Data Governance to Counter Hybrid Threats against Critical Infrastructures

Gabriel Pestana 1,* and Souzanna Sofou 2

1 INOV—INESC Inovação, 1000-029 Lisbon, Portugal
2 SATWAYS Ltd., 14122 Athens, Greece; s.sofou@satways.net
* Correspondence: gabriel.pestana@inov.pt; Tel.: +351-964-008-918

Abstract: Hybrid threats exploit vulnerabilities in digital infrastructures, posing significant challenges to democratic countries and the resilience of critical infrastructures (CIs). This study explores integrating data governance with business process management in response actions to hybrid attacks, particularly those targeting CI vulnerabilities. This research analyzes hybrid threats as a multidimensional and time-dependent problem. Using the Business Process Model and Notation, this investigation explores data governance to counter CI-related hybrid threats. It illustrates the informational workflow and context awareness necessary for informed decision making in a cross-border hybrid threat scenario. An airport example demonstrates the proposed approach’s efficacy in ensuring stakeholder coordination for potential CI attacks requiring cross-border decision making. This study emphasizes the importance of the information security lifecycle in protecting digital assets and sensitive information through detection, prevention, response, and knowledge management. It advocates proactive strategies like implementing security policies, intrusion detection software tools, and IT services. Integrating Infosec with the methodology of confidentiality, integrity, and availability, especially in the response phase, is essential for a proactive Infosec approach, ensuring a swift stakeholder response and effective incident mitigation. Effective data governance protects sensitive information and provides reliable digital data in CIs like airports. Implementing robust frameworks enhances resilience against hybrid threats, establishes trusted information exchange, and promotes stakeholder collaboration for an emergency response. Integrating data governance with Infosec strengthens security measures, enabling proactive monitoring, mitigating threats, and safeguarding CIs from cyber-attacks and other malicious activities.

Keywords: hybrid threats dimensions; data exfiltration; situational awareness workflow; BPMN; CIA; Infosec lifecycle

1. Introduction

Hybrid threats are well-coordinated and synchronized actions that aim to exploit a country’s vulnerabilities and often seek to undermine fundamental democratic values and liberties. Hybrid actors can exploit natural and manmade disasters to urge citizens to question the credibility of democratic systems. Furthermore, as the digital world offers an attractive context for hybrid threats, the reliance on digital means can potentially decrease the resilience of the production units. In addition, a hybrid threat can become particularly significant when targeting a critical infrastructure (CI) in countries reliant on an open market economy and a transparent democratic decision-making process [1]. Ensuring the uninterrupted operation of CIs is essential for safeguarding EU autonomy, a priority underscored by the supply chain disruptions during the pandemic [2]. The EU-HYBNET H2020 project [3] also brought together pan-European practitioners and stakeholders to identify challenges and map innovative solutions for countering hybrid threats.

During the last few years, several researchers have increasingly studied hybrid threats in scientific, military, and political contexts. The conceptual hybrid threats [4] model was
developed around four main pillars: actors (and their strategic objectives), domains, tools, and phases. This work highlights the importance of early detection and attribution to counter hybrid threats while also providing a guide for those variables that authorities should look upon to identify the onset of hybrid activity at an early stage. Previous studies in hybrid threats also include the introduction of composite indicators [5], with the aim of forming an analytical strategic-level method that could play a role as an early warning engine to support policy makers. Additionally, a recent work on the resilience against hybrid threats [6] proposed an ecosystem consisting of three spaces—civic, governance, and services—representing the three sectors of society. As explained in this work, resilience in the services space supports the good functioning of society by taming the effects of hybrid threat activity and lowering their disruptive potential.

As hybrid threats require a multi-layered response [4] and due to the specific nature of resilience against them [6], it is important to reinforce, besides policy makers and authorities (i.e., the governance space), the services space as well. This paper focuses on the side of critical infrastructure’s owners and managers and discusses tools that can, besides enhancing early detection and real-time response, ensure accountability and facilitate trusted information exchange and collaboration among different stakeholders.

As hybrid threats require a multi-layered response [4] and specific resilience strategies, it is essential to reinforce both the governance space (e.g., policymakers and authorities) and the services space. This paper focuses on CI owners and managers, discussing tools that enhance early detection and real-time response while ensuring accountability and facilitating trusted information exchange and stakeholder collaboration. This paper also tackles the challenges of integrating data governance with information security (Infosec) to counter hybrid threats in critical infrastructures like airports. It highlights the harmonization of data governance in airport security, particularly in the response phase, to enhance controls and activity monitoring while preserving evidence chain integrity. This approach boosts accountability and trustworthiness in digital information management. The research findings align with this study’s objectives, emphasizing three key areas.

1. Implementing robust frameworks enhances resilience against hybrid threats. Integrating data governance frameworks with Infosec practices enables organizations to improve data security, access controls, and incident response procedures. This integration enhances breach detection, aids in identifying attackers, and serves as an effective countermeasure. The structured approach strengthens the organization’s capability to withstand and recover from cyber-attacks and other malicious activities, thereby boosting overall resilience.

2. Establishing trusted information exchanges and promoting stakeholder collaboration for an emergency response necessitates securing information exchange with external parties, including organizations from the tourism and logistics sectors, regulatory bodies, and emergency response teams. Implementing secure data-sharing protocols and fostering collaboration enables airports to enhance their emergency response capabilities and improve coordination to address security incidents.

3. Integrating data governance with Infosec strengthens security measures by combining data protection protocols with proactive monitoring and threat mitigation strategies. This approach allows airports to detect and respond to real-time security incidents, preemptively address potential threats, and safeguard critical infrastructures from cyber-attacks and other malicious activities. These principles underscore this study’s focus on harmonizing data governance practices with Infosec strategies to strengthen the security posture of critical infrastructures and improve emergency response capabilities in the face of evolving cyber threats.

The research challenge addresses a framework for conceptualizing hybrid threats as multidimensional and time-dependent problems, focusing on potential attacks against airport CIs, particularly those targeting internal CI vulnerabilities. It explores the data governance aspect within CI-related hybrid threats, demonstrating examples using the Business Process Model and Notation (BPMN) [7]. This notation is an ISO/IEC 19510
standard [7] for a graphical representation of business process diagrams, facilitating the clear communication of internal business procedures and collaborations. The BPMN helps standardize response procedures across different parts of an organization or even across multiple organizations. This ensures that responses to hybrid threats are consistent and follow best practices, reducing the chances of errors and omissions during critical incidents. Standardized processes also make it easier to train new staff and scale operations. The standard offers formal guidelines and the best practices for visual models depicting informational workflow. For further details, refer to Appendix A.

Upon detecting an Infosec incident, the response phase of the Infosec lifecycle involves organized actions to contain, mitigate, and neutralize the threat. During this phase, Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) can be visualized in an Infosec Dashboard, facilitating real-time monitoring and automated incident responses. This capability is essential for reactive and proactive measures, allowing the decision makers to respond swiftly and effectively to security threats. For further details on reactive incident responses, the reader is referred to Appendix B. Visualizing such indicators in an Infosec Dashboard significantly improves threat detection and enhances the security and resilience of airport infrastructures against cyber threats.

