Journal of
Cybersecurity and Privacy

MDPI

Article

An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure

Habib El Amin [1,2,3,*], Abed Ellatif Samhat [2], Maroun Chamoun [1], Lina Oueidat [2] and Antoine Feghali [3]

[1] CIMTI, Faculty of Engineering, University of Saint Joseph, Beirut 1104, Lebanon; maroun.chamoun@usj.edu.lb
[2] Centre de Recherche Scientifique en Ingénierie (CRSI), Faculty of Engineering, Lebanese University, Hadath 1533, Lebanon; samhat@ul.edu.lb (A.E.S.); lina.oueidat@ul.edu.lb (L.O.)
[3] Potech Labs, P.O.TECH, Beirut 1107, Lebanon; tony@potech.global
* Correspondence: habib.amine@net.usj.edu.lb

Abstract: Emerging cyber threats' sophistication, impact, and complexity rapidly evolve, confronting organizations with demanding challenges. This severe escalation requires a deeper understanding of adversary dynamics to develop enhanced defensive strategies and capabilities. Cyber threat actors' advanced techniques necessitate a proactive approach to managing organizations' risks and safeguarding cyberspace. Cyber risk management is one of the most efficient measures to anticipate cyber threats. However, it often relies on organizations' contexts and overlooks adversaries, their motives, capabilities, and tactics. A new cyber risk management framework incorporating emergent information about the dynamic threat landscape is needed to overcome these limitations and bridge the knowledge gap between adversaries and security practitioners. Such information is the product of a cyber threat intelligence process that proactively delivers knowledge about cyber threats to inform decision-making and strengthen defenses. In this paper, we overview risk management and threat intelligence frameworks. Then, we highlight the necessity of integrating cyber threat intelligence and assessment in cyber risk management. After that, we propose a novel risk management framework with integrated threat intelligence on top of EBIOS Risk Manager. Finally, we apply the proposed framework in the scope of a national telecommunications organization.

Keywords: cybersecurity; cyber risk management; cyber threat intelligence; critical infrastructure

check for updates

Citation: El Amin, H.; Samhat, A.E.; Chamoun, M.; Oueidat, L.; Feghali, A. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. *J. Cybersecur. Priv.* **2024**, *4*, 357–381. https://doi.org/10.3390/jcp4020018

Academic Editor: Giorgio Giacinto

Received: 28 April 2024
Revised: 2 June 2024
Accepted: 6 June 2024
Published: 9 June 2024

1. Introduction

With digital transformations, interconnectivity, and intelligent systems, digital breaches have become more severe and widespread. Incompetent cybersecurity is proven to cause increasing losses [1] and can range from relatively minor to catastrophic financial damages, highlighting the critical need for robust cyber risk management [2]. Organizations employ cyber risk management frameworks to identify, assess, treat, and monitor their digital risks. Despite substantial investments in cyber readiness, many organizations lack proper situational awareness of the threat landscape and their adversaries [3]. The shift of critical infrastructures towards automation and digital connectivity has increased their vulnerability to diverse external threats such as state-sponsored groups, organized crime, and activists [4]. These adversaries continuously refine their strategies, outpacing the organizational cyber defenses. Despite the significant projected growth in the risk management market to address the rising frequency and complexity of cyberattacks [5], organizations still face escalating challenges. These challenges push cybersecurity spending beyond budgeted amounts due to penalties, revenue losses, and other costs stemming from security breaches [6].

Risk management often accounts only for the internal context, without consideration for threat actors [7]. Therefore, it has become necessary to analyze adversaries continuously during risk management. Threat assessment is already a pillar in existing cyber risk management frameworks, such as EBIOS Risk Manager. However, it still does not include information about cyber threats. A more complete approach is required by integrating the cyber threat intelligence process output into the cyber risk management process, allowing more precise risk assessments and timely adaptations. Threat intelligence provides valuable information about threat actors that can be utilized to adapt risk assessment strategies and prioritization [8,9].

Given the dynamic nature of cyberattacks and the inherent unpredictability of their associated risks, organizations are compelled to rely on threat intelligence as a strategic approach for responding to highly unpredictable and elusive cyber threats [10]. While cyber threat intelligence has been a necessary process supporting organizations in responding to cyberattacks, it is still a novel practice. It requires better exploitation in other security practices, especially cyber risk management. It provides essential information for risk managers [11], allowing them to consider their organizations' context and adversaries, thereby breaking the knowledge imbalance between attackers and defenders, leading to better risk assessments and mitigation prioritization.

Cyber threat intelligence provides knowledge about threat actors, their corresponding objectives, and their means to reach these objectives. Strategic, operational, tactical, and technical threat information can be utilized to identify, evaluate, and respond to risks. Enhancing the efficiency of cyber risk management is one of the main objectives of a cyber threat intelligence program [12]. However, integrating cyber threat intelligence into practical organizational practices remains uncommon [10,13].

Cyber risk assessment can produce overwhelming security weaknesses and corresponding remediations for an organization to implement, making the remediation plan overwhelming. Considering adversaries' techniques and tactics can improve the risk assessment output regarding results, prioritization of security controls, and proactive response to emerging threats [14].

This paper's novelty and contribution lie in its proposal for enhancements through the continuous integration of cyber threat intelligence into an existing cyber risk management framework. We consider EBIOS Risk Manager as the baseline risk management framework and propose new modifications to its process. Then, we apply the designed framework to critical national infrastructure.

The remainder of this paper is structured as follows. Section 2 overviews relevant work in cyber risk management and cyber threat intelligence to highlight the gap addressed by our contribution. Section 3 presents the proposed risk management framework with integrated cyber threat intelligence. Next, Section 4 lays out an application of the proposed framework. Finally, Section 5 concludes the paper.

2. Background and Related Works

This section provides an overview of the established cyber risk management frameworks, cyber threat intelligence frameworks, and the integration of cyber threat intelligence into cyber risk management.

2.1. Cyber Risk Management

Risk management is a critical process that seeks to identify, evaluate, and control risks that threaten an organization's business objectives. In the realm of cybersecurity, risk management focuses on risks affecting digital information, including the availability, confidentiality, and integrity of systems.

Numerous frameworks for cyber risk management have been developed in the literature and industry. Comprehensive reviews, analogies, and comparisons of these established frameworks can be found in [15–17].

Various frameworks, guidelines, and tools have been created in the cybersecurity industry to manage cyber risks effectively. Notable examples include ISO 27005 [18], a standard framework published by the International Organization for Standardization and the International Electrotechnical Commission. The US government has designed NIST Special Publication 800-30 [19] as a detailed risk management process for governmental organizations. OCTAVE [20] offers a flexible risk-based strategic assessment and mitigation planning framework, while EBIOS [21] is a workshop-based framework developed by the French National Agency for Cybersecurity (ANSSI) based on the ISO 27005 guidelines. MONARC [22] is a method that assists organizations in identifying and evaluating potential information security risks and implementing appropriate risk management measures, emphasizing a structured approach to risk assessment, asset identification, threat analysis, and vulnerability assessment. BSI200-2 [23] is a risk management standard developed by the German Federal Office for Information Security, offering a systematic approach to identifying, assessing, and managing information security risks. The European Union has introduced ITSRM [24], a risk management method for evaluating and certifying information technology products and systems. ISACA, a global professional association for information technology governance, has developed ITRAM2 [25] to help organizations identify, evaluate, and manage technology-related risks, focusing on integrating risk management processes.

In addition to industry-established frameworks, the cybersecurity research literature has proposed novel frameworks, processes, and tools for effectively managing cyber risks in emerging technologies. Examples include ADAMANT [26], an information security management system compliant with ISO standards; LISRA [27], a risk assessment framework simplifying the construction of attack scenarios in specific domains; and CSCCRA [28], a risk assessment methodology designed for evaluating risks in dynamic cloud environments with multiple service providers. Some research contributions, like [29], have even suggested integrating the safety of cyber–physical devices into existing risk management frameworks based on ISO standards. Others, such as [30], have proposed layered cyber risk management frameworks tailored to the unique challenges of the Internet of Things. Moreover, innovative approaches like the blockchain-based risk and information system control framework introduced in [31,32] leverage decentralized blockchain technology to ensure risk management security.

EBIOS Risk Manager is among the more recent industry-based risk management frameworks that account for threat actors by addressing them as risk origins (ROs). EBIOS has evolved through multiple iterations, culminating in the EBIOS Risk Manager. This workshop-based approach strongly emphasizes collaboration among stakeholders within the same organization. It establishes security baselines and objectives, starting with risk sources and considering the ecosystem and adversaries. EBIOS Risk Manager employs a top-down approach and prioritizes efficiency over exhaustiveness. The EBIOS Risk Manager process consists of five workshops involving individuals from the assessed organization performing risk assessment and management. These workshops are [21]:

i Scope and Security Baseline: The first workshop in the framework defines the study's scope, participants, and timeframe and identifies missions, business assets, and supporting assets while assessing feared events and their impact severity. It also establishes the security baseline and differential as the foundation for subsequent risk assessment and management activities. This workshop involves the top management, the business teams, the security manager, and the IT teams.

ii Risk Origins: The second workshop focuses on identifying and characterizing Risk Origins (ROs) and their associated high-level target objectives (TOs). The most relevant RO/TO pairs are selected, and the outcomes are documented in a risk origins mapping, providing a structured understanding of the risks. Thus, this workshop can be an entry point for benefiting from threat intelligence information about threat actors. This workshop involves top management, business teams, the security manager, and, optionally, a specialist in digital threats.

iii Strategic Scenarios: The third workshop aims to provide a comprehensive view of the ecosystem and map the digital threats relative to the studied object. This information is used to develop high-level strategic scenarios, which outline potential attack paths from risk origins to their targets. These scenarios determine the severity of the risk scenarios, and by the end of the workshop, security measures for the ecosystem can be defined, contributing to improved risk management. This workshop involves the business teams, functional architects, the security manager, and a cybersecurity specialist optionally.

iv Operational Scenarios: In the fourth workshop, an approach similar to the preceding one is adopted, but the focus shifts to critical supporting assets, where technical scenarios are constructed to outline the methods of attack expected to be used by the risk origins in executing the strategic scenarios. Subsequently, the level of likelihood of each operational scenario derived from this workshop is assessed, determining the likelihood of the overall risk scenario. This workshop involves the IT teams, the security manager, and, optionally, a security specialist.

v Risk Treatment: In the last workshop, the culmination of all studied risks is summarized to formulate a comprehensive risk treatment strategy. This strategy is further delineated into security measures integrated into a continuous improvement plan. Additionally, this workshop entails the development of a summary of residual risks and establishing a risk monitoring framework. This workshop involves the top management, the business teams, the security manager, and the IT teams.

