information

IMPACT FACTOR 3.1

CITESCORE 5.8

Article

QISS: Quantum-Enhanced Sustainable Security Incident Handling in the IoT

Carlos Blanco, Antonio Santos-Olmo and Luis Enrique Sánchez

Special Issue

Quantum Information Processing and Machine Learning

Edited by

Dr. Wenbin Yu, Dr. Yadang Chen and Dr. Chengjun Zhang

MDPI

https://doi.org/10.3390/info15040181

information

Article

QISS: Quantum-Enhanced Sustainable Security Incident Handling in the IoT

Carlos Blanco [1,*,†], Antonio Santos-Olmo [2,†] and Luis Enrique Sánchez [2,†]

[1] Department of Computer Science and Electronics, University of Cantabria, 39005 Santander, Spain
[2] Techonologies and Information Systems Department, University of Castilla-La Mancha, 13071 Ciudad Real, Spain; antonio.santosolmo@uclm.es (A.S.-O.); luise.sanchez@uclm.es (L.E.S.)
* Correspondence: carlos.blanco@unican.es
† These authors contributed equally to this work.

Abstract: As the Internet of Things (IoT) becomes more integral across diverse sectors, including healthcare, energy provision and industrial automation, the exposure to cyber vulnerabilities and potential attacks increases accordingly. Facing these challenges, the essential function of an Information Security Management System (ISMS) in safeguarding vital information assets comes to the fore. Within this framework, risk management is key, tasked with the responsibility of adequately restoring the system in the event of a cybersecurity incident and evaluating potential response options. To achieve this, the ISMS must evaluate what is the best response. The time to implement a course of action must be considered, as the period required to restore the ISMS is a crucial factor. However, in an environmentally conscious world, the sustainability dimension should also be considered to choose more sustainable responses. This paper marks a notable advancement in the fields of risk management and incident response, integrating security measures with the wider goals of sustainability and corporate responsibility. It introduces a strategy for handling cybersecurity incidents that considers both the response time and sustainability. This approach provides the flexibility to prioritize either the response time, sustainability or a balanced mix of both, according to specific preferences, and subsequently identifies the most suitable actions to re-secure the system. Employing a quantum methodology, it guarantees reliable and consistent response times, independent of the incident volume. The practical application of this novel method through our framework, MARISMA, is demonstrated in real-world scenarios, underscoring its efficacy and significance in the contemporary landscape of risk management.

Keywords: cybersecurity; sustainability; incident response; quantum programming; quantum annealing

Citation: Blanco, C.; Santos-Olmo, A.; Sánchez, L.E. QISS: Quantum-Enhanced Sustainable Security Incident Handling in the IoT. *Information* **2024**, *15*, 181. https://doi.org/10.3390/info15040181

Academic Editors: Wenbin Yu, Yadang Chen and Chengjun Zhang

Received: 18 February 2024
Revised: 22 March 2024
Accepted: 25 March 2024
Published: 27 March 2024

1. Introduction

In current society, Cyber-Physical System (CPS) and Internet of Things (IoT) environments play an increasingly important role. These connected devices enable interaction between the physical and digital worlds. They include computing, storage and communication functions that enable them to manage objects in the physical world [1,2] and provide services that deliver significant benefits in numerous areas such as healthcare, energy supply, transportation, industrial automation and smart homes [3–6].

However, their fast evolution and adoption has led to many of them being designed and launched into the market without adequate attention to security aspects, resulting in an increased number of vulnerabilities that can be exploited by malicious actors. In addition, the wide variety and large number of connected devices further increase the threat landscape. From security cameras and smart home appliances to vehicles and industrial systems, all these devices can be potential targets for cyber attacks. Heterogeneity in terms of manufacturers, communication protocols and operating systems makes it difficult to implement consistent and effective security measures across the entire CPS and IoT infrastructure [7,8].

Therefore, CPS and IoT systems present significant challenges in terms of security that should be adequately addressed; otherwise, there would be considerable consequences in terms of security and privacy. On the one hand, their application areas often correspond to critical infrastructures, where the disruption or compromise of these systems can have devastating consequences, ranging from disruptions to public services to risks to security and human life. On the other hand, they collect and process large amounts of sensitive data, such as personal information, health data or confidential business data. Lack of security in these systems can result in data leaks, theft of personal or financial information and potential reputational damage to organizations.

To address these threats, the ISO/IEC 27.001 standard establishes key guidelines. According to this standard, an Information Security Management System (ISMS) is central to an overall management structure that seeks to preserve the security of information within organizations. By implementing an ISMS, organizations can establish policies, processes and controls to protect their critical information assets. This allows them to mitigate risks and safeguard the confidentiality, integrity and availability of the sensitive data they handle.

Risk management plays a fundamental role within an ISMS and in the current scenario, in which cybersecurity incidents are increasing in both intensity and impact, making both methodologies and tools that allow companies to address, understand and manage their cybersecurity risk in an adequate manner necessary [9–11].

Risk assessment and risk management solutions face challenges in their applicability and effectiveness. Lack of awareness and inaccurate risk assessments contribute to the majority of security incidents [12]. Moreover, current approaches offer a static view of risks, despite the fact that risks are dynamic and evolve along with threats and vulnerabilities [13].

To overcome these limitations, in previous works, we have developed a methodology called "MARISMA" (Methodology for the Analysis of Risks in Information Systems using Meta-Patterns and Adaptability) [14] supported by a technological environment called "eMARISMA" (www.emarisma.com, accessed on 26 March 2024). MARISMA is a methodology based on the reuse of knowledge for RAM purposes using structures known as "patterns" that allow different types of cases to be supported. In this sense, a pattern was developed to manage and control risks in CPSs considering the inherent needs of this type of systems (MARISMA-CPS) [15]. This template is based on the main standards and recommendations for CPSs, the IoT and risk management (ISO/IEC 27.000 and IEC 62443, ENISA (Ross, 2017) and the CPS framework by NIST (Griffor, 2017)).

However, there are still many challenges to be addressed. Systems are exposed to a large number of incidents on a daily basis that need to be corrected to restore system security. But each incident can be resolved by applying various courses of actions, and it is necessary to have mechanisms in order to select the most appropriate response.

In a previous work [16], we developed a quantum algorithm that selects as a response the minimum set of courses of action that cover all incidents. However, this work leaves out crucial aspects that are improved in this proposal.

On the one hand, the time needed to apply the course of action is a crucial aspect, since it minimizes the possible damages suffered [17]. But on the other hand, in a society involved in an ecological transition, the responsible use of resources should also be taken into account and the most sustainable course of action should be favored [18,19].

This paper contributes to this challenge by improving incident responses considering both the speed and sustainability of the response.

