businesses

Article

A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience

Panagiotis Katrakazas * and Spyros Papastergiou

Maggioli S.p.A. Greek Branch, 15124 Athens, Greece; spyros.papastergiou@maggioli.gr
* Correspondence: panagiotis.katrakazas@maggioli.gr

Abstract: The escalating complexity and sophistication of cyber threats necessitate advanced solutions that not only counteract these threats but also proactively adapt to the evolving needs of diverse stakeholders involved in digital infrastructures, such as telecom operators, cloud service providers, and end-users in sectors like healthcare and finance. This research addresses a crucial gap by focusing on a systemic, AI-powered approach to stakeholder needs analysis in cybersecurity. By aligning closely with stakeholder requirements, the proposed framework aims to offer dynamic, responsive cybersecurity solutions that enhance the resilience of digital infrastructures against evolving cyber threats. This research systematically maps the landscape of stakeholder needs in cybersecurity across different sectors through qualitative methods like interviews and focus groups, supplemented by data from the CyberSecDome project's pilot cases and open calls. Requirements for an AI-driven framework are then formulated based on these data to identify patterns and predict stakeholder needs. The analysis reveals critical challenges faced by stakeholders, including limited threat intelligence sharing, insufficient automation in incident response, and regulatory hurdles related to data protection laws and evolving cybersecurity legislation. There is a strong interest in leveraging AI for enhanced intrusion detection, real-time threat intelligence sharing, and privacy-preserving information exchange.

Keywords: stakeholder needs; artificial intelligence; cybersecurity; systemic approach; digital infrastructures

Citation: Katrakazas, P.; Papastergiou, S. A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience. *Businesses* **2024**, *4*, 225–240. https://doi.org/10.3390/businesses4020015

Academic Editor: Lester Johnson

Received: 13 March 2024
Revised: 11 June 2024
Accepted: 12 June 2024
Published: 17 June 2024

1. Introduction

The escalating sophistication and frequency of cyber threats targeting critical digital infrastructures has become a pressing global concern. As interconnected systems and networks underpin essential services across sectors like finance, healthcare, energy, and transportation, ensuring their resilience against cyber-attacks is paramount for maintaining economic stability and public safety. This challenge is further compounded by the rapidly evolving nature of cyber threats, which often exploit previously unknown vulnerabilities and leverage advanced techniques like artificial intelligence (AI) and machine learning [1,2].

While significant efforts have been made to enhance cybersecurity measures, a comprehensive understanding of the diverse needs and challenges faced by stakeholders across critical infrastructure sectors is crucial for developing effective, tailored solutions [3,4]. Previous studies have highlighted the importance of stakeholder engagement and collaboration in cybersecurity, but there remains a lack of systematic approaches for analyzing and addressing the specific requirements of different stakeholder groups [5,6].

Recognizing this gap, the CyberSecDome project (GA: 101120779) [7] aims to develop an AI-driven framework from a stakeholder needs analysis in cybersecurity. By leveraging data from pilot cases and open calls involving telecom operators, cloud service providers, aviation operators, and sectors like healthcare and finance, this research endeavors to map the landscape of stakeholder needs and translate them into actionable insights for enhancing cyber resilience.

The proposed methodology involves a multi-pronged approach. First, qualitative methods such as interviews and focus groups will be employed to identify and categorize stakeholders' cybersecurity needs. This will be supplemented by quantitative data analysis from the CyberSecDome project [7] to uncover patterns and trends. Subsequently, an AI model will be trained on these data to predict and analyze stakeholder needs dynamically. The framework's effectiveness will be evaluated through pilot testing and stakeholder feedback, with a particular focus on its ability to enhance incident response, threat intelligence sharing, and collaborative defense mechanisms.

While the integration of AI in cybersecurity has shown promise, concerns have been raised regarding ethical considerations, data privacy, and the potential for AI systems to perpetuate biases or be exploited by adversaries [8]. This study aims to address these challenges by incorporating privacy-preserving mechanisms and adhering to ethical guidelines for AI development and deployment.

By bridging the gap between stakeholder needs and cybersecurity solutions through an AI-driven, systematic approach, this research has the potential to contribute significantly to the field of cybersecurity. It not only advances the theoretical understanding of stakeholder analysis but also offers practical tools and insights for enhancing the resilience of critical digital infrastructures against evolving cyber threats.

The rest of the article is structured as follows: Section 2 reviews current cybersecurity measures for critical information infrastructures, discussing the challenges posed by quantum computing, the impact of the COVID-19 pandemic, and the importance of continuous network security efforts. Section 3 synthesizes key studies on AI in cybersecurity, stakeholder analysis, and critical infrastructure protection, identifying a gap in integrating AI-enhanced solutions with stakeholder analysis methodologies. Section 4 details the multi-pronged approach used to map stakeholder needs, including qualitative methods like interviews and focus groups, supplemented by quantitative data analysis. Section 5 presents findings from a comprehensive questionnaire distributed to stakeholders, highlighting key insights into organizational demographics, cybersecurity practices, incident management, and the role of AI in enhancing cybersecurity. Section 6 addresses challenges and pitfalls encountered during the stakeholder analysis process and emphasizes the added value of addressing these challenges. The article concludes by summarizing the key findings and their implications for future research and development in cybersecurity.

2. State of the Art in Cybersecurity for Critical Information Infrastructures

Critical information infrastructures (CIIs) are the backbone of a nation's economy, security, and health, as they encompass the essential services that support daily social and economic activities. However, with the increasing integration of information technologies, CIIs are facing unprecedented cybersecurity challenges.

The advent of quantum computing presents both an opportunity and a challenge for cybersecurity within CIIs. Quantum-resistant cryptographic solutions are becoming essential to protect against future threats that could exploit the power of quantum computers to break traditional encryption methods [9]. At the same time, a holistic approach to cybersecurity is critical for the effective protection of CIIs. This approach must encompass technical, policy, human, and behavioral aspects to address the complex nature of cyber threats. The integration of these aspects is vital for developing robust cybersecurity strategies that can adapt to evolving threats [10].

