A Practical Human-Centric Risk Management (Hrm) Methodology

Kitty Kioski *, Eleni Seralidou , Nineta Polemi

Posted Date: 4 December 2024

doi: 10.20944/preprints202412.0255.v1

Keywords: Human-centric risk management; Adversary profiles; User maturity; Socio-technical risk assessment; Cyber psychology

Article

A Practical Human-Centric Risk Management (HRM) Methodology

Kitty Kioskli [1,*], Eleni Seralidou [1] and Nineta Polemi [2]

[1] trustilio B.V., Vijzelstraat 68, Amsterdam 1017 HL, The Netherlands
[2] University of Piraeus, Department of Informatics, Piraeus 185 34, Greece
* Correspondence: kitty.kioskly@trustilio.com

Abstract: Various standards (e.g., ISO 27000x, ISO 31000:2018) and methodologies (e.g., NIST SP 800-53, NIST SP 800-37, NIST SP 800-161, ETSI TS 102 165-1, NISTIR 8286) are available for risk assessment. However, these standards often overlook the human element. Studies have shown that adversary profiles (AP), which detail the maturity of attackers, significantly affect vulnerability assessments and risk calculations. Similarly, the maturity of the users interacting with the ICT system in adopting security practices impacts risk calculations. In this paper, we identify and estimate the maturity of user profiles (UP) and propose an enhanced risk assessment methodology, HRM (based on ISO 27001), that incorporates the human element in the risk evaluation. Social measures, such as awareness programs, training, and behavioral interventions, alongside technical controls, are included in the HRM risk treatment phase. These measures enhance user security hygiene and resilience, reducing risks and ensuring comprehensive security strategies in SMEs.

Keywords: human-centric risk management; adversary profiles; user maturity; socio-technical risk assessment; cyber psychology

1. Introduction

Human threats pose significant risks to Information and Communication Technologies (ICT) system security but are often overlooked in traditional risk management. These threats include malicious or unintentional actions like unauthorized access, intellectual property theft, system sabotage, and user errors. They exploit human vulnerabilities such as lack of awareness, inadequate security culture, poor cyber hygiene, and low cyber maturity among users. Factors like lack of training, stress, cognitive issues, and multitasking further exacerbate these risks. Attackers often use social engineering techniques to manipulate users into compromising security through methods like phishing and disinformation.

ISO 27001 mandates regular risk assessments to identify and mitigate potential threats and vulnerabilities, including those related to human factors. Effective risk management should consider security culture, employee behavior, and psychological profiles. Tailored risk treatment measures should include both technical controls and social interventions such as awareness programs, training, and co-creation workshops. Small Medium Enterprises (SMEs) should begin by identifying employee vulnerabilities and implementing targeted social controls to reduce these risks.

The Human Centric Risk Management (HRM) methodology proposed in this paper integrates socio-psychological techniques with existing technical risk management tools to address human threats. HRM uses open-source risk management tools (e.g., ENISA, OWASP, MISP, Cyberwatching) and co-creation workshops to identify and estimate human-related vulnerabilities and effectively manage these risks.

The rest of the paper is organized as follows:

1.1. Human Centric Risk Management (HRM) Objectives and Main Principles

The Human Centric Risk Management (HRM) methodology integrates human factor considerations into the ISO 27001 framework [1], enabling SMEs to manage their security risks more effectively by incorporating profiles of their ICT users (e.g., administrators, defenders, operators, employees, third parties). HRM proactively identifies and addresses human threats, implementing best practices for security management to strengthen SMEs' overall security posture and protect valuable assets from evolving cyber threats.

Numerous standards (e.g., ISO 27000x [2], ISO 31000:2018 [3]) and methodologies (e.g., NIST SP 800-53, NIST SP 800-37 [4]) exist for risk assessment, evaluating cybersecurity risks for each threat as the product of vulnerabilities (weaknesses) of the assets, impact (consequences), and the frequency and probability of the threats occurring:

$$\text{Risk} = \text{Threat (T)} * \text{Vulnerability (V)} * \text{Impact (I)} \tag{1}$$

Alternatively, literature sometimes defines risk as (Katsumata et al, 2010; Al-Zahrani, 2022):

$$\text{Likelihood (L)} = \text{Threat (T)} * \text{Vulnerability (V)} \tag{2}$$

$$\text{Risk} = \text{Likelihood (L)} * \text{Impact (I)} \tag{3}$$

However, these standard evaluations often overlook the threats related to adversaries or ICT users. Several studies [5–7] have shown that adversaries' profiles (AP) (i.e., traits that impact the maturity of the adversary to conduct a successful attack) affect the estimation of vulnerabilities and, consequently, the calculation of risks. Similarly, ICT user profiles (UP) (i.e., traits that impact their maturity to adopt secure behavior) influence risk estimation and treatment plans, necessitating both technical and social measures (e.g., awareness raising, training, behavior change interventions, co-creation workshops).

Existing standards and methodologies focus on technical controls to treat risks, often ignoring the necessary social mitigation measures that help ICT users strengthen their personal security hygiene and resilience to cyber-attacks. These social measures reduce human vulnerabilities and the occurrence of human threats, ultimately decreasing risks and ensuring appropriate technical and human-related controls are implemented within the specific operational environment of the SME.

HRM delves deeper into the human element of users who defend and interact with the SME's ICT to identify human threats and vulnerabilities, proposing targeted technical and social controls that can be easily adopted by employees. HRM methodology proposes that the traditional risk models can be enhanced by considering the strength of Adversary Profile (AP) and the minimum strength of ICT User Profiles (UPs):

$$\text{Risk} = T * V * I * AP * 1/UP \tag{4}$$

or alternatively:

$$\text{Risk} = L * I * AP * 1/UP \tag{5}$$

HRM's compliance with ISO 27001, with its emphasis on human factors, ensures a holistic approach to risk management that effectively reduces human vulnerabilities and strengthens cybersecurity resilience within SMEs.

