applied sciences

MDPI

Article

A Survey on Cyber Risk Management for the Internet of Things

Emily Kate Parsons *,†, **Emmanouil Panaousis** †, **George Loukas** † and **Georgia Sakellari** †

Internet of Things and Security Centre, University of Greenwich, London SE10 9LS, UK; e.panaousis@greenwich.ac.uk (E.P.); g.loukas@greenwich.ac.uk (G.L.); g.sakellari@greenwich.ac.uk (G.S.)

* Correspondence: emily.parsons@gre.ac.uk

† Current address: Old Royal Naval College, University of Greenwich, Park Row, London SE10 9LS, UK

Abstract: The Internet of Things (IoT) continues to grow at a rapid pace, becoming integrated into the daily operations of individuals and organisations. IoT systems automate crucial services within daily life that users may rely on, which makes the assurance of security towards entities such as devices and information even more significant. In this paper, we present a comprehensive survey of papers that model cyber risk management processes within the context of IoT, and provide recommendations for further work. Using 39 collected papers, we studied IoT cyber risk management frameworks against four research questions that delve into cyber risk management concepts and human-orientated vulnerabilities. The importance of this work being human-driven is to better understand how individuals can affect risk and the ways that humans can be impacted by attacks within different IoT domains. Through the analysis, we identified open areas for future research and ideas that researchers should consider.

Keywords: IoT cyber risk management; cyber risk assessment; cyber risk control; security controls; Internet of Things; survey; IoT

check for updates

Citation: Parsons, E.K.; Panaousis, E.; Loukas, G.; Sakellari, G. A Survey on Cyber Risk Management for the Internet of Things. *Appl. Sci.* **2023**, *13*, 9032. https://doi.org/10.3390/app13159032

Academic Editors: Gregory Epiphaniou and Carsten R. Maple

Received: 29 June 2023
Revised: 31 July 2023
Accepted: 2 August 2023
Published: 7 August 2023

1. Introduction

The commercial growth of the Internet of Things (IoT) technology has been exponential due to its benefits to multiple organisations and individuals in a vast number of environments. IoT is changing daily domestic life [1–4]. However, the use of this technology comes at a potential cyber risk that can impact, harm, or damage systems and users negatively. In such cases, organisations may actively use IoT in a more regulated way; however, IoT is not just for organisations but individuals who may dwell within IoT domains that are not regulated. Unlike organisations with home workers, organisations that use IoT have more control over how risk is managed due to centralised cyber risk strategies built from standards, legislation, and regulations. Unfortunately, despite centralised strategies, IoT devices carry limited security capabilities due to processing constraints [5], which impacts the ability to accurately control devices at the same level as traditional IT devices. This problem supports the need for IoT cyber risk management methods that can function alongside traditional IT but consider IoT specific issues.

At a very high level, cyber risk management is comprised of three main components: risk *identification*, risk *assessment* and risk *control* [6]. The risk *identification* phase gathers data needed for risk *assessment*, which aims to determine the value of risk. This determination is then used to establish risk *control*, which allows for the implementation and evaluation of cyber security controls to mitigate risk. Given the well-known nature of how risk management should function, many types of cyber risk management standards are available for organisations to ensure that their assets and employees are protected, with some of the most well known coming from NIST and ISO/IEC. In the context of IoT, some methodologies may not always be fit for this purpose but could be used to ensure a standardised system using well-known risk factors.

According to NIST, cyber risk is defined as the "risk of depending on cyber resources" [7] and the IoT domain is no exception. In connection, cyber risk management is a "comprehensive process that requires organisations to (i) frame risk; (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis" [7]. Meanwhile, an asset is anything that has value to an organisation or a person that needs to be protected against IoT attacks [8], where using a cyber risk management model can be used to minimise the impact on users and assets with the use of a formalised process. The problem with traditional static requirements is that security controls are deployed "around the external facing nodes of a network" [9] within unchanging network domains [10], something that is commonly dynamic within IoT. Due to this, static requirements applied to IoT security may not be most suitable due to the IoT scalability, with environments using a vast number of IoT nodes [9,10].

Another factor of concern within the IoT domain is that of *users*, addressing not only how they are impacted by attacks but how they may become *human vulnerabilities*. The perspective of a human vulnerability within security research is often related to humans being the weakest security link, considering the potential manipulation from social engineering attacks. Figure 1 shows common user roles within various IoT domains, with such users having differing security responsibilities. While technical protection for systems is important, if not used correctly or the user is manipulated by an attacker, an attack may still be successful in achieving its goal [11]. It is argued that members of the public will often acknowledge the threat of cyber attacks but do not necessarily know the steps to mitigate them [12], and with many IoT threats, users that are not aware of how to use safeguards may be putting themselves at risk and possibly their employers too. The human factor of cyber risk carries incredible importance, as human vulnerabilities are often considered to be the weakest link within information security [13], and thus, it is integral to ensure that organisations train employees to form an awareness and understanding of cyber risks. In turn, users can succumb to a different type of attacker tactic depending on a manner of distinct factors, such as emotions and awareness of security, thus requiring a personalised set of countermeasures for risk mitigation to be effective [14].