The COVID-19 pandemic has accelerated the shift to remote work, introducing new cybersecurity risks. Home offices often lack the robust security measures of centralized offices, and the blending of personal and professional device use increases the risk of data breaches. Organizations must focus on securing distributed workforces by identifying new vulnerabilities and implementing appropriate security controls [11]. Securing networks is a critical preventative measure against cyber threats. Continuous monitoring, assessments, and mitigation are necessary to protect the various components of a network, including servers, cloud services, IoT devices, and physical assets. The European Common

Criteria-based cybersecurity certification scheme (EUCC) builds on the Mutual Recognition Agreement ('MRA') of Information Technology Security Certificates of the Senior Officials Group Information Systems Security ('SOG-IS') using the Common Criteria, including the group's procedures and documents, which promotes the adoption of common policies and best practices to secure networks effectively [12]. However, as new kinds of cyber-attacks are emerging that exploit browser-based control systems in industrial facilities [13], they can be difficult to detect and can compromise the control of critical infrastructure systems. Research into these vulnerabilities is ongoing, with the aim of developing more secure systems that can withstand such threats.

As it is shown, the cybersecurity landscape for CIIs is complex and ever-changing. The state of the art in cybersecurity requires a multi-faceted approach that includes a holistic view of security, adaptation to remote work challenges, adherence to best practices, continuous network security efforts, and vigilance against emerging threats. Collaboration between academia, industry, and government agencies is essential to develop and implement effective cybersecurity measures for the protection of critical information infrastructures.

3. Literature Review on AI in Cybersecurity, Stakeholder Analysis, and Critical Infrastructure Protection

The integration of artificial intelligence (AI) in cybersecurity represents a significant shift towards more dynamic, predictive, and efficient approaches to protecting digital infrastructures. This section synthesizes key studies and existing frameworks related to AI in cybersecurity, stakeholder analysis, and the protection of critical infrastructure sectors such as healthcare, finance, and telecommunications.

3.1. AI in Cybersecurity

Recent literature underscores the transformative potential of AI in enhancing cybersecurity measures. Kaur et al. provide a comprehensive review of AI use cases for cybersecurity, proposing a taxonomy based on the NIST cybersecurity framework [1]. Their analysis highlights AI's capabilities in automating repetitive tasks, accelerating threat detection, and improving response accuracy. Similarly, Chowdhury and Gkioulos emphasize AI's role in improving system response, robustness, and resilience against cyber-attacks, particularly in critical infrastructure sectors [14].

3.2. Stakeholder Analysis in Cybersecurity

Stakeholder analysis emerges as a crucial methodology for understanding the diverse cybersecurity needs across different groups. Fischer-Hübner et al. conducted interviews with European stakeholders from security-critical sectors, identifying common challenges and requirements such as trust building, privacy and identity management, and the need for resilient systems [4]. This study underscores the importance of engaging stakeholders in the cybersecurity process to ensure that solutions are aligned with real-world needs and operational challenges.

3.3. Cybersecurity in Critical Infrastructure

The protection of critical infrastructure from cyber threats is a growing concern, given the increasing reliance on digital technologies in sectors like healthcare, finance, and telecommunications. Literature in this area focuses on the development of cybersecurity training programs [14], the application of AI for threat detection and response [1,15], and the exploration of emerging trends in cybersecurity for critical infrastructure protection [16,17]. These studies highlight the need for comprehensive solutions that combine robust risk assessment, advanced technologies like AI, and stakeholder engagement to protect critical infrastructures effectively.

3.4. Synthesis and the Need for an AI-Enhanced Stakeholder Analysis Framework

The review of existing literature reveals a gap in the integration of AI-enhanced solutions with stakeholder analysis methodologies for cybersecurity in critical infrastructure sectors. There is a clear need for a holistic framework that can conduct an in-depth analysis of stakeholder cybersecurity requirements and develop tailored AI-powered solutions to meet those needs. Such a framework would leverage the latest AI capabilities while ensuring that the solutions remain grounded in real-world stakeholder perspectives and operational challenges.

By bridging this gap, the proposed AI-enhanced stakeholder analysis-based framework can pave the way for more effective and widely adoptable cybersecurity measures that protect critical infrastructures and services upon which modern societies depend. This approach not only enhances the security posture of critical infrastructures but also fosters a collaborative environment where stakeholders are actively engaged in the cybersecurity process, ensuring that solutions are both technologically advanced and practically relevant.

4. Materials and Methods

This research addresses a critical gap in the current cybersecurity landscape by focusing on a systemic approach to stakeholder needs analysis. By leveraging AI, the project aims to create a dynamic, responsive cybersecurity framework that not only protects digital infrastructures but also aligns with the specific needs and expectations of various stakeholders. This approach is expected to contribute significantly to the field of cybersecurity, offering insights into how AI can be harnessed to enhance digital resilience in a stakeholder-centric manner.

To map the landscape of stakeholder needs in cybersecurity across different sectors, focusing on the unique challenges and expectations of each stakeholder group identified in the CyberSecDome project [7], including telecom and cloud service providers, aviation operators, and sectors like healthcare and finance, a comprehensive questionnaire was designed. The questionnaire [18] is focused on the elicitation, analysis, and documentation of stakeholders' requirements associated with incident detection and response for digital infrastructures and systems.

The Stakeholders' Analysis Questionnaire was an effective strategy for engaging stakeholders during the stakeholder analysis process. The specific methods used to engage stakeholders through this questionnaire included a comprehensive question design, as the questionnaire covered a wide range of topics relevant to stakeholders, such as organizational profiles, incident management, cybersecurity tools and practices, challenges and expectations, regulatory aspects, and collaboration.