The remainder of this paper is structured as follows. Section 2 views an airport as a system of systems, highlighting it as a critical infrastructure within smart city ecosystems. It details data exfiltration examples and scenarios illustrating vulnerabilities that hybrid threats could exploit. Section 3 emphasizes integrating data governance with Infosec to enhance security, safeguard sensitive information, and ensure reliable digital data in airports. This integration supports the proactive monitoring of threat vulnerabilities and effective incident responses using BPMN diagrams and standardized sequence flows to automate hybrid threat scenario simulations and improve threat detection. Section 4 presents findings to enhance hybrid threat detection and mitigation, stressing the need for robust data governance frameworks to address internal threats like information leakage. The impact of hybrid threats is illustrated with a case study. Section 5 concludes by stating that integrating data governance with the BPMN within the Infosec lifecycle automates response actions, enhancing defenses against hybrid threats. This alignment improves threat detection and response, and it also states that collaborative stakeholder engagement and proactive monitoring are crucial for effective threat mitigation and resilience against cyberattacks.

2. Nature of a Hybrid Attack for the Case of Critical Infrastructures

According to ISO 21839:2019 guidelines [8], an airport should be seen as a system of interconnected subsystems. This standard defines a system of systems as a collection of task-specific or dedicated systems collaborating to achieve capabilities beyond what any individual system can accomplish alone. This forms a cohesive and intricate entity composed of various interrelated components. An airport is, therefore, a complex system that manages interactions among numerous independent subsystems within a broader context.

These subsystems, including aircrafts, support vehicles, baggage handling machinery, control towers, and emergency services, can operate autonomously. However, for seamless airport functionality, they must harmonize and cooperate effectively [9]. Combining their resources makes these autonomous and potentially distributed systems form a unified, complex system susceptible to cascading effects (e.g., in the presence of hybrid threats). This interdependency means vulnerabilities in one subsystem can propagate throughout the network, increasing overall susceptibility to hybrid threats [10]. Three possible scenarios illustrating vulnerabilities within an airport system that hybrid threats could exploit are provided below:

1. Cyber–physical infrastructure vulnerability: malicious actors gain unauthorized access to the airport’s computer systems, including those managing flight scheduling, baggage handling, and air traffic control.
- Exploitation: a cyber intrusion might disrupt flight operations, leading to flight delays, cancellations, or misdirections. Simultaneously, physical sabotage can target the components of a critical infrastructure, such as power supply systems or communication networks.

- Consequence: the combined cyber–physical attack results in chaotic airport operations, potentially compromising passenger safety, causing economic losses, and undermining public trust in airport security measures.

2. Insider threats exploiting operational gaps: an insider with access to sensitive airport information collaborates with external threat actors.

- Exploitation: the insider provides information, access credentials, or physical access to critical areas to external actors, facilitating unauthorized access or tampering with airport systems.

- Consequence: this collaboration allows hybrid attackers to bypass conventional security measures, potentially leading to disruptions, theft, or damage to airport infrastructures. Insider involvement complicates threat detection and attribution, making mitigation and effective responses more challenging.

3. Supply chain vulnerability: airport procurement processes are compromised, allowing malicious actors to introduce compromised components or software into airport systems.

- Exploitation: malicious actors infiltrate the airport’s supply chain, introducing malware-infected equipment or compromised software during procurement or maintenance activities.

- Consequence: the compromised components or software create backdoors or vulnerabilities within airport systems, allowing attackers to exploit weaknesses, disrupt operations, or exfiltrate sensitive data. Supply chain compromises may remain undetected for extended periods, posing significant challenges for incident response and recovery efforts.

These three airport hybrid threat dimensions outline potential vulnerabilities with particular risks regarding data exfiltration, which can occur in two ways: through outsider attacks and via insider threats [11]. Table 1 provides examples of common types of data exfiltration. As cybercriminals’ methods for data exfiltration become more sophisticated, they can better evade detection [10,12,13]. Therefore, it is essential for organizations to closely monitor airport systems and implement continuous tracking mechanisms to detect and prevent data exfiltration effectively.

Data exfiltration presents a significant threat to organizations, risking sensitive data loss, operational disruptions, financial losses, and reputational harm [14]. These vulnerabilities are often exploited in hybrid attacks, making detection challenging due to sophisticated methods that mimic regular network traffic, evading detection for extended periods. Organizations require tools for the real-time detection of malicious network activity. Intrusion detection systems (IDSs) fulfill this role by monitoring network activity, identifying anomalies and potential threats, alerting administrators of suspicious behavior, and triggering automated responses, enabling swift threat analyses [15]. Combating data exfiltration demands proactive measures, including robust prevention strategies during the response phase. This entails deploying strong access controls, monitoring network traffic for anomalies, and providing comprehensive employee training.

Approaching a hybrid threat entails addressing it as a multidimensional and time-dependent problem [16]. Each dimension encompasses different actions of a different nature, with different durations and evolutions. In the context of a democratic nation, hybrid attacks manifest across specific dimensions, which may unfold concurrently or sequentially, each with its own duration. For instance, consider the following:

- Dimension 1: a disinformation campaign targeting European borders, promoting ideological extremism and violence, commencing in Month 1, with a duration of $x$ time units.
- Dimension 2: attack on critical infrastructures like airports or renewable energy facilities, leading to supply chain disruptions, beginning in Month 2, with a duration of \( y \) time units.
- Dimension 3: foreign investments in critical entities, starting in Month 3, with a duration of \( z \) time units.

**Table 1. Types of data exfiltration.**

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples of the Types of Data Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social engineering and phishing attacks</td>
<td>Social engineering and phishing deceive individuals into downloading malware or revealing account credentials. In social engineering, it may unknowingly surrender sensitive data or compromise security. Phishing emails mimic legitimate sources, luring recipients into clicking malicious attachments or entering credentials on spoofed websites, enabling malware injection or credential theft.</td>
</tr>
<tr>
<td>Outbound emails</td>
<td>Cybercriminals use emails to exfiltrate any data that sit on organizations’ outbound email systems, such as calendars, databases, images, and planning documents. These data can be stolen from email systems as email and text messages or through file attachments.</td>
</tr>
<tr>
<td>Downloads to insecure devices</td>
<td>This data exfiltration method poses an accidental insider threat. It occurs when a malicious actor accesses sensitive corporate data on a trusted device and transfers it to an insecure one, like a camera or smartphone lacking corporate security, risking data exfiltration.</td>
</tr>
<tr>
<td>Uploads to external devices</td>
<td>This type of data exfiltration typically comes from malicious insiders. The inside attacker can exfiltrate data by downloading information from a secure device and then uploading it onto an external device. This external device could be a laptop, smartphone, tablet, or thumb drive.</td>
</tr>
<tr>
<td>Human errors and non-secured behavior in the cloud</td>
<td>In this case, insecure cloud access poses data exfiltration risks, allowing malicious actors to manipulate virtual machines, deploy malware, and send malicious requests. Human errors and procedural issues compound the risk, potentially compromising protection measures.</td>
</tr>
</tbody>
</table>