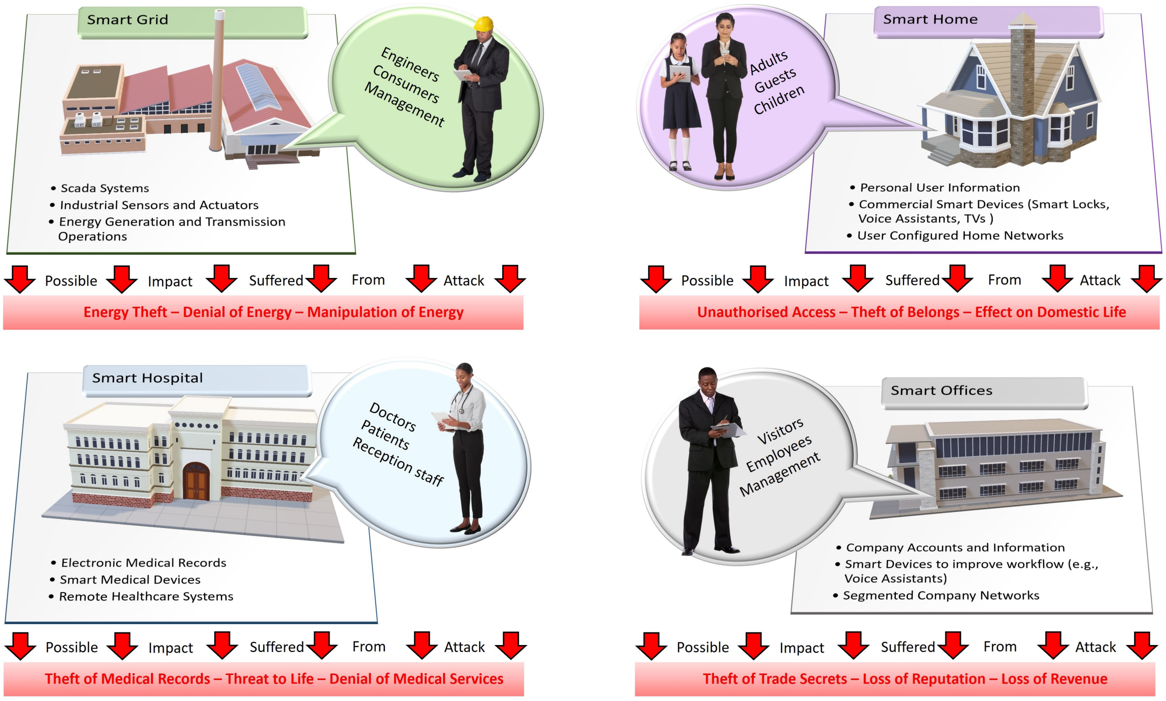
Smart Grid
Engineers
Consumers
Management
• Scada Systems
• Industrial Sensors and Actuators
• Energy Generation and Transmission Operations
Possible Impact Suffered From Attack
Energy Theft – Denial of Energy – Manipulation of Energy
Smart Home
Adults
Guests
Children
• Personal User Information
• Commercial Smart Devices (Smart Locks, Voice Assistants, TVs)
• User Configured Home Networks
Possible Impact Suffered From Attack
Unauthorised Access – Theft of Belongs – Effect on Domestic Life
Smart Hospital
Doctors
Patients
Reception staff
• Electronic Medical Records
• Smart Medical Devices
• Remote Healthcare Systems
Possible Impact Suffered From Attack
Theft of Medical Records – Threat to Life – Denial of Medical Services
Smart Offices
Visitors
Employees
Management
• Company Accounts and Information
• Smart Devices to improve workflow (e.g., Voice Assistants)
• Segmented Company Networks
Possible Impact Suffered From Attack
Theft of Trade Secrets – Loss of Reputation – Loss of Revenue

Figure 1. Examples of different applications of IoT within different domains. Here, we show typical critical assets and users that exist within each environment, as well as the potential impact of an attack.

Researchers publish IoT cyber risk management frameworks targeting risk assessment and control phases to improve the management of IoT cyber risk within various IoT domains. The critical distinguishable features between IoT domains, such as resources, devices capabilities, and legislation, pose a challenge for future works. Core risk parameters such as users, assets, and impact will likely diverge from traditional IT systems, yet be further complicated by domain differences. As an example, Figure 1 shows a number of use cases for various IoT domains. While there are some noticeable overlaps, the types of critical assets, users and potential impact are significantly different. Therefore, one of the biggest challenges for researchers is identifying and anticipating IoT domain specific issues to better manage the security. In the context of IoT cyber risk management, the solution to this problem means creating an effective IoT cyber risk management framework that is applicable within a particular IoT domain and its requirements.

The main contribution to research is our surveying of papers that propose IoT cyber risk management frameworks to provide insight into how IoT cyber risk management frameworks conduct risk management processes. In doing so, we can better understand how current IoT cyber risk management frameworks work, and identify areas that need improvement. Our paper aims to conduct a thorough analysis and critique of cyber risk management frameworks for the Internet of Things (IoT) that have been published in the literature.

The remainder of this paper is as follows. First, within Section 2 we outline the related work, which is followed by Section 3, which details our methodology and research questions. In Section 4, we delve into the results of the IoT cyber risk assessment portion of the survey, with Section 5 analysing the IoT cyber risk Matment survey results. Using the literature results and insights, we then make recommendations for gaps that future researchers need to fill when creating an IoT cyber risk management framework within Section 6. Finally, we form conclusions in Section 7.

