Deriving Design Principles from the Design journey of a Cybersecurity Readiness Assessment Tool

Abhishek Sharma
Department of Management Studies (DoMS),
Indian Institute of Technology Madras
abhisheksharma.27ju@gmail.com

Rangaraja P. Sundarraj
Department of Management Studies (DoMS),
Indian Institute of Technology Madras
rpsundarraj@iitm.ac.in

Abstract

The need for assessing cybersecurity readiness of an organization has been growing in importance. However, the existing research literature lacks a system for evaluating this aspect. This research paper describes the design journey of designing a Cybersecurity Readiness Assessment Tool (CRAT) using a Design Science Research (DSR) perspective. Since designing software is complex, we follow an iterative approach to design and develop CRAT. Through the DSR iterations, we deduce Design Principles (DP) emanating from our development journey.

Keywords: Cybersecurity Readiness Assessment, Design Science Research, Design Principles, FEDS, Software design journey

1. Introduction

Organizations worldwide are grappling with escalating cyber threats that can lead to substantial financial losses and operational disruptions. In the face of incidents like Wannacry, SolarWinds Breach, Log4j, and Microsoft Exchange server attacks, proactive cyber readiness is emerging as a pivotal strategy (Oz et al., 2022). Cyber adversaries have extended their targets to critical sectors like government, military, manufacturing, and financial services, necessitating a robust defense (Biswas et al., 2021; Arce, 2022; Meland et al., 2020; Blumenthal, 2022).

Effectively countering these threats demands a keen understanding of technological trends and the integration of industry-standard security practices (Koustic and Pigni, 2022; ISO/IEC 27001:2022, 2022). This involves the identification of organizational-level factors, their interplay, and the corresponding countermeasures that influence security outcomes (Georgiadou et al., 2022). Among prevailing cybersecurity frameworks like ISO, CIS, PCI DSS, and COBIT, the responsibility for implementing, adopting, and evaluating cybersecurity readiness ultimately rests with organizational decision-makers (ISO/IEC 27001:2022, 2022; Benz and Chatterjee, 2020). Amidst the array of options, the focus on cyber readiness stands out due to its proactive approach. In contrast to reactive strategies, readiness empowers organizations to anticipate and preemptively mitigate the evolving landscape of cyber threats (Georgiadou et al., 2022; Baskerville et al., 2022). It equips executives to gauge their organization's resilience against a gamut of sophisticated attacks driven by various motives (Lallie et al., 2021). To navigate this complex landscape, the CRAT prototype, grounded in Design Science Research (DSR) principles, was developed to assess cyber readiness from an organizational perspective (Ryan et al., 2012; Apiola and Sutinen, 2021). DSR ensures both theoretical soundness and practical applicability in IS artifact development (Venkatraman et al., 2016; Venkatraman et al., 2018). This alignment emphasizes actionable outcomes bridging theory and practice (Nagle et al., 2016).

To assess cyber readiness, decision-makers prioritize mechanisms to fortify security against threats and vulnerabilities (Wallner, 2014; Ganin et al., 2020). This prototype concentrates on these factors and related countermeasures, enabling comprehensive threat and vulnerability assessment. Using the DSR framework, it advances theory and furnishes practical tools for readiness enhancement. In software design, iterative development, as with DSR, is vital. It informs best practices and guidelines for similar projects. Thus, we address RQ1: How to deduce design principles from the development of CRAT and what lessons can be learnt out of the process.

We will look through the design journey of CRAT. We observed digital nudging (Weinmann et al., 2016; Schneider et al., 2018) along the way. Through this we redesigned the tool to incorporate different UI formats into MCDM (Multi-Criteria Decision Making) method. The final prototype is evaluated, focusing on decision outcomes and end-users' performance (time and cognitive effort), yielding design principles through CRAT's iterations. This paper's structure is as follows: Section 2 outlines foundational literature, Section 3 details CRAT's four iterations, Section 4 derives three

URI: https://hdl.handle.net/10125/107077
978-0-9981331-7-1

design principles from these iterations, and Section 5 provides implications. Concluding remarks are in Section 6.

2. Foundations and Related Work

We review literature on two main streams of research: (i) Cybersecurity and Readiness Assessment (ii) DSR Perspective and Design Principles.