1.2. HRM Tools for Estimating Technical Risks

Any available open source risk assessment (RA) and Risk Management (RM) tool can be used to assess technical cyber risks as for example the ENISA, OWASP, MISP, Cyberwatching tools:

ENISA Risk Management (RM) Toolbox [8]: This toolbox includes methodologies for risk assessment, treatment options, incident response procedures, and guidelines for developing cybersecurity policies. It interprets risk scenarios using its own terminology, asset classifications, and threat taxonomies, standardizing results to a common risk matrix for comparable outcomes. The ENISA toolbox offers guidance, templates, and best practices for risk assessment, treatment, and communication in cybersecurity risk management.

OWASP Risk Assessment Calculator [9,10]: This tool helps organizations conduct risk assessments focused on web application security, identifying and prioritizing risks based on impact, likelihood, and exposure. Key features include risk identification, analysis, prioritization, documentation, and customization. The OWASP Risk Assessment Calculator enhances web application security and helps mitigate cybersecurity risks proactively.

MISP Project [11]: is an open-source Threat Intelligence and Sharing Platform that facilitates the exchange of threat intelligence and Indicators of Compromise (IoCs) related to malware, attacks, and other threats within a trusted community. It uses a distributed model to share technical and non-technical information in closed, semi-private, or open communities. This enhances the detection of targeted attacks, improves accuracy, and reduces false positives. According to MISP documentation, it is used to store, share, and collaborate on cybersecurity indicators and malware analysis, as well as to detect and prevent attacks, frauds, or threats against ICT infrastructures, organizations, or individuals. MISP is designed for information sharing rather than risk management.

Cyberwatching Cyber Risk Temperature Tool [12]: it consists of a questionnaire divided into two main sections: the first asks the respondent to provide a personal evaluation of their company's IT security, while the second includes technical questions. The questions cover various topics to analyze the company in different areas, such as:

Specific knowledge of the company's cybersecurity;
The methodologies employed within the company;
The distribution of administrative fees on systems;
The information segmentation policy;
Authentication policies for accessing corporate systems;
Previous assessments conducted.

Based on their scores, SMEs will be categorized into different profiles according to their vulnerability level.

1.3. HRM Socio-Psychological Instruments for Estimating Social Risks

Socio-psychological instruments play a crucial role in managing human threats within the context of risk management by assessing and mitigating the impact of human factors on cybersecurity and organizational safety. These instruments evaluate psychological and social behaviors that influence security practices. For instance, the Security Behavior Intentions scale, measures attitudes toward security behaviors like password management and software updates, which are essential for maintaining robust cybersecurity practices [13].

Moreover, addressing psychosocial risks in the workplace is integral to a comprehensive risk management approach. Psychosocial risks such as excessive workloads, lack of role clarity, and inadequate managerial support can lead to stress, anxiety, and depression, negatively impacting employees' mental health and increasing their vulnerability to cyber threats. Structured interventions, including training programs and awareness campaigns, are necessary to enhance employees' mental health and mitigate these vulnerabilities.

By incorporating socio-psychological factors into the risk management framework, organizations can better understand and address the human elements that contribute to security risks. This holistic approach improves the overall security posture and resilience against cyber threats, as it considers both technical and human aspects of cybersecurity [14].

HRM uses the Behavior Model (B=MAT) developed by Fogg [15] to identify the type of cue needed to encourage the appropriate action, depending on an individual’s motivation and ability to perform the act. According to Fogg, the likelihood of a behavior (B) occurring is a product of Motivation (M), Ability (A), and the appropriate Trigger (T), hence referred to as the B=MAT model.

Models such as the Five Factor Theory (FFT) and behavioral theories like Fogg's B=MAT model provide frameworks for understanding motivations and actions. These models can be used to analyze the security behaviors of users.

In HRM, we use extended psychological profiles as defined in [16] to analyze not only motivations, abilities, and triggers (Fogg’s model) but also personality traits and social characteristics.

Cyber profiling is the instrument used to identify human threats and vulnerabilities of ICT users as a proactive measure to select targeted social controls that will reduce employees’ vulnerabilities to human threats. HRM methodology uses a multidimensional cyber psychological profile for users to evaluate the factors that determine secure behaviors.

Co-creation workshops are also used to develop a comprehensive and effective risk treatment plan. These workshops are participatory events where ICT users collaborate. The adoption of security measures is streamlined through these workshops, designed to directly engage users in the development process, thereby enhancing the likelihood of triggering secure behavior. The fundamental goal of HRM co-creation workshops is to leverage the collective intelligence and diverse psychological profiles of ICT users, a strategy shown to foster broader engagement in cybersecurity practices [17].

Key features of HRM co-creation workshops include:

Diversity of Participants: These workshops prioritise the inclusion of a diverse range of ICT users, such as organisational insiders (e.g., CISOs, risk managers, incident handlers, defenders, administrators, and general employees), suppliers or supply chain partners, and third parties (e.g., suppliers, auditors, external penetration testers). This diversity is crucial for capturing a wide array of perspectives and experiences, which enriches the security discourse [18];

Collaboration: Participants are encouraged to collaborate in a structured setting, facilitated by experienced leaders. This approach mirrors effective teamwork strategies that are essential for problem-solving and innovation in cybersecurity [19];

Interactive Activities: Employing methods such as brainstorming sessions, design thinking exercises, and prototyping fosters a creative and engaging environment. These activities are foundational to generating practical and innovative solutions [20];

Risk Treatment Generation and Refinement: The workshops focus on co-developing a comprehensive set of social and technical measures that ICT users embrace and comprehend, which are refined through collaboration into viable security controls. This process aligns with best practices in risk management [21].