2. Related Work

The National Institute of Standards and Technology (NIST) and the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) both carry extensive documentation on cyber risk management. NIST carries a number of popular documents that form the basis of cyber risk management: NIST 800-30 "Risk Management Guide for Information Technology Systems" [15]; NIST 800-53 "Security and Privacy security controls for Federal Information Systems and Organizations" [16]; NIST-800-160 "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" [7]; and NIST 800-39 "Managing Information Security Risk: Organisation, Mission and Information System View" [17]. NIST often works in tandem with ISO/IEC, referring to one another, with ISO/IEC standards being internationally recognised, for example, ISO 27001 [18] compliance is an international standard to manage information security. Despite thorough documentation, NIST and ISO/IEC predominately focus on organisational processes and compliance, which may not be applicable for IoT domains such as smart homes. Not only this, but the NIST cyber security framework is not translated into automated tools and does not allow for the quantification of risk, while ISO 27001 requires a level of compulsory compliance [19]. Kandasamy et al. [19] review well-known cyber risk assessment methodologies and how they are suitable for IoT domains, focusing on NIST, ISO, OCTAVE [20], and TARA [21]. The authors analyse well-known risk management standards and their suitability for IoT domains, based on strengths, weaknesses, and the type of approach used. This paper primarily assesses healthcare and medical IoT devices and assessing well-known frameworks and the uses for IoT, rather than assessing novel IoT cyber risk management frameworks that consider IoT-specific concepts.

Meanwhile, Heartfield et al. [22] conducted an extensive survey assessing cyber threats within smart homes, exploring attack vectors, types of impacts, and defences considering both humans and systems while providing taxonomic classification examples. For the attack vector, the authors classify areas that could be targeted within the smart home, for example wired and wireless communications. Impact types are defined on system and domestic life levels, with the system impact being cyber and physical, while the impact on domestic life explores direct consequences to life, emotions, and user experience. For defences, the authors examine the limited existing smart home countermeasures for the smart home. The open research challenges proposed relate to the improvement of smart home defences, such as the need for cyber–physical intrusion detection systems (IDSs) and better cyber hygiene. While relating to IoT, this paper does not address cyber risk management methodologies but it explores important risk factors, such as threats and impact, documenting the types of threats and impacts smart home users may come across.

In comparison, Nifakos et al. [23] focus on human behaviours that affect the security posture of a healthcare organisation. This paper also documents the types of threats and defence strategies, while assessing the impact of human factors and reviewing use cases of data breaches within healthcare; however, it does not consider IoT. The major challenge found within this work is that training and awareness for healthcare organisations need to be standardised and become inclusive, promoting cyber hygiene and a better understanding of attacks. The main difference between Nifakos et al. [23] and Heartfield et al. [22] is not only the domain addressed but that Nifakos et al. [23] assess well-known risk assessment standards and methodologies like NIST, using them to explore why the human factor of cyber risk is crucial.

Related, Lee et al. [24] contribute a literature review on IoT cyber risk management methods exploring the quantitative and qualitative approaches that organisations may use, such as NIST and ISO/IEC 27005. Due to the limited number of IoT cyber risk management approaches, the authors do not limit the literature review to IoT methods; instead, they review qualitative and quantitative approaches which could be used in an IoT context. The authors conclude that none of the frameworks explicitly address IoT cyber security.

The limited number of works that address cyber risk management frameworks only put emphasis on the most well-known ones, such as NIST. While these frameworks provide standards and methods to best assess and mitigate risk, they do not consider the types of IoT domains and the potential differences that cyber risk management may have on IoT technology. For example, the consideration of smart homes and cyber–physical attacks may be overlooked in normal cyber risk management models. To sum up, prior surveys do not address IoT cyber risk management frameworks.

3. Materials and Methods

In this section, we outline our methodology for collecting articles and the research questions generated from our analysis. Since our aim within this survey is to review models and frameworks that dwell within the IoT cyber risk management space, we chose to adopt PRISMA flow modelling for our literature review process driven by Akinrolabu et al. [25] and Fernandez et al. [26]. This process establishes an eligibility criterion to find the relevant articles that we want to review. The PRISMA flow model in Figure 2 outlines our process for collecting articles. Firstly, we identified peer-reviewed works using IoT cyber risk management keywords in the databases of ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink, Elsevier, and MDPI. Next, we removed non-English language published papers, then filtered out articles published prior to 2015. We chose 2015 because according to Google Trends, the search terms “IoT” and “Internet of Things” started to rapidly increase in 2015 [27]; we assumed that this trend implies an increased level of global interest in IoT, and therefore we decided to review the literature from 2015 onwards. According to the PRISMA protocol, we then screened articles based T+A+K, which assesses the title (T), abstract (A) and keywords (K) to determine if the paper is suitable for discussions into IoT cyber risk management models and frameworks. We then removed any duplicate papers. Finally, we reviewed all papers based on the full content to ensure that contributions from the selected articles propose IoT cyber risk management models and frameworks.

