Bridging the Gap between Security Competencies and Security Threats: Toward a Cyber Security Domain Model

Florian Schütz
University of Goettingen
florian.schuetz@uni-goettingen.de

Florian Rampold
University of Goettingen
florian.rampold@uni-goettingen.de

Kristin Masuch
University of Goettingen
kristin.masuch@uni-goettingen.de

Patricia Köpfer
University of Stuttgart-Hohenheim
patricia.koepfer@uni-hohenheim.de

Dominik Mann
University of Goettingen
dominik.mann@uni-goettingen.de

Julia Warwas
University of Stuttgart-Hohenheim
julia.warwas@uni-hohenheim.de

Simon Trang
University of Goettingen
simon.trang@uni-goettingen.de

Abstract

Security incidents are increasing in a wide range of organizational types and sizes worldwide. Although various threat models already exist to classify security threats, they seem to take insufficient account of which organizational assets the threat events are targeting. Therefore, we argue that conducting more job-specific IT security training is necessary to ensure organizational IT security. This requires considering which assets employees use in their daily work and for which threat events employees need to build up IT security competencies. Subsequently, we build a framework-based Cyber Security Domain Model (CSDM) for IT-secure behavior. We follow the Evidence Centered Assessment Design (ECD) to provide a deep-dive analysis of the domain for IT-secure behavior. As the leading result relevant for research and practice, we present our CSDM consisting of 1,087 cyber threat vectors and apply it to five job specifications.

Keywords: Organizational Cybersecurity, SETA Programs, Security Competencies, Cyber Security Domain Model, Evidence-Centered Assessment Design

1. Introduction

Security incidents are increasing every year (ENISA, 2021). Consequently, these can result in meaningful financial damages (Jouini et al., 2014). This highlights the need for organizations to understand security gaps and threats regarding their information systems and assets. Since humans are often seen as the weakest link in the information security chain (Abawajy, 2014), security threats can be prevented when employees are aware of potential security risks and have comprehensive information security competencies. According to Gerić and Hutinski (2007), information systems are exposed to various security threats, which both researchers and practitioners classify in many ways. A security threat can be defined as any adverse incident that causes integrity or confidentiality violations of organizational assets, individuals, or organizations (Blank & Gallagher, 2012; Gerić & Hutinski, 2007). Security education and training awareness programs (SETA) have been introduced in organizations to address this issue (Posey et al., 2015; Thomson & von Solms, 1998).

However, studies have shown that these tend to be less efficient than they should be (Alshaikh et al., 2020; Kirova & Baumoel, 2018). Several researchers note that the main reason for this lies in “one-size-fits-all approaches” (Hu et al., 2021; McCoy & Fowler, 2004; Valentine, 2006). This implies that employees receive the same security training regardless of their job and competencies (Valentine, 2006). In research fields such as vocational education, the concept of competence plays a crucial role in explaining the relation between job performance and behavior (Seeber, 2016; Winther, 2010). Competence in this context is understood as "the latent cognitive and affective-motivational underpinning of domain-specific performance in varying situations" (Blömeke et al., 2015). Regarding the IT security domain, Rampold et al. (2022) have shown that both conceptual and design-focused SETA literature to date has insufficiently considered the findings of competence research.

Since the vocational education domain applies this construct mainly to commercial and industrial

URI: https://hdl.handle.net/10125/103375
978-0-9981331-6-4

professions (Achtenhagen & Winther, 2008; Klotz, 2015; Seeber, 2016), we argue it can be transferred to understand better why employees fail to comply with IT security standards and are exposed to various security threats. In fields of research such as vocational education, domain models are built to get an in-depth overview of domain-related requirements and tasks (Winther, 2010). We argue that an IT security domain model is critical as a first step to educating employees on security-related behaviors. In this context, various threat models in IT security were identified and analyzed in terms of their dimensions. Furthermore, common ISMS standards (i.e., ISO 2700x, NIST Framework) were also reviewed to understand better the possible range of IT security measures in organizations.

IT security threat classification is not a new research topic. Approaches such as security threat classifications from Gerić and Hutinski (2007) and Jouini et al. (2014) provide guidance on protecting information systems and assets. These models include several dimensions, such as threat source, intention, frequency, and area of interest.

However, previous threat models are complex and are not developed under the lens of a framework-based approach. As vocational education research points out, the domain needs to be analyzed in detail to gain a comprehensive understanding of the required competence in the field of interest. We, therefore, aim to build a framework-based domain model for IT-secure behavior that can be adjusted to any job specifications and formulate the following research question:

What security threats does a domain model for IT-secure behavior need to consider when addressing security training for employees based on their job specifications?

To provide this specification in a valid scientific manner, we integrate approaches from vocational competence research (Pellegrino, 2010; Rausch et al., 2016) and security threat classifications from IS research. We apply the first step of the Evidence Centered Assessment Design (ECD) framework in a three-stage approach by Mislevy et al. (2003) to provide a deep-dive analysis of domain analysis for IT-secure behavior. Our results suggest that it is crucial to consider the assets employees use in their daily work and for which threat events employees need to be sensitized. The outcome is a Cyber Security Domain Model (CSDM) that consists of two dimensions (threat area & threat event) with 1,087 threat vectors. Our introduced CSDM, therefore, not only considers the operationally conceivable threat events (e.g., phishing attack) separately but at the same time in which threat areas or at which critical assets the threat can emerge. We also show how the CSDM can be leveraged to identify specific security threats relevant to different job specifications. In this way, employees can be trained on the threat events that may occur with corresponding assets. Thus, job or even task-specific skills can be acquired in contrast to general IT security training.