These coordinated actions aim to exploit vulnerabilities within a country, undermining trust in its democratic system and security. This paper primarily delves into Dimension 2 of hybrid threats, where innovations that have been identified [17] to respond to hybrid threats include, among others, smart message routing and notification services such as the Emergency Message Content Router (EMCR). When applied in airport scenarios such as in the SATIE H2020 project (https://cordis.europa.eu/project/id/832969/results (accessed on 15 July 2024)), these tools facilitate communication and collaboration between airport operators and public safety agencies, enhancing response coordination during natural disasters or hybrid attacks. However, internal hybrid attacks and inadvertent support for such actions through negligence or errors necessitate additional consideration. The subsequent discussion elaborates on the benefits of integrating data governance, such as prompt response awareness, preemptive security escalation, and comprehensive logging for non-repudiation, which support response efforts and mitigate cascading effects in critical infrastructure attacks.

Section 3 provides an overview of the challenges in implementing response strategies within the Infosec lifecycle, particularly in complex systems like airports. Airports face unique challenges due to their size, traffic volume, and need for seamless operations. Additional difficulties include coordinating multiple stakeholders, integrating diverse security systems, and a real-time analysis of vast data to identify and mitigate threats in a swift manner. Effective response strategies must balance security and operational efficiency, which is challenging when isolating affected systems without disrupting services. Existing protocols and available skilled personnel further constrain rapid decision making and response actions. Despite these challenges, well-implemented response strategies can significantly mitigate incidents’ impacts by enabling prompt containment and neutralizing threats, ensuring airport operations’ safety and reliability.
3. Results Addressing the Governance of the Digital Information Landscape

Within the digital information landscape for CIs and emergency response scenarios, data governance involves understanding the content circulation patterns that underlie this landscape, thus tracing the trajectory of digital information dissemination during emergencies [18]. This enables the establishment of an accountable and verifiable ownership framework to form a chain of evidence at every stage of the data’s journey. It encompasses a comprehensive framework defining data management, use, protection, accuracy, and integrity. This data governance framework entails establishing policies, processes, and standards to ensure data protection and fitness for purpose, covering various aspects such as quality, security, privacy, and compliance with relevant regulations [19]. By creating a structured and consistent approach to data management, data governance enables decision makers to make informed decisions, maintain accuracy and integrity, and address risks associated with inaccurate information or the mishandling of data.

Efficient data governance relies on collaboration, clear communication, and defined roles for accountability. This framework includes processes to manage, protect, and monitor data, enforce policies, prevent unauthorized access, and maintain data accuracy through quality rules, integrity checks, and audits. Techniques like encryption, access controls, and lineage tracking safeguard data integrity and prevent unauthorized modifications. Integrity controls, such as checksum mechanisms or hash functions, detect alterations or inconsistencies, ensuring the trustworthiness of datasets [20].

In a scenario involving an international airport targeted by a hybrid attack, malicious actors disrupt operations through cyber intrusions and the physical sabotage of CIs. Stakeholders such as airport authorities, airlines, and security agencies must collaborate to coordinate their response efforts. Ensuring the integrity and authenticity of exchanged information is crucial to prevent misinformation and misinformed decision making. Establishing trusted frameworks for information exchange during emergencies involves verifying sources, tracking dissemination, and maintaining audit records. Airport authorities can leverage data governance protocols to authenticate security incident reports, while security agencies can ensure the integrity of collected digital evidence. Integrating data governance with Infosec enhances data confidentiality, integrity, and availability (i.e., following a CIA methodological approach); promotes standardized infrastructure protection; and improves emergency response coordination. This collaborative approach enhances response efficiency and aids in identifying false content sources, fostering a more informed digital information landscape.

Data governance and monetization emerge as essential concepts to combat information manipulation and ensure data reliability in a data-centric approach [20]. Another relevant concept relates to metadata and data categorization to establish accountability and maintain the integrity of digital information. An algorithmic analysis of individual behaviors, fueled by personal data, raises ethical concerns and underscores the importance of individual data privacy and governance [21]. Standardized chains of evidence bolster information integrity, fortify an emergency response, combat disinformation, and protect personal privacy in the digital information ecosystem.

3.1. Digital Information Security Framework

The Infosec lifecycle should be seen as a strategic framework guiding organizations in safeguarding digital assets and sensitive information across four phases. It enhances the response by lifting the security level and by offering accountability.

Figure 1 illustrates an Infosec strategy aiming to mitigate vulnerabilities and address diverse cyber threats throughout the lifecycle by utilizing security policies, software tools, and IT services in the prevention, detection, response, and knowledge management phases.
The BPMN provides a standardized tool for modeling workflows and decision points, enhancing situational awareness, ensuring compliance with security protocols, and identifying potential vulnerabilities. It is particularly valuable for analyzing hybrid threat response actions within the information security lifecycle, especially for critical infrastructures like airports. The BPMN enables organizations to swiftly adapt processes to emerging threats, ensuring response strategies remain relevant and effective. Table 2 details how this integration improves hybrid threat response actions. The BPMN’s flexibility allows for quick adaptations, maintaining robust and appropriate response strategies. It also enhances risk management and mitigation by mapping processes and prioritizing necessary security controls.

Table 2. Impacts of using BPMN in modeling the Infosec lifecycle when analyzing hybrid threats.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Added Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Comprehensive visualization and understanding</strong></td>
<td>The BPMN provides a standardized method for visualizing and understanding information flow and actions within complex processes. These standardized response procedures ensure consistency and best practices, which are crucial for effective threat mitigation. When applied to hybrid threats, this visualization allows stakeholders to see the entire threat detection, analysis, and response process. This holistic view helps identify potential vulnerabilities and bottlenecks that could be exploited in a hybrid attack.</td>
</tr>
<tr>
<td><strong>Enhanced coordination and communication</strong></td>
<td>Clear, standardized diagrams facilitate cohesive efforts across different teams and stakeholders in threat responses, enhancing coordination and communication. By having a common visual language, everyone from IT security teams to management can understand the processes and their roles, leading to better communication and coordinated response efforts.</td>
</tr>
<tr>
<td><strong>Scenario simulation and analysis</strong></td>
<td>Implementing standardized response procedures across different parts of an organization or across multiple organizations improves efficiency and adaptability by integrating with existing systems. This enables automated response actions based on predefined rules and events, leading to quicker responses to hybrid threats. Additionally, it allows for the simulation of various threat scenarios to analyze potential impacts and refine response plans. Testing “what-if” scenarios provides valuable insights into the resilience of the Infosec framework, enhancing preparedness for real-world incidents.</td>
</tr>
<tr>
<td><strong>Risk management and documentation</strong></td>
<td>The BPMN provides detailed, structured documentation of threat response processes, which is crucial for regulatory compliance and audits. It shows that the organization has well-defined procedures, aiding in post-incident analyses and improving processes through lessons learned. Additionally, the BPMN helps identify critical points for implementing or enhancing security controls. This proactive risk management approach addresses potential vulnerabilities before exploitation, creating tools for prioritizing risks based on their impact on business processes.</td>
</tr>
</tbody>
</table>

The BPMN offers unique advantages over other methodologies by providing clarity and precision through its graphical representations, which enhance our understanding of complex workflows. Its interdisciplinary integration capabilities allow for a unified view across IT, security, operations, and management, fostering effective collaboration.
Unlike static methodologies, the BPMN supports real-time process monitoring, ensuring ongoing insights and quick responses to new threats. Its scalability makes it ideal for critical infrastructures such as airports, promoting consistent and coordinated responses. The visual nature of the BPMN also improves training and awareness, helping employees understand their roles and responsibilities better, leading to quicker response times and improved preparedness. These benefits position the BPMN as a superior methodology for enhancing response actions to hybrid threats, ensuring the robust protection of CIs.