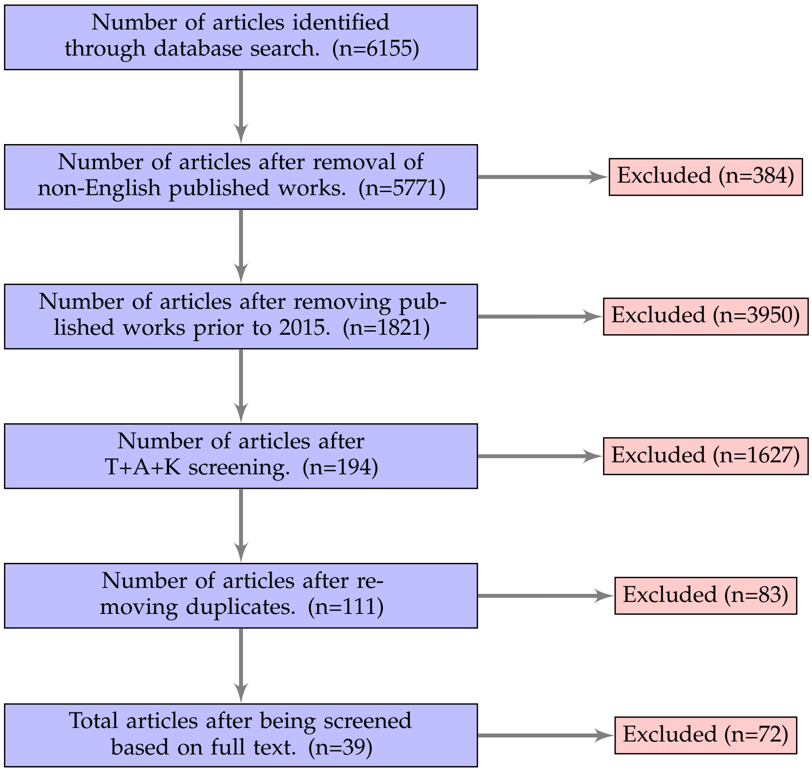
Number of articles identified through database search. (n=6155)
Number of articles after removal of non-English published works. (n=5771)
Excluded (n=384)
Number of articles after removing published works prior to 2015. (n=1821)
Excluded (n=3950)
Number of articles after T+A+K screening. (n=194)
Excluded (n=1627)
Number of articles after removing duplicates. (n=111)
Excluded (n=83)
Total articles after being screened based on full text. (n=39)
Excluded (n=72)

Figure 2. The proposed PRISMA flow model for article selection and results.

Research Questions

Overall, we gathered 39 papers in the domain of IoT cyber risk management. To discuss the fundamentals of IoT cyber risk frameworks, we answered four research questions based on a well-known cyber risk management model from ISO 31000:2009 [28], splitting our work into two high-level processes, IoT cyber risk assessment and IoT cyber risk treatment.

- RQ1: How does the current literature undertake IoT cyber risk identification? IoT cyber risk identification involves processes that uncover various risk parameters needed to assess risk, with cyber risk identification needing to be clearly defined so that the data collected are useful. The most fundamental risk parameters categories defined within NIST and ISO frameworks are assets, users, threats, vulnerabilities, security controls, impact, and likelihood. For IoT, before threats and vulnerabilities can be determined, the elements of an IoT system (assets, users, and existing controls) need to be identified first, ref. [29]. Traditional IT threats and vulnerabilities are well documented within many repositories, for example the National Vulnerability Database (NVD) [30] and Common Vulnerabilities and Exposures (CVE) [31]. However, IoT has the caveat of heterogeneous components (for example, sensors), which suggests that an IoT cyber risk management framework must extend existing threats and vulnerabilities to factor in IoT elements. Due to well-established risk management concepts, impact and likelihood are required to assess risk. This is because impact reflects the result of an attack, which leads to a degree of harmful consequences and, in all likelihood, reflects the probability of an attack [22]. IoT cyber risk management frameworks must ensure that assessed risk values are meaningful and well defined with a clear rationale. For each of the risk parameters uncovered in the IoT cyber risk identification phase, we want to know how IoT frameworks handle this process.

- RQ2: How does the current literature calculate IoT cyber risk? Once risk identification processes are completed, risk needs to be analysed and evaluated. IoT cyber risk calculation requires various methods to analyse and evaluate risk producing results in qualitative, quantitative, or semi-quantitative ways [32]. There are many approaches that could be used to assess and quantify risk, with IoT cyber risk management frameworks using methods like the use of risk matrices, graph modelling, and the use of vulnerability databases to uncover risk values. Without a risk assessment that calculates meaningful risk results, providing in-depth knowledge about IoT security would be difficult. This means that comparing the results to determine if risks are acceptable (risk evaluation) [7] is much harder with critical risks potentially being missed. Given what we discussed, we use this research question to uncover the methods used to perform the IoT risk calculation to determine meaningful results.

- RQ3: How does the current literature control IoT cyber risk? Cyber risk treatment involves processes that deal with how to handle risk responses involving the action of "accepting, avoiding, mitigating, sharing, or transferring risk to organisational operations" [15]. Acclimating an effective and efficient risk response is essential to IoT systems to ensure that assets and users are protected from harm. To achieve this, risk decision making (the process of making decisions resulting in positive or negative consequences [33]) is needed to ensure that all IoT constraints and risk assessment results are factored into the risk response. Controlling IoT risk will likely differ from traditional IT due to novel innovations and functionalities within environments that we have not seen before. Therefore, making IoT risk decisions requires security goals to be clearly defined, with these goals considering the new functionalities to assure conformity. Another element relates to the number of resources (such as money and time) available to an IoT domain and the trade-off between them, for example, if a control is implemented, there will be a cost to run and maintain it [34]. Finally, risk decision making needs to be optimised by minimising negative and maximising positive consequences and probabilities [35]. Given what we discussed, we use this research question to uncover the ways in which IoT risk control takes place, and the ways in which resources and security objectives are factored into frameworks.

- RQ4: How does the current literature monitor IoT cyber risk? Cyber risk treatment considers that the implementation of security decision making is not a static process. Risk parameters may change over time, which influences the level of risk, potentially deeming acceptable risks to become unacceptable. For example, security measures may degrade over time, becoming less effective, a long-standing issue with IoT devices, as they are not always designed with security at the forefront and lack security capabilities [36]. This decrease in effectiveness requires dynamic updates for the risk results and controls, including the monitoring user and asset behaviours as well as new attacks. The remaining IoT risk upon the implementation of controls also needs to be monitored to ensure that values do not go over a given threshold. Monitoring is integral to ensure that risk results and security measures are as accurate as possible; due to this, we want to know how IoT frameworks handle this process.

