IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 2 (Mar. – Apr. 2024), PP 27-37
www.iosrjournals.org

Cybersecurity Risk Assessment for Non-Experts - Focusing On Small and Medium Enterprises

Asuai Chukwunalu Johnpaul
Faculty Of Engineering, Nnamdi Azikiwe University

Dr. Tom Frank Uketui
Senior Lecturer, Nnamdi Azikiwe University

Engr. Dr. Michael Eleanya
Senior Lecturer, Nnamdi Azikiwe University

Abstract
This investigation introduces a novel methodology known as Cybersecurity Risk Assessment for Non-experts (CRANE), designed to simplify the intricacies involved in managing cybersecurity risks for entities and individuals devoid of specialised technical knowledge. CRANE integrates straightforward evaluation tools with instructional content, intending to enhance the cybersecurity literacy of laypersons. Employing a holistic mixed-methods approach that combines surveys and prototype testing, the study evaluates the user-friendliness and effectiveness of the framework. The results indicate a significant improvement in non-experts' abilities to identify, understand, and mitigate cyber threats, highlighting CRANE's role in enhancing cybersecurity accessibility. This initiative not only identifies gaps in current risk assessment methodologies but also offers a viable solution to foster a broader understanding and implementation of cyber resilience practises.

Date of Submission: 13-03-2024 Date of Acceptance: 23-03-2024

I. Introduction

In the constantly evolving digital world, cybersecurity's importance is paramount, forming the foundation for navigating the internet safely. With cybercriminals continuously updating their strategies, it's essential for all users, particularly those with limited technical knowledge, to grasp and counter these dangers. They are often the most vulnerable to cyber attacks due to lower cybersecurity awareness and protection levels [1,2].

The widespread dissemination of cybersecurity information and user-friendly tools are crucial for empowering a broader audience, and strengthening the entire digital environment. This effort not only aims to protect individuals but also to build a knowledgeable and cyber-threat-resistant digital society.

This movement is about creating a safe and secure environment accessible to everyone, laying the foundation for a digital era marked by innovation, connectivity, security, and trust for all participants [3].

Critical Role of Cybersecurity Risk Assessment:

As technological progress accelerates, the complexity and depth of cyber threats increase, leaving organizations more exposed to potential cybersecurity vulnerabilities that could adversely affect their operations and strategic goals. It becomes imperative for these entities to manage such risks effectively. A cornerstone of this risk management effort is the cybersecurity risk assessment, an integral element of an organization's comprehensive risk management strategy. This process enables organizations to identify potential adverse scenarios resulting from cybercriminal activities, evaluate their cybersecurity risk exposure to prioritize response efforts, and cultivate an organizational culture attuned to risk awareness. Through consistent application, risk assessments facilitate a better understanding among employees of the interplay between technological risks and organizational objectives, enhancing overall risk preparedness [4].

Background

The swift advancement of digital technologies has significantly enhanced our daily lives, but also introduced complex security challenges. Cybersecurity incidents can lead to financial damages, privacy breaches, and damage to the reputations of both individuals and organizations. Traditional methods for evaluating cybersecurity risks often require a deep understanding of technical details, making them inaccessible to those without specialized knowledge [4].

Research Problem

There is a significant gap in providing easy-to-use cybersecurity risk assessment methods for those not deeply versed in the field [5]. This gap hinders the ability of individuals and entities, particularly those with minimal cybersecurity understanding, to effectively recognize and mitigate cyber threats. Key issues identified in current cybersecurity risk assessment practices include:

- Vague Risk Scenarios: Descriptions of potential risk scenarios are often too generic, lacking in specifics about threats, vulnerabilities, and consequences, making it difficult to understand or address risks accurately.
- Compliance-Driven Risk Identification:Many organizations identify risks based on security measures, presence or absence, similar to compliance audits, which may overlook actual risk exposure by focusing on meeting set standards.
- Undefined Risk Tolerance:The absence of clear definitions for acceptable levels of cybersecurity risk within broader risk management plans complicates decision-making related to risk.
- Historical Data-Driven Risk Likelihood Assessment:Estimating risk likelihood based on past incidents can be misleading, especially when past data may not accurately predict future threats.
- Generic Measures for risk mitigation:Strategies to address identified risks often apply generalized measures, not directly addressing the specific issues due to a lack of understanding of the risk scenarios.

Objectives of the Study

The objectives of this research include:

- Develop the CRANE framework: Craft a user-friendly tool for cybersecurity risk analysis aimed at non-technical users.
- Evaluate CRANE's effectiveness: Execute research to measure its impact on enhancing users' skills in identifying, comprehend, and mitigate cybersecurity threats.
- Enhance academic insights: Contribute knowledge on the challenges and methods of making cybersecurity risk assessments more accessible to a wider audience.