We contribute to existing security and vocational education literature in at least three ways. First, the domain model can be used to design SETA programs for different peer groups. Second, our CSDM builds the first step inside the ECD framework and can be interpreted as a prerequisite for a specific and competence-based approach to model assessments for competence measurement in the domain of IT-secure behavior. Third, we are the first to initiate a framework-based approach to provide a security threat classification.

2. Research Background

2.1. Security Threat Classification

Ensuring security is a significant challenge in organizations. We can observe two trends influencing the odds of security incidents becoming more likely. First, as digitalization advances, the range of assets involved in working environments increases steadily. Second, attackers tend to use more sophisticated methods to obtain private information than in the past (ENISA, 2021). Consequently, it is vital to have a deep understanding of security threats that cause the vulnerability of information systems and assets. Several international security standards, such as NIST and ISO/IEC, exist to provide guidance for safely encountering security threats. In this context, there have been various interests in security threat classification to develop countermeasures to overcome security risks (Jouini et al., 2014). To provide an overview, we elaborate on former security threat classification approaches in the following.

Gerić and Hutinski (2007) present an information system security threat cube classification (C3 model) composed of three superordinate dimensions. The first component, *security threat frequency,* provides information on the likelihood or frequency of a specific security threat. Next, the authors define the *area of security threat activity* as another dimension. This dimension includes the focus domain, such as information systems and assets being the target of a security threat. Gerić and Hutinski (2007) distinguish between physical, personnel, communication, data, and operational security. Lastly, the authors identify the *security threat source* as a component of their threat classification. Threat sources are divided into insiders (persons with granted system authorization) and outsiders (external persons of the organization without system permissions).

Jouini et al. (2014) extended the basic idea of a multi-dimensional framework to classify security threats. Grounded on a literature-based list of criteria for threat classification, they develop a five-dimensional model including the *security threat source*, *agents*, *motivation*, *intention,* and *threat impacts*. While security threat agents represent the actors in charge of security incidents, motivation describes whether the attack is malicious or non-malicious. Furthermore, the intention indicates if a threat agent deliberately placed an attack on a system or asset. Finally, the threat impact defines possible consequences of a threat action, such as destruction, corruption, and theft/loss of information.

In addition, Alhabeeb et al. (2010) propose a threat classification model grounded on three classification dimensions. However, in contrast to the C3 model, the presented model mainly focuses on the *attacker's prior knowledge about the system*. Moreover, it contains the *criticality of the area* of the threat and the *loss* caused by the threat. Compared to the C3 model, this approach focuses on deliberated threats caused by attackers. The authors assume that the attacker's insider knowledge about the target system structure has a crucial influence on the threat impact.

However, the presented security threat classifications have in common that they take multiple dimensions into account when classifying threats by impact. The disadvantage of this approach is the growing complexity of each additional dimension. Moreover, it is questionable whether dimensions such as threat source and agent are relevant for building cyber security domain models since they do not relate to the competence of persons to recognize a threat situation.

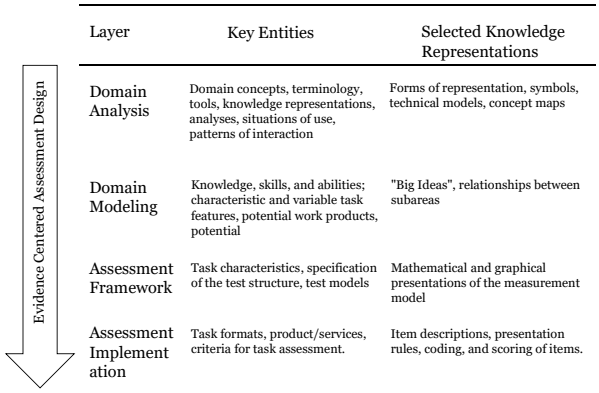
2.2. Domain Analysis in the Vocational Education Domain

In research fields, such as the vocational education domain, results from competence modeling highly depend on reproducing the professional situation as authentically and realistically as possible (Seeber, 2016). Following Seeber (2016) and Klotz (2015), the measurement of professional competencies demands that the requirements of the domain be determined as precisely as possible to measure competencies in the field of interest. Domain analyses are often conducted for this purpose (Rausch et al., 2016; Seeber et al., 2016; Weber et al., 2016). Regarding vocational education research, a domain is defined as a specific subject area that can be characterized by specific situations of action of involved actors (Klieme et al., 2003; Seeber, 2016). Hence, domain analysis starts with a detailed investigation of job-specific tasks of the domain, using interviews, shadowing, or related qualitative methods (Seeber, 2016). Domain analysis is used in numerous studies in the field of vocational education and training, for example, in the ASCOT research initiative (Weber et al., 2016). In these terms, it is applied as a prerequisite for designing and implementing competence tests in varying domains. In the following, we will introduce related projects in the vocational education domain to provide examples of how they can contribute to assessing a domain analysis for IT-secure behavior.

Weber et al. (2016) present results from a model-based assessment tool to measure intrapreneurship competence reliably and validly. The basis for the modeling is the comprehensive domain analysis of intrapreneurship competence. Scientific literature, training materials, curricula, and job advertisements are analyzed to capture the necessary information (Weber et al., 2016). Furthermore, intrapreneurship activities are observed in practice, and information about typical requirements is collected on-site (Weber et al., 2016).