3.1.1. Prevent—Sets the Groundwork

During the prevention phase, the focus lies on proactively implementing measures to avert potential security breaches. It commences with identifying and mapping existing assets, marking the inception of the Infosec lifecycle by pinpointing data and information requiring protection. Following asset identification and documentation, a thorough security assessment is conducted, involving a review of current Standard Operating Procedures (SOPs) and vulnerability scans. This phase entails deploying robust security policies, conducting regular risk assessments, and implementing information security controls to establish a resilient defense against potential threats and vulnerabilities. This assessment includes analyzing physical infrastructures, human interactions with processes, and company policies.

Throughout prevention, security policies, controls, and processes are tailored based on established SOPs, addressing assets, vulnerabilities, and threats. Risks’ likelihood (i.e., the probability of the risk occurring) and impacts (i.e., the severity of the consequences if the risk does occur) are assessed, prioritizing resources to mitigate critical risks. Proactive adjustments influence detection and response activities, ensuring a dynamic strategy. In this phase, supply chain security, integral to supply chain management, addresses risks associated with external entities, logistics, and transportation. It aims to identify, analyze, and mitigate risks collaboratively with supply chain stakeholders, aligning with risk management principles to implement appropriate mitigation actions encompassing both physical security and cybersecurity.

3.1.2. Detect—Identifies Security Incidents

Detection involves promptly recognizing security incidents, enabling the timely identification and notification of compromises. This proactive approach facilitates a swift stakeholder response to emerging threats, minimizing the impact of Infosec incidents. Essential to this process is the continuous monitoring of network activities, log analyses, and intrusion detection systems, which are pivotal in identifying attack signatures, file or configuration changes, and suspicious activities. In this phase, the Infosec strategy aligns with CIA methodology, integrating risk management and legal regulations to define policies, procedures, and principles within a broader cybersecurity program. Guided by risk assessments, Infosec deploys SOPs and establishes business processes to protect information assets across formats and states. Regular risk monitoring and continuous updates to treatment plans are essential given the dynamic landscape of emerging assets, vulnerabilities, threats (including hybrid ones), and controls. The primary objective is to identify, track, and document attacks, with the detection system providing detailed alerts and reports regarding unauthorized data transfers and access attempts. Ultimately, this phase aims to strengthen the information security infrastructure, aligning it with established information security policies.

3.1.3. Response—Addresses Incidents in Real-Time

The response phase commences upon detecting an Infosec incident and involves swift, organized actions to contain, mitigate, and neutralize the threat. This may include isolating affected systems, investigating the incident’s nature, and executing predefined incident response plans. An effective response strategy aims to minimize impacts and prevent escalations, highlighting the importance of timely reactions for the detection process to be
valuable. Therefore, incident responses should be meticulously planned, with a written and management-ratified plan prioritizing event types and adopting either a preventive or reactive approach, specifying notification and response levels proportional to the threat’s severity. A reactive incident response waits for visible signs of intrusion (e.g., triggered by IoCs) before taking action, addressing known risks after they occur. In contrast, a proactive incident response preemptively tries to find weaknesses (e.g., by analyzing IoAs through simulation modeling). It enhances processes to spot threats beforehand, identifying and addressing security issues before they escalate and prioritizing preparations for an attack rather than reacting to it.

3.1.4. Knowledge Management—Ensures Ongoing Resilience and Improvement

Analyzing and reporting incidents after they occur is essential to strengthening the Infosec cycle. Decision makers gain valuable insights by investigating who, what, where, why, and when aspects, thereby improving their understanding of Infosec risk management and avoiding uninformed future decisions. This process can lead to the development of new contingency plans to address vulnerabilities not covered by existing SOPs. Knowledge management practices optimize information utilization, accessibility, and storage, refining security strategies based on risk assessments regarding CIA methodology. The final stage of the lifecycle involves monitoring existing security measures; adapting to new threats; and adjusting prevention, detection, and response actions through SOP reviews or creations. By integrating lessons learned from both physical and cybersecurity issues, this comprehensive knowledge management approach ensures faster response times and effective threat mitigation, thus promoting robust business continuity.

3.2. Application of Data Governance for the Response Phase

A Business Process Diagram (BPD) serves as a versatile tool to depict the data sequence flow during the Infosec response phase while modeling actions to automate the handling of IoCs for reactive incident responses. Additionally, it can represent the automatic prioritization of IoAs for proactive incident responses. As outlined in Figure 2, by incorporating appropriate BPMN elements, the diagram can visually illustrate the data flow through the stages of the incident response process. Through this visualization, organizations can streamline their response processes, ensure the timely identification of the digital assets to audit and take proper response actions to security incidents, and effectively manage both reactive and proactive strategies to address emerging threats.
A business process encompasses coordinated activities within organizational and technical settings to achieve a specific goal, such as those required during the Infosec–response phase. The BPMN aims to standardize process modeling and notation, catering to various perspectives and modeling approaches [22]. It offers a user-friendly notation accessible to business analysts, technical developers, and managerial stakeholders [23]. A business rule activity (e.g., A1–A4) models process flow governance, standardizes decision tree diagrams, and automates business logic through decision tables and analytical expressions.

Figure 3 illustrates the standardized sequence flow for subprocess A5, focusing on a reactive incident response triggered by IoCs due to perceived intrusions. Table A2 provides examples of IoCs that could impact airport operations during a cyber threat. By displaying these IoCs on an Infosec Dashboard, airport authorities can monitor real-time threats and automate appropriate responses, ensuring the integrity and security of airport operations.

Given the known Infosec risks, external stakeholders may need to be informed to activate countermeasures, such as generic Infosec controls. This keeps stakeholders synchronized and ready for incident resolutions and activates constant tracking mechanisms to monitor suspicious actions. Coordinated reactions aim to mitigate the operational impact of threats and track vulnerabilities, particularly concerning data exfiltration. Decision makers can monitor incident responses by analyzing progress through data visualization tools like an Infosec Dashboard.