In a typical production-level operation, a large volume of security incidents can occur on a regular basis, even more so if we consider environments consisting of several IoT devices. This is why for the design of our solution, we design a quantum computing approach, which allows us to respond adequately and in near-constant time to scenarios with a large number of incidents.

Section 2 of this paper proceeds to explore the background and related works on sustainable security incident response and quantum optimization; Section 3 presents

our proposal based on quantum programming for the selection of the courses of action needed to restore system security considering response times and sustainability criteria; our proposal is validated in Section 4 by means of an application example; and finally, Section 5 presents the key findings from the study and outlines future research directions to be undertaken.

2. Context and Literature Review

Currently, the computational requirements and challenges associated with implementing a quantum approach for incident management in IoT environments are significant and reflect both the cutting-edge nature of quantum computing and the complexity of IoT ecosystems. Among these challenges, the foremost is that access to quantum computing resources is limited, and the technology is still in its developmental phase. Moreover, developing algorithms that effectively leverage the strengths of quantum computing requires substantial effort, as many classical algorithms do not directly translate to quantum environments, necessitating the creation of new quantum-specific algorithms. Finally, the scalability issues associated with the IoT are noteworthy, as these environments involve a large number of devices generating massive volumes of data. Therefore, designing quantum algorithms capable of efficiently managing these data and responding promptly to incidents is a non-trivial challenge.

To address these challenges, we propose various strategic approaches. On the one hand, we utilize hybrid systems that combine the strengths of quantum computing with the reliability and scalability of classical computing. This approach allows for efficient problem-solving while managing the limitations of current quantum technology. On the other hand, our methodology involves the development of custom quantum algorithms specifically designed for the task of incident management in IoT environments. These algorithms are designed to be scalable and efficient, taking into account the unique properties of quantum computing. Quantum simulators are also used to test and refine the algorithms. This approach allows for addressing potential issues and optimizing the performance of the algorithms in a controlled environment. Through these approaches, the proposed process aims to overcome the computational challenges associated with implementing quantum computing for incident management in IoT environments, paving the way for more efficient, scalable and sustainable cybersecurity solutions.

This part contains fundamental information regarding the research topics addressed in this paper, sustainable security incident response and quantum optimization. In particular, the first subsection provides an overview of the sustainable security incident response process and discusses some open research problems. In the next subsection, we discuss the foundation on which quantum computing is based, applying it to optimization problems.

2.1. Sustainable Management of Security Incidents

As outlined in the introductory section, security incidents represent unwanted occurrences that negatively affect the various dimensions of the valuable assets constituting a company's information system [20]. Such incidents stem from inadequacies in the security controls designated to safeguard these assets, specifically through vulnerabilities within the information systems. These vulnerabilities, when exploited by threats, lead to the assets being compromised and damaged [21].

To mitigate the repercussions of these incidents, organizations endeavor to implement the most fitting incident response strategies [22]. The domain of security incident management and response is presently a vibrant area of research with several pertinent unanswered questions [23]. A critical inquiry within this field is how organizations can attain sufficient situational awareness concerning vulnerabilities, threats, and potential security incidents [24]. Recent research efforts in this sphere have focused on devising models to elucidate how organizations can achieve cybersecurity situational awareness [25], highlighting that prompt and effective incident response not only bolsters cybersecurity awareness but also enhances the overall cybersecurity position of businesses [26].

Consequently, businesses of any scale must possess robust and effective tools that aid incident management. Importantly, these tools and processes must offer mechanisms that assist in decision making to efficiently identify and prioritize security incidents needing resolution [27]. This necessity arises from the potential for a high volume of incidents throughout an information system's life cycle, notably during significant updates like the release of a new application version or the introduction of a new information system or tool in the technical architecture of the organization. Therefore, addressing the specific efficiency and effectiveness requirements of these novel incident management support systems is of paramount importance [28].

However, in our study, the paramount issue confronting organizations is the agility with which they manage and respond to security incidents [29]. This agility necessitates responding to incidents as swiftly as possible [28,30]. Yet, addressing this challenge is becoming progressively tougher due to the increasing volume of incidents and their interconnected nature. In scenarios where systems are inundated with hundreds of events, it becomes imperative for incident response teams to swiftly identify and prioritize the most critical incidents for analysis.

As such, when planning the resolution of an incident, we encounter different types of scenarios. In some cases, responding to an incident is straightforward and involves activating a specific control (for example, installing antivirus software). However, we often find that the resolution of the incident is more complex and involves the execution of procedures with multiple action steps and even the intervention of different resources (technical and human). It is therefore necessary to apply the concept of a course of action (CoA), which the NIST defines as "a time-phased or situationally dependent combination of risk response actions" [31].

In this sense, when organizing and prioritizing incident resolution, it is vital to choose the most appropriate course of action. In traditional decision-making systems, the resolution time is often the key factor in determining the best choice. However, as sustainability becomes an increasingly relevant aspect in measuring the efficiency of an information system [32], it is becoming increasingly necessary for decision making in this area to consider which possible course of action is more sustainable. In this way, given a set of incidents to resolve, we would achieve a balance between time and sustainability when calculating the most efficient courses of action to apply. Nevertheless, manual prioritization is impractical due to its potential to hinder timely decision making. As noted by several scholars, responding to security incidents demands sophisticated event processing techniques for immediate capture, processing, integration, and analysis of data. This also involves examining the cause-and-effect connections among incidents [26].

We have seen this in practice through MARISMA [15,33], which is our dynamic approach to risk analysis and management that we have designed, improved and extended and which we have been applying to many types of companies and technologies (electric, hydrocarbons, governments, health, shipbuilding, chemical industry, etc.) for more than a decade with clients in eight Latin American countries. MARISMA was conceived as a complete and adaptable risk management framework, which includes a detailed methodology and a tool that automates many of the tasks of the methodology and supports improvement and extension to different technological contexts based on metadata, metamodels, ontologies and risk patterns.

In MARISMA and our developed tool, we have instituted a security incident management workflow that integrates essential data such as threats and their types, assets and asset groups, dimensions of risk and security measures. This workflow comprises several pivotal steps: (i) gathering detailed information about the security incident, including its description, causative factors, the individual accountable and the timeframe for resolution; (ii) utilizing the collected information and accessible metadata to determine the hierarchy of elements implicated in the security incident, including threats, assets and controls, while also establishing related details like the incident's severity and implementing a temporary reduction in the coverage level of affected controls until the incident is addressed;

and (iii) upon resolving the incident, facilitating knowledge management and learning by documenting the lessons learned, the costs associated with resolving the incident and any final observations.

