments or malware prevention.
- **Detection and Analysis** – The next step is the detection and analysis of possible security incidents. The attack vectors, sings of incidents and precursors of incidents have to be clearly identified by establishing procedures and software like IDPSs or SIEMs. Also, an effective incident analysis have to be carried out for resolving it quickly and accurately. The incident has to be documented, prioritized and reported to the relevant authorities.
- **Containment, Eradication, and Recovery –** First it is necessary to contain the incident for avoiding further propagation. It is necessary also to gather some evidences of the security incident and to identify the attacking host. Then, it is time for eradicate the incident and restore the systems to normal operation.
- **Post-Incident Activity** – This is the most often omitted part of the incident response, learning and improving. It is important to use the experience for improving the response procedure and systems

[131] NIST SP 800-61, p.21

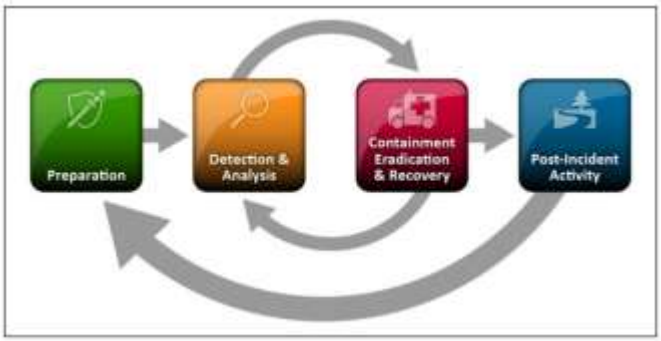

Figure 1. Incident response process according to NIST SP 800-61.[132]

3.3.2.3 Digital Single Market Strategy

Another relevant security set of best practices is the Digital Single Market Strategy for Europe of 2015 (DSM).[133] This is one of the most relevant strategic goals of European Union. To support that goal, cybersecurity is recognised in this document as one of the vital fields that needs immediate actions at European level.

This strategic decision is enforced and driven by the already mentioned European Cybersecurity Strategy and the opportunities created by H2020.

From the perspective of ENISA, the establishment of the NIS public private platform was announced in the Cybersecurity Strategy of the European Union. It shares the same objective as other security frameworks such as the NIS Directive. The NIS Platform helps to implement the measures set out in the NIS Directive and ensure its convergent and harmonised application across the EU. The work of the Platform will draw from international standards and best practices

3.3.2.4 ENISA Incident Management Guide

[132] NIST SP 800-61, p.21

[133] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192, last accessed on 2021-07-28

ENISA also provides a good practices and practical information guideline for the management of network and information security incidents.[134] The main focus of the guide is the incident handling process, which involves the detection and registration of incidents, followed by triage (classifying, prioritising, and assigning incidents), incident resolution, closing and post-analysis.

This guide also includes a formal framework for CERTs, covering the roles, workflows, basic policies, cooperation, outsourcing, and reporting to management.

3.3.2.5 Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard[135] (PCI DSS) is a standard for means of payment issued by credit card issuing companies with a view to protecting the credit card data of clients executing transactions from any origin.
The standard is applicable to:

- Traders
- Service providers (third parties and payment gateways)
- Any IT infrastructure element (Hardware and Software) in scope or connected to any environment containing credit card data.
- Transactions, either electronic ones or on paper

Who:

- Stores credit card data.
- Transmits credit card data.
- Processes credit card data.

In order to ensure:

[134] ENISA Good Practice Guide for Incident Management, available at: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management, accessed on 2021-07-28

[135] Payment Card Infrastructure Data Security Standard, available at: https://www.pcisecuritystandards.org/document_library, accessed on 2021-07-26.

- That minimum security controls are deployed to protect the sensitive data of clients and consumers.

PCI DSS is organized into six different ambits, including security incident handling in ambit 6. Maintain an Information Security Policy[136]:

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

3.3.2.6 EU Cybersecurity Act

The EU Cybersecurity Act[137] defines a continual and reinforced authority for ENISA, as the European Cybersecurity Agency, and also specifies a structure for the European Union that will be used for the development of the cybersecurity certification for Information and Communications Technology (ITC) products, including IoT devices, processes and services that will be recognized in all EU Member States.

3.3.2.7 EU Blueprint

[136] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1627306708508, accessed on 2021-07-26.

[137] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2019/881/oj, accessed 2021-07-28

The EU Blueprint is used for the Coordinated Response to Large-Scale Cyber Incidents.[138] It offers cross-border response procedures, the taxonomy of cyber incidents as well as rapid and effective cooperation and preparedness.

Applying these facilitates the planning of activities to improve security in applications, processes, and controls, requiring mapping business priorities with security priorities, assessing current state using the maturity model safety program and setting maturity model state target. For each case, procedures and processes collects internationally accepted best practices for managing incidents.

3.4 Human factors of cybersecurity governance

This section turns attention towards the human-factor based aspects of cybersecurity, through analysis of current standards, guidelines, and best practices, especially in relation to incident handling in the context of cybersecurity governance. The SOTER project follows a broad understanding of incident handling, as it is understood to not only refer to completed *action after a cybersecurity incident occurs* (e.g., incident reporting) but also to the organisational and individual capacities to *detect early potential incidents*. It starts with an overview of key elements on training and awareness in sectoral guidelines (section 3.4.1), adds information on requirements from leading standards (section 3.4.2), and then discusses current relevant initiatives for improving cybersecurity in the human factors domain (sections 3.4.3 to 3.4.6). While only a few aspects of these discussions are currently represented or just superficially addressed in the regulatory landscape, the contents point to potentially significant improvements to address human factor related cybersecurity incidents.

3.4.1 EBA Guidelines on ICT and Security Risk Management

Information security policy

- The information security procedure required to be established under the Payment Services Directive[139] and the relevant national law transposing this directive should allocate the main roles and responsibilities of information security management, setting out requirements for both staff and contractors of the financial institution.[140]

[138] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, https://eur-lex.europa.eu/eli/reco/2017/1584/oj, accessed 2021-07-28
[139] Art 5 (1) lit f Directive (EU) 2015/2366.
[140] EBA/GL/2019/04, p. 18.

- Based on this information security policy, financial institutions should implement security measures in order to mitigate ICT and security risks, including measures in regard to logical, physical and ICT operations security, security monitoring, information security reviews, assessment and testing as well as information security training and awareness.[141]

Information security training and awareness

- Information security training and awareness is considered one of 7 key measures to mitigate ICT and security risks.[142] The other 6 are organisation and governance in accordance with paragraphs 10 and 11; logical security; physical security; ICT operations security; security monitoring; information security reviews, assessment and testing[143].
- Monitoring the threat landscape and situational awareness can be considered as a task to be fulfilled by dedicated IT security personnel.[144]
- According to EBA, PSPs "should establish periodic security awareness programmes" to ensure that staff and contractors "are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks"[145].
- Periodic security awareness programmes "should require PSP personnel to report any unusual activity and incidents."[146]
- PSPs should not only enhance the security awareness of their employees but also of payment service users on "security risks linked to the payment services by providing PSUs with assistance and guidance"[147]
- Training programmes should be established for all staff and contractors[148]

[141] EBA/GL/2019/04, p. 18.
[142] EBA/GL/2019/09, p. 18.
[143] EBA/GL/2019/04, p. 18.
[144] EBA/GL/2017/17, p. 23 and according to the revised EBA Guidelines on ICT and security risk management, regular threat monitoring is considered important as well, see: EBA, EBA/GL/2019/04, p. 17.
[145] EBA/GL/2019/04, p. 22.
[146] EBA, EBA/GL/2017/17, p. 24, the Guidelines in place currently also provide for the reporting of ICT and security risks, see: EBA, EBA/GL/2019/04, p. 15–16.
[147] EBA, EBA/GL/2017/17, p. 24, the Guidelines in place currently also provide for the reporting of ICT and security risks, see: EBA, EBA/GL/2019/04, p. 28.
[148] EBA/GL/2019/04, p. 22.