A model-driven simulation diagram is dynamically activated for the proactive response approach to automate platform-independent simulations of potential hybrid threat scenarios. Figure 4 shows the standardized sequence flow for subprocess A6 (presented in Figure 2), which focuses on proactive responses to potential threats. This process identifies possible hybrid threats and can activate descriptive actions to test the system’s capability to respond to known Infosec situations. It can also trigger predictive actions based on data analysis models to identify potential vulnerabilities or create Infosec hypotheses to test the system’s reaction capability. These situations can be managed separately or combined to further challenge the system’s response capabilities. In such simulations, strength tests...
monitor the Infosec controls activated as the severity level increases, providing decision makers with information on potential vulnerabilities that require attention. The focus is on IoAs, displayed on the Infosec Dashboard, and their impact on airport security operations.

![Diagram of subprocess A6—proactive incident simulation response.](image)

Integrating data governance with business process management (BPM) presents a promising strategy for tracking the path of digital information dissemination during emergencies. Robust data governance establishes strict policies governing data management and integrity, including clear guidelines for data access, usage, and quality standards. Concurrently, BPM offers a structured framework for visualizing end-to-end business processes, ensuring a comprehensive understanding of information flow during emergencies, particularly in cross-border scenarios.

This integrated approach enhances visibility into data sources, strengthens data quality and integrity, and addresses both internal and external threats. Along with BPM, data governance incorporates cybersecurity measures into processes, bolstering resilience against cyber threats, which can be a dimension of a hybrid threat. Additionally, it manages risks associated with compromised data from external sources, facilitating secure data exchange protocols. The integration extends to resilience planning, establishing response strategies for data-related incidents and addressing vulnerabilities arising from personnel knowledge gaps through embedded training initiatives within BPM processes. Aligning data management practices with dynamic business processes creates a holistic strategy for tracking digital information dissemination during emergencies, fostering adaptive and resilient emergency response capabilities. Improved efficiency metrics resulting from this approach may include cost reductions from attack avoidance and reduced response times through scenario simulations for better preparedness plans.

4. Discussion

In safeguarding CIs from the intricate challenges posed by hybrid threats, a central research challenge lies in formulating holistic strategies within the digital landscape. The vulnerability dimensions revealed by data governance are manifold. Internally, risks stem from potential data leaks or breaches initiated by insiders, incorporating aspects of human behavior, errors, negligence, or intentional malicious actions (Internal Threats). This dimension also extends to risks involving compromised data affecting decision-making processes due to data integrity and quality issues, aggravated by vulnerabilities in the supporting digital systems and networks (Cybersecurity Weaknesses).

Supply chain vulnerabilities pose an additional dimension, introducing risks associated with compromised data from third-party providers or partners. Inadequate resilience
measures, including the absence of response plans and recovery strategies, constitute another data governance vulnerability (Insufficient Resilience). The absence of knowledge and training among personnel regarding data governance and cybersecurity practices introduces vulnerabilities that hybrid threats could exploit (Lack of Situational Awareness).

Several authors have studied supply chain disruption risks, while the pandemic stimulated further research. The study in [21] analyzed a supply chain disruption recovery problem in the COVID-19 pandemic with supply disruption risks and manufacturer capacity fluctuations in a four-tier supply chain with make-to-order manufacturing. It was shown that when the number of disrupted suppliers is high, the manufacturer adopts a combination of emergency procurement and product design changes. These types of solutions support the manufacturers in establishing an optimal recovery strategy whenever the supply chain system experiences supply disruptions, which is especially relevant in times of a pandemic or war. It is, however, also important to note that data governance can offer further support by fortifying the CI in cases of supply chain disruptions, such as studying possible vulnerabilities arising from emergency procurement.

Interconnected CI systems also might create vulnerabilities, as a threat to one system may trigger cascading effects on others, and this is further intensified in cases of a supply chain disruption problem. The CIs’ interdependence raises concerns in cases of non-compliance with data standards, protection, and privacy regulations, leading to potential legal consequences and reputational damage. Addressing these dimensions is imperative for formulating effective strategies to fortify CIs against the multifaceted challenges of hybrid threats.

Furthermore, it should be highlighted that the inherent dimension of data governance threats originates within the organization. Acknowledging internal threats underscores the significant probability of information leakage from internal resources, either intentionally or unintentionally, emphasizing the need for data governance frameworks to address and preemptively manage threats that may arise from internal sources, thereby enhancing the overall resilience of CIs against hybrid threats.

Leveraging data governance in conjunction with business process management is a strategic approach aimed at enhancing the detection and mitigation of hybrid threat incidents, particularly those targeting vulnerabilities within internal CIs.

4.1. Social, Environmental, and Other Impacts

A potential hybrid attack on a CI can have, if successful, a series of negative impacts. These primarily include endangerment and harm to human lives. Disasters, especially in the case of CBRNE, can also influence mortality for weeks, months, or years in the future and can cause cascading effects on physical and mental health [24]. Additionally, severe environmental damages are expected after an attack, especially in cases of CBRNE CIs, with immeasurable consequences. Furthermore, substantial economic losses are expected in the medium and long term for the CI, the affiliated economic entities, and the local society that economically depends on the CI. For example, an airport as a system of systems can host various small SMEs, which, in turn, can be supplied by several other economic entities, all of which will be negatively affected. In addition, besides direct economic damages, the credibility of a CI after an attack will be severely damaged. It should also be mentioned that the insufficient preparedness of CIs has amplified the consequences of extreme events in the past [25]. Considering the cascading effects of other interconnected CIs, the negative impact on the stability and autonomy of the region can also be significant. Therefore, it remains relevant to investigate measures to increase CI preparedness continuously.

In the face of rising hybrid threats, smart airports must adopt a cross-border data-centric approach to ensure robust cybersecurity measures. A data governance framework will provide an airport bustling with activity the digital and physical means to intertwine in a seamless orchestration, defining business rules and establishing or adopting standardized policies, together with roles and responsibilities to ensure seamless data exchanges between various stakeholders, including airport authorities, airlines, security agencies, and
regulatory bodies. By aligning with EU regulations such as GDPR and the NIS Directive, airports can create a unified defense mechanism that enhances the detection and mitigation of threats.

Considering an airport facing a cyber-attack, where hackers aim to disrupt vital systems like flight schedules and baggage handling, close coordination with EU authorities becomes crucial to mitigate these risks effectively. Furthermore, airports can strengthen their resilience against hybrid threats through joint cybersecurity exercises and simulations. This collaboration enables the sharing of threat intelligence, aligns cybersecurity measures, and ensures swift and efficient responses to incidents. Moreover, centralized monitoring systems, integrating data from diverse sources, offer a comprehensive, real-time view of potential threats.

Establishing a regulatory framework with rigorous controls and audit procedures becomes imperative to maintain data integrity and compliance. Stringent access controls limit data access to authorized personnel, mitigating insider threats. Continuous data integrity checks and regular audits uphold data accuracy and trustworthiness, bolstering the airport’s overall security posture. This proactive approach safeguards critical systems and cultivates a collaborative environment where information seamlessly flows across borders, enhancing the capacity to counter hybrid threats.