Co-creation workshops with various stakeholders enhance innovation and ensure relevant outcomes. Bringing together company management, ICT users, supply chain partners, industrial collaborators, policymakers, and researchers, these workshops develop effective risk mitigation plans and policies. Ramaswamy and Ozcan [22] highlight the strategic advantage of co-creation in fostering innovation and competitive advantage. By incorporating diverse perspectives, these workshops produce user-centric solutions, leading to higher adoption rates and greater stakeholder satisfaction. HRM supports the idea that security policies are better embraced when all ICT users and stakeholders participate in their creation.

The HRM developed an extended profile based on traits that identify the ICT users' secure behavior and the adversaries' profiles as have been developed by the authors [23] and outlined in this paper.

2. User Profiles

2.1. ICT User Profile (UP)

The proposed traits (Table 1) in the ICT user profile (UP) that define their maturity in adopting security practices include personality traits, social characteristics, technical skills, and capabilities relevant to their business roles within the SME. For instance, security professionals (e.g., CISOs, Risk Managers, auditors) are expected to possess skills defined in the European Cybersecurity Skills Framework (ECSF)[24], while general employees should have skills related to personal cyber hygiene [4,25].

Personal cyber hygiene practices encompass using strong passwords, regularly updating software, using reputable antivirus software, avoiding public Wi-Fi for sensitive transactions, recognizing and avoiding phishing attempts, regularly backing up data, reviewing and adjusting privacy settings, ensuring secure file sharing, and maintaining physical security.

Additional traits proposed in Table 1 include motivations that encourage secure user behavior, as well as triggers (opportunities/measures) that SMEs can adopt.

Table 1. HRM-multi dimensional profile of ICT user with secure behavior example.

HRM ICT users' profiles (HRM-UP)	
Personality Traits	
Vigilance	Consistently remains alert and attentive to potential security threats, and is proactive in identifying and addressing suspicious activities.
Responsibility, Curiosity	Takes full ownership of their role, with an innate curiosity that drives them to deepen their understanding of cybersecurity threats and vulnerabilities.
Adaptable-Openness to experiences	Displays flexibility and openness to new security technologies, strategies, and approaches that enhance their security posture. Possesses a blend of intellect and creativity, demonstrates originality, and shows a keen scientific interest alongside a spirit of adventurousness.
Resilient	Has the capacity to cope with stress, setbacks, and failures, demonstrating resilience by quickly bouncing back and steadfastly maintaining a strong focus on achieving security objectives.
Social Traits	
Social exposure	Adapts to conventional social norms with ease, excelling in forging strong bonds with each co-worker. Collaborates effectively with colleagues, security teams, and external partners to tackle security challenges, sharing information and insights for collective benefit.
Conventional relationships	Effortlessly establishes professional virtual relationships, fostering collaborations and creating synergies.
Ethical	Individuals with integrity prioritise honesty, transparency, and respect, steadfastly adhering to ethical principles and professional codes of conduct.

The assessment of secure behavior levels among ICT users is facilitated through the use of anonymized questionnaires, a method supported by research indicating its effectiveness in gathering sensitive data [26].

To select appropriate social measures for improving security behavior, co-creation workshops are employed.

2.2. Adversary Profile (AP)

Similarly, the estimated attackers' profile proposed by Kioskli and Polemi [27](see Table 2) offers a comprehensive, multi-dimensional, and measurable profile of attackers based on psychological, behavioral, societal, and technical abilities, as well as personality traits, using the Five Factor Model (FFM) and Fogg's Behavioral Model.

Table 2. Estimated Attackers' Profiles (Kioskli & Polemi, 2020) (HRM-AP).

Personality Traits	**Description & Examples**
Extraversion	Gregariousness (e.g., Social engagement in attackers' groups); Assertiveness/Outspokenness (e.g., Leadership skills); Activity/Energy level (e.g., Enjoys a busy life); Positive Emotions/Mood (e.g., Happiness)
Conscientiousness	Orderliness/Neatness (e.g., Well-organized) Striving/Perseverance (e.g., Aims to achieve excellence) Self-Discipline (e.g., Persistent engagement to goals) Dutifulness/Carefulness (e.g., Strong sense of duty) Self-Efficacy (e.g., Confidence to achieve goals)
Openness to experiences	Intellect/Creativity Imaginative (e.g., Intellectual style) Scientifically Interested/Originality (e.g., Evidence-based) Adventurousness (e.g., Experiences of different things)

Social - Behavioural Traits	Description & Examples
Selected social exposure	Difficult to adapt to conventional social norms (e.g., Events) Easy to build virtual anonymous, professional relationships (e.g., Using anonymous identity has contacts with other attackers in the Deep Web) Easy to build strong e-bonds in hacking communities (e.g., These communities are closed to the public)
Not conventional relationships	Difficult to build physical relationships or contacts Easy to build professional (with other attackers) virtual, anonymous relationships under their moral code (us versus them approach)
Not talkative	Difficult to initiate small casual talks or social talks Difficult to express him/herself
Manipulative	Easy manipulating people via electronic means (e.g., phishing)

2.3. Measuring Profiles

The HRM profile calculations (UP and AP) will adopt the scales in [28] where indicative measures are proposed (see Table 3):

Table 3. HRM- Quantification of UP /AP.