Instead, Rausch et al. (2016) elaborate on a competence model, including a domain analysis for industrial clerks. The related project examines a specific occupational field in a domain with the problem-solving competence of controlling (Rausch et al., 2016).

Seeber et al. (2016) conducted a domain analysis for two different domains, including medical health and commercial administration. The project's objective is to develop and test a competence model for the professional competence of medical assistants (Seeber et al., 2016). Characteristics of the domain of medical assistants are analyzed, and typical work processes and results are determined (Seeber et al., 2016).



Layer	Key Entities	Selected Knowledge Representations
Domain Analysis	Domain concepts, terminology, tools, knowledge representations, analyses, situations of use, patterns of interaction	Forms of representation, symbols, technical models, concept maps
Domain Modeling	Knowledge, skills, and abilities; characteristic and variable task features, potential work products, potential	"Big Ideas", relationships between subareas
Assessment Framework	Task characteristics, specification of the test structure, test models	Mathematical and graphical presentations of the measurement model
Assessment Implementation	Task formats, product/services, criteria for task assessment.	Item descriptions, presentation rules, coding, and scoring of items.

Figure 1. ECD Framework (based on Mislevy & Haertel, 2006 and Seeber, 2016).

In many cases, domain analyses are wrapped into the ECD framework, which aims to provide a blueprint for designing educational assessments (Mislevy et al., 2003; Mislevy & Haertel, 2006). In the learning context, ECD is based on an educational assessment that involves evidentiary reasoning to infer from specific actions of learners in testing situations what their actual level of knowledge or competence is (Mislevy, 2013).

The baseline approach covers five different layers sequentially built on each other (Mislevy, 2013). By applying the ECD framework, assessment designers are provided with consistent guidelines to foster reusable design components that can be referred to when structuring assessments. Figure 1 depicts the design process consisting of domain analysis, domain modeling, conceptual assessment framework, and assessment implementation, but without delivery.

The ECD design process starts with analyzing the specifically selected domain. Relevant information about the domain characteristics is systematically collected to delineate and define reference points or target values of the competence to be measured. In addition to specific knowledge representations, skills, and abilities, this also includes the elaboration of typical tools, instruments, requirement situations, and interaction patterns that may become relevant during test processing (Mislevy, 2013; Pellegrino et al., 2014). The main objective is to acquire deep knowledge about specific issues and situations that people from a particular profession face in their working environment (Mislevy, 2013; Seeber et al., 2016).

Authenticity must be ensured in the domain analysis through close reference to practice. This can be achieved through various methodological approaches, e.g., by analyzing relevant guides and expert interviews. In the further course of instrument development, technology-based tests can support the design of authentic scenarios. In a vocational education and training study, e.g., the test scenarios were embedded in a model company to depict typical action situations and thus ensure authenticity (Rausch et al. 2016).

The following step is domain modeling and the differentiation of a competence model based on theoretical assumptions about professional competence and its hierarchically structured requirements (Seeber, 2016). The domain/competence model is transferred into assessments in the assessment framework, including task design (Mislevy, 2013; Seeber, 2016). Finally, the assessment implementation involves formulating criteria for task assessment and preparing for operational instancing (Mislevy & Haertel, 2006). The relevance of domain analysis in the research field of vocational education informs our research in several ways. First, it deals with the overall question of *what* knowledge, skills, and other attributes should be assessed in a specified domain. This knowledge can be transferred to, on the one hand, define a tool stack for measuring IT-security competencies or, on the other hand, leverage from it to build customized SETA programs that incorporate the most important content for acquiring these abilities and skills. Per the ECD framework, vocational education provides a methodical approach that builds the basis for assessing security threats in the domain of IT-secure behavior.

3. Toward a Cyber Security Domain Model

We analyzed the domain for IT-secure behavior to follow the layer domain analysis in the ECD framework. With regard to vocational education research, a domain is defined as a specific subject area that can be characterized by specific situations of action of involved actors (Klieme et al., 2003; Seeber, 2016). However, it is non-trivial to distinguish between different job specifics in the context of IT-secure behavior. This is mainly for two reasons. Firstly, they relate to a wide variety of professions. Instead of analyzing a domain towards typical tasks or activities, we are interested in typical potential security threats. Secondly, resources are bound due to time and cost factors. Thus, it does not seem reasonable to analyze particular job specifications towards typical security threats in their working environment. Instead, we apply a top-down approach by investigating all kinds of possible security threats that can be faced by any type of employee, regardless of the profession. The outcome of the domain analysis can be applied to either measure professional IT-security competence or as an input to design tailored SETA programs. Therefore, we follow a three-stage approach to conducting a domain analysis inspired by the first layer in the ECD design process, which is presented in the following.

	Stage 1: Object Classification	**Stage 2: Object Analysis in the Domain**	**Stage 3: Object Reduction**
Steps	• Determine objects to be classified • Investigate sub-components of objects	• Define target domain • Browse relevant literature and documents	• Sort out unreasonable security threats
Method	• Literature Analysis	• Document Analysis • Literature Analysis	• Applied security knowledge
Source	• Literature on Security threat classification	• Documents and Literature on security threats and their sub-dimensions	• Researchers from the IS security domain
Outcome	• Security Threat Classification Objects	• Domain Model	• Reduced Domain Model

Figure 2. Domain Analysis for IT-secure Behavior.