By promoting a unified view of potential threats through shared threat intelligence and collaborative response mechanisms, smart airports fortify their cybersecurity posture. This integrated approach ensures operations’ security and data protection, fostering trust in the airport’s ability to safeguard its critical infrastructure from hybrid threats. Implementing these strategies establishes a robust defense against cascading hybrid threats. Through concerted regulatory efforts, enhanced coordination with EU authorities, and the utilization of centralized monitoring systems, smart airports can preemptively mitigate risks and ensure uninterrupted operations, fortifying themselves against cyber-attacks and preserving the aviation ecosystem’s integrity and security.

4.2. Prevention of Cascading Effects

An important dimension of the problem relates to cascading effects and the multiplying catastrophic impacts on European security and autonomy. Accustomed to risk-based decisions, insurance companies were among the first to point out that CIs operated in isolation just decades ago, with no apparent risk of a chain reaction in the case of an attack. However, their operation is now geographically interconnected and across sectors [26]. The Directive 2022/2555 [27] emphasizes the growing vulnerability of small- and medium-sized enterprises (SMEs) to supply chain attacks in the European Union. These attacks exploit SMEs’ comparatively lax cybersecurity risk management measures, notably concerning risks associated with their supply chain and relationships with data storage providers.

The dependencies between CIs have been defined as a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated with the state of the other [28]. In this work, the authors examined, in detail, four principal classes of interdependencies: physical, cyber, geographic, and logical. Suo et al. [29] proposed a decision-support method for CI risk assessments, holistically considering complexity, dual interdependency, vulnerability, and uncertainty. The authors analyzed three types of CI interdependencies, geographic, functional, and stochastic, treating CIs as a system of systems to model their interdependent network structure. Figure 5 illustrates a hypothetical impact assessment result for interdependent CI airports, displaying interdependencies with straight lines and color-coded assets representing the severity of potential damages. This scenario extends to multiple EU airports with functional interdependencies affecting the supply chain, such as connecting passenger or cargo flights. Figure 5 visualizes the significant impact of cascading effects from a hybrid attack on airports and local and European economies. Integrating data governance can enhance CI resilience by bolstering threat prevention, detection, response, and mitigation, thereby mitigating the impact of cascading effects.
The problem of risk assessments of CIs is continuously being studied, and recent work [30] provides a comprehensive approach for analyzing and evaluating risks of CIs, offering tools for decision makers to ensure the resilience and security of CIs.

4.3. Case Study

The data governance strategies in this case study address internal and external threats to critical infrastructures like airports. They prevent information leakage, detect insider threats, and include personnel training initiatives for internal threats. Strict policies, access controls, automated monitoring, encryption, and lineage tracking help identify and prevent suspicious activities. Training initiatives within business process management address vulnerabilities from personnel knowledge gaps, ensuring employees are well-versed in data security protocols.

The focus is on preventing data exfiltration and bolstering cybersecurity measures for external threats. Robust system monitoring, continuous tracking, and advanced detection tools protect sensitive information from unauthorized access and exfiltration attempts. Data governance frameworks integrate cybersecurity measures, including security policies, intrusion detection software, and secure data exchange protocols, to safeguard against malicious activities targeting CIs. The Digital Twin concept facilitates real-time monitoring and scenario simulations, improving the organization’s capacity to identify and mitigate security threats proactively. By creating a virtual replica of an airport’s critical infrastructure, Digital Twins allows for the continuous observation and analysis of operations. This combination of strategies strengthens defenses against hybrid threats from internal and external sources, ensuring quicker and more efficient responses and streamlined stakeholder actions.

Additionally, indicators such as IoCs and IoAs can be used to trigger alerts. These alerts provide timely insights into potential threats, enabling the security team to simulate various attack scenarios and devise effective countermeasures, in particular because of the following:

- In a real-world scenario, airports have utilized IoCs to prevent hybrid threats by identifying malicious activities early. For instance, during a cyberattack on an airport’s
baggage handling system, the Infosec Dashboard detected unusual network traffic patterns and unauthorized access attempts, which are typical IoCs. By analyzing these indicators, the security team identified a malware infection attempting to disrupt operations. Swiftly isolating affected systems and implementing containment measures prevented widespread disruption. The Infosec Dashboard provided real-time alerts and detailed reports, enabling the team to trace the malware’s origin and block similar future attacks, thus safeguarding the airport’s critical infrastructure. As explained in Figure 4, external stakeholders are notified of the incident (A.6.8) and receive information to prevent supply chain disruptions, which are cascading effects.

- Similarly, IoAs have been employed to mitigate threats by focusing on the methods and tactics used by attackers. When an airport faced a coordinated physical and cyberattack, the Infosec Dashboard identified IoAs, such as repeated failed login attempts, phishing emails targeting airport staff, and unusual user behavior patterns. These indicators highlighted an impending attack, prompting the airport’s security team to activate incident response plans. Enhanced physical security measures and immediate cybersecurity protocols, such as enforcing multi-factor authentication and conducting staff training on recognizing phishing attempts, were implemented. This proactive approach, guided by IoAs, enabled the airport to thwart the attack, ensuring passenger safety and operational continuity.

The IoCs and IoAs discussed above, which are triggered by IDS tools, can be introduced as alerts in a Converged Security Information Management System (CSIM). The ENGAGE CSIM software developed by Satways Ltd. has been deployed by several public safety agencies and has been validated by various end users for its provided functionalities and its user-friendly Graphical User Interface. In this system, alerts received by the IDS can be prioritized based on rules provided by the end user. Additionally, a list of suggested actions for managing these alerts can be proposed to the operator assigned by the end user, according to the latter’s Standard Operational Procedures. These procedures are integrated into the ENGAGE system and are mapped to specific alarm types. It is important to note that, during an emergency situation, the collaboration among the various operators of the entity that is experiencing the incident, but also among the operators of other public safety agencies that are involved in handling the specific incident (event), is crucial for an effective response. The ENGAGE platform offers an advanced collaboration functionality and supports two modes of collaboration and communication: (i) among the entity’s operators that have access to a specific event as well as (ii) among the entity’s operators and operators of other public safety agencies that are involved in a specific event.

The collaboration perspective of the ENGAGE platform includes a map depicting all the geolocated operational information related to the specific event and an area where the information-sharing functionality is provided. Apart from exchanging text messages, the users—both the entity’s operators and users from other public safety agencies involved in the specific incident (event)—can add geolocated information directly on the map. The map itself and the information shared on it are very useful for response activities in that they enhance users’ situational awareness.

The sharing of operational information among the agencies involved in a specific situation can be enabled by the Emergency Message Content Router, a smart message routing and notification service provided by Satways Ltd. The routing of the information is based on international standards, ensuring the interoperability of the service and the information that is shared. Access to the information is based on specific rules, thus ensuring that only the agencies and the personnel with the related responsibilities and access rights will receive the information.