Levels	Description	Semi-Quantitative Values		UP/AP score of profile	Indicative Social Measures needed
Very High (VH)-5	Sophisticated	96-100	10	> 96% of each of the traits in each category	social and technical threat intelligence updates, ethical training, advance cybersecurity exercises
High (H)-4	Experienced	80-95	8	> 80%	ethical training , cybersecurity exercises, social and technical threat intelligence updates, ethical training
Medium (M)-3	Moderate	21-79	5	> 21%	secure behaviour intervention, training in operational cybersecurity, cybersecurity exercises
Basic (B)-2	Basic	5-20	2	> 5%	awareness , secure behaviour interventions , training in operational cybersecurity exercises

Low (I) -1	Insufficient	1-4	0	< 5%	awareness , secure behaviour interventions , training in basic concepts, basic cyber exercises

3. Phases of the HRM Methodology and Implementation

HRM methodology compromises of the following main three (3) phases according to standards (Figure 1):

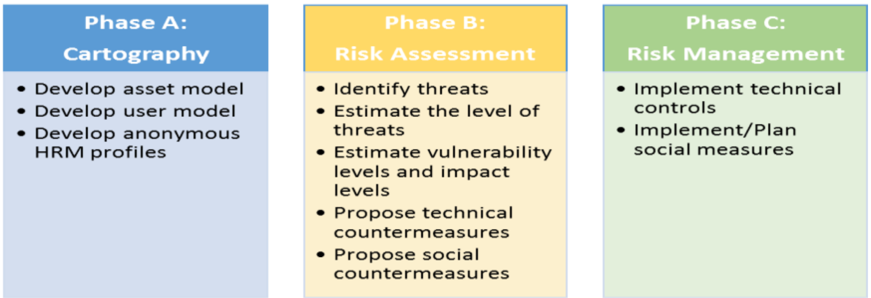
Phase A:
Cartography
Develop asset model
Develop user model
Develop anonymous HRM profiles
Phase B:
Risk Assessment
Identify threats
Estimate the level of threats
Estimate vulnerability levels and impact levels
Propose technical countermeasures
Propose social countermeasures
Phase C:
Risk Management
Implement technical controls
Implement/Plan social measures

Figure 1. HRM Phases.

Phase A: Cartography (Set Boundaries)

A1: Develop asset inventory

An inventory of all assets under assessment should be developed and maintained, recording details such as in Table 4:

Table 4. Asset Inventory example.

	General Information	Technical Specifications	Location and Owner	Network Configuration (for Servers)	Implementation of Controls - History of Updates
1	Asset ID: Unique identifier for each piece of equipment.	Processor: Type and speed of the processor.	Location: Physical location of the asset.	IP Address: Network IP address.	Controls Implemented
2	Asset Type: Differentiates between PCs and servers.	RAM: Amount of memory in GB.	Owner of Asset (Assigned to): Name of the employee responsible of the asset.	Role: Function or role of the server (e.g., file server, web server).	Update History of controls
3	Brand/Model: Specific model of the hardware.	Storage: Size and type of storage (e.g., SSD, HDD).	Owner/ User(s) of asset : interacting entity	-	Testing date of controls
4	Serial Number: Manufacturer's serial number.	Operating System: Installed	-	-	-

Date of purchase …..	operating system and version.

3.1.

A2: Model the interaction of the assets

Provide diagrams that identify the interrelations of the assets under assessment using a Business Model Processing (BMP) tool using specific symbolism e.g. solid lines with arrows indicate the direction of data flow between devices (e.g., from workstations to servers, servers to storage). Dotted lines might indicate wireless connections or less direct interactions (e.g., mobile devices connecting via Wi-Fi). An example of an asset model is (Figure 2):

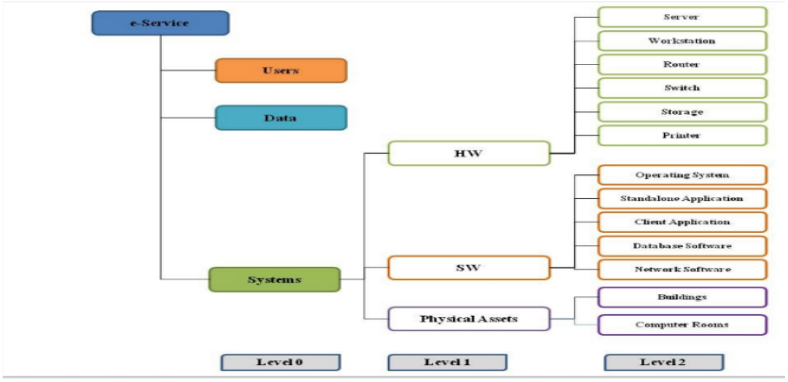

Figure 2. Asset Model.

There are various open source BPM tools that can be used¨ e.g. bpmn.io (https://bpmn.io/), Modelio (https://www.modelio.org/index.htm), Camunda Modeler (https://camunda.com/), Bizagi Modeler (https://bizagi.com/en), Bonita BPM (https://www.bonitasoft.com/), Activiti (https://www.activiti.org/), jBPM (https://www.jbpm.org/), ADONIS: Community Edition (https://www.adonis-community.com/en/).

A3: Develop user model

Identify all ICT users (found in phase A1 above for all assets under assessment) that own or use the asset(s) of the ICT system which is in the perimeter of this assessment. Develop a user inventory including information e.g. as shown in the next Table (Table 5):

Table 5. User Inventory.

	User ID: 001	User ID: 002	….
General Information	Name: Full name of the employee/ Role/ Location/Contact	…	-
System & Credential System Access	Privileges, List of systems the user has access to (e.g., CRM, ERP, Email),	…	-
Supervisor & Interrelations	Direct supervisor or manager Interactions with other users (model interaction)	…	-

Furthermore, a user model describing the interaction among users e.g. in Figure 3:

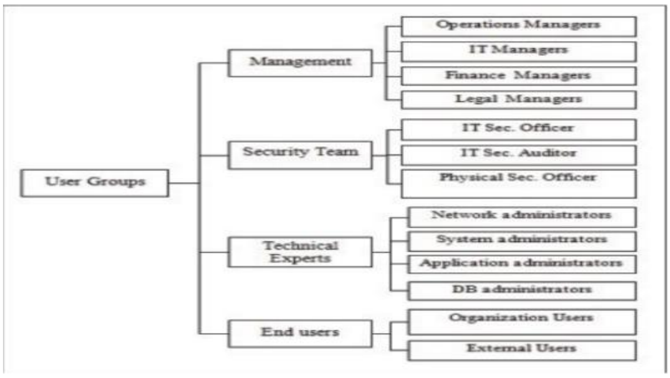

Figure 3. User Model.