2.1. Cybersecurity and Readiness Assessment

In the domain of cybersecurity, the spectrum of threats encompasses malware, social engineering attacks, and insider threats, each carrying the potential to trigger data breaches, financial losses, and operational disruptions (Meland et al., 2022; Mambetov et al., 2023). The escalation of advanced persistent threats (APTs) and nation-state-sponsored attacks intensifies concerns, underscoring the necessity for a robust defense against significant data breaches and industrial espionage (Sharma et al., 2023). Amidst this landscape, four compounding factors emerge: the dynamic nature of threats demanding continuous vigilance, the intricate interconnections within the digital ecosystem, the scarcity of cybersecurity expertise, and the intricate balance between security and system usability (Abraham et al., 2019; Kabanda et al., 2018; Green et al., 2020). In response, organizations face an imperative to adopt a scalable cybersecurity defense strategy encompassing comprehensive threat awareness and vulnerability comprehension. In addressing these challenges, the concept of cybersecurity readiness emerges as a pivotal strategic choice. Readiness assessment (RA) is a crucial step in evaluating an organization's preparedness. Researchers and practitioners have been developing frameworks and models to assess readiness across various technology domains (Venkatraman et al., 2022; Sharma and Venkatraman, 2023). RA requires the involvement of multiple stakeholders and criteria in decision-making (Venkatraman and Sundarraj, 2023). It assists in tailoring strategies to address specific gaps and challenges. Previous research has focused on a wide range of areas, including ERP, health information technologies, health information exchange, telemedicine, health analytics, blockchain, cloud, cybersecurity, big data, cloud manufacturing, e-governance, e-health, and other digital technologies (Venkatraman and Sundarraj, 2022; Sharma and Venkatraman, 2023).

Despite this, there is a scarcity of literature for cybersecurity readiness assessment. While other tools like framework for assessing an organization's cybersecurity culture (Georgiadou et al., 2022), PwC's Cyber Readiness Health Check (PwC, 2023), and CISA's CSET Ransomware Readiness Assessment (CISA, 2021) serve various cybersecurity assessment needs. However, if organizations aim for more precise decision-making in prioritizing countermeasures against evolving threats and vulnerabilities, a simple checkbox assessment won't provide much depth or sophistication. These threats are dynamic and multifaceted, often requiring nuanced strategies for effective mitigation. Through CRAT prototype, on the other hand, we offer a comprehensive approach by leveraging Multi-Criteria Decision Making (MCDM) methods. This allows it to consider various factors, providing a tailored and robust assessment in today's complex cybersecurity landscape.

2.2. DSR Perspective and Design Principles

Design Science Research (DSR) is a methodology to develop innovative, practical solutions for real-world problems, including those in cybersecurity (Hevner et al., 2010; vom Brocke et al., 2020). It allows for iterative refinement and enhancement through frequent evaluation and feedback loops. DSR, although widely applied, has limited literature on developing cybersecurity readiness tools (Baskerville et al., 2022; Georgiadou et al., 2022). Our research bridges this gap by deriving Design Principles (DP) from the iterative DSR process, offering valuable insights and best practices for IS artifact development (Michalke et al., 2022). These principles, essential for future researchers and practitioners, enhance the knowledge base in the field of cybersecurity and DSR, aiding the design of relevant and effective RA systems (Venkatraman and Sundarraj, 2022; Michalke et al., 2022). Sharing our design journey contributes to knowledge dissemination and the advancement of cybersecurity and DSR (Georgiadou et al., 2022; Baskerville et al., 2022; Baskerville et al., 2018).

2.3. Gaps and Contributions

The research conducted in this study addresses two significant research gaps in the field of cybersecurity readiness assessment and design science research. The first research gap pertains to the sparse literature on cybersecurity readiness assessment. With the escalating frequency and complexity of cyber attacks, organizations face the critical task of evaluating their preparedness to defend against these threats. However, existing literature on cybersecurity readiness assessment is limited to a technical rather than an organizational approach (Georgiadou et al., 2022). This makes it challenging for organizations to effectively evaluate their cybersecurity posture. Second, even

though DSR is well applied in various domains (Gregor et al., 2020), its application to cybersecurity is limited (Baskerville et al., 2022). There is also limited literature on deriving or deducing design principles (Michalke et al., 2022) for cybersecurity readiness assessment tools. By developing CRAT using a DSR approach, our study fills the gap by providing a theoretically sound framework feasible for assessing cybersecurity readiness. The findings from this research will contribute to the existing knowledge base and assist organizations in proactively identifying vulnerabilities and enhancing their cybersecurity defenses. Further, by identifying and sharing these design principles, the study contributes to the body of knowledge in DSR, offering insights into effective design strategies and approaches for developing cybersecurity readiness assessment tools.

Overall, this research study fills the research gaps by providing a comprehensive approach, entailing three areas, namely Cybersecurity, RA and DSR. Further, contributing to the knowledge base and deriving design principles from the development process.

3. Overview and Design Journey of CRAT

Following Hevner et al.'s guidelines (2004), we adopted an iterative DSR approach to develop CRAT, a tool designed to address complex cybersecurity readiness challenges in organizational contexts (Sharma and Venkatraman, 2023). The development process integrated the GRAFTA framework. However, it's important to note that software development is inherently cyclical and iterative. In our case, CRAT's development unfolded across four crucial iterations, with each one building upon the last (see Figure 1). These iterations ultimately led to the formulation of valuable design principles, summarizing key lessons learned during the development and evaluation phases.