The purpose of the survey was to gather comprehensive insights from diverse stakeholders regarding their cybersecurity challenges, needs, and requirements. Intending to engage with organizations across critical sectors such as healthcare, finance, telecommunications, and cybersecurity providers, the survey aimed to capture a holistic understanding of the real-world cybersecurity landscape. This stakeholder-centric approach was crucial for informing the development of the AI-driven framework that can effectively address the unique cybersecurity challenges faced by different stakeholders and enhance the overall resilience of digital infrastructures. The survey served as a foundational step in the research process, enabling the collection of valuable data from stakeholders directly involved in cybersecurity operations, technology development, and critical infrastructure management. By analyzing the survey responses, the research team could identify common challenges, emerging threats, and specific requirements that need to be addressed through innovative cybersecurity solutions. This data-driven approach ensures that the to-be-developed AI-driven framework is grounded in the practical realities and needs of stakeholders, increasing its relevance, effectiveness, and potential for widespread adoption.

The questionnaire (see Supplementary Materials) was distributed to a diverse group of stakeholders, including those from cybersecurity, academia, technology system providers, and other critical information infrastructure sectors, ensuring a broad range of insights.

Moreover, a dedicated webinar was hosted by EIT Digital [19]. The questionnaire allowed for both quantitative (e.g., rating scales) and qualitative (e.g., open-ended questions) data collection, providing a rich dataset for analysis. The questionnaire was distributed in a manner that was easy for stakeholders to access and complete, as indicated by the 35 responses and the average time to complete being 24:18 min.

One of the key components was to ensure the respondents' anonymity and privacy, which likely encouraged more honest and detailed responses, which is crucial for accurate stakeholder needs analysis. By asking stakeholders about their current tools and practices, the questionnaire helped identify gaps and opportunities for improvement in cybersecurity incident management. More importantly, the questionnaire addressed regulatory challenges and the importance of collaboration, which are key factors in the adoption and effectiveness of cybersecurity measures.

Stakeholders were asked about potential barriers to adopting new cybersecurity technologies, providing insights into the challenges that need to be addressed for successful implementation. The most important option of the questionnaire was the received feedback on AI and intrusion detection systems, as stakeholders were queried on their perceptions of AI in cybersecurity and the usefulness of intrusion detection systems, which can inform the development of AI-enhanced solutions.

To derive functional and non-functional requirements from the questionnaire, a systematic methodology was employed. This methodology involved several steps designed to analyze the responses and translate them into specific requirements that can guide the development of a system or solution. The detailed methodology is presented as follows:

- Step 1: Data Collection and Preprocessing
    - Collect Responses: Ensure all questionnaire responses are collected and organized. This involves compiling the data from various respondents into a structured format, such as a spreadsheet or database.
    - Preprocess Data: Clean the data to remove any inconsistencies or errors. This may include standardizing the format of responses, handling missing data, and categorizing open-ended responses.
- Step 2: Categorization of Responses
    - Identify Themes: Review the questionnaire responses to identify common themes or categories. For example, themes could include incident management tools, cybersecurity challenges, regulatory compliance, and stakeholder collaboration.
    - Group Responses: Group the responses under the identified themes. This helps in understanding the commonalities and differences in stakeholder perceptions and needs.
- Step 3: Analysis of Responses
    - Quantitative Analysis: For closed-ended questions, perform quantitative analysis to identify trends, patterns, and areas of consensus or divergence among respondents. This can involve calculating frequencies, averages, and other statistical measures.
    - Qualitative Analysis: For open-ended questions, conduct qualitative analysis to extract insights, opinions, and specific needs or challenges mentioned by the respondents. Thematic analysis or content analysis techniques can be useful here.
- Step 4: Derivation of Requirements
    - Identify Functional Requirements: Based on the analysis, identify the functional requirements, which are specific features or functions that the system must provide. For example, if many respondents highlight the need for improved incident response tools, a functional requirement could be the development of an automated incident response system.

    - ○ Identify Non-Functional Requirements: Similarly, identify the non-functional requirements, which relate to the system's operation, such as performance, usability, reliability, and security. For example, if respondents emphasize the importance of easy-to-use cybersecurity tools, a non-functional requirement could be that the system interface must be user-friendly.

- Step 5: Validation and Prioritization
    - ○ Stakeholder Validation: Present the derived requirements to a subset of stakeholders or experts for validation. This ensures that the requirements accurately reflect the stakeholders' needs and challenges.
    - ○ Prioritization: Prioritize the requirements based on factors such as the frequency of mention, the importance perceived by respondents, and alignment with strategic objectives. This helps in focusing development efforts on the most critical requirements.
- Step 6: Documentation
    - ○ Document Requirements: Clearly document the functional and non-functional requirements, including descriptions, justifications, and any assumptions or constraints. This documentation serves as a foundation for the subsequent design and development phases.

5. Results

The questionnaire results indicate a recognition of the importance of robust incident management, a willingness to collaborate and share information, and an interest in AI and advanced tools like DAIR to enhance cybersecurity practices. However, challenges such as integration complexities, limited threat intelligence sharing, and the need for improved automation in incident response are areas that require attention. These insights can inform the development of the AI-enhanced framework for stakeholder needs analysis in cybersecurity, ensuring that it addresses the key concerns and expectations of stakeholders. An analysis of the key findings of the questionnaire is presented in the following subsections.

5.1. Organisational Demographics

The majority of respondents are from the cybersecurity sector (14 out of 35), followed by technology system providers (8 out of 35) (Figure S1). Most organizations are private (27 out of 35), with a few public ones (6 out of 35) (Figure S2). The size of the organizations varies, with very large (>250 employees) being the most common (13 out of 35), followed by small (10–50 employees) and micro–very small (<10 employees), suggesting a diverse range of organizational scales (Figure S3).

5.2. Cybersecurity Practices, Expertise, and Perceptions

Information security is the most common area of expertise among respondents (16 out of 35), followed by technology and IT engineering (7 out of 35) (Figure S5). The existing cybersecurity certification procedures and standards are perceived as good by the majority (14 out of 35), with some finding them satisfactory (11 out of 35) or very good (6 out of 35) (Figure S6). Interoperable solutions and practices affecting knowledge management in threat and risk processes are perceived as neutral by most respondents (16 out of 35) (Figure S7).