A4: Develop and estimate anonymous HRM -UP and potential HRM-AP

In this phase we will first develop an enhanced user inventory following the next steps:

a) For all ICT users compile anonymous profiles using Table 1.

b) Measure the UP profiles using the scales in Table 3 during the co-creation workshops.

c) Develop the HRM- User inventory by adding to user inventory in Table 6, the UP scores and social measures implemented and pending.

Table 6. HRM-User Inventory.

	User ID: 001	User ID: 002	…
General Information	Name: Full name of the employee/ Role/ Location/Contact	…	-
System & Credential System Access	Privileges, List of systems the user has access to (e.g., CRM, ERP, Email),	…	-
Supervisor & Interrelations	Direct supervisor or manager Interactions with other users (model interaction)	…	-
UP score	See Table 3 above	...	-
Social Measures Implemented/Required	See Table 3 above	….	….

Then we will identify and measure the profiles of the potential adversaries by following the next steps:

a) From past history (previous attacks, company/sectoral threat intelligence) compile the profiles of the potential adversaries using Table 2.

b) Measure the Adversaries Profiles (AP) using the scales in Table 3 utilizing past experience, threat intelligence, crowd sourcing.

3.2. Phase B: Risk Assessment

Risk assessments should identify, quantify, and prioritise information security risks against defined criteria for risk acceptance and objectives relevant to the organisation.

The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

Assessing risks and selecting controls may need to be performed repeatedly across different parts of the organisation and information systems, and to respond to changes.

The process should systematically estimate the magnitude of risks (risk analysis) and compare risks against risk criteria to determine their significance (risk evaluation).

The information security risk assessment should have a clearly defined scope and complement risk assessments in other aspects of the business, where appropriate. The steps we follow are:

B1- Identify the threats (physical/cyber/ human)

B2-Estimate the level of threats

B3- Estimate vulnerability levels and impact levels

B4- Estimate the risk level

B5- Propose technical countermeasures

B6- Propose further social measures

To propose appropriate social measures, co-creation workshops will be employed. In these workshops, ICT users collaborate to generate and refine ideas for social and technical security measures, ensuring these are pragmatic and readily adoptable [29].

3.3. Phase C: Risk Management (Treatment)

Having identified and evaluated the risk level in the risk assessment phase, as it was described in the previous paragraphs, the next step involves the identification of the actions that must take place in order to manage the detected threats and propose specific treatment plans, according to the Interoperable EU Risk Management Framework [8]. More specifically, the risk treatment process is mapped with the ISO 27005 and its objective is the selection of the treatment options that are suitable for the risks that have been identified. Some potential treatment options may include risk mitigation, avoidance, sharing etc.

For the implementation of technical and social measures, we use co-creation workshops where the SME governance members share business intelligence and cost-benefit analysis expertise to select those selected measures for implementation and testing. The proposed technical and social measures (from Phase B (B5) can be implemented immediately, can be postponed or ignored. A risk treatment plan needs to be compiled and Tables 4 and 5 need to be updated.

4. User Profiles

A small and medium healthcare enterprise, operating across two separate facilities, offers e-health services to its personnel and patients. These services encompass, amongst others, e-diagnosis, e-prescriptions, and the handling of patients' sensitive data.

Through this use case all phases of the above HRM methodology will be demonstrated step by step.

4.1. Phase A (Cartography)

Steps A1-A2:

The interconnected facilities enable users with varying access levels to retrieve private patient data from a shared, encrypted database. Each facility operates with a server and personal computers networked together, facilitating communication with the database. Given this setup, the enterprise must implement comprehensive security measures to safeguard its ICT systems effectively.

In the current use case, a doctor connects to a specific PC with his/hers own personal account in order to check patients' data. During that process it comes to his/her attention that many sensitive data are missing. The doctor's personal account has a specific data access policy that allows accessing, entering and altering the data only for his/hers patients from any computer in the HSME's facilities.

Following the HRM methodology in the first phase (Cartography), firstly an asset inventory must be developed, where the identification of all assets under assessment must be included. In the current use case, as it is depicted in figure 4, all physical, telecom, IT, data, services and users' assets are recorded. Hence, the facilities' buildings, the telecommunication and network equipment, the database, the software, hardware and data, the communication services for the data exchange, the users, like doctors and patients, are identified and documented.

Hardware devices, software applications, personnel, physical location, utilities, and organizational infrastructure fall into this category. In the current use case, primary assets include accessing patient data for treatment and personal patient information accessed by doctors. Supporting assets encompass PCs, servers, and networks in the hardware category; doctors, system administrators, and personnel with access as normal or privileged users in the personnel category; suppliers of specific systems; physical rooms or offices housing hardware equipment in the location and utilities category; and existing cloud, network, and hosting services in the organizational infrastructure category. The information can be summarised in the next asset inventory (Table 7):

Table 7. Asset Inventory.