Using the prior research questions, we conduct an analysis of the 39 papers in the domain of IoT cyber risk management and identify core concepts related to this field based on our findings. An overview of the survey results can be seen within Figure 3, which outlines the fundamental themes our analysis uncovers. In the next section, we explore our results by providing a literature review of the fundamental IoT cyber risk management themes found within papers and provide insight into key areas.

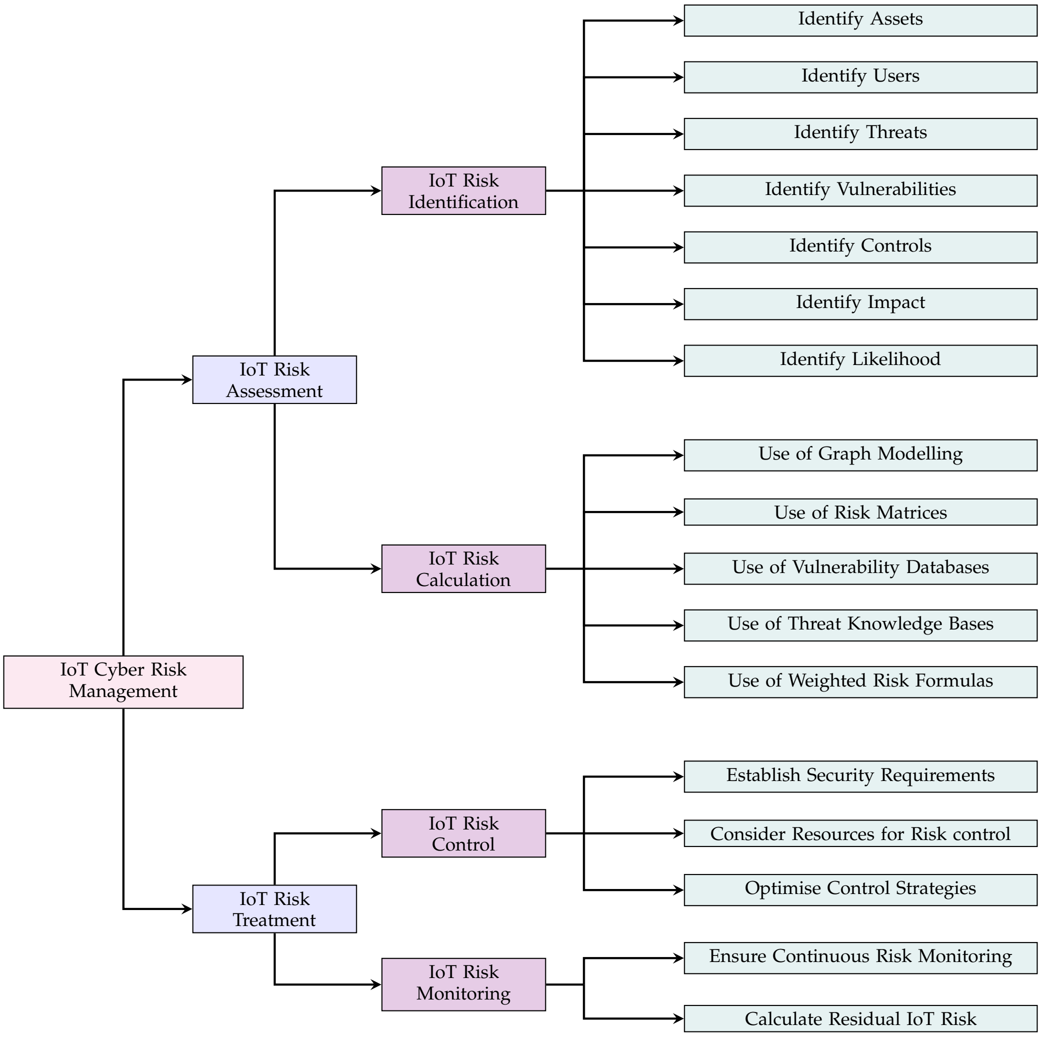

Figure 3. The proposed taxonomy of IoT cyber risk management concepts surveyed and the number of applicable papers. Each arrow signifies the filtering of surveyed papers that apply to each category.

4. Cyber Risk Assessment for IoT Survey Results

IoT cyber risk management strategies assess and determine IoT risk based on risk *assessment*, which uses data from risk *identification* processes. According to ISO [18], risk assessment can be broken down into three major processes, risk identification, risk analysis, and risk evaluation. Within the identification phase, the context of the system is built, with all entities that need to be protected being identified, as well as the potential threats to each entity. This information is then used to analyse risk, assessing probability and impact, with the risk evaluation being used to determine whether risk is tolerable. Therefore, the goal of carrying out cyber risk assessments is to formulate a risk acceptance criteria, perform a risk assessment, and produce results that are meaningful [18].

For IoT cyber risk assessment, additional challenges different to traditional IT are present, with IoT breaches having been well documented within the vast number of environments that harness IoT, with one of the most notable being the Mirai botnet DDoS attacks affecting OVHcloud, Dyn, and Krebs on Security [37]. Overall, the identification and calculation of IoT risk must consider integral differences to become sufficient, with the surveyed papers discussed in this section showing the commonalities and differences in how these processes are undertaken; an overview of the results is found within Table 1.

Table 1. A breakdown of the various papers showing elements of IoT Risk Identification and methods of IoT cyber risk calculation. A tick symbol (✓) represents a paper's inclusion to a category, while a dash symbol (-) represents a paper that is nonapplicable to a category.