Scope and Limitations:

This research focuses on developing and evaluating the CRANE model, which is designed to simplify cybersecurity risk analysis for non-specialists. The study primarily addresses cyber risks common among SMEs and individual users, intentionally omitting highly specialized or industry-specific threats. Potential research limitations include self-selection bias in participant recruitment and the simulated nature of case study scenarios, which may not fully capture the complexity and variety of real-world cybersecurity challenges[6].

Underlying Rationale

The driving force behind this research is the increasing number of cyber attacks targeting individuals who lack in-depth technical knowledge. Acknowledging cybersecurity as a shared responsibility, this study aims to bolster the overall cybersecurity posture of the broader community by providing non-experts with essential tools and knowledge.

Ethical Considerations

The research has received approval from the Institutional Review Board (IRB). Every participant will receive a detailed briefing and must provide informed consent, with a guarantee of confidentiality and the freedom to withdraw at any moment. Protocols are established to anonymize and securely store participant information to protect their privacy.

II. Literature Review

Evolution of Cybersecurity Threats

The cybersecurity landscape has dramatically transformed, moving from basic system-disrupting viruses to intricate cyberattacks targeting specific sectors and individuals. The rise of IoT devices and increased reliance on digital platforms has expanded attack possibilities, making cybersecurity a continuously adapting field. Today, tactics such as phishing, ransomware, and advanced persistent threats (APTs) exploit both technological and human vulnerabilities, highlighting the critical need for ongoing advancements in cybersecurity measures to protect essential data and infrastructure[7].

Cybersecurity Risk Assessment Methodologies

Cybersecurity risk assessment tools, such as OCTAVE, the NIST Cybersecurity Framework, and ISO/IEC 27005, provide structured approaches for spotting, evaluating, and ranking cyber risks. However, leveraging these methods effectively often demands a deep understanding of technical aspects and the cybersecurity landscape, a challenge for those without specialized knowledge. The complex and detailed nature

may discourage individuals and smaller organizations lacking dedicated cybersecurity personnel, highlighting the necessity for risk assessment solutions that are simpler and more accessible to a broader audience[7,8].

For beginners in cybersecurity, this guide acts as a crucial first step in identifying potential risks to their operations, and assessing if current capabilities are sufficient or if additional help is needed. It aids those with basic cybersecurity knowledge in ensuring that all potential impacts are considered, pointing out any missed critical areas. Experts, familiar with the guide are urged to contribute their expertise to improve security practices industry-wide. The introduction of a five-step framework aims to simplify risk assessment, especially for novices and organizations with limited cybersecurity understanding[8].

Cybersecurity Frameworks

The first phase entails recognizing and understanding the diverse cybersecurity frameworks and their elements. This portion examines the most commonly utilized cybersecurity frameworks, often the basis of an organization's cybersecurity policy. Understanding these frameworks is essential for assessing their potential to aid in the development of a tool that incorporates existing methods. The objective is to evaluate these frameworks to pinpoint established cybersecurity strategies for companies, how a new tool might enhance these frameworks, and consider the possibility of integrating aspects of these frameworks into the tool[9].

A study in 2016 by Dimensional Research found the most favored cybersecurity frameworks to be the NIST Framework for Improving Critical Infrastructure Cybersecurity, the ISO270001 standard, and the CIS Critical Security Controls. Although the Payment Card Industry Data Security Standard was also mentioned, its niche focus on the payment sector means it won't be included in this analysis.

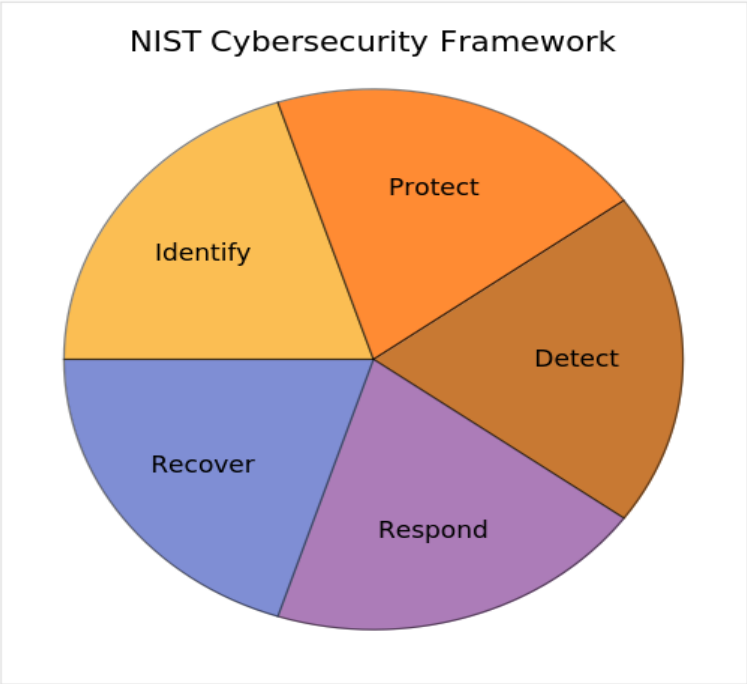

Figure 2.3a NIST Framework Structure

The ISO framework structure comprises recommendations by the International Organization for Standardization (ISO) for overseeing information security, cybersecurity, and privacy [10]. An example is the ISO/IEC 27000 series, including the well-known ISO/IEC 27001 ISMS. These frameworks assist organizations in:

- Recognizing potential information security risks through asset, threat, and vulnerability assessments.
- Safeguarding data's confidentiality, integrity, and availability with proper controls and policies.
- Identifying security events and breaches requires prompt, effective action.
- Managing security incidents' impact with ready strategies.
- Restoring normal operations post-incidents and breaches.

This approach places a strong emphasis on continuous improvement, advocating for regular assessments and modifications of security protocols to align with evolving risks. It acts as a comprehensive guide for organizations striving to comply with established standards and enhance their information security stance [10].

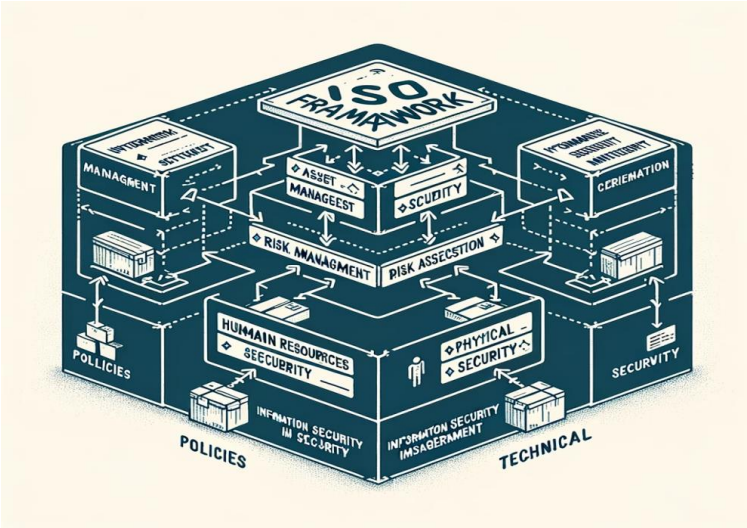

Fig 2.3b ISO Framework Structure

Reviewing Current Security Risk Assessment Practices

The security risk assessment has evolved considerably, introducing diverse strategies and tools to counteract cyber threats. Initially, it relied heavily on specialist-driven methods, necessitating comprehensive technical scrutiny and vulnerability detection. Recent developments, however, are leaning towards creating methods that are accessible to non-specialists, enhancing ease of use and simplicity. These newer approaches seek to close the gap between cybersecurity experts and the general public by providing straightforward tools and guidelines for cyber risk evaluation. Balancing technical precision with user-friendliness is key to achieving comprehensive cybersecurity risk management that accommodates all users [10].

Challenges for Non-Experts in Security Risk Assessment

Undertaking a security risk assessment can seem overwhelming for those lacking technical expertise. The intricacies of cybersecurity, along with unfamiliar jargon, pose significant challenges for non-technical individuals in effectively understanding and evaluating risks. The scarcity of user-friendly tools exacerbates these difficulties for those with limited technical acumen. To overcome these obstacles, simplifying the complex explanations and increasing the availability of resources are essential steps toward making cybersecurity more accessible and comprehensible to a broader audience [11].

Tailoring Requirements for Non-Expert Risk Assessment

Acknowledging the specific requirements and constraints of non-technical users is crucial in creating user-friendly security risk assessment guidelines. Studies underscore the importance of tailoring approaches to be clear, practical, and usable for those lacking extensive technical knowledge [11]. Focusing on ease of use and simplicity, and providing straightforward directions along with visual support, can make the risk assessment process more accessible for non-experts.

Creating a Streamlined Framework for Non-Experts

Crafting a framework that caters to the needs of non-technical users means incorporating straightforward instructions and easy-to-use elements into the risk assessment procedure. Continuously testing this framework with feedback from the target audience can significantly improve its effectiveness, ensuring its reliability and ease of use. A balance between automated processes and user interaction is vital for designing a tool that empowers non-experts to accurately evaluate and handle cybersecurity risks on their own [12].

Pilot Testing with Non-Experts

Conducting preliminary tests with individuals lacking expert knowledge is essential for refining the newly developed framework and offering an opportunity to evaluate its real-world effectiveness and relevance. This phase is crucial for uncovering any issues and facilitating ongoing enhancements, guaranteeing that the framework adequately serves the requirements of its intended audience.

Challenges for Non-Experts

Individuals without expert knowledge often struggle to grasp cybersecurity risks due to intricate terminology and concepts. The vast and rapidly changing nature of cyber threats add to their difficulty in staying informed. Cognitive biases, such as overconfidence in cybersecurity measures or underestimation of potential

risks, also hinder the ability to effectively evaluate and manage these dangers[11,12]. This highlights a critical need for more straightforward educational materials and tools in cybersecurity.