5.3. Incident Management and Tools

A significant number of organizations (23 out of 35) do not use tools to support incident management processes across preparation, run-time, and recovery (Figure S8). Most organizations (25 out of 35) provide a security management plan (Figure S9) and employ incident handling procedures (Figure S10). This analysis provides insightful data on how organizations perceive and manage cybersecurity incidents, as it focuses on the effectiveness of current incident investigation processes, the quality of incident investigation, response, and analysis capabilities, and the importance of having robust incident investigation capabilities.

Respondents were asked to rate the effectiveness of their organization’s current incident investigation process in identifying and addressing cybersecurity incidents. The responses varied, with 0 indicating it as “Not important at all”, 6 as “Slightly important”, 10 as “Moderately Important”, 12 as “Important”, and 7 as “Very Important” (Figure S28). This distribution suggests that while there is a general consensus on the importance of effective incident investigation processes, opinions vary on how effective current processes are. The fact that a significant number of respondents rated it as “Important” or “Very Important” underscores the critical role of incident investigation in cybersecurity management.

The average rating for the quality of organizations’ incident investigation, response, and analysis capabilities was 3.54 out of 5 (Figure S29). This indicates a moderate level of satisfaction among respondents with their current capabilities. While not exceptionally high, this average suggests that many organizations feel their incident investigation processes are somewhat effective but recognize there is room for improvement.

When asked about the importance of having robust incident investigation capabilities, including root cause analysis, to enhance cyber resilience, the responses highlighted a strong consensus on its criticality (Figure S30). The emphasis on robust incident investigation capabilities reflects the understanding among stakeholders that in-depth analysis and understanding of incidents are essential for preventing future occurrences and strengthening cybersecurity defenses. These results reveal several key insights:

- Need for Improvement: The moderate satisfaction level with current incident investigation capabilities suggests a need for improvement. Organizations may benefit from investing in more advanced tools, training, and processes to enhance their ability to investigate and respond to cybersecurity incidents effectively.
- Critical Role of Incident Investigation: The high importance placed on robust incident investigation capabilities indicates that stakeholders recognize the critical role these processes play in enhancing cyber resilience. This underscores the need for continuous improvement and adaptation of incident investigation practices to keep pace with evolving cyber threats.
- Potential for AI Integration: Given the strong agreement on the potential benefits of AI in the intrusion detection process, there is an opportunity to integrate AI and machine learning technologies to improve incident investigation processes.

Therefore, AI could help automate the analysis of incident data, identify patterns, and speed up the root cause analysis, thereby enhancing the overall effectiveness of incident investigation.

5.4. Cybersecurity Incidents and Response

The majority of organizations (22 out of 35) have not been affected by cybersecurity incidents over the past 3 years (Figure S11), which could indicate effective preventive measures or underreporting due to lack of detection capabilities. Most organizations (24 out of 35) employ a centralized solution to correlate incident information and responses for an organization-wide perspective (Figure S12). This suggests a trend towards centralized incident management systems that can provide a holistic view of cybersecurity incidents. The presence of skilled and trained personnel on security and incident handling practices is reported to be partial, with most organizations having some but not all personnel trained (19 out of 35), and a smaller number having most of their personnel trained (14 out of 35) (Figure S13). This indicates a need for more comprehensive training and skill development in cybersecurity incident handling.

The biggest challenges faced by organizations in incident detection and response include limited threat intelligence sharing (13 out of 35) and insufficient automation in incident response (11 out of 35) (Figure S14). These challenges highlight the need for better threat intelligence mechanisms and more automated response capabilities to improve incident detection and response.

Stakeholders on the other hand have clear expectations for systems that enhance the resilience, security, privacy, and accountability of digital systems and infrastructures. Improved incident response time (11 out of 35) and enhanced threat intelligence sharing (10 out of 35) are among the top expectations (Figure S15). This reflects the demand for faster and more collaborative approaches to managing cybersecurity incidents. There is also willingness among organizations to share incident data and findings in a privacy-preserving manner to enable collaborative learning about threats across organizations and sectors, with 18 out of 35 respondents agreeing or strongly agreeing to this practice (Figure S31). This willingness is crucial for developing collective defense strategies and learning from each other's experiences.

The Dynamic and Adaptive Incident Response (DAIR) tool, which will dynamically select and adopt responses to cyber incidents, is viewed as useful by stakeholders, with 23 out of 35 respondents agreeing or strongly agreeing that it would be useful for their organization (Figure S33). This indicates a positive reception towards innovative tools that can adapt to the dynamic nature of cyber threats.

5.5. Threat Intelligence and Regulatory Challenges

The questionnaire results shed light on the critical role of threat intelligence in cybersecurity and the regulatory challenges that organizations face in this domain. There is a clear need for mechanisms that support dynamic threat intelligence sharing in a privacy-preserving and compliant manner. As cybersecurity threats continue to evolve, fostering collaboration while navigating the complex regulatory environment will be essential for enhancing the resilience and security of critical information infrastructures.

The frequency at which organizations receive threat intelligence information varies, with 11 respondents receiving it daily, 12 as needed, 7 monthly, and 3 weekly (12 out of 35) (Figure S16). This variation suggests that while some organizations prioritize real-time or frequent updates, others may rely on periodic reviews or specific triggers to seek out intelligence.

The questionnaire results highlight a significant interest in threat intelligence sharing, with a majority of respondents indicating a willingness to share incident data and findings in a privacy-preserving manner (Figure S17). This willingness underscores the recognition of the value of collaborative threat intelligence in enhancing cybersecurity defenses across different sectors. The methods and practices for sharing threat intelligence information among stakeholders are crucial, especially in light of regulatory challenges (Figures S54 and S55). Organizations must find ways to collaborate and share intelligence effectively while ensuring compliance with data protection and privacy regulations.