Given that adaptability to new contexts (both technological and non-technological) and new technological paradigms is one of the key aspects in the design of the MARISMA framework, this has enabled its application in the past to different domains and specific technological sectors. In this work, demonstrating its application to a different and specific context involves the sustainable management of security incidents within Internet of Things (IoT) environments through the integration of quantum computing to optimize the selection of courses of action in response to security incidents. Thanks to the customizable patterns and the support tool, once domain experts have defined the specific elements and taxonomies of the new domain to which it will be applied, the MARISMA framework allows for the adaptation of the risk analysis and management process to this specific new domain.

Thanks to the adaptability and the potential for customization of the key risk management components through configurable patterns and the support tool, MARISMA is equipped to conduct risk analyses in any technological landscape in general. Moreover, it can adapt its application to specific technologies (Big Data, the IoT or CPSs) and specific sectors. This level of adaptability is maintained regardless of the domain's complexity or the size of the company, facilitating straightforward implementation for both small- and medium-sized enterprises (SMEs) and complex emerging technologies.

The limitations currently faced by the MARISMA framework for the proposed investigation are related to access to quantum computers, meaning that at present, this part is not applicable to real cases, and quantum simulators have had to be used to demonstrate the existing potential in this research area to solve the posed problem.

The substantial workload required for categorizing and prioritizing incidents to identify the most efficient resolution approach—minimizing response times and utilizing available resources optimally—presents the principal challenge in incident management. Especially during peak periods, such as the initial launch of a system or the introduction of a new service, the volume of incidents can increase significantly, complicating their effective management. This necessitates the prioritization and scheduling of dozens, or even hundreds, of incidents in a short timeframe, requiring intricate calculations, posing considerable difficulty, and leading to significant time costs.

To illustrate this problem, we will show an example (see Table 1) that considers the unique identifier of the incidents, the threat that has caused the incident together with the course of action intended to mitigate that threat, the main control that has been affected by the threat and the calculation of the estimated number of hours needed to resolve the incident via the suggested course of action. As indicated in Table 1, while each incident is associated with a single threat, it can impact one or several controls. To address and potentially prevent the recurrence of the incident, the implementation of these controls requires examination and correction, so different courses of action can be considered to resolve the incident.

Traditionally, management and response to security incidents have been focused on rapid resolutions, often overlooking sustainability. However, efficient and environmentally friendly resource management is essential. Incorporating sustainability into these practices not only enhances effectiveness in immediate recovery but also strengthens organizational resilience and sustainability in the long term in a context where social and environmental responsibility is increasingly important.

In this framework, each response strategy to incidents (each course of action) is rated with a sustainability label, ranging from A, being the most sustainable, to G, the least sustainable. This approach ensures that decisions are not made solely based on immediate efficiency or speed but also considering the long-term environmental impact.

This approach balances the need for quick and effective responses to security incidents with the commitment to act sustainably and responsibly. By integrating sustainability as a

key factor in decision making, organizations can not only effectively manage current risks but also strengthen their future resilience, sustainability and reputation among stakeholders, marking a significant evolution in risk management and incident response.

Table 1. Datasets of incidents.

IdIncident	IdThreat	Threat	CoA	IdControl	Control	Time (h)	Sustainability
1	DD	DDoS	C11	GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing	6	A
1	DD	DDoS	C12	GP-TM-17	Ensure standalone operation	6	E
2	DSIL	Data/sensitive information leakage	C21	GP-TM-47	Risk segmentation	3	B
3	IOI	Interception of information	C31	GP-PS-06	Implement test plans to verify whether the product performs as expected	8	F
4	CPH	Communication protocol hijacking	C41	GP-PS-09	Perform privacy impact assessments before any new applications are launched	40	B
4	CPH	Communication protocol hijacking	C42	GP-TM-25	Protect against 'brute force'	40	C
5	FOD	Failures of devices	C51	GP-PS-05	Design architecture by compartments	24	B
6	FOS	Failure of system	C61	GP-TM-17	Ensure standalone operation	8	A
7	MI	Modification of information	C71	GP-PS-09	Perform privacy impact assessments before any new applications are launched	24	F
7	EK	Exploit Kits	C72	GP-TM-20	Backward compatibility of firmware updates	2	B
7	SV	Software vulnerabilities	C73	GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing	6	B
8	ED	Environment Disaster	C81	GP-TM-06	Restore secure state	72	B
8	IOI	Interception of information	C82	GP-TM-25	Protect against 'brute force'	16	C
9	CPH	Communication protocol hijacking	C91	GP-TM-43	IoT devices should be restrictive in communicating	8	B

2.2. Quantum Optimization

Quantum computing represents a novel paradigm that leverages the unique aspects of quantum physics, offering substantial potential advancements in the computing arena. This potential is well acknowledged in scholarly works, as highlighted in key publications [34]. Crucial to the practical application of quantum computing is the development of programming languages and methodologies. These tools are imperative for providing structured and elevated descriptions of quantum algorithms that are independent of the specific hardware utilized [35].

The field of quantum programming has garnered significant attention following the development of efficient quantum algorithms by pioneers such as Shor [36] and Grover [37]. This interest persists, although the discovery of new quantum algorithms remains a formidable challenge. One of the primary reasons for this is the inherent complexity of quantum programs, which are typically depicted as quantum circuits [38].

A key differentiation between quantum and classical programming lies in the use of quantum bits or qubits, as opposed to standard bits [39]. In quantum programming, qubits are manipulated through quantum gates to perform various operations. Quantum computation, especially under the circuit model of quantum programs (QPs), involves these gates. They serve as fundamental operations for altering the qubits' amplitude and phase [39]. Quantum circuits and their corresponding gates can be visually represented, as illustrated in Figure 1. They are also expressible via syntax-based notations in various quantum programming languages such as Q# and QASM. These programming languages have been developed to simplify the articulation of quantum algorithms, transforming quantum circuit concepts into a sequence of textual programming statements. They address the core aspects of quantum programming and are tailored to meet the exigencies of practical quantum computing applications. Specifically, these languages facilitate the expression and conceptualization of quantum algorithms, which are vital for the real-world application of quantum computing. Thus, quantum programming environments are pivotal in advancing quantum computers from theoretical constructs to practical tools for scientific exploration and discovery [40].

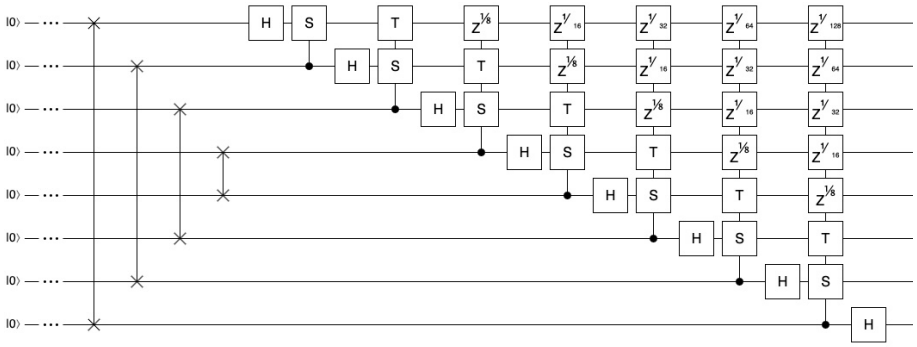

Figure 1. Example of a quantum circuit.