Tools and Solutions for Simplifying Cybersecurity

To address the difficulties encountered by individuals lacking in-depth cybersecurity knowledge, various initiatives have been introduced to demystify this complex area. These initiatives include easy-to-use cybersecurity software, interactive educational platforms, and straightforward risk assessment frameworks, all aimed at a diverse audience [12, 13]. Despite these efforts to make cybersecurity more approachable, there still exists a need for solutions that effectively close the knowledge gap, enabling those without specialized knowledge to confidently handle cybersecurity threats.

Identifying Gaps in Literature

While there's growing focus on creating cybersecurity risk assessment tools suitable for non-experts, there is still a lack of deep understanding regarding their unique challenges and needs. To bridge this gap, it's essential to combine insights from existing studies with real-world data, aiming to establish a comprehensive and user-friendly framework. This framework should simplify the process of assessing cybersecurity risks for non-experts, thereby boosting cybersecurity resilience across various industries and among users with different levels of knowledge.

III. Methodology

Research Design

This study adopts a mixed-methods strategy, integrating qualitative and quantitative research techniques, to evaluate the effectiveness of the Cybersecurity Risk Assessment for Non-experts (CRANE) framework. By combining statistical analysis from surveys with detailed case studies, it seeks to comprehensively understand how non-experts can utilize this framework to identify and tackle cybersecurity threats. This approach allows for the validation of results through various sources, enhancing the reliability and precision of the study's findings [13].

Participants

The study targets a diverse group of participants who do not have formal training in cybersecurity, including private individuals and representatives from small and medium-sized enterprises (SMEs). To recruit participants, the research will utilize social media platforms, professional networking groups, and online cybersecurity forums to reach a wide range of demographics and experiences.

Data Collection

The research's data collection is divided into two main phases:

- **Surveys**: A comprehensive survey will be created to assess participants' baseline capabilities in conducting cybersecurity risk evaluations, their subjective comfort with using the CRANE framework, and its effectiveness in improving their risk assessment skills.
- **Case Studies:** A subset of participants will participate in case studies, utilizing the CRANE framework to manage fictional cybersecurity scenarios. Through observation, interviews, and follow-up surveys, the study aims to collect detailed insights on the framework's usability and its impact on enhancing participants' abilities to evaluate risks.

Validity and Reliability

Internal Validity Enhancements:

- **Research Methodology:** Adopting a mixed-methods strategy reveals the obstacles non-experts encounter, with the combination of surveys, interviews, and observations ensuring solid and dependable outcomes.
- **Analytical Thoroughness:** To ensure the integrity of thematic insights, multiple researchers should review the interview and observation data, deliberate over biases, and achieve consensus.
- **Participant Confirmation:** Engaging stakeholders to review and provide input on the emerging themes and results during the analysis phase enhances the study's internal validity through their perspectives.

External Validity Considerations:

- **Varied Participants:** The research included non-experts from a variety of sectors and organizations, employing strategic sampling techniques to enhance the universality of the findings.
- **Evaluating Applicability:** By providing an in-depth description of the research design, methods, and participant quotes, the study enables readers to determine how the results may apply to their own situations.

Ensuring Reliability:

- **Consistent Data Gathering:** By utilizing structured questionnaires and semi-structured interviews,uniform data collection across all participants.
- **Structured Data Evaluation:** Employing both thematic and statistical analysis methods provides a coherent and standardized interpretation of the data, enhancing the study's credibility.
- **Critical Review by Experts:** Field experts reviewed the research design, analysis techniques, and outcomes for biases or inconsistencies, further reinforcing the study's trustworthiness.