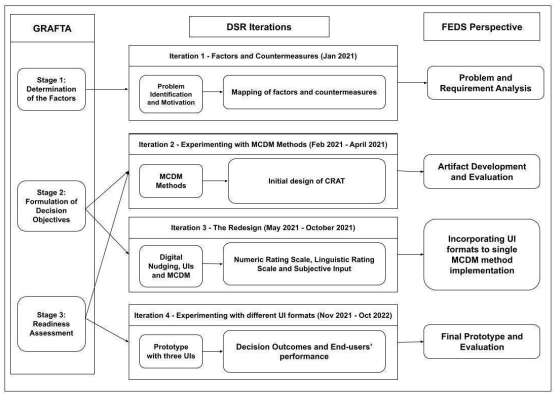

Figure 1: GRAFTA , DSR iterations and FEDS.

Our study provides a practical demonstration of the DSR methodology's efficacy in crafting solutions for intricate real-world challenges, such as cybersecurity readiness. We utilize four essential components to describe the problem space given by Maedche et al. (2019): stakeholders, needs, goals, and requirements, which encapsulates the steps needed for GRAFTA framework as mentioned below:

1. Stakeholders: These encompass a diverse spectrum, including decision-makers, cybersecurity experts, IT teams, and end-users. Each group contributes unique perspectives and distinct requirements. The ultimate goal is to develop a tool where multiple stakeholders are needed for performing readiness assessment(Venkatraman and Sundarraj, 2023; Sharma and Venkatraman, 2023). For the initial prototype, we recruited students with a background in Information Systems to gather feedback and user experience based on the readiness assessment.

2. Needs: Stakeholders' needs revolve around assessing readiness, addressing evolving threats, and ensuring usability. These aspects emphasize the importance of practicality in addressing cybersecurity challenges.

3. Goals: Our objectives aim to enhance organizational cybersecurity readiness and resilience. Decision-makers seek threat resilience, cybersecurity experts provide actionable mitigation strategies to the threats, and IT teams implement secure yet user-friendly solutions.

4. Requirements: FEDS (Framework for Evaluation in Design Science Research)-based (Venable et al., 2016) evaluation is crucial as it provides a structured and rigorous framework for assessing CRAT's effectiveness and usability. This approach ensures a comprehensive and objective evaluation of the tool's performance, preparing it for real-world applications in cybersecurity assessment.

In addition to this, GRAFTA will provide steps for conducting readiness assessment, offering a systematic approach to address cybersecurity challenges effectively. From an organizational perspective this framework will facilitate in aligning resources, understanding evolving threats, and implementing measures that enhance their overall cybersecurity posture, ultimately fostering resilience in the face of cyber threats.

3.1. Iteration 1: Factors and Countermeasures

In cybersecurity readiness, the GRAFTA framework emphasizes the importance of understanding the factors and countermeasures influencing cyber resilience. Researchers highlight that factors to assess cybersecurity must consider both internal and external dimensions (Georgiadou et al.,

2022; Baskerville et al., 2018). We therefore utilize the Threat Vulnerability and Consequences (TVC) model, highlighting the interplay between threat-based and vulnerability-based factors (Ganin et al., 2020). TVC has been regularly used for handling cybersecurity issues (Willis, 2007; Sukumar et al., 2023; Ambika, 2022). Thus, the TVC model not only provides theoretical insights but also guides practical solutions by identifying and assessing risks, aiding resource allocation, and prioritizing countermeasures. Viewing cybersecurity assets (encompassing an array of digital resources, data, and systems that are vital to an organization's functioning) through the threat, vulnerability, and countermeasure lens enhances organizational resilience and informs strategic decision-making (Georgiadou et al., 2022; Ganin et al., 2020). This approach optimizes response mechanisms against cyber threats.

Threat factors (e.g., Ease of Attack, Impact of a Successful Attack) and Vulnerability factors (e.g., Physical Domain, Information Domain, Social Domain) are vital components (Ganin et al., 2020; Hart et al., 2020; Meidan et al., 2023; Collier et al., 2013; Takahashi et al., 2018; Wang and Lu, 2018). Common cybersecurity countermeasures, including Hardware and Software Upgrades, Personnel Training, Insurance Against Data Losses, Data Handling Policy, and Doing Nothing, are identified through literature (Ganin et al., 2020; Armenia et al., 2021; Phua, 2009; Al-Matari et al., 2018; Baskerville et al., 2018; Chowdhury and Gkioulos, 2021; Gao et al., 2020; Dhotre et al., 2022).

The problem space of Iteration 1 focuses on understanding and prioritizing cybersecurity factors and countermeasures within the GRAFTA framework. It establishes a foundation by exploring the interplay between threat and vulnerability factors, with the aim of addressing cyber threats and vulnerabilities effectively.