Respondents anticipate several key regulatory challenges in the cybersecurity domain, including compliance with data protection laws and evolving cybersecurity legislation (Figure S17). These challenges reflect the complex regulatory landscape that organizations must navigate, balancing the need for robust cybersecurity measures with legal and compliance obligations.

The varied frequency of receiving threat intelligence information and the strong interest in sharing such information highlight the need for dynamic, real-time threat intelligence platforms. These platforms should enable organizations to share and receive updates in a timely manner, enhancing their ability to respond to emerging threats.

The willingness to share threat intelligence information, coupled with concerns about regulatory challenges, underscores the delicate balance between collaboration and compliance. Organizations are seeking ways to enhance cybersecurity collaboration without compromising on regulatory obligations, particularly in terms of data protection and privacy. The interest in privacy-preserving mechanisms for sharing incident data suggests also a demand for solutions that enable collaboration while protecting sensitive information. Technologies such as federated learning, secure multi-party computation, and blockchain could play a role in facilitating secure and compliant threat intelligence sharing. The anticipation of regulatory challenges indicates a need for continuous monitoring and adaptation to the evolving legal landscape. Organizations must stay informed about changes in cybersecurity legislation and data protection laws to ensure their practices remain compliant.

5.6. Investment Factors and Adoption Barriers

The emphasis on the need for enhanced security as the primary factor influencing investment decisions underscores the critical importance organizations place on protecting their digital assets and information. This aligns with the growing recognition of cybersecurity as a fundamental component of business operations in the digital age. The primary factors influencing the decision to invest in cybersecurity technologies include the need for enhanced security (20 out of 35 respondents), regulatory compliance (7 out of 35), and cost-effectiveness (5 out of 35) (Figure S19). This indicates that while security enhancement remains the top priority, compliance with regulations and the financial aspect of cybersecurity solutions also play significant roles in investment decisions.

The significance of regulatory compliance and cost-effectiveness as factors influencing investment decisions reflects the complex environment in which organizations operate. Balancing the need to comply with legal requirements and manage costs effectively while ensuring robust cybersecurity poses a challenge for many organizations.

The concern over integration complexities with existing systems as a major barrier to adoption points to the technical challenges organizations face in implementing new cybersecurity solutions. The potential barriers or challenges anticipated by respondents in the adoption of cybersecurity projects include integration complexities with existing systems (19 out of 35), lack of stakeholder buy-in (8 out of 35), regulatory hurdles (3 out of 35), and resource constraints (5 out of 35) (Figure S20). These results highlight the multifaceted nature of challenges organizations anticipate, with technical, organizational, legal, and financial aspects all playing a part. Ensuring compatibility and minimizing disruption to existing operations are key considerations that need to be addressed.

The lack of stakeholder buy-in and resource constraints highlight organizational and financial challenges in adopting cybersecurity projects. Gaining support from key stakeholders and allocating sufficient resources are crucial steps in overcoming these barriers. Anticipated regulatory hurdles suggest that organizations are aware of the evolving legal landscape surrounding cybersecurity. Staying informed and adaptable to regulatory changes is essential for successful implementation and compliance.

5.7. Collaboration and Infrastructure Protection

Collaboration among different digital infrastructures and systems for incident detection and response at national and European levels is considered important (13 out of 35) or very important (11 out of 35) by most respondents (Figure S22). This shows that a majority of respondents (34 out of 35) consider collaboration among different digital infrastructures and systems to be important or very important for incident detection and response procedures. This highlights the need for increased cooperation and information sharing between organizations and sectors to effectively address cybersecurity threats. The majority of organizations agree (18 out of 35) or strongly agree (7 out of 35) that they employ effective tools and methods for protecting critical infrastructure from cybersecurity issues. However, there is still room for improvement, as seven respondents are neutral, and three disagree with the statement (Figure S23).

5.8. Intrusion Detection Systems (IDSs)

Most organizations (26 out of 35) agree or strongly agree that they currently leverage an intrusion detection system (IDS) (Figure S24). The questionnaire results show that a network-level IDS is considered a robust first line of defense by most respondents, with 25 finding it useful but preferably coupled with other measures (Figure S25). The performance of IDSs in terms of analyzing traffic and detecting intrusions is rated as extremely important by 16 respondents, highlighting the critical role of timely and effective intrusion detection (Figure S26). The widespread adoption of IDSs among respondents highlights their critical role in cybersecurity strategies. However, the effectiveness of IDSs can be further enhanced through integration with other cybersecurity tools and technologies, including those powered by artificial intelligence (AI) for improved detection capabilities by providing more accurate and faster detection of complex threats.

While there is confidence in the current cybersecurity measures, the dynamic nature of cyber threats necessitates ongoing improvements and innovations in cybersecurity tools and collaboration mechanisms. This includes leveraging advanced technologies such as AI and machine learning for predictive analytics and automated incident response, as well as developing more effective platforms for privacy-aware information and knowledge sharing among stakeholders.

5.9. AI in Cybersecurity

The analysis of the AI in cybersecurity aspects from the Stakeholders' Analysis Questionnaire reveals a strong consensus among stakeholders on the potential benefits of AI for enhancing cybersecurity measures, particularly in the area of intrusion detection systems (IDSs). The answers from the questionnaire indicate that stakeholders have a high level of agreement on the value of AI in the intrusion detection process. A total of 18 respondents strongly agree, and 13 agree that AI-powered algorithms could benefit the intrusion detection process, for example, by dynamically identifying new attack patterns (Figure S27). This suggests a widespread belief in the efficacy of AI in adapting to and recognizing evolving cyber threats, which is crucial given the rapidly changing nature of cyber-attacks.