General Information	Technical Specifications	Location and Owner	Network Configuration (for Servers)	Implementation of Controls - History of Updates
Asset ID: Unique identifier for each asset.	Software Suite for Patient Records, Network infrastructure etc.	Location: Physical location of the asset.	Wired and Wireless setup	Controls Implemented
Asset Type: Software or Hardware	Software suite for patients records / Server hardware for data storage	Owner of Asset (Assigned to): Name of the employee responsible of the asset.	Role: Function or role of the software or hardware	Update History of controls
Brand/Model: Specific model of the software or hardware.	Electronic Medical Records (EMR) System, Database Management Platform etc.	Owner/ User(s) of asset : Doctor, Nurse, admin etc	-	Testing date of controls
Serial Number: Manufacturer's serial number. Date of purchase …..	Software versions, Hardware specifications	-	-	-

All the above mentioned, provide valuable information from a technical perspective. Additionally, the description of all assets' interdependencies and the development of the user model of the ICT system under assessment in the healthcare entity must be conducted.

Focusing on the user functions of one facility of the HSME, the users that are involved are doctors, patients, nurses, system admins, system technicians and additional staff. All the users have access to the HSME's Personal Computers with accounts that have different user access rights, depending on their specialty. For example, each doctor has access to his/hers patient data only or nurses have access to specific medication depending on their department placement. The system admin has access to the server and personal computers in all user accounts and data stored in the database. The system technicians have additional access to all systems infrastructures including PC's, network devices etc. (Figure 4).

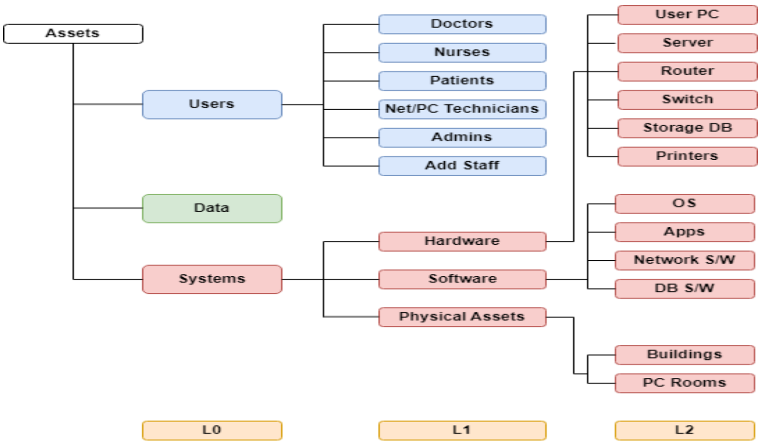

Figure 4. HSMEs users'/assets model.

In the current HRM methodology phase, the next step includes the anonymous user profile development and secure level behaviors estimation, taking into account the included information in table 1, in order to produce the social mitigation measures to enhance the users' secure behavior.

Step A3:

The users that interact with the in our scenario are: 2 doctors, 2 patients, 1 nurses, 1 admin, 1 technician and 1 additional staff. The co-creation workshops have been conducted and the scores of the profiles have been estimated as summarized in the next Table (Table 8):

Table 8. HRM-User Inventory.

	User ID: 001-doctor1	User ID: 002-nurse	**....**
General Information	Name: Full name of the employee/ Role/ Location/Contact	…	
System & Credential System Access	Privileges, List of systems the user has access to (e.g., CRM, ERP, Email),		
Supervisor & Interrelations	Direct supervisor or manager Interactions with other users (model interaction)		-
UP score	Basic (B)-2		
Social Measures Implemented/Required	According to Table 3 the measures needed are: awareness , secure behaviour interventions , training in operational cybersecurity exercises		

4.2. Phase B: Risk Assessment

Moving to the next phase of the HRM methodology, Risk Assessment strategies are implemented. The ENISA RM Toolbox is utilized to execute Phase B strategies. According to the toolbox, the initial steps involve defining attack/risk scenarios and identifying assets from a technical perspective, which were covered in the previous phase. The following paragraphs outline the subsequent technical representation steps.

Additionally, it is important to note that the ENISA RM Toolbox includes four libraries: Terms mappings, Assets mappings, Threats mappings, and Risk-Impact levels mappings.

In the first library, based on the current use case scenario, we identify the frameworks and methodologies terminology. Utilizing the toolbox glossary and terminology sample library, we search for definitions of terms and incidents to fully understand the system's situation based on ISO/IEC 27005:2018 and the ENISA IT Security Risk Management Methodology v1.2. For example, the definition of "Threat" according to ISO/IEC 27005:2018 is "potential cause of an unwanted incident, which can result in harm to a system or organization," matching 100% with ISO/IEC 27000:2018's definition.

In the second library, we identify the assets of the current scenario. Specifically, primary assets in HSMEs include all core business processes, functions, services provided to external parties, and information/data supporting business processes or activities of the organization, as outlined in ISO/IEC 27005:2018. These assets are sensitive and include processes essential for the organization's mission. Information and data are also classified as primary assets, encompassing vital information necessary for the organization's mission or business, as defined by national privacy laws. Similar principles are applied in the IT Security Risk Management Methodology v1.2.

Steps B1 and B2 -Identify the threats (physical/cyber/ human):

Following asset identification, the next step involves threats mapping using the third library of the ENISA RM Toolbox. This library allows for the identification of various threat types according to the IT Security Risk Management Methodology v1.2 and ISO/IEC 27005:2018. It provides additional details such as threat types, security dimensions, involved assets, and examples.

For the current use case, Table 9 lists the identified threats. These threats can occur unintentionally or intentionally through accidental or deliberate actions, impacting assets such as hardware devices or software and applications, affecting Confidentiality, Integrity, and/or Availability.

The identified threats in this case include hardware or software failures, user errors, and unauthorized access, covering a range of severity levels (Table 9).

Table 9. Threats Identification.