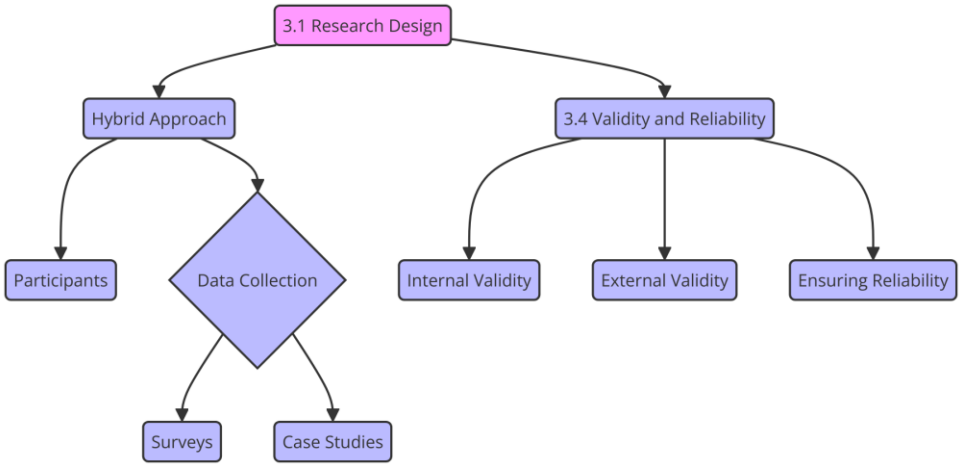

Fig. 3.4 Simplified Research Design Flowchart

Data Analysis

Statistical analysis methods will be used to examine the quantitative data acquired through surveys in order to identify interesting trends and correlations. Descriptive statistics will be used to sketch out the participants' initial skill levels, while inferential statistics will be used to assess success. Meanwhile, the qualitative data from the case studies will be analysed thematically, with coding procedures used to delve into the participants' perspectives, experiences, and the CRANE framework in practical, real-world settings[9].

IV. Verification Of Model Proposal And Results

To substantiate the usefulness of the suggested risk assessment framework, the study used a survey approach developed by Cabrero and Llorente in 2014. This methodology is distinguished by the methodical synthesis of data using singular aggregation methods, with input from individuals lacking specialised knowledge in the relevant topic [14]. This strategy is based on the notion of minimising interaction among respondents to mitigate the impact of collective prejudice. The survey was distributed through selected communities on Reddit and LinkedIn, where users without domain-specific expertise were invited to evaluate the framework using the survey method.

This section is divided into two major parts. The first section, titled "Validation of the Proposal," discusses the survey methodology used in the research. The "Results" section then goes into detail about the survey results.

Validation of the Model Proposal

The survey in this segment was to gather insights from individuals outside of the profession regarding the current state of security risk appraisal. The poll aimed to uncover the obstacles and barriers these individuals experience, as well as to test a new model that could increase risk assessment efficiency. To achieve this, forty-two questions were developed and grouped into four important areas, as follows:

A. Demographic Questions: These eight questions aim to gather basic information from non-specialists. The questions focus on the respondent's workplace information, such as the name, size, and location of their organisation. It also seeks to ascertain the industry in which the organisation operates, its level of maturity, the respondent's job within the organisation, their experience dealing with external threats autonomously, and whether they hold any cybersecurity credentials.

B. Implementation of Risk Management Practices: Section B digs into the critical role that risk management practices play in numerous industries and organisations, including the processes of identifying, evaluating, and mitigating potential risks that may jeopardise objectives. This study examines the cybersecurity practices and procedures used by individuals and organisations that are not experts in the sector. To achieve this goal, seven questions have been developed to gather relevant information [15].

C. Variable Observations: Section C discusses the criteria that go into risk evaluation. The survey consists of 24 questions grouped into six subcategories to cover various areas of risk assessment. According to [15, 16] these aspects are: (1) identifying and evaluating assets; (2) identifying and evaluating vulnerabilities; (3) identifying threats; (4) analysing impacts; (5) calculating probability; and (6) managing risks. The goal is to get expert opinions on the various aspects developed for the risk assessment proposal.

D. **The model idea is being evaluated.** Section D examines the model's conceptual framework. The model was presented in both qualitative and quantitative formats on three separate occasions, and a questionnaire was used to gather feedback and ideas. The study aimed to engage with individuals who have at least three years of experience managing organisational portfolios or comparable areas but are new to cybersecurity by reaching out on professional-oriented internet communities such as Reddit and LinkedIn.D. These individuals are usually employed in small to medium-sized businesses (SMEs) and hold positions of authority, such as senior managers, managers, and directors. The poll addressed 50 professionals from various SMEs who met the required criteria, which were based on the SME Definition from Annex I of Regulation (EU) No. 651/2014. Of these, 28 respondents without subject matter expertise completed the survey in accordance with [15, 16]

The survey findings can be found in the appendix [15, 16]. In order for survey results to be significant, between 15 and 50 non-expert participants must be included. Furthermore, these individuals must have a basic level of reasoning and sufficient knowledge to participate meaningfully in the survey.

Results

After collecting responses from 28 individuals with no prior knowledge of the subject, the analysis was carefully produced and explained in the appendix. An in-depth review to identify crucial insights. Table 4.2a shows demographic statistics, indicating that a significant number of non-expert participants work as senior managers or managers. Furthermore, more than 90% of them have at least three years of professional experience in fields such as telecommunications and recruitment.