- According to EBA guidelines, "financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including information security"[149]
- Payment service providers "should establish a **training programme** for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce **human error, theft, fraud, misuse or loss**."[150]
- According to the EBA, training programmes should be provided annually or "more frequently if required"[151]. The guidelines do not specify in which cases more frequent trainings are required.
- Management "should ensure that the allocated budget is appropriate to fulfil the ICT operational needs and security risk management processes on an ongoing basis.[152]
- Information sharing: Information sharing has been considered by the EBA as part of their guidelines for the implementation of PSD 2 but have been subsequently removed. The now repealed guideline from 2017 still *encouraged* participation in information sharing platforms with "other PSPs and relevant third parties such as operators of payment systems, industry associations, etc."[153]

3.4.2 Requirements from leading standards

The listed requirements in this sector complement the legal requirements for awareness and training discussed in section 2.4 and from sectoral guidelines (3.4.1).

Education and determination of competence: According to ISO 27001, an "organization shall

- determine the necessary competence of person(s) doing work under its control that affects its information security performance;

[149] EBA/GL/2019/04, p. 14.
[150] EBA/GL/2019/04, p. 22.
[151] EBA/GL/2019/04, p. 14.
[152] EBA/GL/2019/04, p. 14.
[153] EBA/GL/2017/17, p. 94; although this encouragement is no longer included in the most recent version of the Guidelines (EBA/GL/2019/04), it nevertheless shows that such topics continue to be discussed and might become again relevant in future recommendations or guidelines.

- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- retain appropriate documented information as evidence of competence."154

Cybersecurity Awareness and Training:

- ISO 27000 considers the following as a critical success factor for information security management: "an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly."[155]
- ISO 27001: "Employee training to understand the problem of social engineering and to recognize situations that might be an indicator of, or precursor to, a social engineering attack and understand how to apply company policy procedures to social engineering attacks for protection information".[156]
- According to ISO 27001, personnel "shall be aware of:
    - the information security policy
    - their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
    - the implications of not conforming to the information security management system requirements."[157]
- Awareness should also be enhanced in regard to "detection, prevention and recovery controls to protect appropriate against malware".[158]

[154] ISO/IEC 27001:2017, Section 7.2.
[155] ISO/IEC 27000:2019, section 4.6.
[156] Humphreys, E. (2016). Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, p. 112
[157] EN ISO/IEC 27001:2017 section 7.3.
[158] EN ISO/IEC 27001:2017 section 12.2.1.

- "All employees of the organisation and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function"[159]

Cybersecurity and recruiting:
ISO 27001 provides some guidance on aspects of recruitment, in order to ensure that the human resources employed in an organisation do not negatively impact on the cybersecurity levels of the organisation. This includes the conducting of background checks. Prior employment history, screening and clear outlining of roles and responsibilities. It is all deemed as part of the Information Security Management System (ISMS), and is contained within *Annex A.7 - Human Security Management*.

Involvement of Management
ISO 27000 also proposes that both support and commitment should be sought from all levels of management, especially those at the top of the management tree. This is considered a critical success factor for information security management systems, and an integral part of any organisation's human factor-based security strategy.[160]

Personnel security controls
The SANS Institute identifies four "personnel security controls"[161] (SANS 2008):

- Background checks and screening
- Confidentiality, nondisclosure, authorized use agreements
- Job descriptions
- Training in security awareness and compliance

3.5 Human aspects of cybersecurity best practice

Organisational and informational security is a compound of human and technology. Modern perspectives of cybersecurity view the field as falling within socio-technical studies, resilience as being composed of a delicate balance of technology and human factors (the individual and the collective). This section outlines the ongoing SOTER research, and also aligns the research

[159] EN ISO/IEC 27001:2017 Annex A.7.2.2.
[160] ISO/IEC 27000:2019, section 4.6.
[161] SANS 2020: Security Assessment Guidelines for Financial Institutions, https://www.sans.org/reading-room/whitepapers/auditing/security-assessment-guidelines-financial-institutions-993, accessed 2021-07-22.

with existing evaluations of human factor cybersecurity, including analysis of publications from respected organisations such as North Atlantic Treaty Organisation (NATO), the United States Department of Defence (DoD), and the European Cybersecurity Agency (ENISA).

In order to understand the best practices in the financial service sector, it is important to understand the organisations and institutions that have provided research and guidance on the human factors and behaviour related threats. These high-level research outputs can then be used to understand sector specific threats and provide context for how organisations have developed best practice protocols for human factor elements.

3.5.1 List of agencies and organisations for human factor cybersecurity governance

There are number of authoritative sources, organisations, and entities that produce guidance and information concerning the human factor of cybersecurity. Delineating each of their work helps frame the issue within a sector specific context. Some of the most notable bodies are:

- The European Cybersecurity Agency (ENISA)
    - European Cybersecurity Skills Development in the EU[162]
    - European Cybersecurity Culture[163]
    - European Cybersecurity Behavioural Aspects[164]
- European Banking Authority Guidelines on ICT and Security Risk Management[165]
- North Atlantic Treaty Organisation Technical Report on Human Factors[166]
- United States Department of Defence Insider Threat Mitigation[167]

[162] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union, accessed 2021-07-26.
[163] https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, accessed 2021-07-26.
[164] https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, accessed 2021-07-26.
[165] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management, accessed 2021-07-26.
[166] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, accessed 2021-07-26.
[167] https://apps.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf, accessed 2021-07-26.

3.5.1.1 The European Cybersecurity Agency (ENISA)

The European Cybersecurity Agency have a predominant role within the EU to provide best-practice support and guidance to Member States and further afield. They are designated a role in developing aspects of best practice for cybersecurity within and across sectors, including specific thematic support for the critical sectors. They have developed research and guidance on human-factor themes of cybersecurity, including the development of three reports that focus directly on core aspects of human factor-based cybersecurity resilience within organisations

3.5.1.1.1 European Cybersecurity Culture in Organisations

A recent human factor-based exploration by ENISA was the documented published in February 2018, which presented a desk-based research exercise of cybersecurity culture within organisations. They outline the three predominant methods for creating a "good" cybersecurity culture (CSC) within an organisation:

- **Top-down approach:** initiated by the Board, CEO and/or the most senior C-suite individual with responsibility for cyber security.
- **Mid-level approach:** initiated by mid-management with responsibility for cyber security or corporate culture (e.g. CSO).
- **Bottom-up approach:** initiated by an individual within a business unit who identifies a need.[168]

The authors also identify the seven core dimensions of CSC:

- Behaviours
- Attitudes
- Cognitions
- Compliance
- Communication

[168] https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, P.15, accessed 2021-07-26.

- Norms
- Responsibilities

3.5.1.1.2 European Cybersecurity Behavioural Aspects

In April 2019, ENISA published a second instalment of their human-factor based research.[169] This was primarily a desk-based research exercise which outlined key studies from the field. The authors also provide a framework for understanding and measuring cybersecurity behaviours within organisations:

Figure 2. Framework for designing interventions for human aspects of cybersecurity[170]

3.5.1.2 European Banking Authority

In the section 3.4 of the "EBA Guidelines on ICT and security risk management", the EBA sets out the requirements for information security managed on ICT systems. Among the measures is the establishment of a training programme that should contain security awareness

[169] Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, accessed 2021-07-2021

[170] *ibid*, p.19

programmes, for all institutions' staff and contractors in order to ensure that they are properly trained to perform their whole set of duties and responsibilities in a consistent manner with the security policies and procedures. The reason of that is to reduce undesirable consequences such as human error, misuse, theft, fraud or loss. They also should be capacitated to properly address information security related risks. Financial institutions should ensure that at least on an annual basis, all staff members receive an appropriate training on ICT and security risks.

3.5.1.3 North Atlantic Treaty Organization

The North Atlantic Treaty Organization (NATO) have developed a comprehensive outline for the development of resilient cybersecurity, entitled the Human Systems Integration Approach to Cybersecurity. The authors of the document state that "technological solutions are being developed to enhance cyber security, there is growing awareness that besides a technical approach, the role of human performance, decision making, and organizational culture are critical to foster the effectiveness of responses to developing cyber threats."[171] They also acknowledge the intricate intertwining of the NATO policy of cyber-defence, and the European Union Cybersecurity Strategy. While the document is specifically targeted as aspects of military defence, it is important to acknowledge the areas of concern that the working group have identified, especially those that are applicable across the range of critical sectors (not specific to solely military implementations):

- Approaches to improve selection, education, training and retention of a cyber force (IT experts);
- Approaches to improve cyber awareness of all defence personnel;
- Methods, techniques and tools to bridge the gap between the cyber force and the operational community in terms of perceptions of cyber threat, procedures and practices for prevention;
- Techniques to enhance organizational resilience to cyber-attacks;
- Methods to improve control behaviour via cyber security policies and targeted Education and Training (E&T);

[171] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, p1-1, accessed 2021-07-26.