Threat	Category	Security Dimension	Action	Assets	Explanation
Hardware or Software failure	Industrial	Availability	Deliberate or Accidental	H/W devices and equipment – S/W and applications	Failures in the equipment (eg. user PC, server, router etc) and/or programs (eg. apps, OS etc.)
User errors	Errors and unintentional failures	Confidentiality, Integrity, Availability	Accidental	H/W devices and equipment – S/W and applications – Organisational infrastructure	Mistakes by persons when using the services, data, etc. For example making a mistake in saving data, or in a PC's usage.
Threat of system / security administrator errors	Errors and unintentional failures	Confidentiality, Integrity, Availability	Accidental	H/W devices and equipment - S/W and applications- Organisational infrastructure	Mistakes by persons with responsibilities for installation and operation of the systems / system's security. For example the PC technician can unintentionally cause the system

					failure of a user PC or server.
Destruction of information	Errors and unintentional failures	Availability	Accidental	All the categories of supporting assets	The accidental loss of the information due to a user's (doctor or nurse) mistake.
S/W vulnerabilities	Errors and unintentional failures	Confidentiality, Integrity, Availability	Accidental	S/W and applications	Defects in the code that cause a defective operation without intention on the part of the user but with consequences to the data confidentiality, integrity, availability or to its capacity to operate. This can be detected in apps or OS for example.
Abuse of access privileges	Willful attacks	Confidentiality, Integrity, Availability	Deliberate	S/W and applications - Locations and Utilities - Organisational infrastructure	When users abuse their privilege level to carry out tasks that are not their responsibility, there are problems. For example a user might use a doctor's account and delete patients' data.
Misuse	Willful attacks	Confidentiality, Integrity, Availability	Deliberate	S/W and applications - Locations and Utilities - Organisational infrastructure	The use of system resources for unplanned purposes, typically of personal interest. For example a user connects an app or to a PC inside the HSMEs facility.

Steps B3-B4:

Based on the identified assets and risks, the risk assessment process can now begin for the current use case scenario. Primary assets at risk include accessing and managing patient health records, prescriptions, dosages, and scheduled health checks, along with compromising the security of personal patient and doctor data.

Supporting assets affected include HSME hardware, software, personnel, system suppliers, and infrastructure. Potential issues include hardware or software malfunctions leading to data loss, unintentional breaches of data confidentiality, integrity, or availability by HSME personnel, and risks associated with system suppliers not meeting HSME requirements. Placement of systems in HSME facilities may also invite unauthorized access.

The OWASP risk rating methodology uses the standard model (Risk = Likelihood * Impact). During risk identification, information on threats, types of attacks, vulnerability levels, and potential impacts is gathered to assess risks.

In this use case, the risk of patient data loss is identified. The first step involves estimating the "Likelihood" level. For example, in the case of unauthorized access threats, where attackers gain unauthorized system access, determining threat agent and vulnerability factors is crucial.

For adversary factors (threat agents), the goal is to estimate the likelihood of a successful attack based on skill level, motive, opportunity, and size, rated on a scale from 0 to 9. In the worst-case scenario, potential threats include anonymous internet users with network and programming skills, high motivation for significant rewards, requiring access or resources, as outlined in Table 10.

Table 10. Threat Agent Factors.

Threat	Skill level	Motive	Opportunity	Size
Unauthorised access	6	9	4	9

For a more realistic assessment, we use the HRM-AP score (refer to Tables 2 and 3), which considers additional traits of the adversary (threat actor).

Regarding vulnerability factors, the aim is to estimate the likelihood of a specific vulnerability in terms of ease of discovery, exploitability, awareness, and intrusion detection, rated on a scale from 0 to 9. Table 11 illustrates a scenario where the vulnerability of unauthorized access is easily discoverable and exploitable using automated tools. Threat agents are aware of this vulnerability, making exploitation feasible through logging and reviewing.

Table 11. Vulnerability Factors.

Threat	Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
Unauthorised access	7	9	6	3

Likelihood also depends on the secure behavior of all ICT users interacting with the asset. According to HRM, accuracy improves by considering this factor. The next step is to estimate the Impact, which includes Technical and Business Impact factors.

Regarding Technical Impact, considerations include confidentiality, integrity, availability, and accountability to gauge the magnitude of impact. Table 12 illustrates scenarios such as extensive critical data disclosure, serious data corruption, and primary services interruption caused by completely anonymous individuals.

Table 12. Technical Impact Factors.

Threat	Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability

Unauthorised access	7	7	7	9

For the Business Impact factors, considerations include financial damage, reputation damage, non-compliance, and privacy violations. Table 13 presents scenarios such as a minor effect on business profit, loss of goodwill in reputation, and a high-profile violation involving thousands of people's data.

Table 13. Business Impact Factors.

Threat	Financial damage	Reputation damage	Non-complience	Privacy violation
Unauthorised access	3	5	7	7

Using the OWASP Risk Rating Calculator [9] it is possible to determine the severity of the risk by calculating it. For the case described in the above paragraphs the results of the calculation produces a High overall risk severity for the unauthorised access threat scenario.

In the above calculations, ICT user profiles have not been fully considered (only partially the AP score). In HRM methodology, we would multiply the OWASP score with the 1/min {UP score} of all users interacting with the asset.

Steps B5 and B6:

HSMEs must mitigate risks by implementing:

Technical Controls: Advanced access control, data encryption, network and endpoint security;
Administrative Controls: Policy development, access management, employee training, and security audits;
Physical Controls: Access control systems, surveillance, alarms, and restricted-access storage;
Social Controls: Enhance software and IT skills based on personality traits, social factors, and technical skills identified earlier.

Effective threat management includes educating employees about cyber threats, training in modern technologies, regular cybersecurity workshops, phishing simulations, incident response programs, data protection seminars, and promoting strong passwords and multi-factor authentication.

By combining these controls, HSMEs can effectively mitigate unauthorized access and patient data loss.