For the case of airports discussed above, SATWAYS has further developed the ENGAGE software for the SATIE H2020 project. In this new version of the software, named the Crisis Alerting System [17], any identified incident is forwarded from the Security Operation Centre (SOC) to the Airport Operation Centre (AOC) and specifically to the Crisis Alerting System (CAS). The CAS is installed at the airport’s AOC, providing AOC
operators with a system that supports decision-making and incident management processes and improves their efficiency. The CAS offers a smart notification and alerting service based on operational rules, among several other functionalities. It enables information sharing among involved actors at every level of coordination, enabling a collaborative response. At the same time, it supports multichannel alerting of passengers and the possibly affected population, with content varying according to their location.

5. Conclusions

This study examines hybrid threats as complex and time-sensitive challenges, focusing on potential attacks targeting CIs such as airports. It investigates how Data Governance aids CIs throughout the crisis management cycle by establishing a chain of evidence to validate information integrity and ensure reliable data transmission to stakeholders, particularly those overseeing field operations and decision-making processes. Maintaining information accuracy and integrity is challenging without a data governance framework, leaving systems vulnerable to undetected suspicious activities and potential regulatory repercussions. Proactive data governance facilitates the prompt identification and resolution of discrepancies, thereby mitigating risks associated with hybrid threats. Measures such as automated access controls, encryption, and lineage tracking should be implemented to protect data from unauthorized alterations or inaccuracies. This study presents three airport hybrid threat scenarios to underscore potential vulnerabilities, especially concerning data exfiltration risks from external attacks or insider breaches, both of which pose significant threats. Organizations must ensure the robust monitoring of airport systems and employ continuous tracking mechanisms to prevent data exfiltration effectively. Investing in prevention strategies and advanced detection tools enhances organizations’ capacity to identify and address risks, safeguarding sensitive information and network infrastructure against evolving threats.

Integrating data governance with the BPMN within the Infosec lifecycle automates response actions based on predefined rules, enhancing defenses against hybrid threats targeting critical infrastructures. This integration allows for real-time detection and immediate, standardized responses to threats from internal and external sources. It ensures consistent, scalable, and adaptable security processes; improves monitoring; and provides comprehensive documentation for post-incident analyses. The visual clarity of the BPMN facilitates cross-functional and cross-border coordination, making it a robust framework for managing complex security challenges effectively.

This paper explains that a standardized chain of evidence strengthens information integrity, emergency responses, disinformation countermeasures, and individual privacy within the digital information ecosystem. Business process diagrams visually represent information workflows, facilitating clear communication and modeling. They serve as a reference tool to model the Infosec lifecycle, particularly addressing security aspects to strengthen defenses against evolving threats. The BPMN, a standard for modeling business processes, bridges business and technical users, fostering effective collaboration and aligning with a Digital Twin approach to model the airport ecosystem’s data governance impact during hybrid attacks. The Digital Twin approach offers an innovative contribution to a regulatory landscape with rigorous controls and audit procedures by creating a precise virtual replica of an airport’s assets. This enables real-time monitoring and scenario simulations, allowing the proactive identification and mitigation of security threats. Being continuously updated with real-time data, Digital Twin helps decision makers simulate hybrid threat scenarios, analyze vulnerabilities, validate data integrity, and ensure regulatory compliance through automated audits. This dynamic model enhances decision making and risk management, providing a robust framework for stringent data governance and reinforcing smart airports’ overall security posture against hybrid threats. Additionally, implementing synchronized reactive responses within the Infosec lifecycle enhances the ability to address visible signs of intrusion and indicators of compromise, thereby improving the security and resilience of airport infrastructures against cyber threats.
The BPMN examples demonstrate how to enhance breach detection and accurately attribute attacks, serving as effective countermeasures against hybrid threats. Existing research focuses on analyzing accountability and the impact of disinformation, providing insights into unintended recipients. Similarly, research in the data governance field has contributed to streamlining the establishment of transparent, accurate, and compliant data management policies, enabling coordinated efforts to mitigate risks, address security incidents, and maintain airport operations’ integrity. Integrating data governance with the BPMN allows organizations to track hybrid threats and effectively establish a resilient security posture. This alignment of data management with dynamic business processes enhances threat detection, accountability, and response capabilities. From a data exfiltration perspective, ensuring data privacy and governance is crucial for mitigating risks from unauthorized interventions. These controls protect data rights and ensure the accuracy and reliability of digital information.

Author Contributions: Conceptualization, G.P. and S.S.; Methodology, G.P.; Investigation, G.P.; Writing—review & editing, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This project received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement no. 883054. This article reflects only the authors’ views, and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Author Gabriel Pestana was employed by the company INOV—INESC Inovação. Author Souzanna Sofou was employed by the company SATWAYS Ltd. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A. BPMN Core Elements and Symbols

The primary purpose of the BPMN is to create clear and understandable business process flowcharts, serving as a common language for stakeholders. It visually represents process steps, aiding comprehension for business users and facilitating decision-making and situational awareness improvements. It bridges gaps in business process management stages, fostering collaboration among stakeholders. As a standard process modeling language, the BPMN uses various symbols and elements, detailed in Table 1, to depict process aspects.

Table A1. Core modeling elements depicted by the notation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>An event (represented by a circle) is something that “happens” during the course of a business process. An event affects the flow of the process and usually has a cause (trigger) or an impact (result). Event markers are circles with open centers to represent different actions (triggers or results). There are three types of events, based on when they affect the flow: Start, Intermediate, and End. Start events can only react to a response (“catch”) to a trigger (incoming action/input). Intermediate events can catch or throw triggers. For events that catch, the markers are unfilled, and for events that throw, the markers are filled. End events can react to sending (“throw”) a trigger (outgoing result/output) from a sequence flow path ending.</td>
</tr>
</tbody>
</table>

| Start | Intermediate Link | Intermediate Throw Link | Intermediate Conditional | End | Escalation |
Table A1. Cont.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>An activity, represented by a rounded-corner rectangle, encompasses generic work to be performed, with two types: a standard activity and a subprocess (identified with a plus sign). Activities with a subprocess marker behave like normal processes once instantiated. They encapsulate processes modeled by activities, gateways, events, and sequence flows. Subprocesses allow complex processes to be split into levels, focusing on specific areas in a single diagram. The business rule activity interfaces with a business rule engine, facilitating input and output exchanges. Loop-marked activities serve as wrappers for inner activities executed multiple times. A call activity references an externally defined activity, fostering reusable process definitions across various processes. Flow objects connected by sequence flows (solid lines with arrowheads) structure business processes in diagrams. Activities can also link to data stores (represented by cylinders) for persistent data. A data store is somewhere where the process can read or write data that persist beyond the process’s scope.</td>
</tr>
<tr>
<td>Gateway</td>
<td>A gateway, depicted as a diamond shape, controls the divergence and convergence of sequence flows, influencing traditional decisions and managing forking and merging path joining. Internal markers denote behavior control types. A diverging Exclusive Gateway (XOR Decision) creates alternative paths in a process flow, where only one path is taken for a given instance. In contrast, a diverging Inclusive Gateway (OR Decision) allows multiple paths with true evaluations, considering each as independent. Default paths, marked by “/”, ensure at least one path is taken if no valid conditions exist. An event-based gateway signifies a process branching point where alternative paths depend on events rather than condition expressions. A specific event, typically a message receipt, determines the chosen path.</td>
</tr>
<tr>
<td>Pool</td>
<td>A pool is the graphical representation of a participant (e.g., stakeholder). It also acts as a “swimlane” and a graphical container for partitioning a set of activities from other pools, usually in the context of B2B situations. A pool can have internal details (whitebox pool) in the process that will be executed, or a pool can have no internal information (blackbox pool) used to model an external participant. Lanes describe who executes a specific set of activities, meaning that a lane represents sub-entities that appear inside the pool lane. A BPMN diagram can contain one or more pools, with all the other objects placed in each lane of the process pool.</td>
</tr>
</tbody>
</table>