- Identification of the specific characteristics of a malicious insider's behaviour and methods or tools to identify this potential threat; and
- Definition of the role of the military commanders to mitigate cyber threat.

It is also important to note that the conclusion of the NATO working group was "that we need a common research perspective to study cyber security that focuses on the interrelatedness between technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance."[172]

NATO provide the Human Systems Integration approach model, which places the human factor alongside (and with equal importance) the more traditional cybersecurity domains of hardware and software. The diagram makes it clear that "systems comprise hardware, software, and people, all of which operate within a surrounding environment (physical, operational, technological, social, political, economic, etc.)"[173]:

[172] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, p.1-1, accessed 2021-07-26.

[173] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, p.2-2, accessed 2021-07-26.

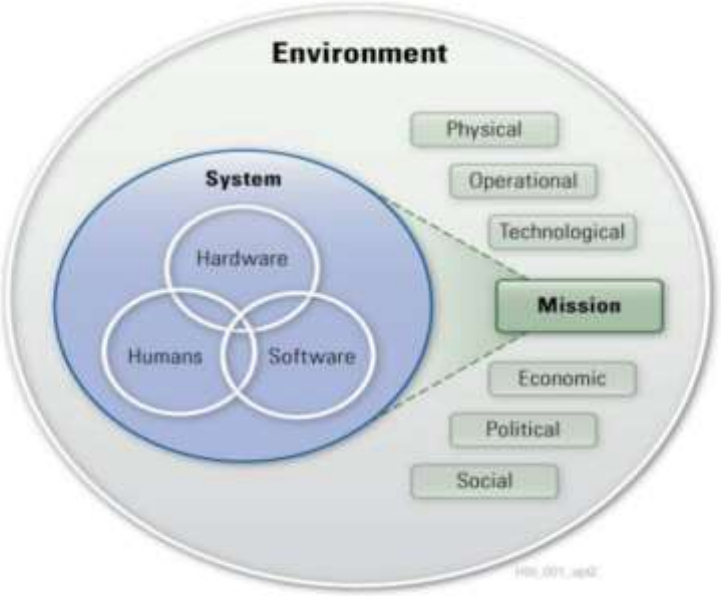

Figure 3. NATO Human Systems Approach[174]

NATO also pay close attention to the aspects of human behaviour, noting the importance of the following questions in the context of understanding the human factor-based vulnerabilities that an organisations face:

- What kinds of errors do users make?
- What tools exist to capture information about user errors?
- How can incorporating an understanding of user behaviour, cognition and decision making improve cyber system security?
- Do personality factors affect cyber security behaviours?
- Is awareness of a cyber threat sufficient to change users' behaviours?
- How does perception of risk influence users' behaviour?
- What do we know about risk awareness and personality with respect to social media? What do we know about insider threats, how to detect them and how to prevent them?

[174] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, p.2-2, accessed 2021-07-28.

From an organisational perspective, NATO also propose a set of mitigation measures, seen as the basis for resilient organisational strategies. These frame certain organisational aspects and feed into concepts of best practice and their proposed relative importance to an organisation, whether told through management or their employees:

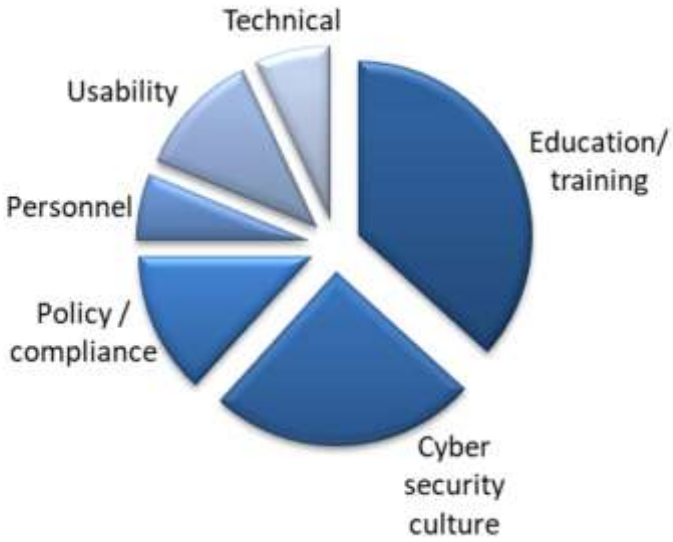

Figure 4. NATO Approach to organisation cybersecurity[175]

3.5.1.4 United States Department of Defence Insider Threat Mitigation

The United States Department of Defence (DoD) have provided guidance on the protecting against insider threats.[176] While this aspect of cybersecurity, and the corresponding recommendations, are primarily applicable to a specific context (United States Defence Forces), it is worth considering their proposed best practice guide within the financial services sector – which is deemed a critical sector for the proper functioning of the European economy. This view is supported with specific guidance from ENISA on the insider threat mitigation[177] which considers five types of insider threat:

[175] https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-259/$$TR-HFM-259-ALL.pdf, p.5-2, accessed 2021-07-28.

[176] United States Department of Defence, DoD Insider Threat Mitigaiton, Final Report of the Insider Threat Integrated Process Team, available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf, accessed 2021-07-22.

[177] ENISA, Threat landscape: Insider Threat, available at: https://www.enisa.europa.eu/publications/insider-threat, published October 2020, accessed 2021-07-22.

1. The careless workers who mishandle data, break use policies and install unauthorised applications;
2. The inside agents who steal information on behalf of outsiders;
3. The disgruntled employees who seek to harm their organisation;
4. The malicious insiders who use existing privileges to steal information for personal gain;
5. The feckless third-parties who compromise security through intelligence, misuse or malicious access to or use of an asset.

ENISA recognise that the insider threat is a real and current threat to organisations; a vulnerability that should not be discounted – especially considering their study found that 83% of organisations surveyed believed it to require mitigation, and that the annual cost to companies deriving from insider threats is €11.45 million[178].

In a similar manner to ENISA, the DoD determine there are four key sources for the insider threat:

1. Maliciousness
2. Disdain of security practices
3. Carelessness
4. Ignorance

3.5.2 Description of best practice

Within the SOTER WP6, the consortium has identified specific some best practices with regards to training, awareness and understanding of human factor cybersecurity.

3.5.2.1 Information Security Competency Assessment-Framework

Information Security Competency Assessment (ISCA) was developed as a framework to understand the level and type of information security culture in an organisation.[179] It is predominantly focused on the classical organisational security triumvirate of confidentiality, availability and integrity. It is also predominantly questionnaire focused. As a summary the assessment covered nine dimensions of information security culture:

[178] *Ibid*, p.3
[179] Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security, 70, 72-94.

1. Protection of information assets
2. Management's perception of information security management
3. Change and willingness of users to change in order to protect information
4. User awareness and training regarding information protection requirements
5. Employees' understanding of the information security policy
6. Effectiveness of investing in information security resources
7. Trust of employees in privacy and secure communication within the organisation
8. Information security governance (such as monitoring)
9. Additional needs for information security training

3.5.2.2 HAIS-Q: Measurement of Information Security Awareness

Parsons et al have developed the Human Aspects of Information Security Questionnaire (HAIS-Q), to quantify human-based information security vulnerabilities.[180] The general concept is that an organisation is able to understand in a comprehensive and robust manner the general levels of cybersecurity awareness (as told through the understanding of policy and process), which in turn effected the levels of 'good' cybersecurity practice, as well as impacting on actions and behaviours, whether told through 'knowledge' or 'attitude'. The authors provide a robust model for understanding the human factors of cybersecurity, similar to that developed within the SOTER project:

[180] Parsons, K, et al. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security 42 (2014): 165-176.