3.2. Iteration 2: Experimenting with MCDM

In order to prioritize the cybersecurity countermeasures, we utilize MCDMmethods, as provided in GRAFTA (Sharma and Venkatraman, 2023). MCDM provides a structured approach to decision-making by considering multiple criteria and alternatives. We construct a matrix that evaluates each countermeasure for each readiness indicator. The decision maker can select the most suitable security countermeasures tailored to their needs. In Iteration 2, the problem space revolves around exploring the feasibility of MCDM methods for prioritizing cybersecurity countermeasures. By experimenting with diverse MCDM methods this iteration aims to uncover decision outcomes. The challenge here is to discern the effectiveness and feasibility of different MCDM approaches in addressing the complex landscape of cybersecurity readiness. A qualitative study was conducted with the two versions (A & B) of MCDM. Version A and B utilized different weighting methods. Through this we looked into whether there would be change in the final ranking of the outcomes with different MCDM ranking and weighting methods.

3.2.1. Qualitative Study

Version A was used by 3 participants, and Version B by 2 participants. We recruited doctoral and masters level students as participants from a major University who were well versed in the field of information systems. They were selected for the study as it is focused on understanding the experiences based on the tool and its decision outcomes. After a brief presentation about cybersecurity readiness assessment, we asked the participants to use the initial prototype version of CRAT in the context of the current cybersecurity posture of the University's department. The participants were not revealed the ranking method or the weighting method in use, so as to not create biases while doing the assessment. Participants were asked open-ended questions based on cybersecurity readiness assessment, perception on the tool, time taken to use the tool, cognitive effort, decision quality and confidence in decision. The post-experiment survey revealed a change of perception towards cybersecurity readiness for each individual participant (Sample quotes: "*Yes, Cybersecurity Readiness assessment would help an organization prioritize the areas in which they should focus their efforts to ward off cybersecurity threats*", "*Yes, it was explained well in the presentation and I think I got a pretty good picture of the same while using the tool*"). They found the tool convenient to use and comprehend (Sample quotes: "*yes it is convenient*,","*Yes, it's methodological and impartial*"). The result further shows that the quality of results matches the expectation of the decision maker (Sample quotes: "*strongly agree with the quality of results reported*", "*Yes to a certain extent it did. The one I wanted a higher priority was given that*") and felt confident to use the results to make decisions (Sample quotes: "*Probably. I would definitely take these results into consideration while making a decision*", "*yes, feeling a little bit confident as the result suggest what to improve*"). This confirmed that the mapping of the readiness factors with countermeasures would be feasible to incorporate in the prototype. The results from the experiment produced the same ranking from the alternatives by using different MCDM methods. Here, FEDS evaluates

purposeful design, artifact design, relevance, utility of the CRAT.

3.2.2. Digital Nudging and artefact redesign

While experimenting with MCDM weighting methods, we encountered variations in input formats while experimenting with Multi-Criteria Decision Making (MCDM) weighting methods. In Version A, users selected readiness factors via a text-based selection process and provided numeric ratings for pairwise comparisons. Conversely, Version B employed a matrix format for numeric ratings. This observation led us to a compelling question: How do distinct user input styles, encompassed within different User Interfaces (UIs), influence decision outcomes? This inquiry aligns with the concept of Digital Nudging (DN), a phenomenon well-documented in the literature (Weinmann et al., 2016; Schneider et al., 2018). DN revolves around the use of subtle and contextually relevant interventions to explore their influence on decision-making behavior (Weinmann et al., 2016). We delved into the study of how DN, in the context of varying UIs, impacts decision outcomes (Schneider et al., 2018). Motivated by this exploration, we embarked on redesigning the tool to incorporate different UIs while maintaining the consistency of cybersecurity readiness factors and countermeasures. This pursuit aimed to shed light on the role of UI as a pivotal factor for the practical usability of a tool, a dimension widely acknowledged in the field of user-centric design (Schneider et al., 2018).

3.3. Iteration 3: The Redesign

We employed three comparative UIs: Numeric (UI1), Linguistic Scale (UI2), eliciting “Text as an input” (UI3). The backend MCDM method used for evaluating these inputs was the same for each UI, thereby eliminating the effect of varying the ranking method. Iteration 3 ventures into the problem space of redesigning the CRAT integrating different UIs. The challenge lies in selecting an appropriate MCDM method that can incorporate inputs from these different UI formats for evaluating cybersecurity readiness. The overarching goal is to understand the impact of different user input formats on the decision outcomes using the same MCDM method.