Figure 1 presents the five workshops of EBIOS Risk Manager.

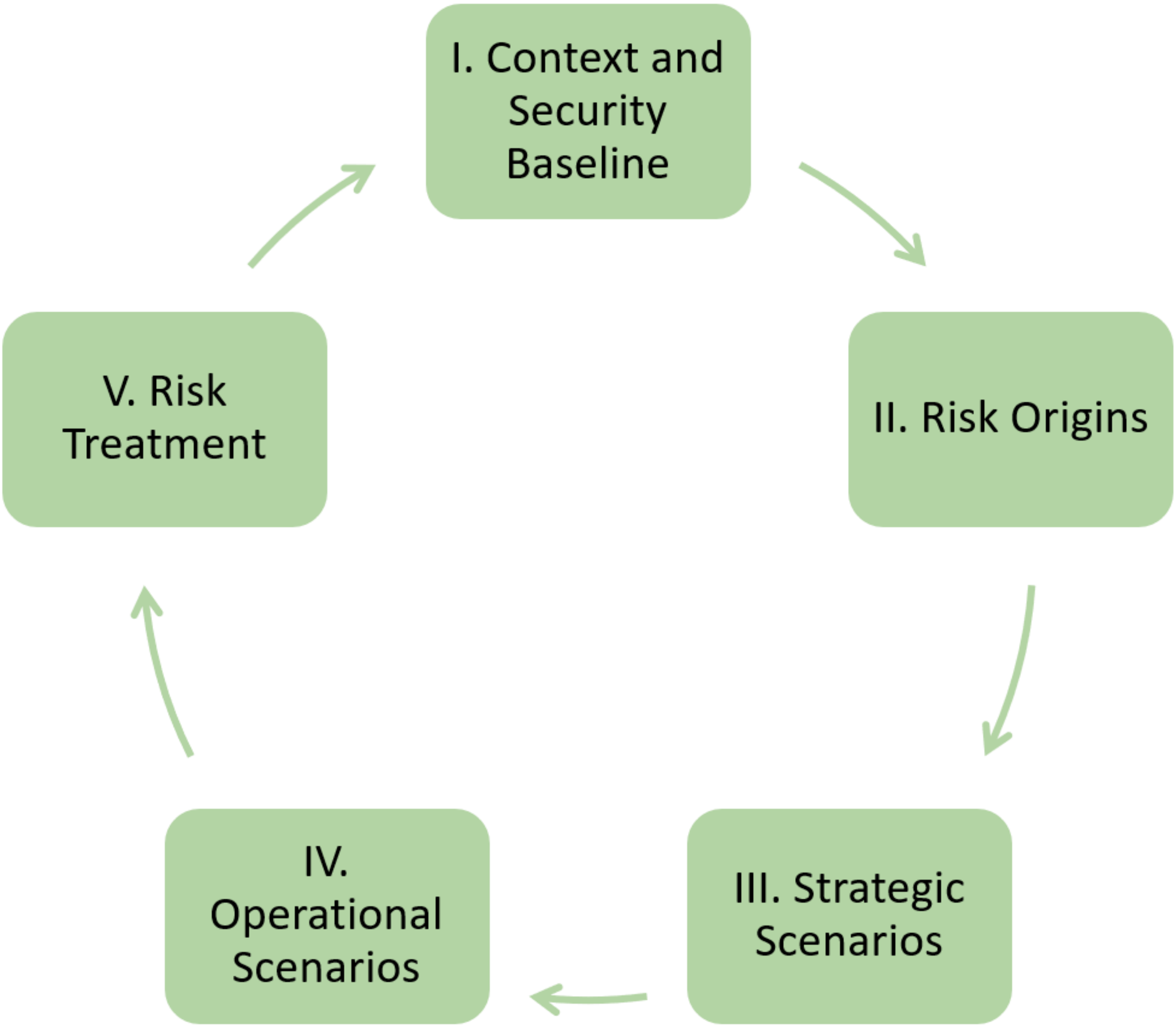

Figure 1. EBIOS Risk Manager workshops [21].

2.2. Cyber Threat Intelligence

Cyber threats have become a significant, enduring threat to nations. Targeted cyberattacks disrupt critical services, causing severe complications on many levels. Breach investigations prove that victims have been compromised long before initial attack detection [1]. Cyber threat intelligence provides the necessary knowledge and means to protect, detect, and respond to cyber threats. It provides the means to change organizations' cybersecurity behavior from reactive to proactive [33]. It strives to balance the knowledge asymmetry between attackers and defenders by gathering and analyzing information about cyber adversaries.

Multiple models and platforms are emerging to produce and disseminate cyber threat intelligence information. The cyber Kill Chain [34] is established to identify and model adversaries' cyberattacks. The Diamond model [35] is an intrusion analysis approach used by information security experts to track cyber threats in each attack attempt. It underlines four components: adversary, capability, infrastructure, and victim. The Pyramid of Pain [36] classifies the types of indicators to identify threat actors. This model emphasizes focusing on threat characteristics that are difficult to modify to detect cyberattacks. The MITRE ATT&CK framework [37] is a matrix of tactics, techniques, procedures, and sub-procedures used to model adversaries' behavior, classify attacks, and assess risks. STIX [38] is a standard language for expressing cyber threat intelligence data and their corresponding observables. TAXII [39] is a standard that defines the format to share threat-related information via services and message exchanges. OpenCTI [40] is an open-source threat intelligence platform that manages threat intelligence data, gathers real-time threat intelligence information, and exchanges intelligence information between organizations. MISP [41] is an open-source platform for collecting, analyzing, and exchanging cyber threat intelligence indicators. The main process phases of producing cyber threat intelligence information are [42]:

i Planning and direction: In this foundational phase, the definition of the overall objective of the threat intelligence process not only sets the stage for subsequent activities but also establishes a strategic framework essential for informed decision-making.

ii Collection: This data acquisition phase, characterized by the comprehensive gathering of raw data from diverse sources such as network traffic, system logs, clear and dark web forums, and more, exemplifies a diverse approach to intelligence gathering, vital for constructing a threat landscape.

iii Processing and exploitation: Within this transformative phase, the intricate conversion of raw data into actionable information represents a critical juncture, emphasizing the importance of data refinement to unlock its true potential in subsequent analytical endeavors.

iv Analysis and production: In this pivotal phase, information is analyzed to evolve into intelligence that might be of the following types:

    (a) Strategic: This high-level intelligence, focusing on threats and their motives within the organization's threat landscape, is for strategic decision-making, providing crucial insights for management executives and organizational board members.

    (b) Tactical: Offering granular insights into threat actors' tactics, techniques, and procedures, this intelligence category is an indispensable tool for architects and system administrators to enhance the organization's defenses against evolving attack vectors.

    (c) Operational: This intelligence category, revealing specific details about incoming attacks, motives, timings, and nature, empowers security managers and defenders with actionable information to proactively safeguard the organization's assets.

    (d) Technical: By encompassing indicators of compromise like IP addresses, file hashes, and domain names, this technical intelligence is for security operational center analysts and incident responders, facilitating rapid and precise responses to security incidents.

v Dissemination and integration: In this phase, characterized by the targeted delivery of information to its intended beneficiaries, effective dissemination mechanisms ensure that the intelligence generated is seamlessly integrated into organizational processes, promoting a cohesive and proactive cybersecurity posture.

vi Feedback: This iterative phase ensures continuous improvement, enhancing the adaptability and efficacy of the threat intelligence process through a dynamic feedback loop.

Figure 2 illustrates the cyber threat intelligence process.