Quantum computing presents revolutionary approaches to computational challenges, surpassing traditional computational methods in efficiency [40]. A qubit, the fundamental unit of quantum computing, can be represented through various subatomic particles, such as electron spins or photons. Unlike classical bits that are binary, a qubit exists in multiple states simultaneously due to quantum superposition. This attribute allows a qubit to hold a value of zero, one, or both simultaneously, with specific probabilities. The value of a qubit is only determined upon measurement, at which point the qubit collapses and requires resetting for further use. Quantum programming, therefore, focuses on navigating and identifying optimal solutions within this probabilistic framework [41].

Quantum optimization often employs search algorithms, notably Grover's algorithm [37], which conducts searches in an undetermined space by encoding solution criteria using quantum oracles. These oracles [42,43] function similarly to high-level programming functions, aiding in constructing search algorithms with a linear complexity.

Additionally, quantum environments like D-Wave's Quantum Leap (https://www.dwavesys.com/, accessed on 26 March 2024) facilitate optimization for NP-hard combinatorial problems using adiabatic quantum optimization [44,45]. This approach involves defining the optimization system as a Hamiltonian, representing both the objective and constraints, and the quantum computer seeks the solution that minimizes the system's energy. Approaches using Ising expressions for this type of optimization are discussed in [46], while gate-based programming alternatives, such as those in the Qiskit textbook [47], implement the quantum approximate optimization algorithm (QAOA) [48].

Quantum adiabatic computing marks a significant advancement in optimization algorithms. It complements classical algorithms, like backtracking, dynamic programming, heuristic searches (e.g., A*), and adversarial searches (e.g., Minimax, branch and bound), by offering new, more efficient techniques. Among these advancements are genetic algorithms [49], classical annealers like simulated annealing [50], and benchmark function algorithms [51]. However, these solutions often struggle with local minima and are less effective with exceedingly large or complex problems. Adiabatic quantum computation emerges as a promising solution for solving complex NP-complete optimization problems in polynomial time [52].

Quantum annealing algorithms typically begin by defining a problem with qubits in a superposition state. Through the annealing process, these qubits collapse to a classical state of either 0 or 1, representing the lowest energy solution. As depicted in Figure 2, the process starts with the qubits in a single-valley energy state (a), evolving through the annealing to a double-well potential state (b) and culminating with a deeper valley representing the optimal solution (c).

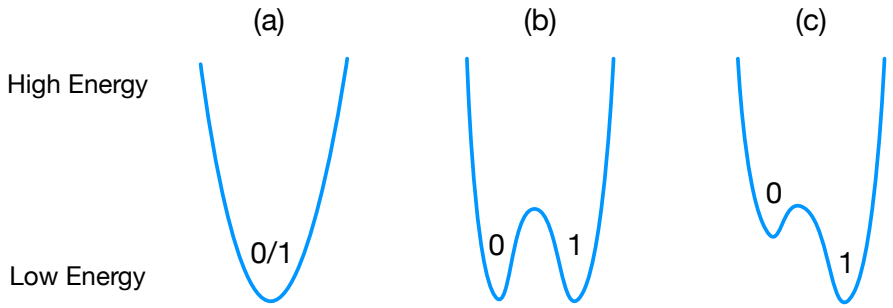

Figure 2. Quantum annealing process (different states).

3. A Proposal for Sustainable Security Incident Management

In our study, we utilize a quantum computing methodology to enhance the efficiency of incident response management within a risk assessment and management framework. This quantum computing strategy is applied to the dataset of detected security incidents, which has information on their associated threats, the courses of action needed to restore the system, the time required to apply them and their associated sustainability. For this dataset, it seeks the lowest energy state, symbolizing the optimal solution for resolving incidents, by prioritizing that the response time is the shortest possible, the results are as sustainable as possible or a combination of both in an indicated percentage.

Our approach incorporates sustainability as a key criterion in the selection of incident management strategies, balancing security effectiveness with environmental responsibility. We assess the sustainability of strategies using criteria such as energy efficiency and environmental impact, assigning each a sustainability label from A to G. This methodology helps us select responses that meet our security objectives while promoting responsible use of resources.

Our process to determine the optimal balance between response time and sustainability considerations is based on a decision process that integrates impact analysis, strategy feasibility and organizational priorities. We use an alpha coefficient, alpha, to adjust the relative importance of response time versus sustainability, allowing stakeholders to define their preferences according to strategic objectives. This process ensures an informed and aligned choice of response strategies, effectively balancing operational efficiency with environmental responsibility.

The following is the proposed algorithmic solution to the problem using quantum algorithms. To accurately design the algorithmic solution for the problem at hand, it is crucial to delineate the variables and entities involved in the algorithm. The variables can be characterized as follows:

Definition 1. *Let I_i be an unique identifier of an incident, corresponding with the incidents in Table 1.*

Definition 2. *Let C_{ij} be a possible course of action for solving control I_i, with j being an identifier for the course of action.*

Definition 3. *Let t_i be the estimated time in minutes necessary for solving the incident I_i, mapping to the time value.*

Definition 4. *Let Sustainability be a label indicating the sustainability rating of the solution based on the course of action selected. This rating is related to the energy and sustainability of the proposed solution, with A being a more sustainable solution than G.*

Definition 5. *Define x_{ij} as a binary variable that, within the algorithm's solution, indicates if the action sequence C_ij is chosen for implementation.*

Definition 6. *Define P as a penalty coefficient, utilized to adjust the significance of constraints within the algorithm's formulation. Its value can be empirically determined to be equal to the highest estimated cost among all the occurrences plus one, thus affecting the whole solution.*

Based on these definitions, we can algebraically articulate the goal by executing a quantum optimization algorithm, which is to be processed by a quantum computer. This problem is summarized as a small example within the scope of Table 2; this table shows a dataset encapsulating a spectrum of security incidents within a computational system, accompanied by an array of potential resolution methodologies, termed 'course of action'. The algorithm's core function lies in the strategic selection of these courses, prioritizing those that yield a superior efficiency in terms of temporal cost or sustainability. This efficiency is quantified via a weighted average, governed by a coefficient α, facilitating adaptability to shifting real-time parameters. Our discourse aims to dissect the fundamental constructs and pivotal considerations integral to the crafting and execution of this optimization algorithm. Through this analytical lens, we endeavor to achieve a thorough comprehension of its operational framework and the consequential impact it bears in the landscape of cybersecurity research and applications.