Figure 2 shows the whole process starting with object classification, which deals with defining security threats. Stage two continues by exhaustively searching for those classified objects in the domain. Finally, the data set is reduced in stage three by sorting out unreasonable objects inside the domain analysis. The outcome is a CSDM for the domain IT-secure behavior.

3.1. Stage One: Classification of the Objects of the Domain Analysis

To analyze security threats in a top-down manner, we need to define of what components a security threat is composed. The related work chapter revealed that security threats could be understood in varying ways. In terms of competent behavior, which includes the situational awareness of the employee towards compromising situations, two distinct facets of a security threat are relevant. Therefore, our domain model distinguishes threat vectors, which are composed of the two dimensions of *threat event* and *threat area* (cf. Figure 3):

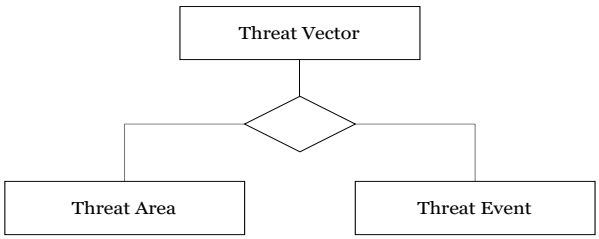


Figure 3. Threat Vectors.

The threat event provides the basis for risk identification by defining threat sources and resulting threat events (Blank & Gallagher, 2012). Although both Gerić and Hutinski (2012) and Jouini et al. (2014) distinguish a threat source dimension primarily binary into external and internal sources, NIST addresses four sub-dimensions in their publication 800-30: adversarial, accidental, structural, environmental (Blank & Gallagher, 2012). However, since the specific threat source is less relevant for creating the domain model than the specific threat event in the operational action setting, Blank and Gallagher's (2012) differentiation of threat source and threat event is subsumed under threat event in the CSDM. The threat event "social engineering" example shows that a separate breakdown of the triggering threat source does not appear reasonable for the domain model created here. In this case, the employee should be able to identify such an attack independently of the attacker (i.e., competitor, former employee) and act appropriately. For example, a commercial employee with a company telephone and a laptop is potentially exposed to this threat. On the other hand, a production employee who does not have any of the IT assets mentioned would not be exposed to this threat. According to Blank and Gallagher (2012), as part of the risk assessment, organizations must assess which threat events should be addressed at what level of granularity (for example, DDoS attack only or additionally naming specific systems). Following Blank and Gallagher (2012), potential threat events can be assigned to one of the following four sub-dimensions: adversarial (e.g., phishing or DDoS attack), accidental (e.g., disclosure of sensitive information by privileged users), structural (e.g., outdated displays), and environmental (e.g., fire, flood).

The threat area dimension, following Gerić and Hutinski (2007), describes those domains in which security threats may be present. For effective risk assessment and defining the generic threat events, it is necessary to consider how the threat events could affect the assets present in an organization (Blank & Gallagher, 2012). Wunder et al. (2011) define the term asset as follows: “Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).” Shamala and Ahmad (2014) found that certain asset classes recur across different information security risk assessments: information, data, physical, software, hardware, and personal assets. Contrary to the asset taxonomy, according to Shamala and Ahmad (2014), the CSDM does not differentiate between information and data assets. Thus, analogous to the Cyber Defense Matrix by Dutta and Al-Shaer (2019), only the term data asset is used in the CSDM. Further, contrary to the differentiation described by Shamala and Ahmad (2014), the category of hardware assets is included in the physical assets within the CSDM. We distinguish between physical (e.g., server, laptop, USB stick) and non-physical enterprise assets (e.g., social media network, accounting software).

3.2. Stage Two: Literature-based Identification of Objects in the Domain Analysis

The second domain analysis stage deals with the search process for security threat vectors. Therefore, a literature analysis for security threat events, on the one hand, and security threat areas, on the other hand, was conducted. In terms of security threat events, we rely on the most recent official special NIST publication 800-30. We refer to a full list of threat events by Blank and Gallagher (2012). Due to limited space, we do not list these here and refer the reader to the primary source. This resulted in 85 elements being adopted.

For relevant threat areas (assets), we conducted a literature search focusing on cyber risk (management) papers. Most of the assets presented in the CSDM below were taken from Biener et al. (2015). For the category of data assets, a list made by Leming (2015) was also partially used. In this context, we define the threat

domain as those possible enterprise assets (e.g., mail program) that can be targeted by different threat events (e.g., phishing attack). Several sources were used to determine possible organizations' values. Particularly in the area of "non-physical" assets, reference was also made to the research area of knowledge management since the systems referenced by Lehner (2021) may also be relevant for ensuring operational IT security. The list of assets includes 43 elements, which can be found in the appendix in Figure 5. The second dimension, threat event, includes threat sources that can potentially cause damage to the threat areas explained earlier. The two dimensions of threat event and threat area result in eight overarching threat vectors for the domain model of the IT-secure behavior domain (see Figure 4).