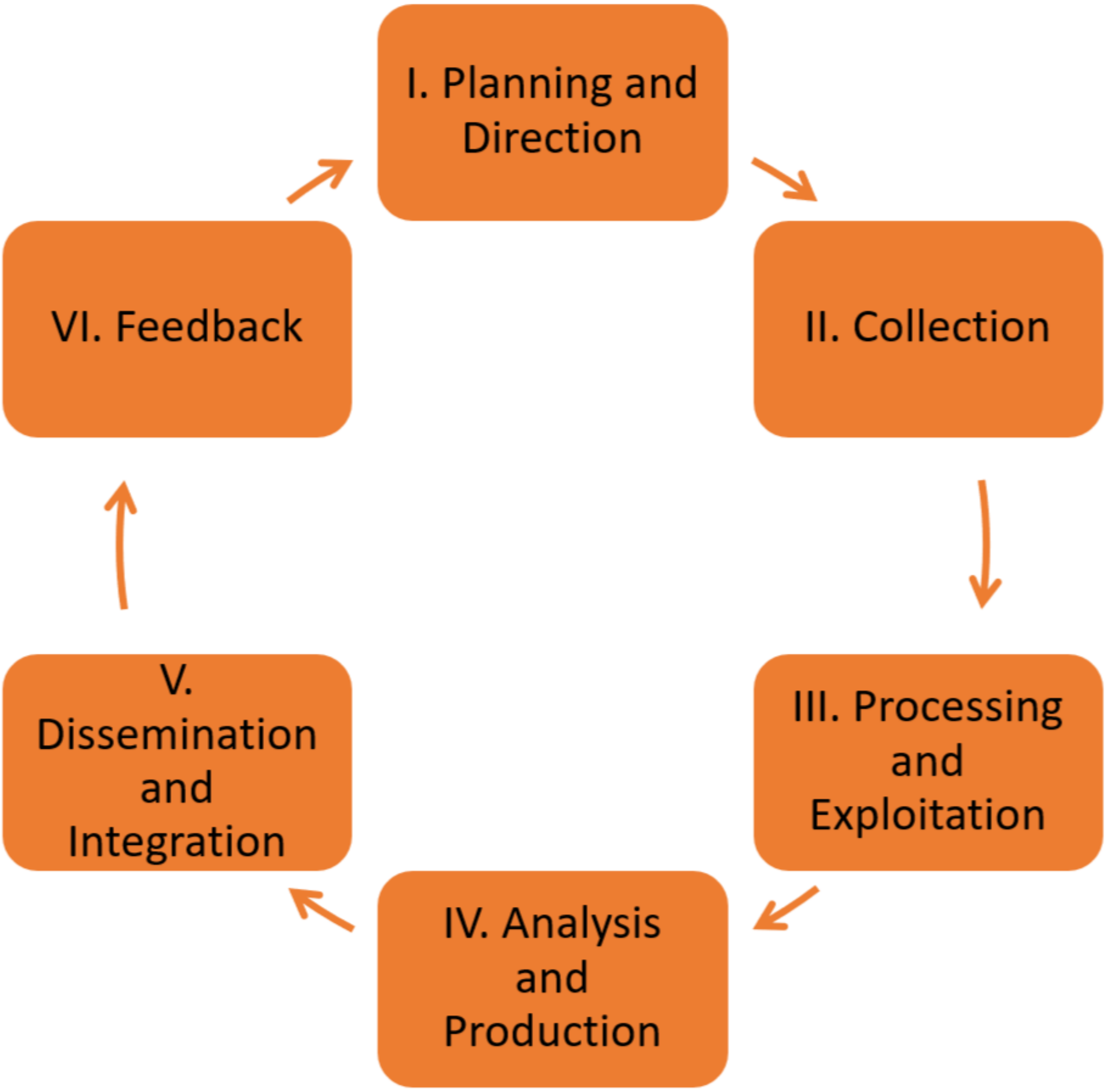
I. Planning and Direction
II. Collection
III. Processing and Exploitation
IV. Analysis and Production
V. Dissemination and Integration
VI. Feedback

Figure 2. Cyber threat intelligence process.

2.3. *Cyber Threat Intelligence and Cyber Risk Management Integration*

Multiple works have already proposed new cyber risk assessment models considering cyber threat assessment. EBIOS [21] defines cyber threat actors as risk origins and accounts for their strategic and operational attack paths based on the scope without concrete consideration for cyber threat intelligence information and its continuous flow. In [43], the authors proposed a hybrid model that integrates threat assessment in the risk assessment process to optimize the risk assessment results better. Their approach was motivated by closing the gap of the need for systematic threat assessment in the risk assessment process. They proposed a new hybrid risk assessment model with threat assessment placed after the vulnerability identification. Thus, the risk assessment results are driven by the identified weaknesses inside the assessed scope, not threats' motives and capabilities, and without support for cyber threat intelligence output. This process can be enhanced by driving the risk assessment by the threat characteristics and improving its results to match realistic scenarios. In [44], the authors extended the work of [43] by introducing MITRE ATT&CK [37] as an approach to build and assess attack scenarios. In [45], the authors propose another hybrid and dynamic risk analysis methodology for cyber–physical systems leveraging well-established sources for threat information for risk analysis with a proof of concept implementation. However, the described methodology does not account explicitly for cyber threat intelligence information and accounts only for vulnerabilities and threat correlation. In [46], a framework is proposed to utilize the MITRE ATT&CK knowledge base in the risk assessment to provide sufficient evidence during the development lifecycle. The framework describes workflows to create strategic, operational, and technical scenarios based on the EBIOS methodology, with explicit consideration for cyber threat intelligence and its continuous information feeds. In [47], the authors highlighted the need for more consideration of cyber threat intelligence in cyber risk management. Countering emerging cyber threats is becoming more challenging for current cyber risk management. A new unified model to assess cyber risks is proposed with cyber threat intelligence integration. However, the model presents a means to determine the necessary risk parameters without a straightforward, systematic process and continuous approach. In [48], the authors established a nationwide risk assessment framework based on vulnerability management and threat intelligence, focusing only on inventorying software and cross-matching with vulnerabilities. Finally, in [49], the authors proposed a novel threat intelligence-based security assessment method without explicitly focusing on risk management and offering a complete risk management framework. Table 1 presents the main differences between the relevant frameworks, considering cyber threat assessment and intelligence in terms of novelty, risk assessment, threat assessment, risk and threat monitoring, integration of cyber threat intelligence, type of cyber threat intelligence considered, and the ability to adjust the risks based on new threat intelligence.

While existing efforts have contributed significantly to integrating threat assessment into risk assessment, existing models often lack a systematic, continuous approach to incorporating cyber threat intelligence. Therefore, such a framework is still non-existent. To address this, our research proposes novel enhancements and modifications to a cyber risk management framework to integrate cyber threat intelligence. By considering EBIOS Risk Manager as our base process, we aim to bridge the knowledge gaps between attackers and defenders, leading to more informed and adaptable risk assessments and mitigation prioritization.

Table 1. Comparison between relevant frameworks integrating cyber threat intelligence with risk management.

Framework	Novelty	Risk Assessment	Threat Assessment	Risk and Threat Monitoring	Integration of Cyber Threat Intelligence	Type of Cyber Threat Intelligence	Capability to Adjust Based on Cyber Threat Information
EBIOS [21]	Workshop-based cyber risk assessment with strategic and operational risk scenarios	✓	✓	✗	✗	✗	✗
Hybrid Model for Risk Assessment [43,44]	Systematic integration of threat assessment in the cyber risk assessment	✓	✓	✗	✗	✗	✗
Hybrid Dynamic Risk Analysis [45]	Hybrid dynamic risk analysis to automatically assign new vulnerabilities to assets and evaluate the impact of successful exploitation for cyber–physical systems	✓	✓	✗	✗	Technical	✓
SAIF [46]	Integration of a risk-based analysis approach based on EBIOS with the MITRE knowledge base to automate the security impact analysis	✓	✓	✗	✓	Strategic, Operational, Technical	✗
Unified Approach [47]	Integrate threat intelligence in cyber risk management focusing on critical infrastructure	✓	✓	✗	✓	Operational and Technical	✗
Novel Approach to National-level Cyber Risk Assessment [48]	Evaluation of risk based on technical information with national vulnerability visibility	✓	✗	✗	✓	Technical	✓
TIBSA [49]	A cyber threat intelligence driven methodology providing practical guidance for information security leaders to make informed decisions in uncertain situations	✗	✓	✓	✓	✗	✓
Our proposed framework based on EBIOS	Integration of threat intelligence in cyber risk management with adaption based on new intelligence for critical infrastructure	✓	✓	✓	✓	Strategic, Tactical, Operational, and Technical	✓

3. Methodology and Process

The design science research process model (DSRP) [50] was followed. The research model includes problem identification and motivation, objective identification for the new framework, design, and development of the cyber threat intelligence integration in the risk management process, demonstration, and evaluation of the framework. The phases' details are presented below.

1. Problem identification and motivation: The existing literature and documentation of cybersecurity risk management and threat intelligence frameworks were reviewed to identify the gaps, including frameworks, methodologies, and industry best practices. Current risk management methodologies often focus on technical vulnerabilities, overlooking the motives and tactics of threat actors, which limits their effectiveness in addressing emerging threats [51]. Integrating cyber threat intelligence into risk management is still uncommon, and there is a need for systematic approaches to incorporate threat intelligence feeds effectively [10,13]. Existing frameworks often struggle to adapt to the dynamic threat landscape, highlighting the importance of considering adversary techniques for proactive risk mitigation [14,52].
2. The solution's objective: This research aims to propose novel threat intelligence integration into an existing risk management process to enhance the process and response to emerging cybersecurity threats.
3. Design and development: This phase includes selecting an existing cybersecurity risk management process and integrating threat intelligence into its different phases. The novel modifications in the EBIOS Risk Manager process aim to integrate the threat intelligence feeds into the different risk management phases. This leads to more accurate risk assessments that consider cyber threat actors' capabilities and objectives and better treatment prioritization.
4. Demonstration: This phase presents the use of the proposed framework to manage the risks in the context of a national telecommunications gateway. The main aim is to demonstrate the framework phases and aspects by assessing and managing risks of a defined scope based on threat intelligence information.
5. Evaluation: This phase aims to evaluate and present the enhancements in the novel framework in contrast with the existing problem. This is achieved by analyzing the proposed framework, the results of its conducted application, and the existing frameworks in addressing the existing problem. This includes limitations such as the necessity of threat intelligence resources and implementation validation, which will be part of future work.

4. The Proposed Enhanced Cyber Threat Intelligence Integrated EBIOS Risk Manager

Threat intelligence and assessment is a dynamic and continuous process. Thus, any cyber risk management framework that integrates the process of systematic threat assessment and intelligence should consider the constant flow of threat intelligence information. The new process should consider both aspects by dynamically handling new threat intelligence information flow and adapting the risk assessment results.

EBIOS stands out as a suitable risk assessment framework to further integrate a cyber threat intelligence process. EBIOS has multiple entry points to integrate threat intelligence feeds of multiple types. First, the threat actors, addressed as risk origins, are identified and assessed based on past incidents and industry-specific threats, which can be enhanced further by threat intelligence information. Moreover, with the scenario-based risk evaluation, it incorporates strategic and operational attack paths, that are identified based on threat actors objectives and the existing scope. These attack paths can be constructed based on threat actors' behaviors, as in [46], by considering threat intelligence information. These enhancements improve accuracy and provide realistic results, enhancing risk assessment scenarios and treatment. Therefore, the proposed framework builds upon EBIOS Risk Manager and integrates the output of a generic cyber threat intelligence process. Consequently, a prerequisite for applying this proposed framework in an organizational context is an active threat intelligence process that continuously generates cyber threat intelligence information and feeds it into the risk management process.