Table 2. Incident and control examples.

Incident	Course of Action	Time	Sustainability
I1	C11	10	B
I1	C12	20	A
I1	C13	60	G
I2	C21	50	A
I2	C22	100	B
I3	C31	1	G
I3	C32	20	F
I3	C33	50	E
I3	C34	10	E

As highlighted in Section 2, while genetic algorithms and classical annealers present viable strategies for addressing certain problems, they often fall short in solving complex optimization challenges within polynomial time. In the realm of quantum computation, two predominant approaches are quantum gate-based circuits and adiabatic quantum algorithms. It is acknowledged that quantum gate-based methods, such as the quantum approximate optimization algorithm (QAOA), can tackle optimization problems comparably to quantum annealers. However, the formulation and implementation of these quantum circuits are notably more intricate and extensive than the Hamiltonian formulation used in quantum annealers, which is simpler, more comprehensible and independent of the quantum platform's specifics.

To address the problem at hand, we propose modeling it as a quadratic unconstrained binary optimization (QUBO) problem, alternatively known as unconstrained binary quadratic programming (UBQP). This approach will encapsulate the objectives and constraints of our problem, enabling the adiabatic quantum computer's solver to identify the minimum energy state. This state corresponds to the optimal combination of variables, or incidents, necessary for an effective solution.

QUBO-based problems are defined through a Hamiltonian, which, in its summation form, delineates both the objectives and the constraints required by the solution. This Hamiltonian is articulated as a Binary Quadratic Model (BQM) and is subsequently transformed into a BQM matrix. This matrix is then processed by the adiabatic solver.

Our primary goal is the minimization of the total cost associated with the issues forming part of the solution. This objective could be articulated in the form of a BQM expression as follows (Equation (1)):

$$Minimize \left(\sum_{i=1} \sum_{j=1} (x_{ij} \times (\alpha \cdot T_{ij} + (1 - \alpha) \cdot S_{ij})) \right) \quad (1)$$

where x_{ij} is the binary variable that determines whether or not the course of action C_{ij} is selected to solve the incident I_i, T_{ij} is the estimated time and S_{ij} is the sustainability rank related to the course of action C_{ij}. Additionally, α is a tuning coefficient for indicating in operating time the weight of time and sustainability in the solution.

In this problem, the constraints are straightforward, we just have to make sure that at least one course of action (C_{ij}) is selected for each indident I_i. This set of constraints can be modeled as shown in Equation (2).

$$\forall i \in N \sum_{j=1}^{K} x_{ij} \geq 1 \quad (2)$$

Based on the definition of the previous equations, the Python code shown in Figure 3 is produced, wherein a QUBO matrix is populated for submission to the quantum annealing sampler. This algorithm generates an upper triangular matrix that outlines the QUBO matrix for the Binary Quadratic Model (BQM).

```
def createBQM(incidents, CoA, time, sustainability):
    Q = defaultdict(int)
    num_coa = len(CoA)
    penalty = max(alfa * time[i] + (1-alfa) * sustainability[i]
        for i in range(num_coa)) + 1

    for i in range(num_coa):
        Q[(i, i)] = -(penalty/(time[i] + (1-alfa) * sustainability[i]))

    for incident in incidents:
        indices = [i for i, incident in enumerate(incidents)
            if CoA['incident'] == incident]
        for i in indices:
            for j in indices:
                if i < j:
                    Q[(i, j)] = Q[(i, j)] + penalty

```

Figure 3. Python code for the quantum algorithm.

4. Validation

In this section, we validate our proposal by applying the developed algorithm to a dataset with real incident data.

The dataset used presents 50 incidents, together with the possible courses of action to respond, the time needed and the associated sustainability label. Table 3 shows the first 10 elements of this dataset.

Table 3. A subset of the incident dataset for validation.

IdIncident	IdThreat	Threat	CoA	Time (h)	Sustainability
1	[SV]	Software vulnerabilities	C5	5	A
2	[ED]	Environmental disaster	C11	17	E
3	[IOI]	Interception of information	C7	41	F
3	[IOI]	Interception of information	C1	41	A
4	[IG]	Information gathering	C1	35	A
5	[DDoS]	DDoS	C5	4	A
5	[DDoS]	DDoS	C6	4	E
6	[VRRBL]	Violation of rules and regulations / Breach of legislation	C5	10	A
7	[LOSS]	Loss of support services	C15	11	D
8	[NO]	Network outage	C1	28	A
9	[CPH]	Communication protocol hijacking	C3	4	G
10	[MIM]	Man in the middle	C3	39	G

To validate our proposal, we applied the algorithm developed (Figure 3), which forms the input matrix for the quantum annealer sampler. In essence, we created the triangular QUBO matrix Q and dispatched it to the sampler using the code depicted in Figure 4. We executed the algorithm utilizing a D-Wave 2000Q lower-noise system equipped with a DW_2000Q_6 quantum processor, which boasts 2048 qubits arranged in a [16, 16, 4] chimera topology.

```
1
2       sampler = LeapHybridSampler()
3       sampleset = sampler.sample(bqm)
```

Figure 4. Python code for quantum sampling.

We have carried out executions considering different configurations indicating different degrees of prioritization of response time (coefficient alpha) and sustainability (coefficient 1-alpha) in the selection of the set of courses of action. Specifically, they were applied considering the following alpha values: 0.0, 0.2, 0.5 and 0.8. The results obtained are presented below.

Following the execution of the code, the sampling outcomes are obtained in a text file, allowing us to review the algorithm's results and the energy associated with each solution identified. The solution that exhibits the lowest energy level is considered optimal, meeting the requirements and objectives of our problem.

Figures 5–8 show the outputs of the algorithm for the data shown in Table 3 considering different values of alpha: 0.0 (which fully prioritizes sustainability over response time), 0.2, 0.5 and 0.8 (which prioritizes time over sustainability).

```
Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 1.0)
Object x3 (incident: [IOI], coa: C1, time: 41, energy: 1, cost: 1.0)
Object x4 (incident: [IG], coa: C1, time: 35, energy: 1, cost: 1.0)
Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 1.0)
Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 30.0)
Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 1.0)
Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 100.0)
Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 1.0)
Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 1.0)
Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 75.0)
Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 1.0)
Object x22 (incident: [ED], coa: C4, time: 9, energy: 20, cost: 20.0)
Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 50.0)
Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 20.0)
Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 20.0)
Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 30.0)
Object x37 (incident: [DDoS], coa: C1, time: 7, energy: 1, cost: 1.0)
Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 30.0)
Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 10.0)
Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 100.0)
Object x45 (incident: [TA], coa: C16, time: 33, energy: 1, cost: 1.0)
Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 100.0)
Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 1.0)
Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 10.0)
cost total: 606.0
Time: 12 seconds
    0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 ... 66       energy num_oc.
2   1  0  0  1  1  0  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
3   1  0  0  1  1  0  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
1   1  0  0  1  1  0  0  1  1  1  1  0  0  1  0  0 ...  0 -1162.846667       1
8   1  0  0  1  1  0  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
14  1  0  0  1  1  0  0  1  1  1  1  0  0  1  0  0 ...  0 -1162.846667       1
27  1  0  0  1  1  0  0  1  1  1  1  0  0  1  0  0 ...  0 -1162.846667       1
66  1  0  0  1  1  0  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
68  1  0  0  1  1  0  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
76  1  0  0  1  1  1  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
19  1  0  0  1  1  1  0  1  1  1  1  0  0  0  0  0 ...  0 -1162.846667       1
...