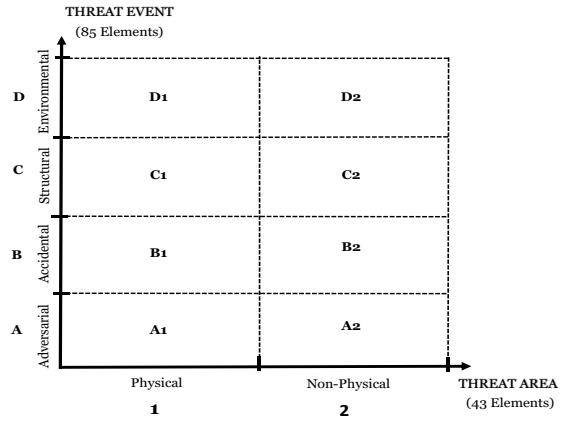


Figure 4. Threat Vector Classification.

Within these eight superordinate threat vectors (A1 to D2) are, in turn, the individual sub-threat vectors (Table 1), which are required as action-relevant reference variables for competence modeling. The functionality of our domain model for the domain IT-secure behavior can be illustrated with three exemplary sub-threat vectors (Table 1).

Table 1. Sample Sub-Threat Vectors.

ID	Threat Event	Threat Area
A1.1.2	Performing a DoS attack	Server
B1.2.2	Spilling sensitive information	Employee
A2.2.9	Performing a phishing attack	E-Mail System

3.3. Stage Three: Reduction of the Domain Analysis

In stage two, we were able to identify 43 threat areas and 85 threat events. As a result, the domain model of IT-secure behavior consequently contains 3,655 sub-threat vectors. However, since not all the 3,655 possible sub-threat vectors in the model (e.g., a combination of the threat event "DDoS attack" and the threat area "USB stick") can occur in operational workflows, the total number of security threat vectors can be diminished reasonably. Therefore, three researchers from IS security domain mutually evaluated each security threat vector for plausibility. Whenever the researchers disagreed, a majority vote was used. If still no agreement could be reached, the security threat vector remained in the domain model. Since these situations have only occurred in borderline cases and the CSDM serves as a basic framework to identify downstream critical threat vectors for specific job profiles, this is assumed to be non-critical. As a result, the total number of security threat events and areas stayed the same while the number of reasonable security threat vectors decreased to 1,087.

4. Application of the CSDM

In the following section, we will discuss the application of the CSDM and how it can contribute to determining the needs for job-specified security programs. Therefore, we define five specific job profiles which can be typically found in small and medium-sized enterprises. These job specifications were divided into (1) IT-administrators/ISMS-responsible employees, (2) internal employees with less than 50% travel share, (3) executives/secretaries, (4) internal employees with more than 50% travel share and (5) management. Employees of these job specifications face different security threats depending on their daily working routine. To provide an easy-to-follow example, we will discuss the implications of the CSDM for two different job specifications.

A hostile threat event is present in the case of a DDoS attack (e.g., cybercriminals commissioned by rival companies to bring down an organization's servers). This threat event does not necessarily affect all employees but only those assigned to the "server" threat area in their daily work. This implies, for example, that IT administrators whose job specification is to look after the company's servers would be directly affected by this threat event. To train IT administrators as efficiently as possible concerning IT-secure behavior, the training measures required for this must be based on their job specifications. However, considering a social engineering attack, internal employees with a high travel share are more affected than those with less travel share since they operate more with cell phones and have more direct contact with customers outside the organization.

In these two examples, the combination of threat events and threat areas pose a different risk for different job profiles and can, therefore, also be assessed according to their individual risk. Followingly, the set of 1,087 security threat vectors can be taken as input for

a qualitative risk assessment for each job specification. A common qualitative approach to categorizing security threat events has been developed by Blank and Gallagher (2012). Contrary to these authors, we did not assess the threat event but the threat vector. Therefore, we first assessed the overall likelihood for each threat vector using the NIST assessment scales G-1 to G-5 (Blank & Gallagher, 2012).

Likelihood = Likelihood of Threat Vector Occurrence x Likelihood Threat Vector Result in Adverse Impacts (1)

Following Blank and Gallagher (2012), the risk for each threat vector is composed of (1) and the overall impact.

Risk = Likelihood x Impact (2)

Like the reduction of security threat vectors in stage three, three researchers mutually determined the risk assessment with a majority voting. Using established five-point scales ("very low" to "very high"), the researchers independently assessed the risk of each threat vector for each of the five job specifications using the NIST assessment scales I-2 to I-3 (Blank & Gallagher, 2012). Each threat vector was considered on its own and compared to the assessment scale description by Blank and Gallagher (2012). Based on the classification, the individual vectors received a value between 1 (“very low”) and 5 (“very high”) for the *Likelihood of Threat Vector Occurrence* and the *Likelihood Threat Vector Result in Adverse Impacts*. The overall Likelihood results in the combination of these two scales and emits a new quantitative scale based on the previously mentioned assessment scales. The same procedure is applied to assess the *Impact* and the *Risk using* the NIST assessment scales H-2 to H-3, respectively I-2 to I-3 (Blank & Gallagher, 2012).