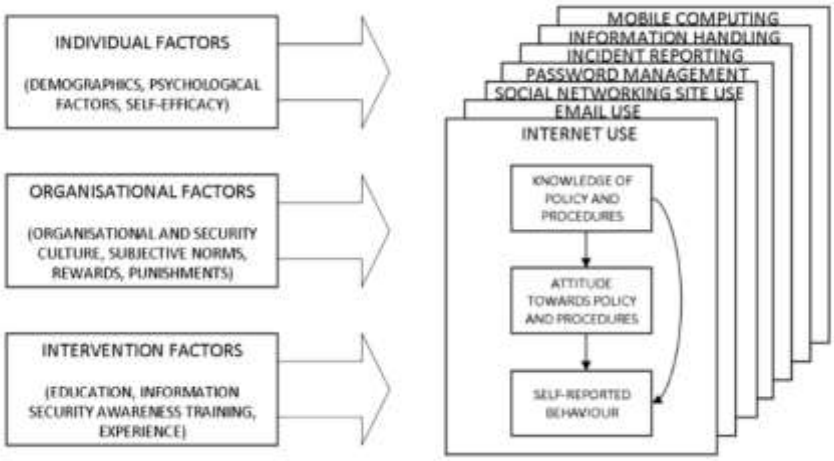

Figure 5. The Human Aspects of Information Security (HAIS) model. (Parsons et al)

Crucially the authors also acknowledging some limitations with the HAIS-Q method, including concerns around self-reporting, and top-down appraisal of employees. However, the authors do conclude with considerable confidence that specific training, education, and awareness campaigns are effective for increasing the general levels of cybersecurity competence and awareness within organisations. D6.1 has provided a fuller investigation into the efficacy of such a questionnaire-based model, and this in turn has fed into the study design within T2.1, and the training actions within WP6.

4 Finance sector specific threats and best practice for mitigation

In this section, examples of cybersecurity related threats that European companies face are provided, along with a brief summary, and the development of recommendations to address them (sections 4.1 and 4.2). As an overview the majority of attacks seek to:

- Take advantage of data breaches and extort or steal money from financial clients, in a criminal manner
- Slowdown the proper functioning of the company, the sector, and the economy, due primarily to acts 'hacktivism'
- Damage the reputation of the financial institution by, for example, publishing customer data
- Politically destabilize an area, region or country
- Reduce the liability of third parties or vendors
- Exploit new technologies and architectures

This section also discusses human factor-specific threats to identify the threat landscape relevant for general cybersecurity awareness and training (section 4.3). It is important to define the threats where the behaviour of employees outside of the cybersecurity governance departments (incl. IT security and risk management) is critical for the success of a cyber-attack.

4.1 Examples of recent finance sector security incidents

Data breaches are a growing threat to all industries, including the financial sector. Entities in the financial sector, such as banks, credit unions, credit card companies, mortgage and loan providers, financial service providers, investment firm, trust companies, payday lenders and pension funds are all vulnerable to the evolving cybersecurity landscape.

In recent years, cyber-attacks have become more prevalent, with most of them becoming more and more sophisticated.

Some examples from recent years:

- The central bank's hacking of the SWIFT payment terminal in Bangladesh in 2016, which led to fraudulent payment messages and the theft of $81 million (financial theft)[181].
- The data leak at Equifax in 2017[182]. This resulted in an estimated 143 million US records containing customer information stolen by hackers. This included social security numbers, dates of birth and credit card details (violation / theft of data)
- The hacking of the Cosmos Bank ATM server in India in 2018[183], which resulted in the theft of $13.5 million through fraudulent credit and debit card transactions (financial theft)
- The Banco de Chile network incident[184], which resulted in a loss of $10 million (financial theft)
- The incident that affected the interbank payment system of the Bank of Mexico, SPEI[185], resulting in a loss of $15 million (financial theft)
- Edenred, a payment solution provider, reported that that it was infected by a malware that affected several computers in the organization[186]. It operates in 46 countries and handled over 2.5 billion payment transactions two years ago. The company confirmed that they set up the measures to prevent future infections as soon as the incident was detected.
- Hackers used PayPal user's accounts to make unauthorized purchases, with a value of 10 thousands euros, by exploiting PayPal's Google Pay integration[187]. Most of the victims were German PayPal users (Feb 2020)

[181] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/, accessed 2021-07-26.

[182] https://techcrunch.com/2017/09/07/equifax-data-leak-could-involve-143-million-consumers/, accessed 2021-07-26.

[183] https://www.reuters.com/article/cyber-heist-india-idUSL4N1V551G, accessed 2021-07-26.

[184] https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075, accessed 2021-07-26.

[185] https://www.bloomberg.com/news/articles/2018-04-28/mexican-banks-are-said-to-have-been-targeted-in-cyber-attack, accessed 2021-07-26.

[186] https://www.bleepingcomputer.com/news/security/edenred-payment-solutions-giant-announces-malware-incident/, accessed 2021-07-26.

[187] https://www.zdnet.com/article/paypal-accounts-are-getting-abused-en-masse-for-unauthorized-payments/, accessed 2021-07-26.

- Southeast Asian Banks Credit Card Breach[188], at March 6, 2020, it was reported that over 200,000 credit card details from top banks in Singapore, Malaysia, the Philippines, Vietnam, Indonesia, and Thailand were stolen and published online.
- Australian Banks DDoS Extortion[189], at February 2020, it was reported that Australian banks and other financial institutions were being extorted with DDoS attacks unless paying a ransom.
- Capital One, at July 2019, as one of the most important financial institutions in USA, suffered a data breach compromising the credit card applications of around 100 million individuals after a software engineer hacked into a cloud-based server[190].

The financial services sector has always been a targeted industry, due to the importance, categories, and potential value of the information available to cybercriminals. Given that financial services sector organisations are routinely targeted, it is important to be constantly aware of the extent and causes of successful cyber-attacks. There is also a distinct need to keep knowledge of the attacks, and the risk mitigation strategies, up to date, so parties can learn from them.

Cybercriminals will continue to target finance sector organisations and their networks, potentially harming a company's good will or reputation. Criminals may also cause substantial political or economic damage in the wider sector through harming large multi-nationals, or firms with ties to government, or those with responsibilities for enacting public policy, or holding government contracts.

Financial institutions must be prepared to adapt to a changing cybersecurity landscape and be prepared to face both new threats but also the most common attacks.

Considering previous analysis, top cybersecurity threats can be summarized as follows:

- Malware: Web Application attacks and malicious code injection, local file inclusion and cross-site scripting.

[188] https://iapp.org/news/a/credit-card-details-breached-in-southeast-asia/, accessed 2021-07-26.

[189] https://www.cyber.gov.au/acsc/view-all-content/alerts/ddos-threats-being-made-against-australian-organisations, accessed 2021-07-26.

[190] https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html, accessed 2021-07-26.

- Intentional attacks: DDoS
- Vulnerability exploitation: Backdoors and supply-chain attacks, including vulnerabilities derived from emerging technologies.
- External party risk and external service providers.
- Global Operational Risks: Chances a company faces in the course of conducting its daily business activities, procedures, and systems.
- Social engineering, including insider threats and phishing.

4.2 Technical threats

The aim of this section is to define a taxonomy for identifying threats related to the finance sector and relevant for the SOTER project.
As ISO 27005[191] states, there is no standard taxonomy that must be followed, but several that could be taken into account for identifying the major challenges that financial organizations faces.
In this section, we have focused on the ENISA threat taxonomy[192], which will be used as a reference, in order to identify which threats are related to financial sector. Only the threats which consider technical issues in cybersecurity are taken into account. Focusing on financial sector and information security, and excluding threats related to natural disasters, physical damage or legal issues, standard risks are created.

To complete this section, we also focus on the security incident taxonomy defined in D3.9 - Incident Response Plan & Reporting Plan, which is based on the "Reference Incident Classification Taxonomy"[193] defined by ENISA.

This taxonomy defines the main security incidents identified in the European context for the finance sector:

[191] https://www.iso.org/standard/75281.html, accessed on 2021-07-19

[192] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view, accessed 2021-07-26.

[193] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy, accessed on 2021-07-12

- **Abusive Content:** Attacks intended to damage the organisation's image or using its electronic media for other illegal uses (such as advertising, extortion or, in general, cyber-crime).
- **Malicious Code:** Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
- **Information gathering:** Attacks intended to collect fundamental information to progress in more sophisticated attacks, through social engineering or identification of vulnerabilities.
- **Intrusion attempts:** Attacks designed to exploit vulnerabilities in the design, operation or configuration of different technologies, in order to break into the organisation's systems.
- **Intrusions:** A successful compromise of a system or application (service). It can be caused remotely, through a known or new vulnerability, or through unauthorized local access. It also includes being part of a botnet.
- **Availability:** By this kind of attack the system collapses due to the large number of packets it receives, resulting in delayed operations or in a crash of the system.
- **Information Content Security:** Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks can possibly intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
- **Fraud:** Incidents related to fraudulent actions derived from identity theft, in all its variants.
- **Vulnerable:** Open resolvers, world readable printers, virus signatures not up to date, and so on.