```

Figure 5. Results fully prioritizing sustainability (alpha equal to 0.0).

```
Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 1.8)
Object x1 (incident: [ED], coa: C11, time: 17, energy: 50, cost: 43.4)
Object x4 (incident: [IG], coa: C1, time: 35, energy: 1, cost: 7.8)
Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 1.6)
Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 2.8)
Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 26.2)
Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 6.4)
Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 80.8)
Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 1.6)
Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 6.8)
Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 60.8)
Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 9.8)
Object x27 (incident: [ROM], coa: C7, time: 37, energy: 75, cost: 67.4)
Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 21.4)
Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 18.6)
Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 31.2)
Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 24.8)
Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 8.8)
Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 80.8)
Object x45 (incident: [TA], coa: C16, time: 33, energy: 1, cost: 7.4)
Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 84.2)
Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 2.0)
Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 14.600000000000001)
Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
cost total: 621.0000000000001

```

Figure 6. Results prioritizing 80% sustainability and 20% time (alpha equal to 0.2).

```
Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 3.0)
Object x1 (incident: [ED], coa: C11, time: 17, energy: 50, cost: 33.5)
Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 2.5)
Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 5.5)
Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 20.5)
Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 14.5)
Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 52.0)
Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 2.5)
Object x18 (incident: [MIM], coa: C1, time: 30, energy: 1, cost: 15.5)
Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 39.5)
Object x20 (incident: [NR], coa: C1, time: 45, energy: 1, cost: 23.0)
Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 46.0)
Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 23.5)
Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 16.5)
Object x34 (incident: [DSIL], coa: C15, time: 36, energy: 30, cost: 33.0)
Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 17.0)
Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 7.0)
Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 52.0)
Object x43 (incident: [TA], coa: C15, time: 31, energy: 30, cost: 30.5)
Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 60.5)
Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 3.5)
Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 21.5)
Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
Object x66 (incident: [IG], coa: C4, time: 18, energy: 20, cost: 19.0)
cost total: 552.0

```

Figure 7. Results prioritizing 50% sustainability and 50% time (alpha equal to 0.5).

Finally, a comparison of the courses of action selected in each case and the number of times they are selected is shown Table 4). We can observe how the different solutions vary in the selection of some courses of action. We see how courses of action with better sustainability labels (such as C1 or C16 with label A) are selected a higher number of times when the algorithm prioritizes sustainability and a lower number of times as time is prioritized. On the other hand, less sustainable courses of action (such as C11 with label E) are not selected when the configuration fully prioritizes sustainability, but nevertheless, when this criterion is relaxed, they start to be selected. In this sense, we can also observe how in the last configuration, where response time is strongly prioritized, very sustainable courses of action such as C1 go from being selected six times to one, while the selection of other less sustainable ones, such as C2 (label G), C9 (with label F), etc., increases.

```
Object x0 (incident: [SV], coa: C5, time: 5, energy: 1, cost: 4.2)
Object x5 (incident: [DDoS], coa: C5, time: 4, energy: 1, cost: 3.4000000000000004)
Object x7 (incident: [VRRBL], coa: C5, time: 10, energy: 1, cost: 8.2)
Object x8 (incident: [LOSS], coa: C15, time: 11, energy: 30, cost: 14.799999999999999)
Object x9 (incident: [NO], coa: C1, time: 28, energy: 1, cost: 22.6)
Object x10 (incident: [CPH], coa: C3, time: 4, energy: 100, cost: 23.199999999999996)
Object x16 (incident: [MI], coa: C16, time: 4, energy: 1, cost: 3.4000000000000004)
Object x19 (incident: [SH], coa: C7, time: 4, energy: 75, cost: 18.199999999999996)
Object x22 (incident: [ED], coa: C4, time: 9, energy: 20, cost: 11.2)
Object x25 (incident: [NR], coa: C14, time: 28, energy: 10, cost: 24.400000000000002)
Object x26 (incident: [ROM], coa: C6, time: 42, energy: 50, cost: 43.6)
Object x30 (incident: [EK], coa: C13, time: 27, energy: 20, cost: 25.6)
Object x31 (incident: [TPF], coa: C13, time: 13, energy: 20, cost: 14.399999999999999)
Object x38 (incident: [FOD], coa: C15, time: 4, energy: 30, cost: 9.2)
Object x40 (incident: [MW], coa: C14, time: 4, energy: 10, cost: 5.199999999999999)
Object x42 (incident: [FOS], coa: C3, time: 4, energy: 100, cost: 23.199999999999996)
Object x43 (incident: [TA], coa: C15, time: 31, energy: 30, cost: 30.799999999999997)
Object x48 (incident: [DSIL], coa: C9, time: 38, energy: 75, cost: 45.4)
Object x51 (incident: [AP], coa: C2, time: 21, energy: 100, cost: 36.8)
Object x52 (incident: [CMD], coa: C16, time: 6, energy: 1, cost: 5.000000000000001)
Object x57 (incident: [DN], coa: C10, time: 33, energy: 10, cost: 28.400000000000002)
Object x62 (incident: [IOI], coa: C10, time: 10, energy: 10, cost: 10.0)
Object x64 (incident: [MIM], coa: C2, time: 28, energy: 100, cost: 42.4)
Object x66 (incident: [IG], coa: C4, time: 18, energy: 20, cost: 18.4)
cost total: 471.9999999999999

```

Figure 8. Results prioritizing 20% sustainability and 80% time (alpha equal to 0.8).

On the other hand, some courses of action with worse sustainability labels (such as C8 and C12 with F and G, respectively) are never selected, as there are alternative courses of action that cover the same incidents with better indexes in time and sustainability.

Table 4. Comparison of results obtained according to different alpha values.