The responses to the questionnaire also highlight the importance of real-time threat intelligence sharing. A dynamic, real-time, and privacy-aware mechanism for sharing threat intelligence information among trusted and authorized entities is seen as significantly beneficial for improving collaborative incident detection and response capabilities, with 10 respondents strongly agreeing and 17 agreeing with this statement (Figure S49). The development of privacy-aware information and knowledge sharing (PIKS) tools is also supported, with 9 respondents strongly agreeing and 17 agreeing that such tools would enhance overall cybersecurity situational awareness and decision-making (Figure S50).

The use of decentralized approaches, such as swarm learning and federated learning, for sharing AI models between different entities without sharing private data, is considered a viable and privacy-aware method for collaborative information and knowledge sharing. This is reflected in the responses, with 7 strongly agreeing and 17 agreeing with the viability of such approaches (Figure S51). This indicates a growing interest in methods that can leverage the benefits of AI while maintaining privacy and data protection.

5.10. Elicitation of Functional and Non-Functional Requirements

Applying the methodology of Section 4 to the Stakeholders' Analysis Questionnaire, one might derive functional requirements such as the need for a centralized incident information system (as indicated by 24 respondents employing such a solution) and non-functional requirements like ensuring the system supports real-time visibility into network operations (highlighted as a challenge by 4 respondents). This systematic approach ensures that the development of cybersecurity solutions is closely aligned with the actual needs and challenges faced by stakeholders across critical information infrastructures.

To effectively link the functional and non-functional requirements derived from the Stakeholders' Analysis Questionnaire, it is essential to map specific questions from the questionnaire to the identified requirements. This mapping ensures that each requirement is directly supported by data gathered from the stakeholders, providing a clear rationale for why these requirements are necessary and how they address the stakeholders' needs and challenges.

Functional Requirements (FRs)

- AI-Empowered Security Tools (FR1)
  Question: "Do you believe AI-powered algorithms could benefit the intrusion detec-

tion process?”
Rationale: A positive response indicates a need for advanced AI capabilities in security tools to enhance detection and response processes.

- Interactive VR-Based Interface (FR2)
  Question: “Would an interactive VR-based interface for situational awareness significantly enhance your cybersecurity operations?”
  Rationale: Affirmative responses suggest a demand for more immersive and interactive tools for managing cybersecurity data and incidents.
- Privacy-Aware Information Sharing (FR3)
  Question: “Is there a willingness to share incident data and findings in a privacy-preserving manner?”
  Rationale: High agreement on this question underscores the need for mechanisms that allow secure and private sharing of threat intelligence.
- Dynamic and Adaptive Incident Response (DAIR) (FR4)
  Question: “How important is the adaptability of incident response tools in handling dynamic cyber threats?”
  Rationale: Responses indicating high importance highlight the necessity for responsive and flexible incident response solutions.
- Intrusion Detection and Prediction (IDP) (FR5)
  Question: “Rate the effectiveness of your current intrusion detection systems.”
  Rationale: Mixed or negative responses indicate a gap that could be filled by improved intrusion detection and prediction tools.
- Automated Penetration Testing (FR6)
  Question: “Do you currently use automated tools for regular penetration testing?”
  Rationale: Negative responses or expressions of a need for such tools justify the development of automated penetration testing capabilities.

Non-Functional Requirements (NFR)

- Usability (NFR1)
  Question: “How user-friendly do you find your current cybersecurity tools?”
  Rationale: Feedback on usability issues supports the requirement for user-friendly design in new tools.
- Scalability (NFR2)
  Question: “Can your current cybersecurity solutions scale with your organization’s growth?”
  Rationale: Responses indicating scalability issues point to the need for highly scalable cybersecurity solutions.
- Interoperability (NFR3)
  Question: “Do your cybersecurity tools effectively integrate with other systems?”
  Rationale: Problems with integration highlight the importance of interoperability in new cybersecurity solutions.
- Compliance (NFR4)
  Question: “How challenging is it to maintain compliance with regulations using your current tools?”
  Rationale: Challenges in maintaining compliance stress the need for tools designed to ease regulatory compliance.
- Performance (NFR5)
  Question: “Are you satisfied with the performance (speed, efficiency) of your current cybersecurity tools?”
  Rationale: Dissatisfaction with current tool performance underscores the requirement for high-performance solutions.
- Security and Privacy (NFR6)
  Question: “Do your tools adequately protect data privacy and security?”
  Rationale: Concerns about data protection validate the need for robust security and privacy features.

- Reliability (NFR7)
  Question: "How often do your cybersecurity tools fail or produce errors?"
  Rationale: Frequent failures or errors indicate a critical need for reliable cybersecurity solutions.

This detailed mapping ensures that each functional and non-functional requirement is directly linked to specific stakeholder feedback, providing a solid foundation for the development and implementation of the CyberSecDome project [7].

6. Discussion

6.1. Challenges and Pitfalls

The Stakeholders' Analysis Questionnaire reveals several challenges and pitfalls encountered during the stakeholder analysis process:

1. Diverse Organizational Profiles: The respondents come from a variety of sectors, including cybersecurity, technology system providers, and other stakeholders. This diversity can make it challenging to identify and prioritize needs across different types of organizations.
2. Variation in Organizational Size: The size of the organizations varies significantly, from micro to very large. This variation implies that the capacity for cybersecurity and incident management can differ greatly, which can complicate the analysis of common needs and solutions.
3. Different Levels of Expertise: Respondents have various areas of expertise, which may influence their perception of cybersecurity needs and the effectiveness of incident management practices. This can lead to a wide range of opinions and requirements that need to be reconciled.
4. Incident Management Tools: A significant number of organizations do not use tools to support incident management processes, which suggests a potential gap in the adoption of such tools or a lack of awareness of their benefits.
5. Challenges in Detection and Response: Respondents identified limited threat intelligence sharing and insufficient automation in incident response as major challenges, indicating a need for improved collaboration and technology support.
6. Regulatory Challenges: Compliance with data protection laws and evolving cybersecurity legislation are anticipated as key regulatory challenges, which can affect the stakeholder analysis process by introducing legal constraints and uncertainties.
7. Integration Complexities: The potential barriers to adopting the project include integration complexities with existing systems, which can be a significant pitfall if not addressed properly.
8. Collaboration Importance: While collaboration among different digital infrastructures is considered very important, achieving this in practice can be difficult due to varying levels of security maturity and the need for interoperable solutions.
9. Skilled Personnel: The availability of skilled and trained personnel on security and incident handling practices varies, which can impact the effectiveness of incident detection and response.
10. Stakeholder Buy-In: A lack of stakeholder buy-in is identified as a barrier, which can be a pitfall if stakeholders are not adequately engaged or convinced of the benefits of the cybersecurity measures proposed.