Using an established risk assessment methodology ensures that our domain model for the IT-secure behavior domain is compatible with national and international standards. The interim result of this work package was a list of the most risk-relevant threat vectors for each job specification (i.e., those with a risk rating of "high" or "very high"). Accordingly, after conducting the risk assessment, the five job specifications contain between 14 and 29 threat vectors with high or very high assessed risk. The five lists of risk-relevant threat vectors form the basis for the conducted expert survey in the field to validate the applicability of the CSDM for different job specifications in the field (Bogner et al., 2009). Six experts were invited to evaluate the remaining threat vectors. The panel of experts comprises a range of information technology (security) professionals employed in different sized organizations in Germany that are mostly partners of a related funded project. This allows for organized and deep knowledge from a practical viewpoint (Mergel et al., 2019; Schulze et al., 2022). To carry out the online expert survey, the software Qualtrics was used to rank the threat vectors for each job specification. The experts were thereby asked to anonymously rank the threats, with rank one representing the most alarming. In addition, the experts could introduce new threat vectors if, in their opinion, missing (very) high-risk threat vectors were not considered. For example, it was proposed to consider Shadow IT and ransomware for IT administrators and data dumping over public networks for internal employees. Zero-Day Attacks and modified malware attacks on servers and mail programs are the most voted threat vectors for an IT administrator. In addition, common themes across the job specifications are, e.g., (Spear-)Phishing Attacks and malware. Figure 6 and Figure 7 in the appendix list the results for two exemplary job specifications to transparently depict the outcome of the expert survey. The results can be used for a domain modeling and assessment framework to build customized and job-specific SETA programs.

5. Discussion

In the following sections, our results will be discussed primarily in terms of the contribution of the research process to literature and practice. Firstly, we will derive the theoretical implications of our work. Secondly, we discuss the practical implications of interpreting the utility and contribution from that perspective.

5.1. Contributions to Literature

Our research goal was to build a framework-based information security threat classification that, on the one hand, provides valuable insights to IS security research and, on the other hand, applies to practitioners. We contribute to several literature streams in multiple ways. First, we situate our research within information security threat literature. More specifically, we categorized security threats which are composed of two-dimensional vectors. This expands existing security threat classifications, focusing on the threat event and the threat area. By doing so, we reduce the complexity of previous approaches while simultaneously keeping the most relevant information. Compared to related threat classifications, we highlight the importance of considering information security assets. Moreover, the CSDM can be extended to any job specifications. Second, we are the first to develop a security threat classification applying a framework-based approach. Therefore, we leverage the ECD framework that has been used to analyze various domains, including mainly

commercial and industrial professions (Achtenhagen & Winther, 2008; Klotz, 2015; Seeber, 2016). This study shows how the first layer of the ECD can be applied in the information security domain.

Our results provide baseline guidance for selecting strategies for job-specific SETA programs going beyond one-size-fits-all approaches. Therefore, we present a framework of paradigmatic-theoretical-shift in the conceptualization of a security-training curriculum that does not begin with a repetition of identical security training content but rather sub-divides the curricular domain into areas of competence that then determine the structure and composition of a SETA program. Moreover, it builds a prerequisite for the assessment design and implementation to measure security competencies in IT-secure behavior. Thus, the CSDM provides a suitable basis for performing a mandatory competency-based cyber risk assessment before taking out Consumer Cyber Insurance.

5.2. Contributions to Practice

Next to contributions to literature, our study holds several practical implications. First, the CSDM builds a generic approach for choosing specific content regarding the most relevant security threats for SETA programs. It acts as a condition for implementing job and qualification-specific security training programs. Thus, organizations are able to observe emerging topics or threats for substantial future security training offers. Second, the CSDM provides an opportunity to narrow selected security threats for different professions. Therefore, our approach is cost-effective since it builds a simplified way to analyze the relevant threat vectors for job specifications. Furthermore, due to our more job-specific SETA design, employees are less confronted with content irrelevant to their daily work, presumably increasing acceptance of and attention to IT security measures. Lastly, the applied CSDM can help practitioners to assess the needs for particular IT-security knowledge, skills, and abilities of their employees. This forms the basis for competence-based approaches that measure needed qualifications to address employees' knowledge gaps when structuring and designing SETA programs. This allows for the creation of employee-specific learning pathways that track progress in acquiring competencies transparently.

5.3. Limitations and Future Research

Our research holds some limitations and opportunities for future research discussed in the following. First, the CSDM is constrained by the number of threat areas and events. As cyber security attacks become more sophisticated and technology evolves (ENISA, 2021), these threat vectors must be continuously adapted based on emerging trends. Second, for the sake of reduced complexity and increased efficiency for competence modeling, we reduced the model to be two-dimensional. Various authors include threat sources (internal and external) in security threat classifications. However, since our research is interested in a downstream competence modeling and testing process, which does not require knowing the direct attacking source, we excluded this dimension. In the next step our research, we plan to validate the applicability of the CSDM in practice.

6. Conclusion

In this research paper, we developed a framework-based information security threat classification. We applied the first two steps of the ECD framework to follow a thorough domain analyzing process similar to fields of research in the vocational education domain. Our proposed CSDM includes 1,087 plausible threat vectors composed of the threat event and the threat area. Afterward, we defined five job specifications to apply the model to a practice-related context. The overall risk was calculated for each threat vector and job specification. In doing so, we highlight the use case for practitioners and researchers to ground the development of security programs for different job specifications and competence-oriented content. This builds a sound basis for competence modeling and assessment design and implementation in the domain of IT-secure behavior.

7. Acknowledgements

This paper has been written as part of the research project “ITS.kompetent” funded by the German Federal Ministry for Economic Affairs and Climate Action. We would like to thank the German Federal Ministry for Economic Affairs and Climate Action for its support.