Depending on the risk taxonomy scheme, these threats and risks can be addressed with different mitigation strategies. Regardless of the taxonomy that is used to classify threats, successful mitigation relies on alignment between IT Security and supporting departments.

Following we present the reference taxonomy based on the ENISA threat taxonomy.

High Level Threat	Threats	Exemplary Mitigation Actions
Physical attack (deliberate/ intentional)	Fraud	Apply segregation of duties to prevent the perpetration and concealment of fraud in the normal course of the activities.
	Information leakage/sharing	Establish a clean desk policy to limit the possibilities of external parties seeing sensitive documents.
	Unauthorized physical access / Unauthorised entry to premises	Review and apply the best practices and standards that can help with evaluating physical security controls. Establish secure areas that protect the valuable information and information assets only authorized people can access. Secure areas need to be protected by the appropriate entry controls to ensure only authorized personnel are allowed access.
	Coercion, extortion or corruption	Apply segregation of duties to prevent the perpetration and concealment of coercion, extortion or corruption in critical activities of the organization.
Unintentional damage / loss of information or IT assets / intentional damage	Erroneous use or administration of devices and systems	Implement an automated policy enforcement tool to reduce the risk of this threat.
	Using information from an unreliable source	Review browsers security policy to notice if TLS certificates are trusted or not. Subscribe to newsletter /mailing lists from trust sources (i.e. national intelligence agencies, CERTs).
	Unintentional change of data in an information system	Properly controlled change management is essential to ensure that the changes are appropriate and properly authorized and carried out to mitigate the opportunity for an accidental compromise.

	Inadequate design and planning or improperly adaptation	Design, document and develop properly the life cycle of IT infrastructure components, including process flows, roles and responsibilities, service level agreements, task hand-off, process controls, status monitoring, metrics, periodic review and process ownership.
Eavesdropping/ Interception/ Hijacking	Interfering radiation	Controls should be adopted to minimize the risk of potential physical and environmental threats, including communications interference or electromagnetic radiation (i.e. TEMPEST NATO certification). In case of critical information systems, consider air-gapped protection.
	Replay of messages	All messages must content preventative measures such timestamps, session keys or random one-time use passwords.
	Network Reconnaissance, Network traffic manipulation and Information gathering	Protect available / non-connected ports of network devices in order to avoid that an attacker can connect a device (i.e. Cisco port security). Install network threat detection engines to detect intrusions in real time.
	Man in the middle/ Session hijacking	Follow OWASP guidelines to avoid Cross-site scripting attacks, which enable an attacker to steal session cookies. Review browsers security policy to notice fraudulent TLS certificates.
Nefarious Activity/ Abuse	Identity theft (Identity Fraud/ Account)	Configure and activity security mechanisms in network devices to avoid ARP/IP Spoofing attacks in order to prevent network identity thieves. Establish authentication procedures based on two-factor authentication. Protect accounts with advanced security measures, such as change of location detection. Protect outbound e-mails with protocols that mitigate impersonation attacks, such as DKIM, SPF or DMARC.

	Receive of unsolicited E-mail	Protect the organization mail server with an antispam system. It should include sandbox mail analysis, URL pre-filtering, IP reputation database and keywords detection.
	Denial of service	Organization should ask its Internet Service Provider for anti-distributed denial of service defence capabilities, which process and clean inbound traffic.
	Malicious code/ software/ activity	Install and keep update anti-malware tools and antivirus software. Promote the utilization of a log correlation tool to prevent malicious activity.
	Social Engineering	Improve the security of the organization mail service in order to avoid impersonation and phishing attacks.
	Abuse of Information Leakage	Update the systems with the required vulnerabilities patches as soon as possible. If needed, enforce a data loss prevention policy.
	Generation and use of rogue certificates	Review browsers security policy to warn and detect rogue certificates.
	Manipulation of hardware and software	Develop and follow systematically hardware reception procedures, to detect tampering and hardware manipulation attacks. Check hashes and digital signatures of software installation files.
	Manipulation of information	The organization should promote the utilization of personal digital certificates to sign the documentation in order to maintain its integrity.

	Misuse of audit tools	Protect the integrity of the records in Information Management Systems with hashing and signature techniques.
	Misuse of information/ information systems (including mobile apps)	Development of an acceptable use policy of information systems that must emphasize on what is an appropriate / inappropriate usage, what type of activity is forbidden, and what consequences will result if the policy is violated.
	Unauthorized activities	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized activities. Detection systems should be configured to provide alerts on suspicious activities by examining allowed and denied users' activity.
	Unauthorized installation of software	Software installation should be managed using a central repository by IT Department which centralized the distribution of trust and legitimate software. An approbation flow should be established to grant the installation of software which is not included in the security policy of the organization. Disable to access to application stores.
	Compromising confidential information (data breaches)	Outsource a digital surveillance service to detect organization accounts in disclosure data breaches. Combine an information classification tool with a data loop prevention system.
	Hoax	Identify trust information sources and verify its integrity.
	Remote activity (execution)	Install and keep update anti-malware tools and antivirus software. Stablish an intrusion detection system and correlation tools to detect remote access tools.
	Targeted attacks (APTs etc.)	Update security systems with IOCs (indicators of compromise) from sources of well-known reputation.

	Failed of business process	Monitor business processes event logs and setup metric and reporting tools.
	Brute force	Block attempts of authentication after users' failures. Introduce captchas codes as a challenge-response test to determine automated brute force attacks.
	Abuse of authorizations	Apply segregation of duties to prevent the abuse of authorization in the management of the systems.

Table 3. Technical threat taxonomy

4.3 Human factor-based threats

To identify human factor-based threats that threaten European companies in the financial services sector face, the Common Attack Pattern Enumeration and Classification (CAPEC™) catalogue has been used as a baseline threat taxonomy. CAPEC™ is a publicly available "catalogue of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities"[194]. The catalogue provides a comprehensive overview of "attack patterns" along with an associated description. Its goal is to provide an up-to-date community resource of common attack methods.

As the CAPEC™ catalogue is the most up-to-date (updated as recently as December 2020[195]) and well-maintained catalogue of attack vectors, it is chosen over ENISA's threat taxonomy, because it has not been updated since 2016. Moreover, the CAPEC™ catalogue provides dedicated consideration of the human factor, manifesting in one of its "Domains of Attack", labelled "Social Engineering". The latter is comprised of attack patterns that focus on "...the manipulation and exploitation of people"[196]. The eight meta attack patterns included in this domain serve as the basis for the human factor threat overview to follow.

4.3.1 Human factor threat tables

In its current version (3.4), the CAPEC™ catalogue features a total of 527 attack patterns structured based on level of abstraction. Based on work conducted for SOTER's D6.2, we identified 8 meta attack patterns – CAPEC™'s highest level of abstraction – that feature the human factor, i.e. are not simply preventable through a technical solution. These meta attack patterns are considered high-level threats and are useful for an initial threat assessment. However, it is possible to deconstruct the threats into standard and detailed attack patterns, reducing the level of abstraction and providing greater insight into the likelihood and severity of specific attack techniques. Moreover, the standard and detailed attack patterns often

[194] Common Attack Pattern Enumeration and Classification (CAPEC™), Available at: https://capec.mitre.org/data/index.html. Accessed 2021/07/08.
[195] Update information available at: https://capec.mitre.org/news/index.html#december172020_CAPEC_List_Version_3.4_Now_Available. Accessed 2021/07/08.
[196] https://capec.mitre.org/data/definitions/403.html. Accessed 2021/07/08.

provide descriptions of at least one of the following: “Execution Flow”, “Prerequisites”, “Skills required”, “Resources required”, “Mitigations” and “Example Instances”[197]. Based on these descriptions and additional research, within D6.2 we analysed every standard and detailed attack pattern corresponding to one of the eight meta attack patterns to filter purely technical from human factor-based threats.

CAPEC™ provides their estimated typical severity as well the likelihood of the attack occurring. Note that these differ for meta attack patterns, standard and detailed attack patterns. To account for this variation in the likelihood of attack and typical severity, the following table provides ranges for these values for the corresponding high-level threat (i.e. meta attack pattern). The ranges were based on the analysis of standard and detailed attack patterns in D6.2.