3.4. Iteration 4: Experiment with different UIs

The final prototype, a web-based application, underwent evaluation via a mixed-method study. Participants assumed the role of a CISO (Chief Information Security Officer) in a cybersecurity scenario involving an XYZ airline company. Their inputs into CRAT were used to examine the impact of digital nudging on decision outcomes (Section 3.4.1), time efficiency, and cognitive effort (Section 3.4.2). The study gathered 155 usable quantitative responses out of 171, supplemented by qualitative feedback and further interviews involving 22 participants taken from the same experiment from a large Indian University. These participants were from the masters and doctoral level who were enrolled for management information systems course, additionally undergraduate level students were also taken who were well versed with information systems. Iteration 4's focus centered on experimenting with diverse user interfaces (UIs) to evaluate CRAT's performance. The challenge involved understanding how distinct UIs influenced decision outcomes, time efficiency, and cognitive effort. Through quantitative and qualitative analyses, this iteration aimed to determine the most effective and user-friendly UI for accurate and efficient cybersecurity readiness assessments. The ultimate goal was to enhance CRAT's usability and applicability in the cybersecurity readiness assessment domain.

3.4.1. Results from Quantitative Data: Decision Outcomes

The analysis considered the most suggested countermeasure (mode of ranks) for each interface. Variations in the rankings were observed for HSU, PT, and DHP (Table 1). These results revealed that the choice of UI could impact the readiness assessment tool's output, highlighting the importance of careful UI selection to ensure alignment with user priorities and preferences.

Table 1: Modes of the rank from each UI for the countermeasures

Countermeasures/ UI	UI1 (n = 55)	UI2 (n = 54)	UI3 (n = 46)
HSU	1	1	2
PT	2	3	3
IDL	4	4	4
DHP	3	3	2
N	5	5	5

3.4.2. Time Performance and Cognitive Effort

Qualitative questionnaires and post-experiment interviews followed established end-users' performance literature (Hostler et al., 2005). Descriptive statistics from the quantitative study (Table 2) indicated that UI3 demanded the longest completion time and the highest cognitive effort.

Table 2: Descriptive statistic and qualitative feedback for Digital Nudging

Parameter	UI1 (n = 55)	UI2 (n = 54)	UI3 (n = 46)
Time Performance (minutes ± Std Dev)	10.18 ± 7.90	10.12 ± 7.20	18.10 ± 9.06
Cognitive Effort Rating (scale 1-5 ± Std Dev)	3.87 ± 1.95	3.33 ± 1.49	2.95 ± 1.60
Qualitative Feedback	Easy to use and comprehend, suggested making it more concise	Well-formatted and easy to understand, suggested making it shorter and changing the scale	Mixed feedback, some found it complex and others found it user-friendly, suggested using a different input format and reducing text
Interview Feedback	Easier to use and not complex	Easier to use and not complex	Complex, frustrating, and required more cognitive effort

UI1 emerged as the most user-friendly and efficient in terms of both time and cognitive effort. UI2 performed well in these aspects but showed no significant difference from UI1 in terms of cognitive effort. Qualitative survey feedback for UI1 emphasized its ease of use and comprehension, with suggestions to make it more concise. UI2 was noted as well-formatted and understandable, but users recommended brevity and scale adjustments. Feedback for UI3 varied, with some users finding it complex and others user-friendly. Recommendations included altering the input format and reducing text volume. Post-experiment interviews corroborated these findings. UI3 was perceived as requiring more cognitive effort and being frustrating to use, while UI1 and UI2 were deemed easier to use and less complex. Both UI1 and UI2 provided accurate results matching user preferences, indicating good decision quality. UI3 consumed more time and cognitive effort. Overall, User Interface 1 and 2 were found to be more user-friendly and efficient in reducing cognitive effort, while improvements were suggested for User Interface 3. In conclusion, the FEDS evaluation of CRAT, developed through DSR, encompassed purposeful design, artifact design, relevance, and research rigor. It scrutinized the tool's objectives, architecture, and applicability

4. Deriving Design principles

Based on the prescription of (Gregor et al., 2020), we derive three design principles from the four iterations. The principles emerging from the development and evaluation of CRAT can potentially be applied to the design and development of other readiness assessment tools across various domains. We will elaborate on three aims (A1, A2, A3) and nine mechanisms (M1 - M9) involved in the derivation of the design principles. The mechanisms describe the means or activities to achieve the aim or describe the functionality of the system.