8. References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Achtenhagen, F., & Winther, E. (2008). Wirtschaftspädagogische Forschung zur beruflichen Kompetenzentwicklung. In N. Jude, J. Hartig, & E. Klieme (Eds.), *Kompetenzerfassung in pädagogischen Handlungsfeldern Theorien, Konzepte und Methoden* (Vol. 26, Issue 26, pp. 117–140).

Alhabeeb, M., Almuhaideb, A., Le, P. D., & Srinivasan, B. (2010). Information security threats classification pyramid. *24th IEEE International Conference on Advanced Information Networking and Applications*

Workshops, WAINA 2010, 208–213. https://doi.org/10.1109/WAINA.2010.39

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2020). Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness. *Proceedings of the 27th European Conference on Information Systems*, 1–14.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Blank, R. M., & Gallagher, P. D. (2012). *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Blömeke, S., Gustafsson, J. E., & Shavelson, R. J. (2015). Beyond Dichotomies: Competence Viewed as a Continuum. In *Zeitschrift für Psychologie* (Vol. 223, Issue 1, pp. 3–13). Hogrefe Publishing. https://doi.org/10.1027/2151-2604/a000194

Bogner, A., Littig, B., & Menz, W. (2009). Introduction: Expert Interviews — An Introduction to a New Methodological Debate. In *Interviewing Experts* (pp. 1–13). Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_1

Dutta, A., & Al-Shaer, E. (2019). "What", "Where", and "Why" Cybersecurity Controls to Enforce for Optimal Risk Mitigation. *2019 IEEE Conference on Communications and Network Security (CNS)*, 160–168. https://doi.org/10.1109/CNS.2019.8802745

ENISA. (2021). *ENISA Threat Landscape 2021. April 2020 to mid-July 2021* (Issue October). https://doi.org/10.2824/324797

Gerić, S., & Hutinski, Ž. (2007). Information System Security Threats Classifications. *Journal of Information and Organizational Sciences*, *30*(1), 51–61. https://hrcak.srce.hr/21445

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, 1–13. https://doi.org/10.1080/08874417.2021.1913671

Jouini, M., Rabai, L. B. A., & Aissa, A. ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Kirova, D., & Baumoel, U. (2018). Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review. *Journal of Information Technology Theory and Application (JITTA)*, *19*(4), 56–83.

Klieme, E., Avenarius, H., Blum, W., Döbrich, P., Gruber, H., Prenzel, M., Reiss, K., Riquarts, K., Rost, J., Tenorth, H.-E., Vollmer, H. J., & Forschung, B. für B. und. (2003). *Zur Entwicklung nationaler Bildungsstandards. Eine Expertise*. https://doi.org/10.25656/01:20901

Klotz, V. K. (2015). *Diagnostik beruflicher Kompetenzentwicklung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-10681-2

Lehner, F. (2021). *Wissensmanagement*. Carl Hanser Verlag. https://doi.org/10.3139/9783446468115

Leming, R. (2015). Why is information the elephant asset? An answer to this question and a strategy for information asset management. *Business Information Review*, *32*(4), 212–219. https://doi.org/10.1177/0266382115616301

McCoy, C., & Fowler, R. T. (2004). "You Are the Key to Security": Establishing a Successful Security Awareness Program. *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services*, 346–349. https://doi.org/https://doi.org/10.1145/1027802.1027882

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), 101385. https://doi.org/10.1016/j.giq.2019.06.002

Mislevy, R. J. (2013). Evidence-Centered Design for Simulation-Based Assessment. *Military Medicine*, *178*(10 Suppl), 107–114. https://doi.org/10.7205/milmed-d-13-00213

Mislevy, R. J., Almond, R. G., & Lukas, J. F. (2003). A Brief Introduction to Evidence-Centered Design. *ETS Research Report Series*, *2003*(1), 1–29. https://doi.org/10.1002/j.2333-8504.2003.tb01908.x

Mislevy, R. J., & Haertel, G. D. (2006). Implications of Evidence-Centered Design for Educational Testing. *Educational Measurement: Issues and Practice*, *25*(4), 6–20. https://doi.org/10.1111/j.1745-3992.2006.00075.x

Pellegrino, J. W. (2010). *The Design of an Assessment System for the Race to the Top: A Learning Sciences Perspective on Issues of Growth and Measurement*. https://www.ets.org/Media/Research/pdf/PellegrinoPresenterSession1.pdf

Pellegrino, J. W., DiBello, L. V., & Brophy, S. P. (2014). The science and design of assessment in engineering education. In A. Johri & B. M. Olds (Eds.), *Cambridge Handbook of Engineering Education Research* (pp. 571–600). Cambridge University Press.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Rampold, F., Schütz, F., Masuch, K., Köpfer, P., & Warwas, J. (2022). Are you aware of your competencies? – The potentials of competence research to design effective SETA programs. *Proceedings of the 30th European Conference on Information Systems*, 1–17. https://aisel.aisnet.org/ecis2022_rp/134

Rausch, A., Seifried, J., Wuttke, E., Kögler, K., & Brandt, S. (2016). Reliability and validity of a computer-based assessment of cognitive and non-cognitive facets of problem-solving competence in the business domain. *Empirical Research in Vocational Education and Training*, *8*(1). https://doi.org/10.1186/S40461-016-0035-Y

Schulze, L., Trenz, M., Cai, Z., & Tan, C.-W. (2022). Conducting Online Focus Groups - Practical Advice for Information Systems Researchers. *Proceedings of the 55th Hawaii International Conference on System*

Sciences, *7*, 3085–3094. https://doi.org/10.24251/hicss.2022.380

Seeber, S. (2016). Vom Domänenmodell zum Kompetenzmodell: Konturen eines Assessmentdesigns zur Messung beruflicher Fachkompetenzen bei Medizinischen Fachangestellten. In H. G. Ebner & J. Seifried (Eds.), *Kompetenzentwicklung im wirtschaftspädagogischen Kontext: Programmatik – Modellierung – Analyse. Digitale Festschrift für Sabine Matthäus* (pp. 1–25).