	IoT Risk Identification							**IoT Cyber Risk Calculation**				
Reference	**Assets**	**Users**	**Threats**	**Vulnerabilities**	**Controls**	**Impact**	**Likelihood**	**Graph Modelling**	**Risk Matrices**	**Vulnerability Databases**	**Threat Knowledge Bases**	**Weighted Risk Formulas**
Abbass et al. [38]	✓	-	✓	✓	-	-	-	-	-	-	-	-
Aiken et al. [39]	-	-	-	✓	✓	-	-	-	-	-	-	✓
Al et al. [40]	✓	-	✓	✓	-	-	✓	-	-	-	-	-
Ali and Awad [41]	✓	✓	✓	✓	-	✓	-	-	-	-	✓	-
Ali et al. [42]	✓	-	✓	✓	-	-	-	-	✓	-	-	-
Alsubaei et al. [43]	-	-	✓	✓	✓	✓	✓	-	-	-	✓	✓
Andrade et al. [44]	✓	✓	✓	✓	-	✓	✓	✓	✓	-	-	✓
Anisetti et al. [45]	✓	-	✓	✓	-	✓	✓	✓	-	-	-	-
Arfaoui et al. [46]	-	-	✓	✓	-	✓	✓	-	-	-	-	-
Chehida et al. [47]	✓	✓	✓	✓	-	✓	-	-	✓	-	✓	-
Christensen et al. [48]	✓	-	✓	✓	-	-	✓	-	-	-	-	-
Danielis et al. [49]	✓	-	✓	✓	-	✓	✓	-	✓	-	-	-
Duan et al. [50]	✓	✓	-	✓	-	✓	✓	✓	-	✓	✓	-
Echeverria et al. [51]	✓	-	-	✓	-	✓	✓	-	✓	✓	✓	-
Garcia et al. [52]	-	-	-	✓	-	✓	✓	-	-	✓	✓	-
George and Thampi [53]	-	-	✓	✓	-	✓	✓	✓	✓	-	-	-
George and Thampi [54]	-	-	✓	✓	-	-	✓	✓	✓	-	-	✓
Ivanov et al. [55]	-	-	✓	✓	-	-	-	✓	-	✓	✓	-
James [56]	-	-	✓	✓	-	-	-	✓	-	-	-	-
James [57]	✓	-	✓	✓	-	-	✓	✓	-	-	-	-
Kalinin et al. [58]	✓	-	✓	✓	-	-	✓	-	-	-	-	-
Kavallieratos et al. [59]	✓	-	✓	✓	-	-	✓	✓	-	-	-	-
Ksibi et al. [60]	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	✓
Lally and Sgandurra [61]	-	-	✓	✓	-	-	-	-	-	-	-	-
Mohsin et al. [62]	-	-	✓	-	-	-	-	✓	-	-	-	-
Mohsin et al. [63]	-	-	✓	✓	-	-	✓	✓	✓	-	-	-
Nakamura and Ribeiro [64]	-	✓	✓	✓	-	✓	✓	-	✓	-	✓	-
Pacheco et al. [65]	-	-	✓	✓	-	✓	-	-	-	-	-	-
Pacheco et al. [66]	-	-	✓	✓	-	✓	-	-	-	-	✓	-
Parsons et al. [67]	✓	✓	✓	✓	✓	✓	✓	-	-	-	✓	✓
Rizvi et al. [68]	-	-	✓	✓	-	✓	-	-	-	✓	✓	-
Ryoo et al. [69]	✓	-	✓	✓	-	-	-	-	-	-	-	-
Seeam et al. [70]	✓	-	✓	✓	-	✓	-	-	-	-	-	-
Shivraj et al. [71]	✓	-	✓	✓	-	✓	✓	✓	✓	-	-	✓
Shokeen et al. [72]	-	-	-	✓	-	-	-	-	-	-	-	-
Tseng et al. [73]	✓	✓	✓	✓	-	-	✓	-	-	-	✓	-
Vakhter et al. [74]	✓	-	✓	✓	-	✓	✓	-	✓	-	-	-
Wangyal et al. [75]	-	-	✓	✓	-	-	✓	-	✓	-	-	-
Zahra and Abdelhamid [76]	✓	✓	✓	✓	-	✓	✓	-	-	-	✓	-

4.1. IoT Cyber Risk Identification

According to NIST, risk identification is the "Process of finding, recognising, and describing risks", which provides the data needed for a risk assessment [7]. Assets and users are the entities that attackers may target and need to be protected. Information is needed to understand the environment and provide a detailed architecture of a system, which may also include users. Once assets are identified, potential threats and vulnerabilities can be uncovered. These components can combine to create negative events. Threats refer to processes or activities that increase the likelihood of such events, while IoT vulnerabilities are weaknesses that could be exploited. Subsequently, existing security controls can be identified, providing information on how each mechanism can mitigate certain threats and the extent to which they can do so. Additionally, risk parameters can be identified to determine the impact and likelihood of potential threats and vulnerabilities. In the next subsections, we discuss the surveyed papers in the context of IoT risk parameters that need to identified. Figure 4 provides insight into the number of papers that will be explored within each subsection.

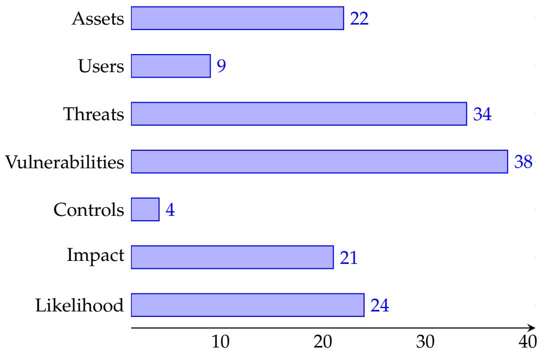

Figure 4. A visual breakdown of the number of papers per IoT risk identification concept. For example, of the 39 collected papers, 22 of them fit into our survey's identified assets category.