A1 (Aim 1) - To ensure that the tool is effective and efficient in its design and intended purpose of evaluating cybersecurity readiness. The mechanisms are as follows:

1. *Identifying key objectives and requirements (M1)*: Through the iterative development of the CRAT prototype, key objectives and requirements were identified to ensure the tool's effectiveness and efficiency in evaluating cybersecurity readiness.
2. *Establishing a clear framework for the design process (M2)*: To develop CRAT, we used DSR iterations. GRAFTA served as a design artifact to assist the development stages. These two approaches helped with the design and development process.
3. *Using a framework for evaluation (M3)*: The FEDS framework was employed at each iteration to evaluate and provide inputs for the next phase of development. This systematic evaluation process (M3) ensured that the CRAT prototype was refined and improved throughout its iterative development.
4. *Analyzing the feedback and outcomes (M4)*: Feedback from each of the iterations were considered in the next. This helped in the continuous development

process. The prototype was designed (Iteration 2) and again redesigned (Iteration 4). This also demonstrated the importance of tool development through the lens of DSR. The decision outcomes, qualitative feedback and interviews from the tool helped in understanding the relevance of the system and the use of DN for evaluating the cybersecurity posture.

Thus the *Design Principle 1 (DP1) can be deduced as Systematic design and development of the tool.* To build CRAT, we need to define system objectives (M1), employ appropriate frameworks (M2), and use an iterative evaluative process (M3) which allows for implementers to improve the system (M4). DP1 is directed towards designers (actor), situated within the design and development process (context), with the rationale of ensuring a methodical approach that results in a meticulously designed, developed, and tested tool. In terms of lessons learned, the need for clear objectives and structured frameworks like DSR which provide a foundation for systematic development for tools like CRAT is important. The FEDS framework's adoption ensured ongoing refinement, emphasizing systematic evaluation's significance in development.

A2 (Aim 2) - To achieve a user-friendly interface that is easy to use, understand, and navigate. The mechanisms are as follows:

1. *Consistent and intuitive navigation structure (M5)*: When a navigation structure is consistent and intuitive, it becomes easier for users to learn and remember how to interact with the interface. It reduces frustration and enhances their overall experience. A well-designed navigation structure allows users to complete tasks and access desired information efficiently.
2. *Time taken to use the tool with the given user interface (M6)*: A well-designed interface streamlines user interactions, allowing users to complete tasks more quickly which is an important metric of the system performance.
3. Cognitive Effort to use the tool with the given user interface (M7): Intuitive navigation allows users to complete the task efficiently and thereby minimize cognitive load required to understand how to navigate the system.

Thus the *Design Principle 2 (DP2) can be deduced as Understanding the usability of User Interface Design.* DP2 focuses on understanding the usability of UI design in the context of CRAT. The aim of this principle is to achieve an interface that is easy to use, understand, and navigate (M5), thereby saving on two important metrics namely time (M6) and effort (M7) which are crucial to system usage. DP2 caters to end-users of diverse technical backgrounds (actor), positioned within the user interface design process (context), with the rationale that efficient UI design usability directly impacts user satisfaction, productivity, and efficiency. In terms of lessons learned, consistent and intuitive navigation improves user experience and efficient UI design saves time and effort.

A3 (Aim 3) - To design a system so as to help people with their decision making. The mechanisms are as follows:

M8. Appropriate use of mapping elements to incorporate inputs: The use of MCDM methods and their refinement through the iterations helps with decision-making. Further, in iteration 2 we experimented with MCDM methods, we ensured the mapping of input corresponds to the input format used by the MCDM method. But in Iteration 3 we focused on the MCDM method which can include different UI formats.

M9: A Core Algorithm for Computing inputs elicited from Diverse User Interface Designs: We employed a suitable MCDM method to compute results from different UI formats. The algorithm was selected and implemented by considering multiple User Interfaces and the inputs that will be computed from each UI.

Thus the *Design Principle 3 (DP3) can be deduced as Adaptability of algorithm to digital nudging.* DP3 focuses on implementing an algorithm to incorporate different UI designs (M9). This adaptation aimed at assisting users in making effective decisions through digital nudging, incorporating various UIs for user input elicitation (M8). DP3 addresses both end-users and designers (actor), contextualized within the algorithm's design to accommodate diverse user interface styles. The rationale behind DP3 underscores the potential impact of incorporating digital nudging techniques on shaping decision outcomes. In terms of lessons learned, effective decision-making requires understanding digital nudging and impact on decision outcomes. This ensures which UI to incorporate further for decision making.

These design principles are valuable for a diverse range of stakeholders. They offer significant guidance to researchers and practitioners involved in the design and development of readiness assessment tools, particularly in the context of cybersecurity. Additionally, they provide essential insights for researchers, industry practitioners, and designers aiming to incorporate digital nudging techniques into decision support systems where decision support systems and user interfaces play a crucial role. Moreover, researchers and practitioners seeking practical knowledge regarding systematic tool development and user-centric design will find these principles beneficial.

5. Implications

The managerial implication of CRAT is that it enables organizations to assess their cybersecurity readiness and prioritize security countermeasures based on their readiness factors. By following the GRAFTA framework (Sharma and Venkatraman, 2023), DSR methodology (Hevner, 2007; Peffers et al., 2012; Hevner et al., 2010; vom Brocke et al., 2020), and the derived design principles (Gregor et al., 2020; Michalke et al., 2022), organizations can develop similar tools for other technology domains, fostering a structured approach to designing and developing innovative artifacts (Venkatraman and Sundarraj, 2023; Hevner et al., 2010; Baskerville et al., 2022; Gregor et al., 2020).