CoA	Sustainability Label	Alfa 0.0	Alfa 0.2	Alfa 0.5	Alfa 0.8
C1	A	6	2	3	1
C2	G	1	1	1	2
C3	G	2	2	2	2
C4	C	1		1	2
C5	A	2	3	3	3
C6	E	1		1	1
C7	F	1	2	1	1
C8	F				
C9	F				1
C10	B	1	2	2	2
C11	E		1	1	
C12	G				
C13	C	2	2	2	2
C14	B	1	1	1	2
C15	D	2	3	3	3
C16	A	3	3	2	2
CoA selected		23	22	23	24

The quantum algorithm becomes more important when we move into real scenarios where the number of incidents is high, i.e., in the order of hundreds or thousands. This number is even greater if we consider a centralized incident management system serving multiple organizations. In these cases, the quantum algorithm responds in a constant time, independent of the number of incidents handled, which is a critical aspect for an incident response system.

5. Conclusions

The significance of security management, risk analysis and particularly risk management, underscored by effective handling and learning from security incidents, is escalating. However, the sustainability aspect of such security management is frequently overlooked. It is crucial, nevertheless, to consider security solutions and controls in light of their sustainability. This approach is not only feasible but necessary in an era of increasing environmental consciousness. Our focus in this paper has been on the context of Internet of Things environments, which are proliferating globally and contributing to a significant rise in security incidents.

In this context, the efficiency with which incidents are addressed and system security is reinstated is of paramount importance for the prompt resolution of security breaches. However, addressing these issues in a sustainable manner, by opting for the most suitable course of action, is not only preferable but also aligns with environmental policies.

The field of quantum computing research is diversifying rapidly, finding applications in numerous and varied contexts. Specifically, in this paper, we have developed an experimental quantum computing application aimed at optimizing the selection of security courses of action in response to various security incident scenarios. This application not only evaluates the required time for each security solution but also considers their sustainability. We have designed and implemented a quantum computing algorithm and, following extensive testing and execution, can affirm that its results are accurate and align with expectations based on quantum principles. The algorithm has a highly efficient execution time, effectively solving the problem in a near-constant timeframe.

This paper illustrates the efficacy of our quantum algorithm in addressing this specific security challenge.

Therefore, it is reasonable to assert that, despite the numerous unresolved challenges in security incident management, particularly in the context of handling extensive datasets, certain issues can be effectively addressed using quantum algorithms. In fact, a key component of our future research involves an in-depth exploration of quantum algorithms and swarm intelligence applied to the extensive dataset of security risks and incidents collected from various organizations. This endeavour aims to enable real-time correlation of security incidents, offering a more comprehensive and efficient approach to responding to security threats.

For future work, several lines of research are proposed. Firstly, there is an intention to apply and adapt the proposed framework and algorithm to other critical sectors that heavily rely on the IoT, such as the energy or naval sectors, to evaluate their effectiveness across a broader range of scenarios and operational contexts. Secondly, efforts will be directed towards integrating the developed model with AI techniques to enhance incident prediction, automate decision making, and improve the customization of responses based on each organization's specific risk profile. Furthermore, the long-term impact of implementing sustainable action courses in security incident management using quantum programming on an organization's carbon footprint will also be examined. Lastly, work will be carried out to integrate these techniques and algorithms within the MARISMA framework. This future work will not only extend the scope of the current research but will also significantly contribute to enhancing the security, sustainability, and resilience of critical systems in the IoT era.

Author Contributions: Conceptualization, all authors; methodology, C.B.; software, A.S.-O.; validation, L.E.S.; writing, review and editing, all authors. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been developed within the ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521), ALBA-UC (TED2021-130355B-C33, id.3611130630-130630-28-521), AETHER-UCLM (PID2020-112540RB-C42), PRESECREL (PID2021-124502OB-C42), MESIAS (2022-GRIN-34202) and Di4SPDS (PCI2023145980-2) funded by MCIN/AEI/10.13039/501100011033 and Unión Europea Next GenerationEU/PRTR.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: https://github.com/GSYAtools/QISS (accessed on 26 March 2024).

Acknowledgments: We express our gratitude for the support provided by Sicaman Nuevas Tecnologías S.L. (https://www.sicaman.com, accessed on 26 March 2024) and Marisma Shield S.L. (https://www.emarisma.com, accessed on 26 March 2024) which enabled the validation of case studies and the utilization of the eMARISMA tool.

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

References

1. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [CrossRef]
2. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]
3. Priyadarshini, I.; Kumar, R.; Tuan, L.M.; Son, L.H.; Long, H.V.; Sharma, R.; Rai, S. A new enhanced cyber security framework for medical cyber physical systems. *SICS Softw.-Intensive Syst.* **2021**, *35*, 159–183. [CrossRef]
4. Jindal, A.; Aujla, G.S.; Kumar, N.; Chaudhary, R.; Obaidat, M.S.; You, I. SeDaTiVe: SDN-Enabled Deep Learning Architecture for Network Traffic Control in Vehicular Cyber-Physical Systems. *IEEE Netw.* **2018**, *32*, 66–73. [CrossRef]
5. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber-physical systems. *Comput. Ind.* **2018**, *97*, 132–145. [CrossRef]
6. Kumar, R.; Narra, B.; Kela, R.; Singh, S. AFMT: Maintaining the safety-security of industrial control systems. *Comput. Ind.* **2022**, *136*, 103584. [CrossRef]