4.1.1. Identification of IoT Assets

NIST [8] defines *asset identification* as being the "use of attributes and methods to uniquely identify an asset". The identification of assets may take place as part of a context-gathering phase, which supplies the information needed to understand the environment [60] and to provide a detailed architecture of the systems [71]. In the case of an IoT domain, the information provided from the identification of IoT assets and users is integral to ensuring that other risk management phases capture the most accurate results.

Despite the similarities between IoT domains, devices operate in diverse ways to achieve different goals. Seeam et al. [70] consider this concept by evaluating various IoT domains and proposing the types of assets that may exist in an environment, as well as the fundamental security goals that threats could circumvent. Meanwhile, Danielis et al. [49] use ISO/IEC 2700 to analyse IoT risk, using primary and supporting assets that are inputted within a dedicated worksheet with the various related attributes. In the work of Anisetti et al. [45], an asset assessment phase is used to identify all assets for an organisation, with these assets holding value and nonfunctional properties.

Health-related IoT like the Internet of Medical Things (IoMT) aim to automate healthcare-related systems while also improving the level of care for patients. Nakamura and Ribeiro [64] concentrate on assessing OCARIoT (Smart Childhood Obesity Caring Solution using IoT), a platform that provides an IoT-based system to coach children into adopting healthy eating and physical activity habits. Within the first phase of the model, the IoT domain's context is built, collecting information about assets. As a complement, the second phase builds a data flow diagram, which shows all the points that could be attacked. In the context of wearable health devices, Tseng et al. [73] establish that assets and their value must be identified so that the the accuracy of data flow diagrams can be improved, suggesting that rigorous qualitative analysis must be used to assess the value of assets. In connection, Vakhter et al. [74] focus on assessing miniaturised wireless biomedical devices and establish a model phase that enumerates protected assets that are tangible or intangible.

Smart cities hold a huge amount of data, assets, and users, which can make risk assessment difficult, with a limited number of datasets which can be used. Kalinin et al. [58] overcome this issue by synthetically creating asset datasets to simulate a large-scale dynamic network. The use of a neural network allows the authors to easily decide the types of assets used, tailored to be smart city specific. Alternatively, Andrade et al. [44] focus on critical assets, rather than trying to identify them all. These assets may have a much higher priority due to a higher damage potential, which may propagate within a smart city network.

Unlike other IoT domains, smart homes carry more freedoms due to not being bound by legislation, with users utilising devices how they see fit, which can pose a significant risk to personal life. According to James [57], one of the most critical security objectives for smart homes is to prioritise the identification of user authorisation, where only specific users should have access to resources. Ryoo et al. [69] suggest that an asset inventory of IoT devices needs to be created, with this inventory outlining the components of a smart home environment. The creation of such an inventory may be automatic or semi-automatic, and the information required relates to capturing device capabilities, which can be used to derive the impact on security and privacy.

Kavallieratos et al. [59] present another smart home model that identifies assets in the second phase of their framework, enabling the development of data flow diagrams. Parsons et al. [67] utilise an adapted version of the Health and Safety Guidance (HSG48) to determine the most appropriate assets and users that may be vulnerable to risks in a smart home. In another study related to smart homes, Ali and Awad [41] utilise the OCTAVE Allegro model, which includes a phase that collects asset information through a profile asset approach, primarily focusing on critical information assets. The authors establish a risk measurement criteria before this phase.

Zahra and Abdelhamid [76] propose a risk analysis methodology using EBIOS [77], which also contains a context-gathering phase, aiming to ensure that the IoT domain is identified and described. This phase collects information about assets, different actors and stakeholders, and the parameters that need to be considered in risk analysis. Echeverria et al. [51] incorporate a phase in their approach that establishes the purpose and requirements of the IoT domain, considering other relevant conditional factors that an organisation should consider when defining the environment.

Sometimes, an organisation may need to prioritise the most critical assets. Abbass et al. [38] propose "ArchiMate based Security Risk Assessment as a Service" (ASRAaaS), which follows a "Do–Act–Check" approach starting with the creation of an inventory which contains identified critical assets using risk profiles. Christensen et al. [48] conduct an assessment of evaluation targets, which consists of multiple assets, and identified the components that an attacker would consider valuable. Finally, Chehida et al. [47] use an IoT domain model to aid in finding assets, which helps to avoid overlapping labels for assets.

In another study, Ali et al. [42] emphasise the importance of identifying assets in IoT systems due to their complex interfaces and architectural layers. The authors illustrate this point by highlighting how a seemingly simple device like a smart thermostat can comprise several components such as firmware, personal information, and more. These components are considered valuable assets, and their identification is crucial for ensuring their security and protection. By providing this insight, the authors shed light on the need for a comprehensive approach to IoT security that considers the different layers and components of a system. Meanwhile, Ksibi et al. [60] focus on analysing the abnormal IoT system usage within a model that requires users to be identified by membership and location to devices, data which would need to be collected before the risk model could analyse risk.

IoT assets will likely be dependent on or authoritative of other assets. For example, in the case that an information asset relies on a server, and this server is within a building [78], if the building was to be destroyed, both the information asset and server would be lost [78]. Such dependencies can allow for easier threat propagation, where if a device is dependent on other IoT nodes, the exploitation of a vulnerability can be amplified [44]. Uncovering dependencies requires the interactions and dependencies of an IoT system to be described [51] .