The framework accounts for different types of cyber threat information and adapts risk management's discrete nature to the continuous flow of threat intelligence information.

The following are the detailed workshops of the proposed framework, as shown in Figure 3.

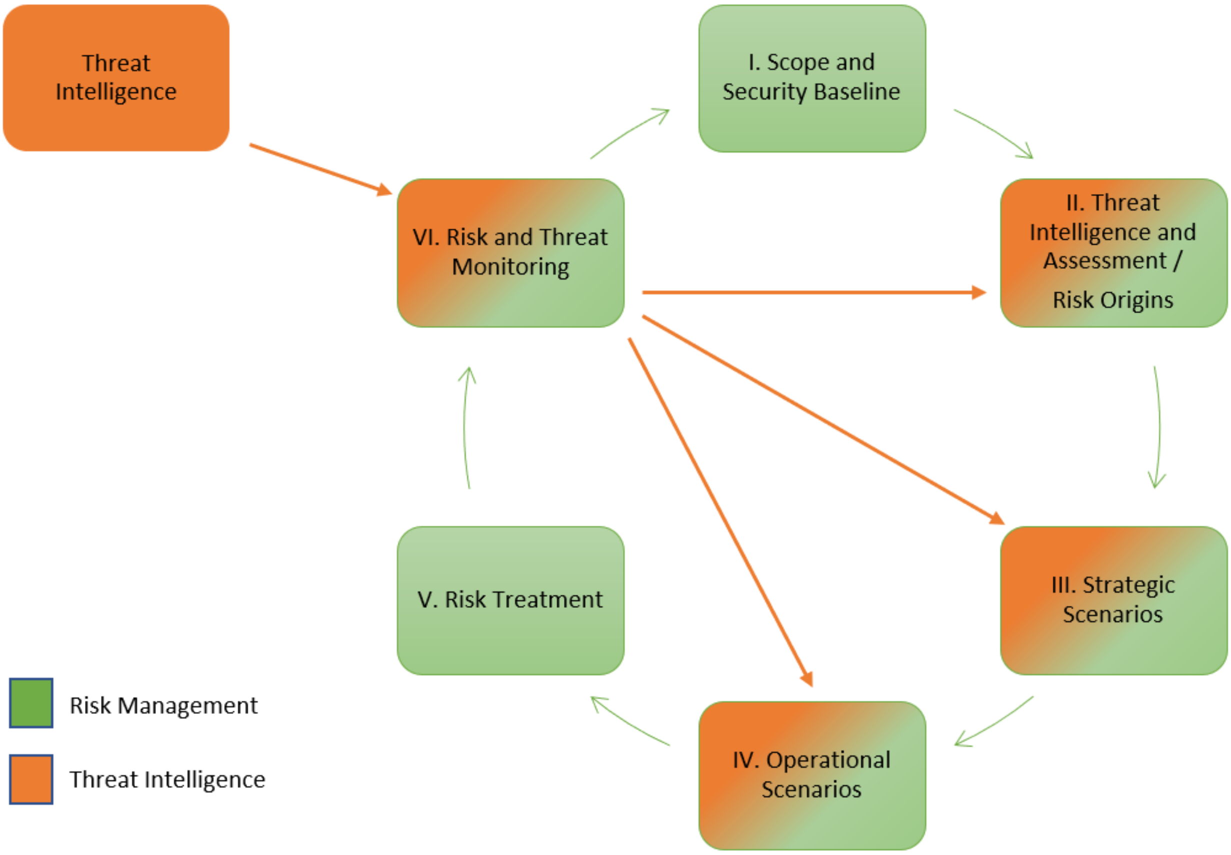
Threat Intelligence
I. Scope and Security Baseline
VI. Risk and Threat Monitoring
II. Threat Intelligence and Assessment / Risk Origins
V. Risk Treatment
III. Strategic Scenarios
IV. Operational Scenarios
Risk Management
Threat Intelligence

Figure 3. Cyber threat intelligence integrated risk management process.

4.1. Scope and Security Baseline

As described in EBIOS, this workshop aims to define the scope, business assets, supporting assets, processes, the corresponding feared events, and the security baseline. The feared events are assessed according to the severity scale in Table 2.

To integrate threat intelligence into the risk management process, it is essential to define the direction and objective of the data obtained from the existing threat intelligence process, such as the relevance of the information in time concerning business assets and processes within the scope.

Table 2. EBIOS severity scale [21].

Scale	Consequences
G4 Critical	Inability of the organization to deliver connectivity services, with possible serious impacts on the safety of assets. The organization will most likely not overcome the situation (its survival is threatened).
G3 Serious	High degradation in the performance of the connectivity services, with possible significant impacts on the safety of assets and reputation. The organization will overcome the situation with serious difficulties but with impact on its image (operations in a highly degraded mode).
G2 Significant	Degradation in the performance of the Internet connectivity services, with no impact on the safety of assets. The organization will overcome the situation despite a few difficulties (operations in degraded mode).
G1 Minor	No impact on operations or the performance of the Internet connectivity services or on the safety of assets. The organization will overcome the situation without too many difficulties (margins will be consumed).

4.2. Threat Intelligence and Assessment/Risk Origins

As described in EBIOS, this workshop identifies the origins of risk and its target objectives and correlates them with the context and the feared events. EBIOS advises organizations to check the high-level threat trends from the news without a deep dive into the threat actors and their specific capabilities.

To complement this workshop, we rely on threat intelligence data to accurately identify threat actors/risk origins interested in targeting the organization or its sector (e.g., healthcare, power plants, service providers, etc.). Thus, the primary inputs required from the threat intelligence process for this workshop are strategic information about emerging threats, threat actors, their motives, and their capabilities. Furthermore, in addition to the existing entities involved, an expert with knowledge about emerging threats and threat actors must participate in this workshop to accurately identify and assess risk origin/target objective pairs.

4.3. Strategic Scenarios

As described in EBIOS, this workshop aims to clearly understand the ecosystem stakeholders and their attributed vulnerabilities. The organization's ecosystem consists of all the stakeholders within the identified scope, first identified, and then, assessed according to the parameters described in EBIOS [53]:

- Dependency: describes the importance of the stakeholder in the specified scope.
- Penetration: describes the level of access of the stakeholder in the specified scope.
- Cyber maturity: describes the security capacities of the stakeholder in the specified scope.
- Trust: describes the interests and intentions of the stakeholder against the organization's objective in the specified scope.

These factors contribute to the calculation of exposure, which describes the stakeholder's susceptibility to cyber threats, and cyber reliability, which describes the trust and confidence in the stakeholder's security measures. The exposure, cyber reliability, and overall threat level are calculated based on the following equations:

$$Exposure = Dependency \times Penetration$$

$$CyberReliability = CyberMaturity \times Trust$$

$$\frac{ThreatLevel = Exposure}{CyberReliability}$$

After determining the stakeholders, high-level strategic scenarios are built to describe how a risk origin can reach the target objective through the stakeholders. The strategic scenarios are assessed to determine the risk scenario impact according to Table 2.

To complement this workshop, we consider strategic and tactical threat intelligence information about the identified risk origins to construct more accurate scenarios. This information reveals how the relevant risk origins might proceed to target the organization through its different stakeholders and suppliers, providing high-level attack paths more reliable than described initially in EBIOS Risk Manager. This allows for a better evaluation of the scenarios' impacts. Additionally, an involved threat intelligence expert should participate in this workshop to contextualize the threat intelligence information.

4.4. Operational Scenarios

As described in EBIOS, this workshop aims to build operational attack scenarios based on strategic scenarios. The operational scenarios describe detailed attack paths for each strategic scenario and are assessed to determine the risk scenario likelihood according to Table 3, taking into account the existing weaknesses in the scope, including known vulnerabilities, access controls, and existing security controls, etc.

To complement this workshop, we consider the tactical and operational threat intelligence data about the selected risk origins to enrich the operational scenarios. Therefore, operational scenarios must be built using MITRE ATT&CK techniques, as described in [44]. These scenarios are constructed by cross-matching the organization's context from the strategic scenarios and the implemented defenses with the risk origins' capabilities and tactics from the threat intelligence process. This approach accurately reflects the potential operational attack paths of risk origins and allows for a better evaluation of the scenarios' likelihood. Moreover, an offensive security expert should participate in this workshop to provide a perspective on the risk origins' attacks that might be conducted against the organization.

Table 3. EBIOS likelihood scale [21].

Scale	Description
V4 Nearly certain	The risk origin will certainly reach its target objective by one of the considered methods of attack. The likelihood of the scenario is very high.
V3 Very likely	The risk origin will probably reach its target objective by one of the considered methods of attack. The likelihood of the scenario is high.
V2 Likely	The risk origin could reach its target objective by one of the considered methods of attack. The likelihood of the scenario is significant.
V1 Rather unlikely	The risk origin has little chance of reaching its objective by one of the considered methods of attack. The likelihood of the scenario is low.

4.5. Risk Treatment

As described in EBIOS, this workshop aims to plan the mitigations by selecting the security measures to be implemented and accepting selected risks. The introduction of threat intelligence information in the previous workshops allows for a more accurate evaluation of the risk scenarios in terms of likelihood and impact, thereby improving the prioritization of risks and their corresponding treatments. No modifications are necessary for this workshop.

4.6. Risk and Threat Monitoring

This phase is not described in EBIOS. It is a continuous phase where risks and mitigations are monitored, and real-time information is fed from the threat intelligence process.