5. Conclusions

In conclusion, the security of ICT systems within SMEs is critically important, especially when addressing human threats. These threats, stemming from a range of human vulnerabilities, are often overlooked in traditional risk management approaches. Regular assessments and tailored risk treatment measures can help SMEs mitigate the negative impacts of human threats. The Human Risk Management (HRM) methodology proposed in this paper builds upon ISO 27001 methodologies and leverages available tools for assessing technical threats and estimating associated risks. For human element-related threats, HRM employs socio-psychological techniques to evaluate the maturity of ICT users in adopting security practices and the strength of potential adversaries. It develops and estimates profiles of ICT users and adversaries, incorporating these estimates into overall risk evaluations.

In the use case presented, a healthcare SME implements the HRM methodology by utilizing existing risk assessment tools and estimating the cybersecurity maturity of healthcare participants interacting with the ICT system. Controls in this use case include regular training sessions for medical staff on recognizing phishing attempts and ensuring proper data handling practices to protect patient information. By enhancing the cybersecurity maturity of employees and fostering a robust cybersecurity culture within the SME, human threats can be significantly reduced, thereby improving overall cybersecurity resilience.

Acknowledgments: The authors would like to acknowledge the financial support provided for the following projects: The 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; the 'Human-centered Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042; the Advanced Cybersecurity Awareness Ecosystem for SME's (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; the 'Harmonizing People, Processes, and Technology for Rubust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101158555; and the 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

References

1. ISO/IEC 27001:2005. Information Technology - Security Techniques – Information Security Management Systems – Requirements. Known as ISO 27001.
2. ISO/IEC – Global standards, https://www.iso.org/home.html, last assessed 2024/9/5.
3. ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of Practice for Information Security Management. Known as ISO 27002.
4. NIST cyber hygiene guidelines, https://www.nist.gov/blogs/taking-measure/stay-safe-and-secure-online-during-cybersecurity-awareness-month-and-all-year, last accessed 2024/9/5.
5. Kioskli K.; Polemi N. Estimating attackers' profiles results in more realistic vulnerability severity scores. In proceedings of the 13th International Conference on Applied Human factors and Ergonomics (AHFE2022), July 24-July 28, 2022, New York, New York, USA, **2022**, 53 (1), 138-150. Springer, Elsevier, CRC.
6. Kioskli K.; Fotis T.; Nifakos S.; Mouratidis H. The Importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. Applied Sciences, Special Issue eHealth Innovative Approaches and Applications, **2023**, 13(6), 1-16.
7. Alwaheidi M.; Islam S.; Papastergiou S.; Kioskli K. Integrating Human Factors into Data-driven Threat Management for Overall Security Enhancement. In: Abbas Moallem (eds) Human Factors in Cybersecurity. AHFE (2024) International Conference. AHFE Open Access, **2024**, vol 127. AHFE International, , USA. http://doi.org/10.54941/ahfe1004778.
8. ENISA risk management toolbox. Available online: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox, last accessed 2024/9/5.
9. OWASP risk assessment calculator. Available online: https://owasp-risk-rating.com/, last accessed 2024/9/5.
10. OWASP Threat Modeling Process. Available online: https://owasp.org/www-community/Threat_Modeling_Process, last accessed 2024/9/5.
11. MISP Project. Available online: https://www.misp-project.org/, last assessed 2024/9/5.
12. Cyberwatching. Available online: The European watch on Cybersecurity & Privacy, https://cyberrisk.cyberwatching.eu/Pages/Home.aspx, last accessed 2024/9/5.
13. Egelman S.; Peer E. The Security Behaviour Intentions scale. Frontiers, **2015**.
14. Nobles C.: Understanding the Human Factor of Cyber Security. IEEE IT Professional, **2018**, 20(3), 7-15. https://doi.org/10.1109/MITP.2018.032501746
15. Fogg B. J. A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology, **2009**, pp. 1-7.
16. Kioskli K.; Polemi N. A psychosocial approach to cyber threat intelligence. International Journal of Chaotic Computing, **2020**, 7(1), 159–165.
17. Williams H. The impact of collective intelligence on cybersecurity. Cyber Psychology, **2020**, 7(3), 111-126.
18. Schneier B. Liars and Outliers: Enabling the Trust That Society Needs to Thrive. Wiley, **2012**.
19. West D. M. Digital Government: Technology and Public Sector Performance. Princeton University Press, **2012**.

20. Brown T. Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation. HarperBusiness, **2009**.
21. Stoneburner G.; Goguen A.; Feringa A. Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30). National Institute of Standards and Technology, **2022**.
22. Ramaswamy V.; Ozcan K. What is co-creation? An interactional creation framework and its implications for value creation. Journal of Business Research, **2018**, 84, 196-205.
23. Kioskli K.; Polemi N. Psychosocial approach to cyber threat intelligence. International Journal of Chaotic Computing, **2020**, 7(1), 159-165.
24. ENISA ECSF. Available online: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework, last accessed 2024/9/4.
25. StaySafeOnline guidelines. Available online: https://staysafeonline.org/resources/online-safety-basics/, last accessed 2024/9/5.
26. Smith J.; Doe A.; James S. The efficacy of questionnaires in the assessment of secure behaviors in IT users. Journal of Cybersecurity Research, **2019**, 12(2), 45-59.
27. Kioskli K.; Polemi N. Measuring psychosocial and behavioural factors improves ttack potential estimates. In Proceedings of the 15th International Conference for Internet Technology and Secured Transactions, **2020**, 216–219.
28. Kioskli K; Polemi N. A socio-technical approach to cyber risk assessment", International Journal of Electrical and Computer Engineering. **2020**, 14(10), 305-309,.
29. Mattelmäki T.; Vaajakallio K.; Koskinen I. What happened to empathic design? Design Issues, **2014**, 30(1), 67-77. DOI: 10.1162/DESI_a_00249

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.