7. Griffor, E.; Wollman, D.; Greer, C. *Framework for Cyber-Physical Systems: Volume 1, Overview*; Technical Report June; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [CrossRef]
8. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
9. Glantz, C.; Lenaeus, J.; Landine, G.; O'Neil, L.R.; Leitch, R.; Johnson, C.; Lewis, J.; Rodger, R. Implementing an Information Security Program. In *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges*; Martellini, M., Malizia, A., Eds.; Terrorism, Security, and Computation; Springer International Publishing: Cham, Switzerland, 2017; Book Section Chapter 9; pp. 179–197. [CrossRef]
10. Thakur, K.; Qiu, M.; Gai, K.; Ali, M.L. An Investigation on Cyber Security Threats and Security Models. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015; pp. 307–311. [CrossRef]
11. Wang, T.; Gao, S.; Li, X.; Ning, X. A meta-network-based risk evaluation and control method for industrialized building construction projects. *J. Clean. Prod.* **2018**, *205*, 552–564. [CrossRef]
12. Turskis, Z.; Goranin, N.; Nurusheva, A.; Boranbayev, S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach. *Informatica* **2019**, *30*, 187–211. [CrossRef]
13. Paltrinieri, N.; Reniers, G. Dynamic risk analysis for Seveso sites. *J. Loss Prev. Process Ind.* **2017**, *49*, 111–119. [CrossRef]
14. Santos-Olmo, A.; Sánchez, L.E.; Rosado, D.G.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals. *Front. Comput. Sci.* **2024**, *18*, 183808. [CrossRef]
15. Rosado, D.G.; Santos-Olmo, A.; Sanchez, L.E.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Comput. Ind.* **2022**, *142*, 103715. [CrossRef]
16. Serrano, M.A.; Sánchez, L.E.; Santos-Olmo, A.; García-Rosado, D.; Blanco, C.; Barletta, V.S.; Caivano, D.; Fernández-Medina, E. Minimizing incident response time in real-world scenarios using quantum computing. *Softw. Qual. J.* **2024**, *32*, 163–192. [CrossRef]
17. Bhardwaj, A.; Sapra, V. *Security Incidents & Response against Cyber Attacks*; Springer: Berlin/Heidelberg, Germany, 2021. [CrossRef]
18. Salam, A. Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Springer International Publishing: Cham, Switzerland, 2020; pp. 299–327. [CrossRef]
19. Zubair, S.; Ahmed, M.; Sikos, L.; Islam, N. Toward a Sustainable Cybersecurity Ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
20. Mahima, D. Cyber Threat in Public Sector: Modeling an Incident Response Framework. In Proceedings of the 2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), Noida, India, 17–19 February 2021; pp. 55–60. [CrossRef]
21. Dion, M. Cybersecurity policy and theory. In *Theoretical Foundations of Homeland Security*; Routledge: London, UK, 2020; pp. 257–284.
22. Prasad, R.; Rohokale, V. Secure Incident Handling. In *Cyber Security: The Lifeline of Information and Communication Technology*; Springer International Publishing: Cham, Switzerland, 2020; pp. 203–216. [CrossRef]
23. Grispos, G.; Glisson, W.B.; Storer, T. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digit. Investig.* **2017**, *22*, 62–73. [CrossRef]
24. 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]
25. Ahmad, A.; Desouza, K.C.; Maynard, S.B.; Naseer, H.; Baskerville, R.L. How integration of cyber security management and incident response enables organizational learning. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 939–953. [CrossRef]
26. Naseer, A.; Naseer, H.; Ahmad, A.; Maynard, S.B.; Masood Siddiqui, A. Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *Int. J. Inf. Manag.* **2021**, *59*, 102334. [CrossRef]
27. Ahmad, A.; Maynard, S.B.; Shanks, G. A case analysis of information systems and security incident responses. *Int. J. Inf. Manag.* **2015**, *35*, 717–723. [CrossRef]
28. van der Kleij, R.; Schraagen, J.M.; Cadet, B.; Young, H. Developing decision support for cybersecurity threat and incident managers. *Comput. Secur.* **2021**, *113*, 102535. [CrossRef]
29. Tam, T.; Rao, A.; Hall, J. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Comput. Secur.* **2021**, *109*, 102385. [CrossRef]
30. He, Y.; Zamani, E.D.; Lloyd, S.; Luo, C. Agile incident response (AIR): Improving the incident response process in healthcare. *Int. J. Inf. Manag.* **2022**, *62*, 102435. [CrossRef]
31. Joint Task Force Transformation Initiative. *SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2011.
32. Kniaz, S.; Brych, V.; Marhasova, V.; Tyrkalo, Y.; Skrynkovskyy, R.; Sumets, A. Modeling of the information system of environmental risk management of an enterprise. In Proceedings of the 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 26–28 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 215–218.
33. Rosado, D.G.; Moreno, J.; Sánchez, L.E.; Santos-Olmo, A.; Serrano, M.A.; Fernández-Medina, E. MARISMA-BiDa pattern: Integrated risk analysis for big data. *Comput. Secur.* **2021**, *102*, 102155. [CrossRef]

34. IBM. *The Quantum Decade. A Playbook for Achieving Awareness, Readiness, and Advantage*; IBM: Armonk, NY, USA, 2021.
35. Clairambault, P.; De Visme, M.; Winskel, G. Game semantics for quantum programming. *Proc. Acm Program. Lang.* **2019**, *3*, 1–29. [CrossRef]
36. Shor, P. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; IEEE: Piscataway, NJ, USA, 2002; pp. 124–134. [CrossRef]
37. Grover, L.K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **1997**, *79*, 325–328. [CrossRef]
38. Altenkirch, T.; Grattage, J. A Functional Quantum Programming Language. In Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS' 05), Chicago, IL, USA, 26–29 June 2005; pp. 249–258. [CrossRef]
39. Sánchez, P.; Alonso, D. On the Definition of Quantum Programming Modules. *Appl. Sci.* **2021**, *11*, 5843. [CrossRef]
40. Gyongyosi, L.; Imre, S. A Survey on quantum computing technology. *Comput. Sci. Rev.* **2019**, *31*, 51–71. [CrossRef]
41. Piattini, M.; Serrano, M.; Perez-Castillo, R.; Petersen, G.; Hevia, J.L. Toward a Quantum Software Engineering. *IT Prof.* **2021**, *23*, 62–66. [CrossRef]
42. Sutor, R. *Dancing with Qubits*; Packt Publishing: Birmingham, UK, 2019.
43. Johnston, E.R.; Harrigan, N.; Gimeno-Segovia, M. *Programming Quantum Computers: Essential Algorithms and Code Samples*; O'Reilly Media: Sebastopol, CA, USA, 2019.
44. Farhi, E.; Goldstone, J.; Gutmann, S.; Lapan, J.; Lundgren, A.; Preda, D. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. *Science* **2001**, *292*, 472–475. [CrossRef]
45. Das, A.; Chakrabarti, B.K. Colloquium: Quantum annealing and analog quantum computation. *Rev. Mod. Phys.* **2008**, *80*, 1061. [CrossRef]
46. Lucas, A. Ising formulations of many NP problems. *Front. Phys.* **2014**, *2*, 5. [CrossRef]
47. Asfaw, A.; Corcoles, A.; Bello, L.; Ben-Haim, Y.; Bozzo-Rey, M.; Bravyi, S.; Bronn, N.; Capelluto, L.; Vazquez, A.C.; Ceroni, J.; et al. *Learn Quantum Computation Using Qiskit*; IBM: Armonk, NY, USA, 2020.
48. Farhi, E.; Goldstone, J.; Gutmann, S. A quantum approximate optimization algorithm. *arXiv* **2014**, arXiv:1411.4028.
49. Rocke, D. Genetic Algorithms+ Data Structures= Evolution programs (3rd). *J. Am. Stat. Assoc.* **2000**, *95*, 347. [CrossRef]
50. Kirkpatrick, S.; Gelatt, C.D., Jr.; Vecchi, M.P. Optimization by simulated annealing. *Science* **1983**, *220*, 671–680. [CrossRef] [PubMed]
51. Dieterich, J.M.; Hartke, B. Empirical review of standard benchmark functions using evolutionary global optimization. *arXiv* **2012**, arXiv:1207.4318.
52. Černý, V. Quantum computers and intractable (NP-complete) computing problems. *Phys. Rev. A* **1993**, *48*, 116–119. [CrossRef]