Depending on the incoming information, the process is re-directed to one of the workshops:

1. Context changes: The whole process should be re-conducted if significant changes occur to the scope.
2. New information about threat actors: If new data are received about a new risk origin targeting the organization or a change in the objectives of a risk origin, the risk assessment is re-executed from the Threat Assessment/Risk Origins workshop to assess the new risk origin.
3. Strategical information: If strategic details that include new information about a risk origin or the compromise of one of the ecosystem stakeholders by a risk origin is received, the risk assessment is re-executed from the Strategic Scenarios workshop to re-assess stakeholders and re-build strategic scenarios.
4. Operational or tactical information: If operational or tactical information that includes new information about a risk origin operations, tactics, or the exploitation of a zero-day vulnerability is received, the risk assessment is re-conducted from the Operational Scenarios workshop to build new scenarios based on the new scope's context and vulnerabilities.

After each redirection, the framework is resumed as usual while keeping the previous iteration results, adding the new findings, assessing the new risk scenarios, and re-prioritizing the treatment plan.

This phase is implemented as regularly scheduled workshops with the necessary involved parties to review the risks' treatment progress and spontaneous ones to review the evolving intelligence information from the threat intelligence process.

5. Framework Application

Multiple case studies were conducted using EBIOS version three in critical infrastructure [54] and IoT [55] environments. In this section, we apply the proposed framework to the scope of the national telecommunications sector. The context consists of a national gateway that provides Internet connectivity for multiple Internet service providers, operated by a private entity, providing services for other private and public entities, and supervised by a national regulatory authority. To conduct the complete study, multiple meetings and interviews were held with the experts responsible for the gateway's security, including the stakeholders responsible for maintaining and operating the gateway. As described by the staff during the interviews, the country's telecommunications are an essential part of its critical infrastructure. Communications with the worldwide Internet ensure critical functionalities. Any disruption that might occur has nationwide consequences.

5.1. Scope and Security Baseline

The study's scope is one international connectivity link, including all assets and processes established to maintain the infrastructure. Any disruption to the connectivity's integrity, confidentiality, or availability causes severe political, social, and economic impacts. The study aims to uncover and analyze potential risk scenarios related to international connectivity and provide a proper remediation and improvement plan. The business assets and services in scope were identified manually during thorough interviews with the experts and stakeholders. The identified assets and services are the international media gateway, the transmission/transport network, and the contract with the external provider. Table 4 presents the assets and their supporting assets.

We identify the feared events associated with each asset and evaluate their severity according to EBIOS scales in Table 2. The main feared events are a sabotage of the Internet services; an espionage of critical information from the transport services; and a breach of the contracts' terms and conditions due to a severe incident. The feared events are presented in Table 5.

Table 4. Business assets and supporting assets details.

Mission	**International Internet Services**				
Business asset	International Internet services		Transport network services	Contract management	
Nature of the asset	Process		Process	Process	
Description	Ensure Internet connectivity with the peer international gateways through applying secure and compliant policies and processes matching the international standards and recommendations. This includes: - Router configuration and maintenance - IP assignment and management tables - Access credentials		Ensure that all the physical connectivities are operational and protected topology-wise and hardware-redundancy-wise. This includes: - Equipment configuration - Equipment interconnectivity	Manage, monitor, and control of network performance compliance with the terms and conditions of SLAs signed.	
Responsible entity	Network and IT Departments		Network Department	Management and IT Departments	
Supporting asset	Network Equipment	Safety and Physical Security	Fiber-Optic Components	Partnership Agreements	SLA Contracts
Description	Ensure gateway connectivity, security, and availability. This includes: - Firewalls - Media gateway - Routers - Switches	Processes and devices in place to ensure the service operational, functional, and physical safety. This includes: - Backup electric power sources - Surveillance system - Access control and notification system - Fire safety system	Fiber-optic components configuration, operations, and maintenance management	All partnership agreements with internal and external stakeholders.	Ensuring all service-level agreements management are met and satisfied by monitoring and managing all required components.
Entity in charge	Equipment Suppliers and External Private Contractor	Safety and Security Department	Equipment Suppliers and Network Department	Management Department and External Private Contractor	Management Department and External Private Contractor

Table 5. Feared events.

Business Asset	Feared Events	Categories of Impact	Severity
International Internet services	Total physical destruction of network gateway components, leading to a total cut-off from the Internet	Mission, Equipment, Human, Governance, Financial, Legal, Image, and Trust	G4
	Manipulation of network components configuration, leading to a total loss of traffic	Mission, Financial, Legal, Image, and Trust	G3
	Hijacking the network components, leading to a total disruption in the network traffic	Mission, Financial, Legal, Image, and Trust	G3
Transport network services	Total physical destruction of the fiber-optic network, leading to a total cut-off from the Internet	Mission, Equipment, Human, Governance Financial, Legal, Image, and Trust	G4
	Mirroring of traffic to perform espionage and spying acts	Governance, Financial, Legal, Image, and Trust	G3
Contracts management	Breaching of contracts terms and conditions	Mission, Financial, Legal, Image, and Trust	G3

5.2. Threat Intelligence and Assessment/Risk Origins

We rely on the cyber threat intelligence process to identify and assess risk origins. Four main risk origin (RO) categories were identified, targeting similar infrastructure in the same industry and regional area:

1. RO-01: State-sponsored threat actor with an objective to sabotage Internet connectivity.
2. RO-02: State-sponsored threat actor with an objective to perform espionage and spying activities.
3. RO-03: Organized crime threat actor with a lucrative objective.
4. RO-04: A competitor with an objective of breaching the contracts' terms in order to gain more clients.

The assessment of the identified risk origins and their target objectives, resources, and motivation is presented in Table 6. To proceed, we consider only the most relevant risk origins RO-01 and RO-02.

Table 6. Risk origins.

Reference	Type	Target Objectives (TOs)	Motivation	Resources
RO-01	State Sponsored	Sabotage Internet connectivity	Highly motivated	Unlimited
RO-02	State Sponsored	Espionage and spying activities	Highly motivated	Unlimited
RO-03	Organized Crime	Disrupt Internet connectivity for lucrative purposes	Rather motivated	Significant
RO-04	Competitor	Breach contracts' terms and conditions along with the service-level agreements to reduce competition	Rather motivated	Significant

5.3. Strategic Scenarios

The stakeholders in the selected scope's ecosystem are mainly equipment suppliers (SPs), service providers (PRs), clients (CLs), and external staff (ST). The identified stakeholders are evaluated in Table 7.

Table 7. Ecosystem stakeholders assessment.

ID	Category	Stakeholder	Role	Dependency	Penetration	Maturity	Trust	Exposure	Cyber Reliability	Threat Level
PR-01	Equipment Supplier	Network gateway provider	Provides routing solutions	3	4	3	3	12	9	1.33
PR-02	Equipment Supplier	Fiber-optic equipment provider	Provides transmission connectivity	3	4	3	3	12	6	1.33
PR-03	Equipment Supplier	Security equipment supplier	Provides network security and protection products	3	3	3	2	9	6	1.50
PR-04	Equipment Supplier	Access control and surveillance supplier	Provides access control, logging, and monitoring to sites	2	2	3	2	4	6	0.67
SP-01	Service Provider	External service provider	Provides external Internet services	3	1	3	3	3	9	0.33
SP-02	Service Provider	Cable provider	Provides fiber connectivity	4	3	2	2	12	4	3.00
CL-01	Client	Internet service provider	Clients	1	1	3	2	1	6	0.17
CL-02	Client	Governmental agencies	Clients	1	1	2	3	1	6	0.17
ST-01	Staff	External staff	Staff members	3	4	2	3	12	6	2.00

Figure 4 shows the ecosystem threat mapping according to the calculated exposure and cyber reliability. The selected threat threshold for this study is 2. Stakeholders with threats above 2 are selected to build the strategic and operational scenarios.

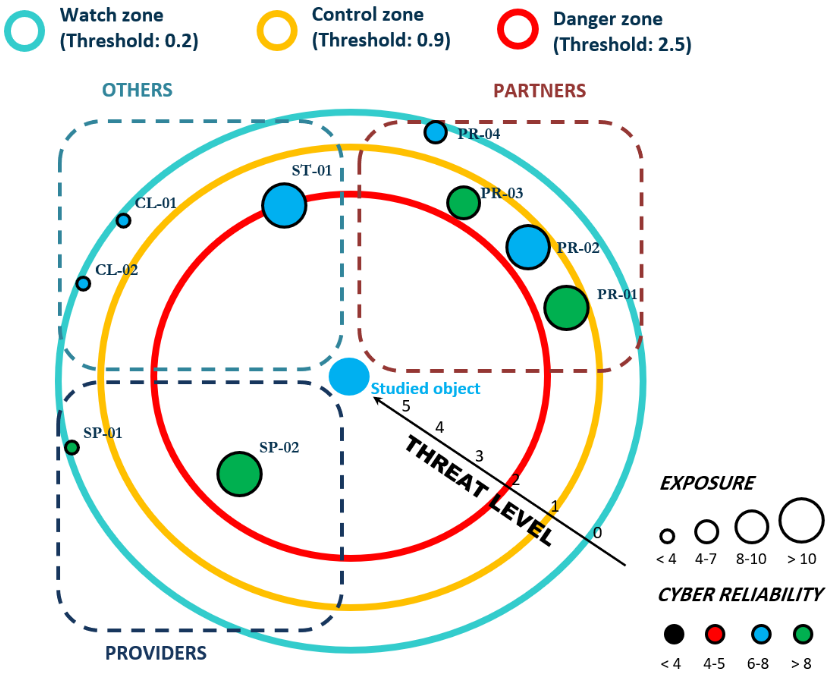

Figure 4. Ecosystem threat mapping.