CAPEC™ also includes mitigation recommendations, which provide general strategies that may be implemented by organizations to reduce the impact of any attacks, if they were to surface. It should be noted that the recommendations are generalized, high-level strategies, which should be complemented with organizational and departmental insights in order to provide a more robust overall cybersecurity strategy. Within the table below, we have suggested mitigation measures as provided by the SOTER Competence Catalogue (D6.2).

High-level threat	Likelihood of Attack	Typical Severity	SOTER Mitigation
Parameter Injection	Medium to High	Medium	Safe Browsing Assurance of Device Safety
Identity Spoofing	Medium to High	Medium to Very High	Safe Browsing Confidential personal data and information handling Business data and information handling Safe Digital Communication Network Handling Social Engineering Recognition Identity Fraud Recognition

[197] Using CAPEC’s complete presentation view.

Resource Location Spoofing	Medium	Medium	Safe Browsing Social Engineering Recognition Network Handling
Action Spoofing	Medium	High	Safe Browsing Social Engineering Recognition Assurance of Device Safety
Software Integrity Attack	n/a	High to Very High	Safe Browsing Safe Digital Communication Assurance of Device Safety Social Engineering Recognition Malware (Infection) Recognition
Information Elicitation	Medium	Low	Confidential personal data and information handling Business data and information handling Responsible sharing of private information Privacy settings for private digital devices and services Social Engineering Recognition Identity Fraud Recognition
Manipulate Human Behaviour	Medium	Medium	Safe Digital Communication Social Engineering Recognition Identity Fraud Recognition Confidential personal data and information handling Business data and information handling Assessment of accuracy and integrity of information Insider Threat Recognition

Obstruction (Physical Security)	Low	High	Physical Safety Physical Environment Sensibility Social Engineering Recognition

Table 4. Human factors threat taxonomy.

4.3.2 Threat considerations for the finance sector

CAPEC™ does not provide a threat taxonomy tailored to the extended financial services sector. Thus, there is also no definitive ranking of cybersecurity threats for the finance sector. ENISA, the European Union Agency for Cybersecurity, developed its own threat taxonomy. While ENISA's threat taxonomy was last updated in 2016[198], the agency also publishes a threat landscape report every year. The annual report includes numerous reports on individual threats, as well as a sector-specific threat ranking which also highlights the top threats in the finance sector. However, note that according to ENISA, "the complexity of the financial sector makes it hard to interpret the threat landscape, as different domains within financial services and banking may face entirely different cyber risks and threats"[199]. Moreover, ENISA does not provide the sources used for the compilation of the threat ranking.

Nevertheless, according to ENISA, the following threats (ranked by prevalence) have seen a significant rise in incidents in the finance sector during the past year or so:

1. Web application attacks[200]
2. Insider threat (unintentional abuse)[201]
3. Malware[202]

[198] Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. Accessed 2021/07/08.
[199] ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis p.7. Report, available at https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/at_download/fullReport. Accessed 2021/07/08.
[200] ENISA Threat Landscape 2020 - Web application attacks. Report, available at https://www.enisa.europa.eu/publications/web-application-attacks/at_download/fullReport. Accessed 2021/07/08.
[201] ENISA Threat Landscape 2020 - Insider Threat. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/at_download/fullReport. Accessed 2021/07/08.
[202] ENISA Threat Landscape 2020 – Malware. Report, available at https://www.enisa.europa.eu/publications/malware/at_download/fullReport. Accessed 2021/07/08.

4. Data theft (Data breach)[203]

Based on ENISA's threat landscape reports, we will explain these threats briefly in turn and argue why further adjustment is needed for a more plausible perspective on human factor related cybersecurity threats in the extended financial services sector.

According to ENISA, **web applications** attacks are on the rise. These attacks include SQL (i) Injection and Cross-Site scripting (XSS) attacks, exploiting weaknesses in web applications and services. However, with one exception (the Flash Injection, see CAPEC) web application attacks commonly do not require to deceive the end-user. This becomes clear from ENISA's suggested mitigation measures as well, hence this attack vector is discarded from the threat ranking related to the human factor.[204]

Insider threats are cybersecurity incidents that result from actions of an "insider", i.e. someone working for or affiliated with the potential victim (organisation). The most common insider threat pattern occurs when the attacker collaborates with an inside actor, often providing monetary incentives to convince the insider. However, it is often difficult to distinguish between legitimate, malicious and erroneous actions of insiders.[205]

Malware is perhaps the best-known cyberattack next to Phishing emails. It comes in all shapes and sizes, ranging from viruses, worms, spyware to ransomware. The common goals of a malware attack are information or identity theft and service disruption.[206] Malware is also a significant threat in the human factor domain because it often depends on the successful manipulation of, for example, an employee of an organisation (e.g., installation of malicious software in the attachment of an e-mail).

---

[203] ENISA Threat Landscape 2020 - Data Breach. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach/at_download/fullReport. Accessed 2021/07/08.

[204] ENISA Threat Landscape 2020 - Web application attacks. Report, available at https://www.enisa.europa.eu/publications/web-application-attacks/at_download/fullReport. Accessed 2021/07/08.

[205] ENISA Threat Landscape 2020 - Insider Threat. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/at_download/fullReport. Accessed 2021/07/08.

[206] ENISA Threat Landscape 2020 – Malware. Report, available at https://www.enisa.europa.eu/publications/malware/at_download/fullReport. Accessed 2021/07/08.

In a **data breach**, sensitive and sometimes confidential information is accessed without proper authorisation, typically by a malicious actor. It is commonly the result of a previously conducted cybersecurity attack, such as a phishing attack. Frequently, data breaches can be attributed to human error.[207]

Based on research conducted in D6.2, we have attempted to match meta attack patterns as provided by CAPEC™ to the corresponding top threats as suggested by ENISA. Web application attacks and related terms are in brackets to signal that the attack vector was excluded from the human factor-based analysis. Other terms in brackets signal that the attack vector is usually a result from a previous successful attack. The table is followed by a brief explanation of the attack patterns used by CAPEC™.

ENISA	CAPEC™
(Web application attacks)	(Parameter Injection) (Action Spoofing)
Insider threat	Identity Spoofing Resource Location Spoofing Information Elicitation Manipulate Human Behaviour (Software Integrity Attack)
Malware	Software Integrity Attack Manipulate Human Behaviour
Data breach	Identity Spoofing Resource Location Spoofing Information Elicitation Manipulate Human Behaviour

Table 5. Comparison of ENISA and CAPEC

As elaborated in D6.2[208], CAPEC™ defines **Identity Spoofing** as the "action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal"[209]. An Identity Spoofing attack may manifest in various ways, certainly most prominently as a Phishing attack. As such, it is relevant to two of the top three threats listed by ENISA.

[207] ENISA Threat Landscape 2020 - Data Breach. Report, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach. Accessed 2021/07/08.

[208] D6.2, pp. 24-37.

[209] https://capec.mitre.org/data/definitions/151.html. Accessed 2021/07/08.

CAPEC™ defines **Resource Location Spoofing** as "an adversary deceiving an application or user and convincing them to request a resource from an unintended location"[210]. By spoofing the location, the attacker may cause an alternate resource (such as malware) to be used. Thus, this attack pattern may be considered as a variant of phishing attacks and is frequently employed in social engineering attacks.

In a **Software Integrity Attack**, "an attacker initiates a series of events designed to cause a user, program, server, or device to perform actions which undermine the integrity of software code, device data structures, or device firmware, achieving the modification of the target's integrity to achieve an insecure state"[211]. It is therefore equivalent to ENISA's malware threat.

The **Information Elicitation** meta attack pattern covers all attacks where an attacker "engages an individual using any combination of social engineering methods for the purpose of extracting information"[212]. This broad definition covers a lot of ground, with the most notable standard attack pattern being Pretexting. It is therefore relevant to virtually every social engineering attack.

Lastly, the **Manipulate Human Behaviour** meta attack pattern is primarily concerned with classic social engineering techniques. It is defined by CAPEC™ as an "adversary exploiting inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the adversary's interests"[213]. Manipulation techniques may take many different shapes, which are represented by numerous standard and subordinate detailed attack patterns listed by CAPEC™. It is immediately apparent that there are potential overlaps with Information Elicitation. Taking both together should encompass many, if not all, typical social engineering techniques.