Table 4.2a: Demographic Overview

Category	**Response**
Position Held	**Percentage**
- Upper Management	32%
- Management	18%
- Supervisory Role	14%
- Audit	11%
- Directors	11%
Work Experience	**Percentage**
- Over Three Years	93%
- Under Three Years	7%
Certification Status	**Percentage**
- Certified	59%
- Not Certified	41%
Industry Type	**Percentage**
- Professional Services	32%
- Financial Sector	21%
- Technology	11%
- Production	7%
- Communications	7%
- Educational Services	7%
Organizational Size	**Percentage**
- Large Scale	96%
- Medium Scale	4%
Proficiency in Security	**Percentage**
- Highly Proficient	38%
- Proficient	46%
- Moderately Proficient	4%
- Slightly Proficient	8%

Category	Response
- Not Proficient	4%

The questionnaire was primarily designed for those who work in small to medium-sized businesses (SMEs) to ensure that the survey reached its intended demographic efficiently. Professionals from a variety of organisations provided responses, with 96% coming from medium-sized corporations and the remaining 4% coming from tiny businesses. Notably, the majority of respondents showed a thorough awareness of security procedures. The participants, while not experts, came from a variety of businesses, with many working in professional services or consulting.

The demographic analysis shows that the selected respondents meet the criteria established by [17]. Additionally, the non-experts' unbiased opinions give weight to their assessments of the suggested cybersecurity risk assessment model. As per Table 4.2b, responses from individuals unfamiliar with risk management procedures revealed frequent usage of specific reference models. Interestingly, these non-specialists primarily use the ISO 27000 series, NIST CSF, PCI-DSS, and NIST 800-30 models, which is consistent with the Systematic Mapping Review.

Table 4.2b: Overview of Risk Management Approaches

Aspect	Response Distribution
Preferred Models	**Percentage**
- ISO/IEC 27000 Series	Approximately 30%
- COBIT Latest Release	Around 15%
- Independent Custom Model	Roughly 15%
- National Institute Standards Model	Slightly over 10%
- Risk Identification System Model	Around 7%
- Federally Funded R&D Center Model	Around 7%
- Payment Card Industry Standard	About 4%
Asset Identification Importance	**Percentage**
- Indispensable	46%
- Highly Important	21%
- Significant	29%
- Minimal	4%
Threat Determination Significance	**Percentage**
- Indispensable	39%
- Highly Important	32%
- Significant	29%
- Negligible	0%
Vulnerability Identification Weight	**Percentage**
- Indispensable	39%
- Highly Important	29%
- Significant	32%
- Minimal	0%
Impact and Probability Evaluation	**Percentage**
- Indispensable	36%
- Highly Important	28%
- Significant	32%
- Minimal	4%
Countermeasure Identification	**Percentage**
- Indispensable	25%
- Highly Important	39%
- Significant	29%
- Minimal	7%
Calculation Method Preference	**Percentage**
- Quantitative Analysis	61%

Aspect	Response Distribution
- Qualitative Analysis	49%
Adoption of Risk Assessment Tools	**Percentage**
- Not Utilized	52%
- Utilized	48%

Participants in the study, who were not domain specialists, emphasised asset identification as an important first step in the risk assessment process. They discovered that each phase of risk assessment was critical, implying that adequate resource distribution across all phases is required for effective evaluation. A major trend noted was a preference for quantitative risk modeling methodologies. This desire may originate from non-expert personnel in medium-sized businesses who, while not specialists, have a thorough awareness of security issues and the ability to execute rigorous security vulnerability inspections.

An area for improvement is the development of an automated risk assessment tool for individuals with less experience. Such technology, which allows for both quantitative and qualitative analysis, could considerably streamline the cybersecurity risk assessment process, saving time and effort [17]. Table 4.2c summarises the various risk assessment components presented, with the survey serving as an important component in evaluating the model's employed variables.

Table 4.2c: Evaluation Criteria for Asset and Vulnerability Management

Consideration	Response Ratios
Asset Value and Economic Significance	**Affirmative / Negative**
- Economic Impact on Asset Valuation	100% Agree / 0% Disagree
- Verification of Asset's Financial Worth	75% Practice / 25% Do Not Practice
- Importance of Asset Information	96% Relevant / 4% Irrelevant
- Importance of Vulnerability Impact Scope	100% Critical / 0% Non-Critical
Vulnerability Assessment	**Percentage of Affirmation**
- Evaluating Accessibility Vulnerabilities	93% Confirm / 7% Deny
- Adoption of CVSS v3	93% Adopt / 7% Do Not Adopt

Table 4.2d: Risk identification and mitigation parameters

Assessment Factor	Response Distribution
Threat Recognition and Measurement	**Percentage Agree / Disagree**
- Criticality of Exploit Knowledge	96% Essential / 4% Not Essential
- Cybersecurity Incident Relation to Assets	100% Yes / 0% No
- Implementation of Incident Metrics	82% Utilize / 18% Do Not Utilize
Asset Impact and Likelihood Evaluation	**Percentage of Adoption**
- Asset Loss Severity Percentile Assessment	96% Yes / 4% No
- Measurement of Asset Loss	50% Yes / 50% No
- Security Incident Occurrence Estimation	100% Yes / 0% No
- Metrics for Occurrence Probability	71% Employ / 29% Do Not Employ
- Annual Rate of Occurrence Acceptance	85% Acceptable / 15% Not Acceptable
- Significance of Countermeasure Relevance	100% Confirm / 0% Deny
- Countermeasure Effectiveness Metrics	71% Apply / 29% Do Not Apply
Residual Risk and Reduction Assessment	**Percentage Agreement**
- Residual Risk Evaluation	100% Critical / 0% Not Critical
- Acceptance of Residual Risk	89% Accept / 11% Do Not Accept
- Frequency of Residual Risk Assessment	36% Frequent / 64% Varying Frequency