The selected critical stakeholders to move forward with the study are the external staff members ST-01 and the cable service provider SP-02. Unlike EBIOS Risk Manager, when building the strategic attack scenarios, we rely mainly on strategic threat intelligence information about the identified threat actors to identify potential strategic attack paths involving the ecosystem's stakeholders. The following are the identified strategic attack paths (SAPs):

1. SAP-11: The attack path that can be used by RO-01 by exploiting a zero-day vulnerability to cut off the gateway services, as RO-01 is a threat group known for its capabilities to utilize zero-day vulnerabilities and develop new exploits. The impact of this scenario is assessed as critical.
2. SAP-12: The attack path that RO-01 can use through ST-01 to cut off the gateway services, as RO-01 is also known to rely on phishing campaigns and supply chain attack strategies. The impact of this scenario is assessed as critical.
3. SAP-21: The attack path that RO-02 can use through SP-02 to perform espionage activities on the international Internet gateway, as RO-02 is a threat group known for software supply chain attacks. The impact of this scenario is assessed as serious.

Figure 5 presents the strategic attack paths.

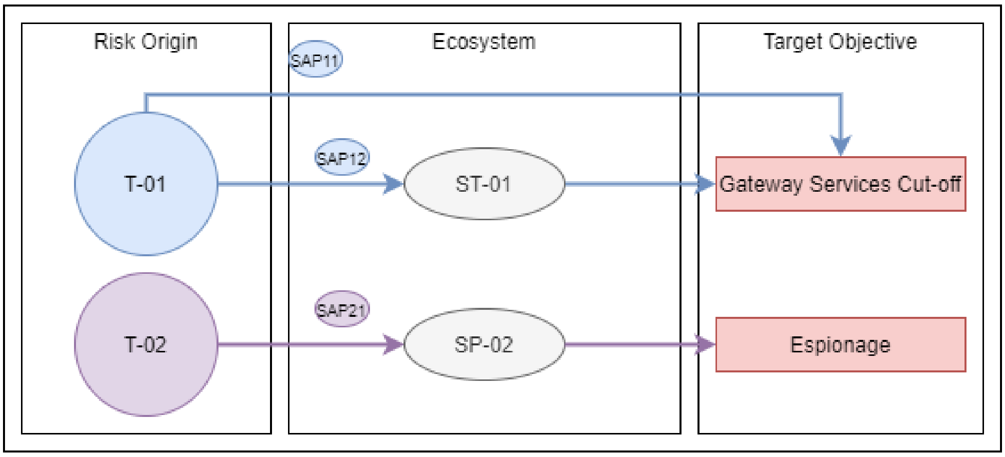

Figure 5. Strategic scenarios of the identified risk origins.

5.4. Operational Scenarios

We rely on each risk origin's strategic scenarios and operational threat intelligence information to build accurate operational scenarios.

1. OAP-111: RO-01 scans the public-facing systems and identifies the used technologies. Once a zero-day vulnerability is discovered in one of the secondary systems, RO-01 develops an exploit and gains access to the internal network. After performing an internal reconnaissance, RO-01 moves laterally to reach the gateway and escalates privileges to gain control over the gateway services and its backups. Finally, RO-01 cuts off the gateway services and their backups. The likelihood of this attack path is assessed as likely.
2. OAP-112: RO-01 scans the public-facing systems and identifies the used technologies. RO-01 aims at discovering and exploiting zero-day vulnerabilities in the public-facing main gateway systems. After that, RO-01 gains access to the main gateway systems, disables the backup services, and cuts off the international connection. The likelihood of this attack path is assessed as very likely.
3. OAP-123: RO-01, knowing that ST-01 is part of the ecosystem, performs identity information gathering on ST-01 staff. Then, it compromises one of the applications used by ST-01 staff (drive by compromise) and sends spear-phishing emails to trick ST-01 users into downloading and executing a backdoor malware. Then, after internal reconnaissance, lateral movement, and privilege escalation, RO-01 reaches the gateway services, disables the backup services, and cuts off the international connection. The likelihood of this attack path is assessed as rather unlikely.
4. OAP-214: RO-02, knowing that SP-02 is part of the ecosystem, performs identity information gathering on SP-02 staff. Then, RO-02 sends spear phishing emails to gain access to one of SP-02's systems. RO-02 deploys spying malware inside one of the administrative software provided by SP-02. After pushing a new update, the new malicious software mirrors network traffic and exfiltrates data. The likelihood of this attack path is assessed as likely.

The operational attack paths and the used MITRE ATT&CK tactics and techniques are presented in Figure 6.

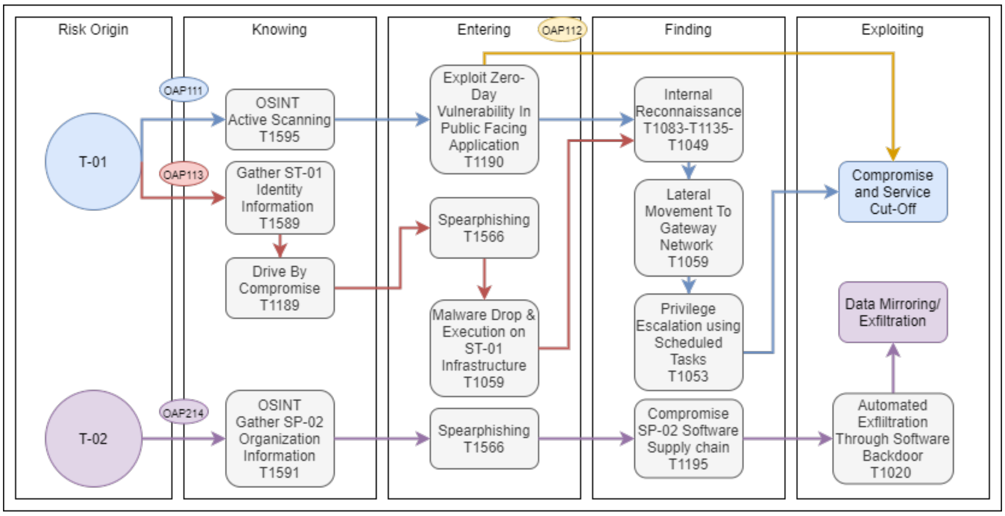
Risk Origin
Knowing
Entering
OAP112
Finding
Exploiting
OAP111
T-01
OAP113
OSINT Active Scanning T1595
Gather ST-01 Identity Information T1589
Drive By Compromise T1189
Exploit Zero-Day Vulnerability In Public Facing Application T1190
Spearphishing T1566
Malware Drop & Execution on ST-01 Infrastructure T1059
Internal Reconnaissance T1083-T1135-T1049
Lateral Movement To Gateway Network T1059
Privilege Escalation using Scheduled Tasks T1053
Compromise and Service Cut-Off
Data Mirroring/ Exfiltration
T-02
OAP214
OSINT Gather SP-02 Organization Information T1591
Spearphishing T1566
Compromise SP-02 Software Supply chain T1195
Automated Exfiltration Through Software Backdoor T1020

Figure 6. Operational attack paths and used MITRE ATT&CK techniques of the identified strategic scenarios.

5.5. Risk Treatment

Based on the identified strategic and operational scenarios, four main risks were identified:

1. R-01: A state-sponsored threat actor sabotages Internet services by exploiting a zero-day vulnerability.
2. R-02: A state-sponsored threat actor sabotages Internet services by obtaining access to one of the stakeholders (ST-01).
3. R-03: A state-sponsored threat actor sabotages Internet services by obtaining access to one of the stakeholders (SP-02).
4. R-04: A state-sponsored threat actor steals information by mirroring the Internet traffic.

Table 8 presents the risks and their assessments in terms of likelihood and impact.

Table 8. Identified risks and their assessment.

ID	Risk	Likelihood	Impact
R-01	A state-sponsored threat actor sabotages Internet services by exploiting a zero-day vulnerability.	V2	G4
R-02	A state-sponsored threat actor sabotages Internet services by obtaining the access of one of stakeholders (ST-01).	V3	G4
R-03	A state-sponsored threat actor sabotages Internet services by obtaining the access of one of stakeholders (SP-02).	V1	G4
R-04	A state-sponsored threat actor steals information by mirroring the Internet traffic.	V2	G3

To remediate the risk scenarios, a treatment plan is established. Table 9 presents the main treatment actions and priorities.

Table 9. Treatment plan.

ID	Treatment	Affected Risks	Priority
TR-01	Establish proper incident response, cyber crisis management, and business continuity procedures.	All	High
TR-02	Perform regular penetration tests on a yearly basis.	All	Medium
TR-03	Implement security information event management (SIEM) solution along with a security operations center (SOC).	All	Medium
TR-04	Require stakeholders to raise cybersecurity awareness among employees.	R-03	Medium
TR-05	Establish a change management policy.	R-04	Medium
TR-06	Enhance the efficiency of vulnerability management and patch management processes already in place.	R-01, R-02	Low
TR-07	Implement a privilege access management (PAM) solution to better control user accesses.	R-01, R-04	Low

5.6. Risk and Threat Monitoring

While following up on the existing risks and the planned treatments, new threat intelligence information emerges about a new risk origin exploiting a zero-day vulnerability for profit. The vulnerability exists in one of the public-facing applications. Thus, according to the framework, we re-conduct workshops two to five:

1. Threat Assessment/Risk Origins: The new risk origin (RO-05) is an organized crime group. RO-05 has a lucrative objective to deploy ransomware, hold data captive, and blackmail by re-selling organizations' data. RO-05 is assessed as highly motivated with significant resources.
2. Strategic Scenarios: The ecosystem stakeholders are still the same. However, they are separate since the threat intelligence information specifies that RO-05 relies on a direct attack path. Figure 7 presents the corresponding strategic scenario. The impact of this scenario is assessed as critical since the vulnerability has been proven to exist in the public-facing application.