From a research perspective, the development of a system for cybersecurity readiness assessment using DSR has important implications. CRAT enhances the understanding of a design process and establishes a foundation for developing similar systems for future research (Baskerville et al., 2022; Baskerville et al., 2018). This study also highlights the value of applying a problem-solving approach to cybersecurity challenges and showcases the iterative nature of design science research (Venkatraman and Sundarraj, 2023; Baskerville et al., 2022). FEDS highlighted the importance of effectively communicating research findings to the intended audience (Venable et al., 2016). Furthermore, researchers can contribute to the broader body of knowledge in the field by documenting and sharing their design experiences, methodologies, and lessons learned, fostering a collective advancement in readiness assessment systems (Georgiadou et al., 2022; Venkatraman and Sundarraj, 2022; Venkatraman et al., 2015; Venkatraman et al., 2016; Venkatraman et al., 2018; Venkatraman et al., 2022; Sharma and Venkatraman, 2023; Venkatraman and Sundarraj, 2023).

6. Conclusion

In conclusion, this study contributes to the field of cybersecurity readiness assessment by developing the CRAT prototype and deriving three design principles from the iterative development process. The use of GRAFTA as a design artifact, the application of DSR methodology, and the evaluation through the FEDS perspective addressed a theoretically sound context to a practically applicable problem in cybersecurity. The derived design principles provide recommendations for creating tools with user-friendly interfaces, incorporating different user interface designs, and adapting algorithms for digital nudging. One limitation of this study is its focus on the development and evaluation of the CRAT prototype within a specific context. Further research is needed to validate the effectiveness and generalizability of the derived design principles across different industries and organizational settings, while also considering the applicability of the FEDS framework in evaluating other design artifacts in the field of cybersecurity readiness and readiness assessment in general. Moving forward, our research agenda extends beyond this theoretical foundation. We are actively working on incorporating industry standards from the ISO 27000 series and conducting interviews with cybersecurity professionals to address practical challenges. However, due to the limitations of this conference paper, we have concentrated solely on the initial prototype. Comprehensive details of the prototype's evolution and its integration with practical industry standards will be presented in forthcoming research publications.

7. References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2018, October). Cybersecurity tools for IS auditing. In 2018 Sixth International Conference on Enterprise Systems (ES) (pp. 217-223). IEEE.

Ambika, N. (2022). Precise Risk Assessment and Management. *Cyber‐Physical Systems: Foundations and Techniques*, 63-83.

Apiola, M., & Sutinen, E. (2021). Design science research for learning software engineering and computational thinking: Four cases. Computer Applications in Engineering Education, 29(1), 83-101.

Arce, D. (2022). Cybersecurity For Defense Economists. Defence and Peace Economics, 1-21.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580.

Baskerville, R., Rowe, F., & Wolff, F. C. (2018). Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 49(1), 33-52.

Baskerville, R. L., Kim, J., & Stucke, C. (2022). The cybersecurity risk estimation engine: A tool for possibility based risk analysis. Computers & Security, 120, 102752.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531-540.

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2021). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. Decision Support Systems, 113651.

Blumenthal, J. (2022). Thinking like a lawyer: why you or your IT team needs to keep your software systems up-to-date. ACM SIGCAS Computers and Society, 50(3), 10-10.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361.

CISA. (2021, June 30). CISA's CSET tool sets sights on ransomware threat. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/news-events/alerts/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 33, 469-470.

Dhotre, P. S., Bihani, A., Khajuria, S., & Olesen, H. (2022). "Take It or Leave It": Effective Visualization of Privacy Policies. In Cybersecurity and Privacy-Bridging the Gap (pp. 39-64). River Publishers.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 40(1), 183-199.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3), 452-462.

Green, A. W., Woszczynski, A. B., Dodson, K., & Easton, P. (2020). Responding to cybersecurity challenges: Securing vulnerable US emergency alert systems. Communications of the Association for Information Systems, 46(1), 8.

Gregor, S., Chandra Kruse, L., & Seidel, S. (2020). Research perspectives: the anatomy of a design principle. Association for Information Systems.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

Hevner, A., Chatterjee, S., Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. Design research in information systems: theory and practice, 9-22.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science-Hevner. Design Science in Information Systems Research Author MIS Quarterly, 28 (1), 75–105.

Hevner, A. R. (2007). A three cycle view of design science research. Scandinavian journal of information systems, 19(2), 4.

Hostler, R. E., Yoon, V. Y., & Guimaraes, T. (2005). Assessing the impact of internet agent on end users' performance. Decision Support Systems, 41(1), 313-323.