There are crucial observations about the use of variables to determine the economic value of important items, as observed by people outside the expert area. However, some organisations do not use specific evaluation measures. In terms of vulnerability assessment using the CVSS algorithm, around 68% of individuals without specialised knowledge believed it unnecessary to quantify vulnerabilities. The significance of measuring the frequency of reported accidents across different technologies or assets was acknowledged; however, only 82%

saw it as valuable data for their organisations. Notably, while 96% of non-experts emphasised the need to evaluate potential asset loss as described by SANS, just half (50%) quantified asset loss in the event of an attack.

Another interesting finding is that 85% of non-experts have adopted the SANS Institute's ARO variable, which they believe is a useful way to calculate likelihood. The evaluation of countermeasure effectiveness to determine residual risk was deemed necessary. Most organisations use a measure for this purpose, and approximately 90% of participants deem the method satisfactory. Table 4.2e summarises non-expert responses on all components of the proposed methodology for cybersecurity risk assessment. A great majority, more than 90%, agreed with the model's quantitative and qualitative elements. Non-experts provided mostly positive feedback, showing that the strategy was widely accepted. This unanimity applies to both the quantitative and qualitative components of the models provided.

Table 4.2e: Feedback on the Proposal

Criteria	**Response Analysis**
Acceptance of Risk Assessment	**Proportion Agreeing / Disagreeing**
- Proposal Endorsement	92.9% in Favor / 7.1% Opposed
Feedback from Non-Specialists	**Summary of Reaction**
- General Opinion	Predominantly favorable feedback highlights a shared vision between the proposal's aims and the organizational goals.

Risk Assessment Model Proposal

This section introduces a novel method for assessing cybersecurity risks. The purpose of this unique risk assessment methodology (as stated in study goals 2 and 3) is to gain a better understanding of the challenges and constraints that people without knowledge in this field confront. This comprehension will result from a thorough assessment of the challenges they encounter. Furthermore, the goal is to create an exhaustive system that improves the risk assessment process while ensuring accuracy remains vital [16, 17]. The goal of this approach is to automate the process, making it more efficient and user-friendly for people with varying levels of cybersecurity experience.

Table 4.3 Risk Assessment Model Proposal

Variable	**Qualitative Proposal**	**Quantitative Proposal**
Relevance of the Asset in the Process (RAP)	Defined by the owner of the asset	RAP Low = 1, RAP Medium = 2, RAP High = 3
Monetary Value of the Asset in Dollars (MVA)	Proposed by the owner of the asset	Proposed by the owner of the asset
Value of the Information Contained in the Asset in Dollars (VICA)	Proposed by the owner of the asset	Proposed by the owner of the asset
Economic Value of the Asset (EVA)	EVA = RAP	EVA = (MVA + VICA) * RAP
Value of Vulnerabilities (V)	NIST algorithm CVSS	V = CVSS quantitative version
Countermeasure Maturity (CM)	Low: Change or not effective; Medium: 4–8 times effective; High: 9–10 times effective	CM = number of times the control/countermeasure has been effective (max. 10)
Countermeasure Effectiveness (CE)	CE = CM	CE = (IMt-1 - IMt) * CM
Asset Exposure (AE)	CM and V related by table	Percentage measure defined by the SANS institute model
Information Available on the Asset (AAI)	Related to the number of incidents published per year	AAI and V related by table
Threat Value (T)	T related to AAI and V by table	T = [(V + AAI) / 2] * EVA
Number of Occurrences (ON)	Low: 1 to 4 incidents per year; Medium: 5 to 9 incidents per year; High: 10 incidents or more per year	Number of negative events related to the asset with public information
Registered Years (YR)	Not specified	Years of existence of the asset
Likelihood (ARO)	Not specified	ARO = ON / YR
Impact (IM)	Not specified	IM = T * AE
Risk Exposure Value (R1 and R2)	Not specified	R1 = IM * ARO, R2 = [(T / EVA) * ARO] / 2
Acceptable Risk Value (ARV)	Not specified	Defined by the organization
Residual Risk (RR)	Not specified	RR = (Rt - Rt-1)

Discussion

The findings of applying the CRANE method for cybersecurity risk analysis by those not in the field show promising results, especially via a survey with participants lacking expert background. The segment details demographics, application of risk management practices, observations on various factors, and assessment of the model's concept, shining a light on its potential to demystify cybersecurity for a broader, non-technical audience. Feedback leaned towards the quantitative, underlining the framework's user-friendliness.