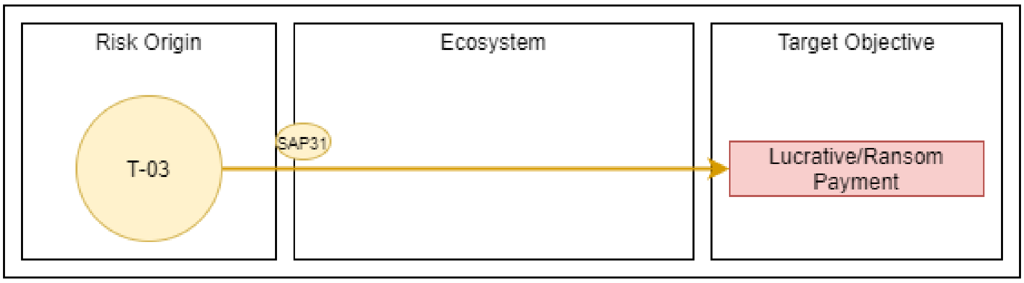

Figure 7. Strategic scenario of the newly identified risk origin.

3. Operational Scenarios: Operational threat intelligence about the risk origin reveals the following potential operational scenario; after actively scanning the public-facing systems, RO-05 can identify the used vulnerable application. RO-05 has to develop and customize an exploit and ransomware. After exploitation, a command and control server connection is established to enumerate the internal network and environment. After propagation and lateral movement through internal services, the ransomware is executed. It infects the majority of the internal systems and exfiltrates data through encrypted channels. Then, existing data are encrypted, and a ransom is demanded. Figure 8 presents the operational scenario of the newly identified risk origin. The likelihood of this attack path is assessed as nearly certain.

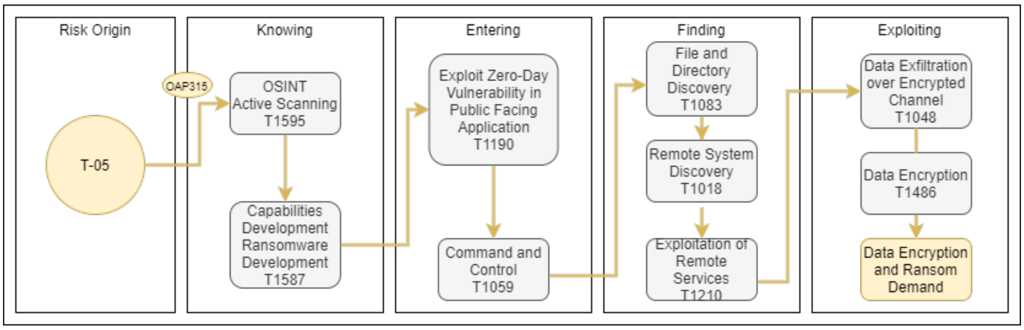
Risk Origin
T-05
OAP315
Knowing
OSINT Active Scanning T1595
Capabilities Development Ransomware Development T1587
Entering
Exploit Zero-Day Vulnerability in Public Facing Application T1190
Command and Control T1059
Finding
File and Directory Discovery T1083
Remote System Discovery T1018
Exploitation of Remote Services T1210
Exploiting
Data Exfiltration over Encrypted Channel T1048
Data Encryption T1486
Data Encryption and Ransom Demand

Figure 8. Operational scenario of the newly identified risk origin.

4. Risk Treatment: The newly identified risk (R-05) is that an organized crime can sabotage Internet gateway services for lucrative purposes. To remediate this risk, the treatment plan is modified as follows:
    - New treatment TR-08 to implement new rules on the firewall to detect any abuse of the vulnerable services. Priority: high.
    - Modify TR-03 priority from medium to high to ensure the detection of anomalies for zero-day vulnerabilities until patches are released.
    - Modify TR-05 priority from medium to low since more demanding actions are required.

6. Framework Evaluation

The application of the proposed framework demonstrates multiple enhancements over EBIOS, addressing new gaps not covered by the existing frameworks, though it still has certain limitations.

6.1. Enhancements over EBIOS

The application that was conducted using the proposed modifications to EBIOS Risk Manager has enhanced the quality of the risk management output. Traditional EBIOS Risk Manager relies on generic threat trend identification, potentially missing specific threats crucial to an organization. This could lead to inaccurate risk assessments. Additionally, it cannot trigger a re-execution of the risk management process based on incoming threat intelligence, potentially resulting in delayed or ineffective risk responses.

The proposed improvements result in a more agile and responsive process based on cyber threat intelligence information. Notably, in workshop two, risk origins are now identified based on threat intelligence information that is directly relevant to the organization's context, improving the accuracy beyond the generic threat trend identification used in traditional EBIOS.

Additionally, workshops three and four benefit from strategic and operational threat intelligence information related to identified risk origins. Extending the traditional EBIOS Risk Manager approach, the integrated threat intelligence data leads to more accurate and realistic risk scenarios, ultimately improving risk assessments and treatment strategies. A significant addition is introducing the "Risks and Threat Monitoring" phase. Unlike EBIOS Risk Manager, this phase ensures ongoing risk visibility and integrates threat intelligence information. This enables the framework to trigger the re-execution of the risk management process based on incoming threat intelligence, allowing for timely and agile adaptation of risk responses and re-prioritization of risk treatments.

Table 10 summarizes the enhancements in the proposed framework over EBIOS Risk Manager by integrating the cyber threat intelligence process.

Table 10. Enhancements in the proposed framework over EBIOS.

Workshop	Proposed Enhancements
Scope and Security Baseline	Determination of the necessary cyber threat intelligence information.
Threat Assessment Risk Origins	Relevant threats identification and assessment based on threat intelligence information.
Strategic Scenarios	Strategic scenarios built based on the organization context, stakeholders, and the identified threats and their corresponding strategic threat intelligence information.
Operational Scenarios	Operational scenarios built based on the organization context, vulnerabilities, and the identified threats and their corresponding operational and technical threat intelligence information.
Risk Treatment	Same as EBIOS.
Risks and Threat Monitoring	Newly introduced workshop. Timely and agile re-execution of the risk management process based on new threat intelligence information.

6.2. Comparative Analysis

As presented in Table 1, while existing frameworks incorporate parts of risk management integrating threat intelligence, the full integration of all types of threat intelligence with the capability to adjust risks based on new intelligence is still not addressed. Our proposed framework, based on EBIOS's comprehensive risk assessment, supports threat assessment, risk, and threat monitoring by integrating cyber threat intelligence, including strategic, tactical, operational, and technical types, with the capability to adjust based on new threat intelligence inputs.

EBIOS [21] and the Hybrid Model for Risk Assessment [43,44], while they account for threat actors' assessment, they lack the integration of threat intelligence. The Hybrid Dynamic Risk Analysis [45] does not explicitly integrate threat intelligence in the risk assessment. Although it dynamically considers new technical information, mainly vulnerabilities, to adapt to analyzed risks, it does not account for other types of new threat intelligence information. SAIF [46] and the Unified Approach Model [47] integrate threat intelligence in cyber risk management but without addressing the adaptation of risks based on new threat intelligence. For instance, the approach of SAIF [46] can be used in phases three and four of our proposed framework to ensure the incorporation of the MITRE knowledge base in the definition of scenarios. The proposed framework in [48] drives a national risk assessment based on a national vulnerabilities inventory. It accounts for threat intelligence and risk adaptions but is only based on new technical vulnerability intelligence information. TIBSA [49] proposes a threat-informed decision-making methodology without a systematic risk management process.

6.3. Limitations

Despite these notable enhancements, it is crucial to recognize several limitations. The conceptual enhancements to EBIOS Risk Manager require further technical implementation and specifications. Resource intensity can be a challenge, as the continuous integration of threat intelligence may require additional personnel and technology resources, posing difficulties for smaller organizations with limited means. Expertise in interpreting and applying threat intelligence data is paramount for maximizing the framework's benefits but may not be readily accessible to all organizations. Concerns related to scalability and sustainability over time warrant careful consideration. In addition, training is essential to make the most of available threat data. Successful adoption of the framework hinges on addressing these limitations and ensuring its long-term effectiveness.

7. Conclusions and Future Work

Organizations are facing imminent and persistent cyber adversaries. Existing cyber risk management frameworks often lack the agility and efficiency to anticipate these threats and protect their digital assets proactively. To address these challenges, this paper has introduced a novel approach to cyber risk management that integrates cyber threat intelligence, ultimately enhancing the organization's ability to anticipate and respond to emerging threats. We conducted an overview of the existing works in both cyber risk management and cyber threat intelligence. A significant gap is identified in current risk management practices, particularly in the lack of considering valuable cyber threat intelligence information. The proposal is to create a new framework that bridges this gap and overcomes these limitations. By integrating the threat intelligence process with EBIOS Risk Manager, we developed a robust and agile risk management framework capable of adapting to emerging cyber threats. We applied the designed framework within a critical telecommunications infrastructure context to validate its effectiveness. The results demonstrated a promising risk management framework driven by cyber threat intelligence data.

In future work, we will extend the proposed enhancements to EBIOS based on STIX feeds. Moreover, we will incorporate this research proposal in the blockchain-based framework [32] to provide a complete collaborative threat intelligence-driven risk management framework while ensuring risk security and privacy, offering risk visibility on the national level and capitalizing on efficient common national threat anticipation. Further applications, case studies, and research can also focus on refining and extending the proposed framework to suit various industry-specific contexts. Another promising area for research is the development of standardized methodologies for measuring the effectiveness of threat intelligence integration within risk management practices.

Author Contributions: H.E.A. conceived and designed the proposed framework, conducted the meetings related to the framework application, and drafted the manuscript. A.E.S. and L.O. contributed to supervising the work along with writing and revising the manuscript. M.C. and A.F. critically revised the manuscript for important intellectual content. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors declare that they have no competing interests. Therefore, no known competing financial interests or personal relationships could have appeared to influence the work reported in this paper.