Appendix B. Examples of Indicators of Compromise

Table A2 presents five examples of indicators of compromise (IoCs) that can be presented in an Infosec Dashboard to monitor and automate the handling of IoCs for reactive incident responses within an airport infrastructure. By presenting these IoCs on an Infosec Dashboard, airport authorities can monitor real-time threats and automate appropriate responses to mitigate risks promptly, ensuring the integrity and security of airport operations.

Table A2. Examples of perceived IoC intrusions.

| Unusual network traffic patterns: sudden increases in network traffic or unexpected outbound connections to unknown IP addresses. |
| Automated response: trigger alerts, block suspicious outbound connections, and initiate packet captures for further analyses. |
| Reactive responses: |
| ● Network isolation: automatically isolate affected segments to prevent further spreads. |
| ● Traffic analysis: initiate a deep packet inspection to identify the nature of the traffic. |
| ● Alerting: notify network security teams to investigate further. |
| ● Blocking: block suspicious IP addresses and ports. |
Table A2. Cont.

<table>
<thead>
<tr>
<th>Unauthorized access attempts: multiple failed login attempts or access from unexpected geographic locations.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated response:</strong> lock affected user accounts, alert security personnel, and log all attempts for forensic analyses.</td>
</tr>
<tr>
<td><strong>Reactive responses:</strong></td>
</tr>
<tr>
<td>- Account lockout: automatically lock affected accounts after a predefined number of failed attempts.</td>
</tr>
<tr>
<td>- Geolocation blocking: block access from suspicious geographic locations.</td>
</tr>
<tr>
<td>- Multi-factor authentication (MFA): enforce MFA for all subsequent login attempts.</td>
</tr>
<tr>
<td>- Incident reporting: alert the security operations center (SOC) and log all details for a forensic investigation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware detection: detection of malware signatures on critical systems or endpoints within the airport network.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated response:</strong> isolate infected systems, initiate automated malware-removal procedures, and conduct a network-wide scan for further infections.</td>
</tr>
<tr>
<td><strong>Reactive responses:</strong></td>
</tr>
<tr>
<td>- System quarantine: automatically quarantine infected systems to prevent lateral movements.</td>
</tr>
<tr>
<td>- Network scanning: perform a network-wide scan to identify other potentially infected systems.</td>
</tr>
<tr>
<td>- Threat intelligence sharing: share the malware signatures with external security partners and agencies for broader awareness.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unapproved configuration changes: unauthorized changes to system configurations, firewall settings, or security policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated response:</strong> rollback unauthorized changes, alert IT administrators, and perform an audit to identify the source of the change.</td>
</tr>
<tr>
<td><strong>Reactive responses:</strong></td>
</tr>
<tr>
<td>- Configuration rollback: automatically revert systems to the last known good configuration.</td>
</tr>
<tr>
<td>- Audit trail: conduct an audit to identify who made the changes and how.</td>
</tr>
<tr>
<td>- Access review: review and update access controls and permissions.</td>
</tr>
<tr>
<td>- Real-time alerts: notify administrators and security personnel about the unauthorized changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data exfiltration indicators: large volumes of data being transferred to external locations or unusual data access patterns.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated response:</strong> halt data transfers, alert data protection officers, and implement data loss prevention measures to prevent further exfiltration.</td>
</tr>
<tr>
<td><strong>Reactive responses:</strong></td>
</tr>
<tr>
<td>- Data transfer halt: automatically stop data transfers to unapproved locations.</td>
</tr>
<tr>
<td>- Data loss prevention enforcement: apply data loss prevention policies to prevent further data leakage.</td>
</tr>
<tr>
<td>- Forensic analysis: launch a forensic investigation to understand the scope and source of the exfiltration.</td>
</tr>
<tr>
<td>- Stakeholder notification: alert key stakeholders, including data protection officers and legal teams, to prepare for potential regulatory actions.</td>
</tr>
</tbody>
</table>

The listed IoCs can be categorized into three recommendations for synchronized Infosec reactive responses to visible signs of intrusion. Each IoC is mapped to specific threats to an airport infrastructure:

1. **Implement automated threat detection systems:** This recommendation deploys advanced intrusion detection systems, security information, and event management solutions to automatically detect and alert security teams to potential intrusions and IoCs. For example, it is used to monitor network traffic for anomalies, such as unexpected outgoing connections to suspicious domains or unusual patterns in data transfer rates.
   - Unauthorized access attempts: security plans can provide step-by-step responses to handle unauthorized access.
   - Unapproved configuration changes: security plans can detail the actions to revert unauthorized changes and secure configurations.
   - Data exfiltration indicators: security plans can guide data exfiltration incidents’ containment and investigation processes.

2. **Establish incident response playbooks:** Develop comprehensive security plans tailored to airport infrastructure threats. These playbooks should outline step-by-step
procedures for identifying, containing, and mitigating security incidents, including procedures for addressing common IoCs. For instance, the security plan could include predefined actions for responding to indicators such as unauthorized access attempts, malware infections, or unusual network activity.

- Unauthorized access attempts: security plans can provide step-by-step responses to handle unauthorized access.
- Unapproved configuration changes: security plans can detail the actions to revert unauthorized changes and secure configurations.
- Data exfiltration indicators: security plans can guide the containment and investigation processes for data exfiltration incidents.

3. Enhance cross-agency collaboration: Foster collaboration and information sharing between airport security teams, law enforcement agencies, and relevant government organizations to ensure a coordinated response to security threats. Establishing real-time channels for sharing threat intelligence and IoC data can enable faster detections and responses to security incidents. For example, sharing IoCs such as suspicious IP addresses, domain names associated with phishing campaigns, or malware signatures can help identify and neutralize threats more effectively across airport infrastructures.

- Unusual network traffic patterns: collaboration can help identify whether unusual patterns are part of a larger attack affecting multiple agencies.
- Unauthorized access attempts: sharing information about access attempts can help other agencies recognize and defend against similar attempts.
- Malware detection: collaborative efforts can lead to the quicker identification and mitigation of widespread malware threats.
- Data exfiltration indicators: coordinated responses can help track and prevent data exfiltration across interconnected systems and agencies.

References


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.