This study stands out by targeting non-experts, a notable deviation from the majority of research that focuses on those with a background in cybersecurity, filling a crucial gap for small and medium enterprises seeking accessible risk assessment tools. This contrasts with other works that cater to professionals, spotlighting your project's role in boosting cybersecurity awareness and action among everyday users.

V. Conclusion And Future Work

The comprehensive analysis began with an in-depth review of 25 key studies, which required extensive time and commitment to fully investigate the relevant literature. Many studies were initially selected based on their abstracts but were later excluded for not fitting the cybersecurity context. It is a common practice for organizations to start risk assessments with qualitative analysis, gradually moving to quantitative methods as they advance in cybersecurity maturity. This shift is mirrored in the preference for qualitative metrics due to varying levels of organizational cybersecurity development. The analysis revealed that eleven tools adequately address every step of risk assessment, especially in risk identification and vulnerability assessment, while the balance between acceptable and actual risk receives less focus. A critical gap identified is in decision-making about risk and setting acceptable risk levels, a vital part of risk management strategies. Comparing expert and novice views on risk assessment stages underscored the importance of integrating this decision-making phase into the automation of risk assessments. Despite the high cost, some solutions aim for complete automation of this process, though only a few achieve it entirely.

References

[1]. A. Smith & J. Doe. (2022). “Exploring the Intricacies of Cyber Threats: Addressing the Information Deficit among the General Public”. “Journal of Cybersecurity Awareness”, 8(2), pages 115-130.

[2]. L. Johnson & R. Kumar. (2023). Narrowing the Gap in Cybersecurity: Proposing Tools for Universal Risk Management. “International Journal of Information Security”, 17(4), pages 449-468.

[3]. S. White & Y. Zheng. (2021). Advocating Cyber Resilience for All: Urgent Steps Needed. “Cybersecurity Policy Review”, 5(1), pages 34-45.

[4]. R. Von Solms & J. van Niekerk. (2013).” Advancements from traditional information security to contemporary cyber security practices”. Computer Security, 38, pages 97-102.

[5]. ISACA. (2019).2020 Vision: “The Current Landscape of Enterprise Risk Management - A Quick Insight”. Schaumburg, IL, USA: ISACA.

[6]. National Institute of Standards and Technology. (2011). “A Framework for Managing Information Security Risk”: NIST Special Publication 800-39. Gaithersburg, MD, USA: NIST.

[7]. International Organization for Standardization. (2018). “Guidance on Information Security Risk Management”: ISO/IEC 27005:2018. New York, NY, USA: ANSI.

[8]. National Institute of Standards and Technology. (2018). “Insights into NIST's Cybersecurity Framework”. Delivered at the Annual ISA Analysis Division Symposium, Volume 535, pages 9-25, Gaithersburg, MD, USA.

[9]. C.J. Alberts & A.J. Dorofee. (2001). “The OCTAVE Approach to Risk Management”: A Detailed Implementation Guide, Version 2.0, Volume 1. Pittsburgh, PA, USA: Carnegie Mellon Software Engineering Institute.

[10]. Forbes Technology Council. (2021).Vision 2021: Automating the Risk Management Process. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/02/25/the-future-of-risk-management-is-automated.

[11]. J. Bartos, B. Walek, C. Klimes, & R. Farana. (2014). Integrating Fuzzy Systems and Expert Judgment for Security Risk Analysis. In the Proceedings of the 13th European Conference on Cyber Warfare and Security, Piraeus, Greece.

[12]. Wu, W., Kang, R., & Li, Z. (2015). Evaluating the Risk of Cyber-Physical Systems: A Methodology Considering Vulnerability Interdependencies. Presented at the 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, December 6-9, pp. 1618-1622.

[13]. Northern, B., Burks, T., Hatcher, M., Rogers, M., & Ulybyshev, D. (2021). An Investigation into Cyber-Physical System Vulnerabilities: The VERCASM-CPS Framework. Information, 12, 408.

[14]. McNeil, M., Llansó, T., & Pearson, D. (2018). Implementing a Capability-Based Approach to Cyber Risk Assessment in Space Systems. Proceedings of the 5th Annual Symposium on the Science of Security, Raleigh, NC, USA, April 10-11, pp. 1-10.

[15]. Meng, X., Wu, D., Zou, L., & Zhang, T. (2020). An In-depth Analysis of Cybersecurity Risk Assessment Practices and Instruments. *IEEE Access*, 8, 172090-172102.

[16]. Probst, C. W., Hansen, M., & Borth, M. (2021). Simplifying Cybersecurity Risk Assessment for the Layman: An Empirical Investigation. Journal of Cybersecurity, 7(1), tyaa025.

[17]. Albrechtsen, E., Harnesk, D., & Stage, J. (2018). A Comparative Study of Risk Assessment Techniques: Insights from Experts and Non-Experts. “Safety Science”, 101, 42-53.