References

1. IBM. Cost of a Data Breach Report 2023. Available online: https://www.ibm.com/security/digital-assets/cost-data-breach-report/ (accessed on 31 May 2024).
2. Shevchenko, P.V.; Jang, J.; Malavasi, M.; Peters, G.W.; Sofronov, G.; Trück, S. The nature of losses from cyber-related events: Risk categories and business sectors. *J. Cybersecur.* **2023**, *9*, tyac016. [CrossRef]
3. Ahmad, A.; Maynard, S.B.; Desouza, K.C.; Kotsias, J.; Whitty, M.T.; Baskerville, R.L. How can organizations develop situation awareness for incident response: A case study of management practice. *Comput. Secur.* **2021**, *101*, 102122. [CrossRef]
4. Verizon. 2024 Data Breach Investigations Report. Available online: https://enterprise.verizon.com/resources/reports/dbir/ (accessed on 31 May 2024).
5. Gartner. Forecast: Information Security and Risk Management, Worldwide, 2021–2027. 2Q23 Update. Available online: https://www.gartner.com/en/documents/4488199 (accessed on 31 May 2024).
6. Bederna, Z.; Szádeczky, T. Managing the financial impact of cybersecurity incidents. *Secur. Def. Q.* **2023**, *41*, 15–35. [CrossRef]
7. Freeman, C.F.; Lewis, R. Bridging the gap between cyber risk management and cyber threat intelligence. *Comput. Secur.* **2017**, *66*, 1–9.
8. Samtani, S.; Abate, M.; Benjamin, V.; Li, W. Cybersecurity as an industry: A cyber threat intelligence perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Spinger: Berlin/Heidelberg, Germany, 2020; pp. 135–154.

9. Mizrak, F. Integrating Cybersecurity Risk Management into Strategic Management: A Comprehensive Literature Review. *Res. J. Bus. Manag.* **2023**, *10*, 98–108. [CrossRef]
10. Kotsias, J.; Ahmad, A.; Scheepers, R. Adopting and integrating cyber-threat intelligence in a commercial organisation. *Eur. J. Inf. Syst.* **2023**, *32*, 35–51. [CrossRef]
11. Akyeşilmen, N. Cybersecurity and Cyberwar: What Everyone Needs to Know. *Cyberpolitik J.* **2016**, *1*, 368–372.
12. Oltsik, J.; Poller, J. Automation and Analytics versus the Chaos of Cybersecurity Operations. *ESG MCAFEE* **2017**.
13. Ferreira, D.J.; Mateus-Coelho, N.; Mamede, H.S. Methodology for Predictive Cyber Security Risk Assessment (PCSRA). *Procedia Comput. Sci.* **2023**, *219*, 1555–1563. [CrossRef]
14. Cheimonidis, P.; Rantos, K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Future Internet* **2023**, *15*, 324. [CrossRef]
15. Giuca, O.; Popescu, T.M.; Popescu, A.M.; Prostean, G.; Popescu, D.E. A Survey of Cybersecurity Risk Management Frameworks. In *Proceedings of the International Workshop Soft Computing Applications*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 240–272.
16. Ionita, D. Current Established Risk Assessment Methodologies and Tools. Master's Thesis, University of Twente, Enschede, The Netherlands, 2013.
17. Lambrinoudakis, C.; Gritzalis, S.; Xenakis, C.; Katsikas, S.; Karyda, M.; Tsochou, A.; Papadatos, K.; Rantos, K.; Pavlosoglou, Y.; Gasparinatos, S.; et al. *Compendium of Risk Management Frameworks with Potential Interoperability: Supplement to the Interoperable EU Risk Management Framework Report*; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2022.
18. *ISO/IEC 27005: 2018*; Information Technology. Security Techniques. Information Security Risk Management. International Organization for Standardization: Geneva, Switzerland, 2018.
19. Initiative, J.T.F.T. *Guide for Conducting Risk Assessments*; Technical Report NIST SP 800-30r1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [CrossRef]
20. Caralli, R.; Stevens, J.; Young, L.; Wilson, W. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*; Technical Report CMU/SEI-2007-TR-012; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2007.
21. Agence Nationale de la Sécurité des Systèmes d'Information. *La Méthode EBIOS Risk Manager—Le Guide*; Technical Report ANSSI-PA-048-EN; Agence Nationale de la Sécurité des Systèmes d'Information: Paris, France, 2019.
22. Mathey, F.; Bonhomme, C.; Rocha, J.; Lombardi, J.; Joly, B. Risk Assessment Optimisation with MONARC. Available online: https://www.monarc.lu/assets/files/publications/2018-HACK.LU-CASES.pdf (accessed on 31 May 2024).
23. BSI-Standard 200-2: IT-Grundschutz-Methodology. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html (accessed on 4 February 2023).
24. European Commission Directorate-General for Communication. Security Standards Applying to All European Commission Information Systems: EU ITSRM, IT Security Risk Management Methodology V1.2. 2020. Available online: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en (accessed on 31 May 2024).
25. Information Security Forum. Security Standards Applying to All European Commission, ISF, Information RISK Assessment Methodology 2 (IRAM2). Available online: https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-2-iram2/ (accessed on 31 May 2024).
26. Brunner, M.; Sillaber, C.; Breu, R. Towards automation in information security management systems. In Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS), Prague, Czech Republic, 25–29 July 2017; pp. 160–167.
27. Schmitz, C.; Pape, S. LiSRA: Lightweight security risk assessment for decision support in information security. *Comput. Secur.* **2020**, *90*, 101656. [CrossRef]
28. Akinrolabu, O.; New, S.; Martin, A. CSCCRA: A Novel Quantitative Risk Assessment Model for SaaS Cloud Service Providers. *Computers* **2019**, *8*, 66. [CrossRef]
29. Poletykin, A. Cyber security risk assessment method for SCADA of industrial control systems. In Proceedings of the 2018 International Russian Automation Conference (RusAutoCon), Sochi, Russia, 9–16 September 2018; pp. 1–5.
30. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
31. Ma, S.; Hao, W.; Dai, H.N.; Cheng, S.; Yi, R.; Wang, T. A Blockchain-Based Risk and Information System Control Framework. In Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 12–15 August 2018; pp. 106–113. [CrossRef]
32. El Amin, H.; Oueidat, L.; Chamoun, M.; Samhat, A.E.; Feghali, A. Blockchain-based multi-organizational cyber risk management framework for collaborative environments. *Int. J. Inf. Secur.* **2023**, *23*, 1231–1249. [CrossRef]
33. Shin, B.; Lowry, P.B. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Comput. Secur.* **2020**, *92*, 101761. [CrossRef]
34. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lead. Issues Inf. Warf. Secur. Res.* **2011**, *1*, 80.
35. Caltagirone, S.; Pendergast, A.; Betz, C. The diamond model of intrusion analysis. *Threat Connect* **2013**, *298*, 1–61.
36. Bianco, D. The Pyramid of Pain. *2013*. Available online: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (accessed on 31 May 2024).

37. Strom, B.E.; Applebaum, A.; Miller, D.P.; Nickels, K.C.; Pennington, A.G.; Thomas, C.B. *Mitre Att&ck: Design and Philosophy*; Technical report; The MITRE Corporation: McLean, VA, USA, 2018.
38. Barnum, S. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (Stix)*; MITRE Corporation: McLean, VA, USA, 2012; Volume 11, pp. 1–22.
39. Connolly, J.; Davidson, M.; Schmidt, C. *The Trusted Automated Exchange of Indicator Information (Taxii)*; The MITRE Corporation: McLean, VA, USA, 2014; pp. 1–20.
40. Filigran—OpenCT—Open Platform for Cyber Threat Intelligence. Available online: https://www.filigran.io/en/products/opencti/ (accessed on 4 February 2023).
41. Wagner, C.; Dulaunoy, A.; Wagener, G.; Iklody, A. Misp: The design and implementation of a collaborative threat intelligence sharing platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, Vienna, Austria, 24 October 2016; pp. 49–56.
42. Army, A. *Land Warfare Doctrine LWD 2-0 intelligence*; The Australian Government Department of Defence: Canberra, Australia, 2014.
43. Haji, S.; Tan, Q.; Costa, R.S. A Hybrid Model for Information Security Risk Assessment. *Int. J. Adv. Trends Comput. Sci. Eng.* **2019**, *8*, 100–106. [CrossRef]
44. Ahmed, M.; Panda, S.; Xenakis, C.; Panaousis, E. MITRE ATT&CK-driven cyber risk assessment. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23–26 August 2022; pp. 1–10.
45. Lyvas, C.; Maliatsos, K.; Menegatos, A.; Giannakopoulos, T.; Lambrinoudakis, C.; Kalloniatis, C.; Kanatas, A. A hybrid dynamic risk analysis methodology for cyber-physical systems. In *Proceedings of the European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 134–152.
46. Belfadel, A.; Boyer, M.; Letailleur, J.; Petiot, Y.; Yaich, R. Towards a Security Impact Analysis Framework: A Risk-Based and MITRE Attack Approach. In *Proceedings of the European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 212–227.
47. Kure, H.; Islam, S. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *J. Univers. Comput. Sci.* **2019**, *25*, 1478–1502.
48. Janiszewski, M.; Felkner, A.; Lewandowski, P. A novel approach to national-level cyber risk assessment based on vulnerability management and threat intelligence. *J. Telecommun. Inf. Technol.* 2019, **2**, 5–14. [CrossRef]
49. Dekker, M.; Alevizos, L. A Threat-Intelligence Driven Methodology to Incorporate Uncertainty in Cyber Risk Analysis and Enhance Decision Making. *arXiv* **2023**, arXiv:2302.13082.
50. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
51. Alnajim, O.A.; Kautzman, D.M. Towards a conceptual cyber risk assessment framework for healthcare systems. *Procedia Comput. Sci.* **2017**, *121*, 785–792.
52. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1153–1176. [CrossRef]
53. ANSSI. *EBIOS Risk Manager: Going Further*; Technical Report; ANSSI: Paris, France, 2019; Version 1.0.
54. Abbass, W.; Baina, A.; Bellafkih, M. Using EBIOS for risk management in critical information infrastructure. In Proceedings of the 2015 5th World Congress on Information and Communication Technologies (WICT), Marrakech, Morocco, 14–16 December 2015; pp. 107–112.
55. Zahra, B.F.; Abdelhamid, B. Risk analysis in Internet of Things using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–7.

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.