Seeber, S., Schumann, M., Ketschau, T., Rüter, T., & Kleinhans, J. (2016). Modellierung und Messung von Fachkompetenzen Medizinischer Fachangestellter (CoSMed). In K. Beck, M. Landenberger, & F. Oser (Eds.), *Technologiebasierte Kompetenzmessung in der beruflichen Bildung – Resultate aus dem Forschungsprogramm ASCOT* (pp. 205–223). Bertelsmann.

Shamala, P., & Ahmad, R. (2014). A Proposed Taxonomy of Assets for Information Security Risk Assessment (ISRA). *2014 4th World Congress on Information and Communication Technologies, WICT 2014*, 29–33. https://doi.org/10.1109/WICT.2014.7077297

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management and Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*, *2006*(6), 17–19. https://doi.org/10.1016/S1361-3723(06)70370-0

Weber, S., Draxler, C., Bley, S., Wiethe-Körprich, M., Weiß, C., & Gürer, C. (2016). Large scale assessments in der kaufmännischen Berufsbildung - Intrapreneurship (CoBALIT). In K. Beck, M. Landenberger, & F. Oser (Eds.), *Technologiebasierte Kompetenzmessung in der beruflichen Bildung – Resultate aus dem Forschungsprogramm ASCOT* (pp. 75–92). Bertelsmann.

Winther, E. (2010). *Kompetenzmessung in der beruflichen Bildung*. Bertelsmann.

Wunder, J., Halbardier, A., & Waltermire, D. (2011). *Specification for Asset Identification 1.1*. https://doi.org/10.6028/NIST.IR.7693

Appendix

	Threat Area (Asset)
Physical	(1) Disk, (2) Server, (3) Computer, (4) Laptop, (5) Phone, (6) USB flash drive, (7) Microfilm, (8) Smartwatch, (9) Printer, (10) Scanner, (11) Tablet, (12) Network cables, (13) WLAN, (14) Site, (15) PO Box, (16) Key, (17) Desk, (18) Safe, (19) Employee ID card, (20) Power line, (21) Water pipe, (22) Gas pipe, (23) AIR conditioning, (24) Employee
Non-Physical	(1) Browser, (2) Accounting system (e.g., Lexware), (3) Online-banking, (4) Payment system (e.g., Payone), (5) DMS (e.g., Sharepoint/OneDrive), (6) Video conferencing system, (7) Instant Messenger, (8) E-Mail system , (9) Collaboration systems (e.g., Asana, Teams), (10) CMS (e.g., Typo3), (11) Version control (e.g., Github), (12) Social Media Systems, (13) LMS (e.g., Successfactors), (14) Data Warehouse Systeme, (15) CAD systems, (16) Homepage, (17) Network (e.g., LAN, PAN, WLAN), (18) VPN (e.g., CISCO AnyConnect), (19) Firewall (e.g., Bitdefender)

Figure 5. Threat Areas of the CSDM.

	Threat Area (Asset)	Threat Event	Risk (Likelihood x Impact)
JS1.1	Server	Disk Error	4
JS1.2	Server	Conduct simple/distributed/targeted denial of service (DoS) attacks.	4
JS1.3	Server	Conduct Brute-Force Attacks	4
JS1.4	Server	Conduct non targeted zero day attacks	4
JS1.5	Laptop	Conduct Brute-Force Attacks	4
JS1.6	Browser	Deploying (modified) malware to internal information systems of the organization	4
JS1.7	E-Mail System	Deploying (modified) malware to internal information systems of the organization	4
JS1.8	E-Mail System	Deploy targeted malware to control internal systems and exfiltrate data	4
JS1.9	Network	Deploying (modified) malware to internal information systems of the organization	4
JS1.10	Network	Conduct non targeted zero day attacks	4
JS 1.11	Firewall	Conduct non targeted zero day attacks	4

Figure 6. Threat Vectors for the Job Specification IT Administrator.

	Threat Area (Asset)	Threat Event	Risk (Likelihood x Impact)
JS2.1	Employee	Wrong access rights	5
JS2.2	Employee	Spilling sensitive information	5
JS2.3	Employee	Conduct Social Engineering attacks	5
JS2.4	Employee	Incorrect handling of critical and/or sensitive information by authorized users	4
JS2.5	Instant Messenger	Conduct Social Engineering attacks	5
JS2.6	E-Mail System	Conduct Social Engineering attacks	5
JS2.7	Collaboration System	Conduct Social Engineering attacks	5
JS2.8	Social Media System	Conduct Social Engineering attacks	5
JS2.9	E-Mail System	(Spear-) Phishing attacks	4
JS2.10	E-Mail System	Injecting malware into the organization's internal information systems (e.g., viruses via email)	4

Figure 7. Threat Vectors for the Job Specification Internal Employee with less than 50 Percent Travel Share.