It is important to note that not all matched threats are "perfect fits". For instance, both insider threats and data breaches from ENISA's threat landscape report may be caused by negligent behaviour of an employee, who clicks on a link in a phishing e-mail[214]. Accordingly, the

[210] https://capec.mitre.org/data/definitions/154.html. Accessed 2021/07/08.
[211] https://capec.mitre.org/data/definitions/184.html. Accessed 2021/07/08.
[212] https://capec.mitre.org/data/definitions/410.html. Accessed 2021/07/08.
[213] https://capec.mitre.org/data/definitions/416.html. Accessed 2021/07/08.
[214] ENISA Threat Landscape 2020 - Insider Threat. Report, p. 8. available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat/at_download/fullReport. Accessed 2021/07/08.

CAPEC™ meta attack pattern Identity Spoofing matches to both, since it includes all variants of phishing attacks. Resource Location Spoofing includes attacks where individuals are lured into visiting a slightly misspelled URL, hence it is a match as well. However, due to the nature of social engineering attacks, the meta attack patterns of Manipulate Human Behaviour and Information Elicitation may also apply. Regarding threat taxonomies in general, it should be again kept in mind that many incidents (esp. those based on criminal/malevolent intent) have a multi-stage structure and are thus not easily classified.

Considering that scientific resources and information on real-life attack scenarios is rather scarce due to security considerations, an important source to shed more light onto the industry-specific threat landscape may be a Working Paper from 2017[215] by ENISA. The paper features an assessment of the training needs of critical sectors as identified by the NIS directive, including the banking and financial market infrastructures sectors. Based on surveys conducted with sectorial stakeholders, ENISA (2017) lists the following industry-specific threats for the banking sector in no particular order[216]:

- Vulnerabilities in Mobile Applications and payment interfaces
- Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)
- Web applications attack
- Data Confidentiality, Integrity and Availability
- Social Engineering
- Identity theft

Clearly, only the latter three of the above list are relevant to human factor-based analysis of threats. Additionally, ENISA (2017) mapped the threats to training needs in the sector, identifying the following as particularly needed[217]:

- Awareness raising
- Data security
- Device and endpoint security

[215] ENISA (2017). Stock taking of information security training needs in critical sectors, pp. 12ff. Available at https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors/at_download/fullReport. Accessed 2021/07/08.

[216] Ibid., pp. 12-13.

[217] Ibid., pp. 14-16.

- Web App security

Again, the recurring theme appears to be a focus on data security (-> data breach), device and endpoint security (-> malware), as well as awareness raising (-> insider threat). Web app security is yet again discarded, as it is targeted at IS professionals.

With this in mind, we may now reconsider the ranking as provided by ENISA's threat landscape report. As far as feasible without further information from a representative sample with the extended financial services sector itself, the ranking of human factor-based threats in finance in ENISA terms is as follows:

1. Insider threat
2. Malware
3. Data breach

However, the term "insider threat" in particular might be misleading. Hence, we have aligned ENISA's terminology with the CAPEC™ terminology to ensure the social engineering focus of the attack vectors is clear, and that "insider threats" comprise more than the disgruntled employee or malicious insider (e.g., identity spoofing, resource location spoofing, information elicitation, manipulate human behaviour, see Table 5).

5 Conclusion and outlook

This deliverable has provided an overview of the current cybersecurity landscape, including an overview of existing regulation, standards, and best practices within the financial services sector. The document detailed existing European legislative frameworks applicable to the sector, along with best practice guidelines and recommendations that underpin aspects of cybersecurity governance, risk mitigation and compliance. This concluding chapter will provide an overview of the document and point towards further efforts by the SOTER consortium as the project develops.

5.1 Summary of existing landscape

As elaborated in this document, cybersecurity in the finance sector is regulated on many different legal levels:

A basic cybersecurity governance framework for the finance sector is laid down in both national statutes (implementing directives by the European Parliament and the Council) and in regulations of the European Parliament and the Council which are directly applicable and binding in the Member States of the European Union. These obligations regarding cybersecurity governance are complemented by guidelines, recommendations and standards issued by bodies with specific expertise relevant for the regulation in this subject matter. These bodies can provide expertise either specifically tailored to the needs of the finance sector (e.g. EBA, ECB), overall regarding the field of network and information systems' security (ENISA) or cover general IT security specifications (ISO, ETSI, BSI or other national offices or agencies for information security). These recommendations, guidelines and standards thus help interpret and comply with the vague legal term "state of the art" while still allowing for a certain flexibility regarding their implementation. Additionally, local supervisory bodies of European Union Member States have issued guidance on IT requirements for financial institutions, further specifying obligations laid down in the existing legal framework.

Regulations, best practises and guidelines analysed in this document aim to establish an incident management framework, structured, and aligned with current Members States, attempting to:

- Increase information security level: structured processes of detecting, reporting and evaluation of an incident allow early recognition of it, and a more effective response in time and resources.

- Improvement of incident prevention by learning lessons from security incidents detected.
- Reduce impact on business activities.
- Enhance incident prevention.
- Establish robust levels of cataloguing and prioritization of incidents, such as for example, ENISA's incident taxonomy or ENISA's Reference Incident Classification Taxonomy.
- Justification of cost and improvement of budgetary control from incident recovery, for any sector or industry.

Regarding human factor-based requirements for overall cybersecurity and incident handling procedures, guidelines – such as the Guidelines issued by the EBA on ICT and security risk management – ensure that financial institutions are granted enough flexibility in raising awareness and training their employees for potential incidents, for example by recommending that information security training and awareness programmes take place at least annually. Considering the need for a risk-based approach, neither the hard law framework, such as PSD2 or GDPR, nor the EBA Guidelines on ICT and security risk management strictly require specific training programmes or intervals for these trainings. The latter only recommend trainings to take place at least annually.[218]In regard to training and awareness programmes the EBA recommendations[219] include the following aspects:

- The implementation of training and awareness programmes in the information security policies and procedures
- Trainings should address the following topics: reduction of human error, theft, fraud, misuse or loss, how to address information security-related risks
- Awareness is not only relevant for employees but also for contractors and payment service users (e.g., employees giving assistance and guidance)
- Trainings should be conducted at least annually or more often if needed
- Management should also be subject to trainings and management should make sure that sufficient budget is available for implementing and upholding security procedures.

[218] EBA/GL/2019/04, p. 22.

[219] For sources on EBA recommendations see section 3.4.1 in this document.

In regard to key information in leading standards (which can be considered as “state of the art”), we mainly focussed on ISO 27000 and ISO 27001.[220] These standards consider training and awareness as key measure to mitigate ICT and security risks. When taken as "state of the art” they bring in the following aspects as requirements for training and awareness in the finance sector:

- Determination of the competence of all staff
- Ensuring of competence through education, training or experience
- Documentation of evidence of competence
- Trainings addressing social engineering, the recognition of relevant situations and the application of security and information policy procedures. Trainings should also inform on implications of not conforming to the information security management system requirements.

This deliverable has also presented a range of best practices from respected European and international entities, such as the European Cybersecurity Agency, North Atlantic Treaty Organisation, and the United States Department of Defence.

It has outlined how understanding cybersecurity from a more holistic perspective is key to creating a resilient organization, and so efforts should be made to understand cybersecurity as complex socio-technical system, as well as efforts to cultivate a good cybersecurity culture and individual behaviours within an organisation.

The deliverable has also presented two established methodologies that may be used to gather an understanding of human factor-based elements within any organization: the Information Security Competency Assessment (ISCA), and Human Aspects of Information Security Questionnaire (HAIS-Q). The methodologies are viewed as tools that can provide insight into how an organization is functioning framed through a human factor perspective and draw insights into what aspects need improving in order to create more complete, holistic, and robust cybersecurity strategy.

As a general outlook, there is an increasing consideration of integrating the human factor elements into more comprehensive cybersecurity frameworks, whether through tighter integration with existing standards and regulations, or with more explicit policies and procedures out into place for both assessment of the human factor in an organisation – whether culture or behaviours - as well as aspects such as continued training and recruitment.

[220] For sources on ISO standards see section 3.4.2. in this document.

5.2 Technical threats and incidents overview

Considering research of previous standards and best practices, there are several points which must be considered in any security framework for mitigating defined security incidents and threats:

- **IT Operations management:** includes all controls defined for mitigate operational risks, as for example, vulnerabilities management, hardening, security policies and procedures, or obsolescence programs, involving not only IT infrastructure but also other elements within the Company: external networks, IoT, remote working, etc.