ISO/IEC 27001:2022 (2022), "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269-282.

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 43(1), 28-36.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.

Maedche, A., Gregor, S., Morana, S., & Feine, J. (2019). Conceptualization of the problem space in design science research. In Extending the Boundaries of Design Science Theory and Practice: 14th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2019, Worcester, MA, USA, June 4–6, 2019, Proceedings 14 (pp. 18-31). Springer International Publishing.

Mambetov, S., Begimbayeva, Y., Joldasbayev, S., & Kazbekova, G. (2023, January). Internet threats and ways to protect against them: A brief review. In 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 195-198). IEEE.

Meidan, Y., Benatar, D., Bitton, R., Avraham, D., & Shabtai, A. (2023). D-Score: An expert-based method for assessing the detectability of IoT-related cyber-attacks. Computers & Security, 126, 103073.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. Computers & Security, 92, 101762.

Meland, P. H., Nesheim, D. A., Bernsmed, K., & Sindre, G. (2022). Assessing cyber threats for storyless systems. Journal of Information Security and Applications, 64, 103050.

Michalke, S., Lohrenz, L., Lattemann, C., & Robra-Bissantz, S. (2022, January). Design Principles for Engagement Platforms-Design Knowledge on Fostering Value Co-Creation. In HICSS (pp. 1-10).

Nagle, T., Sammon, D., & Doyle, C. (2016). Meeting in the middle: bridging the practice research divide from both sides. In ECIS 2016 Proceedings, AISeL Research Papers (pp. 158-1). AIS Electronic Library (AISeL).

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. ACM Computing Surveys (CSUR), 54(11s), 1-37.

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design science research evaluation. In Design Science Research in Information Systems. Advances in Theory and Practice: 7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012. Proceedings 7 (pp. 398-410). Springer Berlin Heidelberg.

Phua, C. (2009). Protecting organisations from personal data breaches. Computer Fraud & Security, 2009(1), 13-18.

PwC. (2023, January). Cyber readiness health check. PwC Singapore. Retrieved from

https://www.pwc.com/sg/en/risk-assurance/assets/cyber-readiness-health-check.pdf

Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. Computers & Operations Research, 39(4), 774-784.

Schneider, C., Weinmann, M., & Vom Brocke, J. (2018). Digital nudging: guiding online user choices through interface design. Communications of the ACM, 61(7), 67-73.

Sharma, A., & Venkatraman, S. (2023). Towards a Standard Framework for Organizational Readiness for Technology Adoption. In Advances in Digital Manufacturing Systems: Technologies, Business Models, and Adoption (pp. 197-219). Singapore: Springer Nature Singapore.

Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2023). Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing, 1-27.

Sukumar, A., Mahdiraji, H. A., & Jafari‐Sadeghi, V. (2023). Cyber risk assessment in small and medium‐sized enterprises: A multilevel decision‐making approach for small e‐tailors. *Risk Analysis*.

Takahashi, T., Panta, B., Kadobayashi, Y., & Nakao, K. (2018). Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information. International Journal of Communication Systems, 31(3), e3470.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a framework for evaluation in design science research. European journal of information systems, 25, 77-89.

Venkatraman, S., & Sundarraj, R. (2023). Assessing organizational health-analytics readiness: artifacts based on elaborated action design method. Journal of Enterprise Information Management, 36(1), 123-150.

Venkatraman, S., & Sundarraj, R. P. (2022). Health-Analytics Readiness Assessment: Elaborated Action Design Research and Nascent Theoretical Implications. IEEE Transactions on Engineering Management.

Venkatraman, S., Sundarraj, R. P., & Mukherjee, A. (2016, May). Prototype design of a healthcare-analytics pre-adoption readiness assessment (HAPRA) instrument. In International Conference on Design Science Research in Information System and Technology (pp. 158-174). Springer, Cham.

Venkatraman, S., Sundarraj, R. P., & Seethamraju, R. (2018, June). Assessing strategic readiness for healthcare analytics: System and design theory implications. In International Conference on Design Science Research in Information Systems and Technology (pp. 116-131). Springer, Cham.

Venkatraman, S., Sundarraj, R. P., & Seethamraju, R. (2022). Exploring health-analytics adoption in indian private healthcare organizations: An institutional-theoretic perspective. Information and Organization, 32(3), 100430.

vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. Design science research. Cases, 1-13.

Wallner, J. (2014). Cyber Risk Management. Wiley StatsRef: Statistics Reference Online.

Wang, C., & Lu, Z. (2018). Cyber deception: Overview and the road ahead. IEEE Security & Privacy, 16(2), 80-85.

Weinmann, M., Schneider, C., & Brocke, J. V. (2016). Digital nudging. Business & Information Systems Engineering, 58, 433-436.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis: An International Journal*, *27*(3), 597-606.