6.2. Added Value of Addressing Challenges and Pitfalls

The Stakeholders' Analysis Questionnaire provides a comprehensive overview of the current state of cybersecurity practices, challenges, and stakeholder perceptions across various sectors. The importance of addressing the challenges and pitfalls identified in the stakeholder analysis (Section 6.1) is crucial for enhancing the effectiveness and relevance of cybersecurity solutions. These challenges and pitfalls provide a realistic view of the obstacles and difficulties that stakeholders face, which must be considered to develop practical and effective cybersecurity measures. Addressing these challenges and pitfalls adds significant value in several ways:

1. Enhanced Solution Relevance: By understanding and addressing the specific challenges faced by stakeholders, the cybersecurity solutions developed are more likely to meet the actual needs and conditions of these stakeholders, thereby increasing the relevance and utility of these solutions.
2. Increased Adoption and Effectiveness: Solutions that effectively address real-world challenges are more likely to be adopted by stakeholders. This increased adoption enhances the overall effectiveness of cybersecurity measures, leading to better protection and resilience against cyber threats.
3. Innovation and Improvement: Identifying and overcoming challenges can drive innovation in cybersecurity technologies and strategies. This continuous improvement cycle can lead to the development of more advanced and effective cybersecurity solutions.
4. Stakeholder Confidence and Trust: Successfully addressing challenges and demonstrating an understanding of stakeholder needs can build trust and confidence among stakeholders. This is crucial for fostering collaborative relationships and ensuring widespread support for cybersecurity initiatives.

The critical analysis and leveraging of findings from the stakeholder analysis study contribute substantially to the cybersecurity body of knowledge in several ways:

1. Guidance for Future Research: Insights from the analysis can guide future research directions, focusing on areas that are most relevant and impactful for stakeholders. This ensures that research efforts are aligned with the evolving needs of the cybersecurity landscape.
2. Basis for Educational and Training Programs: Understanding the challenges and requirements of stakeholders can inform the development of targeted educational and training programs that address specific skills gaps and knowledge needs.
3. Policy and Regulatory Development: The findings can inform policymakers and regulators, helping them to develop more effective cybersecurity policies and regulations that reflect the needs and challenges of diverse stakeholders.
4. Enhanced Collaboration: This study's findings can facilitate better collaboration between academia, industry, and government by highlighting common goals and challenges, thereby fostering a more coordinated approach to cybersecurity.

6.3. Data Quality Concerns

The effectiveness of the proposed AI-enhanced framework heavily relies on the quality and availability of data regarding stakeholders' cybersecurity challenges and requirements. Inaccurate or incomplete data may lead to biased insights and compromised effectiveness of the framework. To mitigate these risks, the design and development of the AI-enhanced framework in CyberSecDome [7] should incorporate specific strategies to ensure data quality, such as the following:

1. Implementing robust data governance policies and establishing a dedicated data quality team to oversee data validation, cleansing, and monitoring processes [20].
2. Utilizing data quality tools that automate the cleansing, validation, and monitoring processes, ensuring that AI models have access to high-quality data consistently.
3. Collaborating closely with stakeholders/data providers to ensure the collection of high-quality inputs and continuously measuring and monitoring data quality metrics to identify and address potential issues before they impact AI performance.

6.4. Privacy Concerns with AI for Stakeholder Analysis

Incorporating AI for stakeholder analysis could potentially trigger privacy worries among stakeholders. It is crucial to prioritize data privacy and adhere to regulations to uphold trust and engagement. This paper should emphasize incorporating privacy-preserving approaches into the AI-enhanced framework, such as the following:

1. Adopting privacy-by-design principles by integrating privacy considerations into the design phase of AI systems and conducting privacy impact assessments to identify and mitigate risks early on [21,22].
2. Using techniques like anonymization, pseudonymization, and encryption for data to protect personal data alongside strong encryption for data at rest and in transit, enhancing data privacy [23].
3. Implementing clear data governance policies and access controls to manage the lifecycle of the data used in AI systems and secure personal data against unauthorized access and breaches [24].
4. Being transparent about data practices and ensuring AI decisions are explainable and understandable to users, fostering trust and accountability [25].
5. Conducting regular privacy assessments and audits to demonstrate compliance with data privacy laws and policies, and being prepared to demonstrate accountability and adherence to privacy standards [24–26].

7. Conclusions

In conclusion, the Stakeholders' Analysis Questionnaire has provided a valuable and comprehensive perspective on the current state of cybersecurity across various critical information infrastructures. The responses have highlighted the importance of robust incident management, the challenges of threat intelligence sharing and automation, and the potential of AI to enhance cybersecurity practices.

Organizations of various sizes and sectors have expressed a moderate level of satisfaction with their current cybersecurity measures, with an average rating of 3.54 out of 5 for the quality of their incident investigation, response, and analysis capabilities. However, the data also indicate a clear recognition of the need for improvement, particularly in the areas of threat intelligence sharing and the automation of incident response processes.

The strong agreement on the potential benefits of AI in cybersecurity, with 18 respondents strongly agreeing and 13 agreeing, suggests a readiness to embrace AI-powered solutions to address the dynamic nature of cyber threats. Moreover, the emphasis on the importance of collaboration among different digital infrastructures for incident detection and response at national and European levels underscores the collective effort required to enhance cyber resilience.