  This is related to Malicious code, Intrusion attempts or Vulnerable security incidents and also to Unintentional change of data in an information system, Manipulation of hardware and software or Targeted attacks threats.

- **Identity and access management:** in order to control not only logical, but also physical, access to IT environments and data.

  This is related to Intrusions or Vulnerable security incidents and also to Misuse of information/ information systems or Unauthorized activities threats.

- **IT asset monitoring and security information and event management:** understanding an asset as an active including IT infrastructure elements, data actives, or even human resources, deploying monitoring tools is a basic necessity in order to identify any anomalous or unidentified event that shall trigger a process execution in order to prevent and mitigate a security incident.

  This is related to Availability or Information gathering incidents and also to Network Reconnaissance, Network traffic manipulation and Information gathering, Man in the middle/ Session hijacking or Brute force threats.

- **Vendor and third-party management:** preventive and even contractual controls seeking to reduce the risk of other parties accessing IT environments.

  This is related to Abusive Content or Availability incidents and also to Vulnerable security incidents and also to Failed of business process, Fraud, Information leakage/sharing or Coercion, extortion or corruption threats.

- **Data classification and retention:** information management, right properties or information assessment in order to control and maintain most valuable assets in the institution.

  This is related to Information Content Security incidents and also to Eavesdropping/ Interception/ Hijacking high level threats and Hoax or Compromising confidential information (data breaches) threats.

- **Awareness and training:** focusing on preventing and identifying a security incident.

  This is related to Fraud security incidents and also to Social Engineering, Abuse of Information Leakage, Unauthorized installation of software or Erroneous use or administration of devices and systems threats.

- **Incident response procedures and continuity plan:** once that a vulnerability is exploited, a risk is materialized, and there exists a security incident, how to contain and resolve it with less damage for the company (reputational, economic and operational damage).

  This is related to Availability, Intrusion attempts or Vulnerable security incidents and also to Denial of service, Malicious code/ software/ activity, Manipulation of information or Unauthorized activities threats.

- **Involvement and decision of the board committee:** to guarantee strategic decisions from top to down and leverage any decision relating to, for example, a security incident, along with the definition of director plans risk-based approach to security.

  This is related to Malicious code, Intrusion attempts or Vulnerable security incidents and also to Brute force, Failed of business process or Social engineering threats.

- **Regulatory and IT Security compliance:** In the European environment, it is mandatory to comply with regulations analysed in this document in order to carry out the business activities covered by this regulations. Also, IT Security compliance with internal policies in the organisation and relevant security standards, like the ones analysed above, is basic to secure the IT systems and to enhance the maturity level of the organization's security.

The security incident handling strategy must consider previous groups, in order to include different aspects in case that a risk materialized and therefore becomes and incident. Especially for financial institutions, incident management must be an agile commitment, to guarantee that threats within the institution are identified, and incidents materialized are addressed, considering continuous IT changes and different paradigms affecting financial sector.

5.3 Threats based on the human factor: An outlook

It is important to keep in mind that the above analysis, and particularly the industry-specific threat ranking, may only preliminary due to lack of representative information and sources. Sharing of information on incidents in the sector is still very limited. Further – and more detailed – analysis is critically dependant on feedback from the stakeholders in the extended financial services sector. Information sharing is considered a critical issue for the financial sector as currently not much information on incidents is shared (besides obligatory reports to the ECB or to data protection authorities). The European Banking Federation is one of the key stakeholders in the finance sector and is also arguing for the establishment of a central reporting and coordination hub in each Member State and identified the lack of common taxonomies as a key issue for this.[221] Therefore, working on the taxonomy landscape is critical for all future regulation and standards on incident reporting. Here we focus on the human factor-specific threat landscape, as these have to be addressed in the awareness and training programmes for staff outside of the IT security units.

Currently, the taxonomies of MITRE (CAPEC and ATT&CK) are the most used taxonomies in the cybersecurity domain. They are easily accessible and continually updated. But overall within the European Union the use of taxonomies seems very fragmented. While the MITRE taxonomies are often used, taxonomies from within the European Union lack the continual work and updates needed for a best practice in maintaining a taxonomy for the cybersecurity threat landscape.

Additionally, currently there is still room for improving a comprehensive and effective overview over threats relevant for general awareness and training. The current lists of attack patterns are dominated by technical-based threats and are therefore only secondarily relevant for non-tech personnel in European organisations. They specifically need awareness

[221] See EBF position on Cyber incident reporting, Brussels, 16 October 2019 EBF_038702 (https://www.ebf.eu/wp-content/uploads/2019/10/EBF-position-paper-on-cyber-incident-reporting.pdf , accessed on 2021-07-21)

on threats, where their own behaviour can really make a difference for the prevention or mitigation of cybercriminal attacks or human error.

For future standardisation it is therefore crucial to maintain a dedicated taxonomy of human factor-based threats. Currently, even CAPEC is not yet covering the whole range of this threat landscape. While social engineering is the main concern here for sure, there are more threats which should be considered, and which have been identified by other taxonomies. For future standardisation it is therefore important to systematically collect a dedicated human factor-based threat taxonomy as a central threat information base for awareness and training measures.

In the follow-up work SOTER will attempt to integrate all relevant elements into a recommendation to establish this threat information base. A recommendation for extending the coverage of human aspects in the existing threat taxonomies will be presented in D5.2. The following taxonomies with their human factor-specific elements will be used:

- MITRE CAPEC[222]: esp. in the attack domain of social engineering
- MITRE ATT&CK[223]: identifying elements in all attack stages:
    - Reconnaissance: Gather victim identity information, gather victim org information, search open websites/domains, search victim-owned websites, phishing for information
    - Resource Development: compromise accounts & infrastructures, establish accounts, stage capabilities, link target, upload malware
    - Initial Access: Phishing, use of valid accounts
    - Execution: user execution
    - Persistence: accounts & maintaining spoofed identities
    - Privilege escalation: internal spearphishing
    - Defence evasion: general social engineering
    - Discovery: information elicitation, pretexting
    - Lateral movement: internal spearphishing
    - Collection: browser and e-mail information

[222] https://capec.mitre.org/, accessed 2021-07-22.
[223] https://attack.mitre.org/, accessed 2021-07-22.

- Credential access: brute force (password security), input capture, unsecured credentials
- Command and Control: manipulate human behaviour
- Exfiltration: manipulate human behaviour
- Impact: impacts based in the human factors-domain (e.g., reputation, legal, social)

- ENISA threat taxonomy (2016)[224]: in the domains of physical attacks, unintentional damage, eavesdropping/interception/hijacking, nefarious activity/abuse and legal
- ENISA attack vector taxonomy (2018)[225]: attack the human element, web and browser based attack vectors, supply chain risks, misinformation/disinformation
- Europol common taxonomy for law enforcement and CSIRTS 1.3[226]: information gathering, fraud
- Open threat taxonomy 1.1[227]: in the domain of personnel threats (e.g., labour/skills shortage, social engineering, errors)
- NIST SP 800-30 taxonomy of threat sources[228]: in the domains of adversarial, accidental and environmental threats
- MISP CERT-XLM Mapping Taxonomy[229]: esp. in the element "content" (harmful speech, violence, copyright, masquerade)Additionally, especially kill chain-based or lifecycle taxonomies (like Cyber Kill Chain, MITRE ATT&CK and US ODNI Cyber Threat Framework) need to be analysed in regard to the relevant of understanding the processual nature of cybersecurity incidents. The hypotheses currently is, that lifecycle considerations are especially important for awareness and training as human factor-based incidents depend on successful step-by-step attack schemes and early disruptions and preventive measures can negate attacks at an early stage.

[224] https://data.europa.eu/data/datasets/enisa-threat-taxonomy-1, accessed 2021-07-22.

[225] See ENISA (2019): ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, p. 125-132 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, accessed 2021-07-22).

[226] See Europol (2017): Common Taxonomy for Law Enforcement and The National Network of CSIRTs, Version 1.3 (https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf, accessed 2021-07-22.

[227] https://auditscripts.wpengine.com/resources/open_threat_taxonomy_v1.1a.pdf, accessed 2021-07-22.

[228] See NIST (2012): Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1 (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, accessed 2021-07-22).

[229] See https://www.misp-project.org/taxonomies.html, accessed 2021-07-22.