The questionnaire has successfully captured the diverse and complex landscape of cybersecurity needs and challenges, providing insights that can inform the development of more effective cybersecurity strategies and tools. As we move forward, it is imperative to leverage these insights to foster a more secure and resilient digital environment, where collaboration, advanced technology, and proactive measures work in tandem to protect against ever-evolving cyber threats.

The findings from this questionnaire serve as a foundation for future research and development in the field of cybersecurity. They emphasize the need for a multi-faceted approach that combines technological innovation with strategic collaboration and regulatory compliance to effectively safeguard our critical information infrastructures.

Supplementary Materials: The following are available online at https://www.mdpi.com/article/10.3390/businesses4020015/s1.

Author Contributions: Conceptualization, P.K.; methodology, P.K.; formal analysis, P.K.; investigation, P.K.; resources, S.P.; writing—original draft preparation, P.K.; writing—review and editing, P.K.; funding acquisition, S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Informed Consent Statement: Not Applicable.

Data Availability Statement: The questionnaire is available at this link: https://forms.office.com/e/7ykL8xq4Bp (accessed on 11 June 2024).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]
2. Report on the Cybersecurity and Resiliency of the EU Communications Infrastructures and Networks | Shaping Europe's Digital Future. Available online: https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks (accessed on 26 May 2024).
3. Sowmya, T.; Mary Anita, E.A. A comprehensive review of AI based intrusion detection system. *Meas. Sens.* **2023**, *28*, 100827. [CrossRef]
4. Fischer-Hübner, S.; Alcaraz, C.; Ferreira, A.; Fernandez-Gago, C.; Lopez, J.; Markatos, E.; Islami, L.; Akil, M. Stakeholder perspectives and requirements on cybersecurity in Europe. *J. Inf. Secur. Appl.* **2021**, *61*, 102916. [CrossRef]
5. Tripathi, N.; Hietala, H.; Xu, Y.; Liyanage, R. Stakeholders collaborations, challenges and emerging concepts in digital twin ecosystems. *Inf. Softw. Technol.* **2024**, *169*, 107424. [CrossRef]
6. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]
7. CyberSecDome. CyberSecDome. Available online: https://cybersecdome.eu/ (accessed on 26 May 2024).
8. Abbu, H.; Mugge, P.; Gudergan, G. Ethical Considerations of Artificial Intelligence: Ensuring Fairness, Transparency, and Explainability. In Proceedings of the 2022 IEEE 28th International Conference on Engineering, Technology and Innovation (ICE/ITMC) & 31st International Association For Management of Technology (IAMOT) Joint Conference, Nancy, France, 19–23 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7. [CrossRef]
9. del Moral, J.O.; deMarti iOlius, A.; Vidal, G.; Crespo, P.M.; Martinez, J.E. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. *arXiv* **2024**, arXiv:2401.03780. [CrossRef]
10. Maglaras, L.; Janicke, H.; Ferrag, M.A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors* **2022**, *22*, 5105. [CrossRef] [PubMed]
11. Impact of COVID-19 on Cybersecurity. Deloitte Switzerland. Available online: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed on 26 May 2024).
12. Implementing Regulation on the Adoption of a European Common Criteria-Based Cybersecurity Certification Scheme | Shaping Europe's Digital Future. Available online: https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme (accessed on 26 May 2024).
13. Pickren, R. *Compromising Industrial Processes using Web-Based Programmable Logic Controller Malware [Artifacts]*; Zenodo: Geneva, Switzerland, 2023. [CrossRef]
14. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 100361. [CrossRef]
15. Camacho, N.G. The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *J. Artif. Intell. Gen. Sci.* **2024**, *3*, 143–154. [CrossRef]
16. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
17. Ani, U.D.; Watson, J.D.M.; Nurse, J.R.C.; Cook, A.; Maple, C. A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. In Proceedings of the Living in the Internet of Things (IoT 2019), London, UK, 1–2 May 2019; pp. 1–15. [CrossRef]
18. Stakeholders' Analysis Questionnaire. Available online: https://forms.office.com/pages/responsepage.aspx?id=XN7JqDm_90mhxmSilxjmqzufS96BADhKmtVBXpFzl0pUMlpJVlhWREdXMlIzSFdOMDBGS0tHUDk1MyQlQCN0PWcu (accessed on 11 June 2024).
19. Admin. Webinar: 'Cybersecurity Matters' by CyberSecDome & Custodes EU Projects. *CyberSecDome*. Available online: https://cybersecdome.eu/2024/02/19/webinar-cybersecurity-matters/ (accessed on 11 June 2024).
20. Apps, S.C. Data Governance: Definition, Framework, Best Practices. Spanning. Available online: https://spanning.com/blog/data-governance/ (accessed on 3 June 2024).
21. Privacy in the New World of AI. *The Promise*. 2023. Available online: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/09/privacy-in-the-world-of-ai-report-final-web.pdf (accessed on 11 June 2024).
22. Georgiadis, G.; Poels, G. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Comput. Law Secur. Rev.* **2022**, *44*, 105640. [CrossRef]
23. Wu, C. Data privacy: From transparency to fairness. *Technol. Soc.* **2024**, *76*, 102457. [CrossRef]
24. Implementing Data Governance Policies for Regulatory Compliance. Intone Networks. Available online: https://intone.com/implementing-data-governance-policies-for-regulatory-compliance/ (accessed on 3 June 2024).

25. Balasubramaniam, N.; Kauppinen, M.; Rannisto, A.; Hiekkanen, K.; Kujala, S. Transparency and explainability of AI systems: From ethical guidelines to requirements. *Inf. Softw. Technol.* **2023**, *159*, 107197. [CrossRef]
26. Chatsuwan, P.; Phromma, T.; Surasvadi, N.; Thajchayapong, S. Personal data protection compliance assessment: A privacy policy scoring approach and empirical evidence from Thailand's SMEs. *Heliyon* **2023**, *9*, e20648. [CrossRef] [PubMed]

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