Insight 1: For RQ1, asset classification needs to be dynamic, fitting various standards and prioritising valuable assets, with the ability to be updated when required. The issue with current methods is that specific critical assets may be overlooked, thus being forgotten in the risk management process, with such classifications like tangible/intangible assets [74], primary/supporting assets [49], functional/nonfunctional asset properties [45] not being IoT specific. This poses the question of how IoT assets should be broken down, for example, a device being of more than one asset due to sensor hardware and how device capabilities can be factored in. As an example of non-specific IoT assets, Al et al. [40] define hardware as an asset type but do not expand on how IoT hardware is classified. The main point of contention is how to ensure that sensors and actuators are assessed for risk, with the identification of these components allowing for them not to be missed. Overcoming this, the work of Ali et al. [42] is one of the only papers that breaks down IoT devices by components, while papers like that of Christensen et al. [48] approaches the aspects of an IoT system that could be targeted by an attacker. There is no agreed-upon method for IoT asset classification, which is likely due to the vast amount of IoT domains with assets, capabilities, and users. IoT asset classification needs to be clear to create an asset inventory (potentially for the first time in the case of IoT domains like smart homes) for ease of understanding critical security objectives [57].

4.1.2. Identification of Users

Users require protection from IoT cyber attacks to ensure safety and to protect users from being harmed. Zahra and Abdelhamid [76] suggest that the context state of an IoT risk framework involves not only the collection of assets but the types of risk actors and stakeholders that could be impacted by an attack. Despite this, there is a significant lack of IoT cyber risk management frameworks that prioritise users, for example, users may be expressed as another asset type [47] rather than an individual entity. Researchers have suggested different approaches to mapping assets and users to threats.

For instance, Chehida et al. [47] and Nakamura et al. [64] propose that the impact of attacks on assets and users should be considered in threat analysis. In contrast, Andrade et al. [44] highlight the importance of considering user interactions with real-world physical devices. By adopting these approaches, researchers can develop a more nuanced understanding of the complex relationship between assets, users, and threats in the context of IoT security. While users could be simply viewed as another asset, other frameworks expand on how users can be modelled within the IoT domain based on a set of attributes.

In contrast, Tseng et al. [73] define trust levels that show the access granted by an application to various users. This reflects privileges and user roles that can be used to model trust levels to aid in the creation of a data flow diagram. Additionally, with the second phase of Al et al. [40], a trust model is defined for a device, comprising software, hardware, and data, all of which the device relies on for its security. Rather than considering privileges, Ali and Awad [41] map users to assets to reflect responsibility for that asset.

Another approach from Ksibi et al. [60] describes user types as the membership (insiders and outsiders) and the location of a user in connection to a device (internal or external users). This is used with a formula that deals with the probability of abnormal usage at a storage and processing level. Finally, in our prior work, Parsons et al. [67] classify individual users by identifying high-risk behaviours, familiarity with security, as well as perception and prevention abilities.

Insight 2: Within the surveyed papers, assets and users are often intertwined, making them integral to answer RQ1. IoT devices have more enhanced capabilities than traditional IT hardware due to sensors and actuators, with the involvement of a controller (such as a smart phone) or automated actions based on environmental stimuli (like motion). The number of papers discussing users is significantly less than assets, with users often being seen as another asset to be protected, which may be sufficient for some IoT domains. The complex relationship between assets and users poses an additional need to know how users interact with devices, with Al et al. [40] and Tseng et al. [73] using trust models to define IoT security assurance. However, with IoT domains like smart homes, where there is little regulation, this approach neglects human interaction and the usage of the system and how this may affect risk. For example, in the work of Parsons et al. [67], the lack or abundance of best IoT practices (such as default passwords) can reduce or increase the risk level of a smart home. In turn, without understanding how users interact with devices, the link between a user and the vulnerabilities they may cause could be missed; thus, critical risks could be overlooked.

4.1.3. Identification of Threats

Threats are circumstances with the potential to adversely impact organisational operations assets, or individuals using attacks that allow for "unauthorised access, destruction, disclosure, modification of information, and/or denial of service" [79] by exploiting vulnerabilities. IoT threats are the events that have the potential to adversely impact IoT assets and users [15]. To identify threats in IoT systems, it is necessary to discover their sources and assess their potential impact. IoT risk management frameworks offer several ways to achieve this, including the use of established threat modelling methods, the development of new threat models, and analysis of attack use cases.

Threat-based risk assessment for IoT involves evaluating potential risks associated with IoT devices by analysing and modelling potential threat scenarios. This approach is an essential part of the overall IoT risk assessment process, helping to identify and prioritise potential risks. As noted in [15], this approach involves modelling, developing, and analysing potential threats to determine the overall risk posed by an IoT device or network.

There are several effective threat modelling methods available, such as STRIDE [80] and LINDDUN [81]. Microsoft's STRIDE threat model is the most widely used in IoT cyber risk management frameworks to identify and quantify potential threats. It divides threats into six categories, namely spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [80]. This model has been extensively referenced in recent research on IoT security, including studies on threat analysis [49,59,69,70], threat vectors [42], and attack surfaces [44]. Therefore, utilising the STRIDE threat model can provide a solid foundation for comprehensive IoT security risk assessment and management.

The issue with using STRIDE is that, while it is good for security risks, privacy risks are often not exhaustive, making it insufficient in places where privacy is of the utmost importance. LINDDUN targets the modelling of privacy-related threats, these being linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, and noncompliance [81], while DREAD (damage, reproducibility, exploitability, affected users, discoverability) [82] allows for the comparing and prioritisation of threats using a rating. Since IoT poses a larger threat to privacy alongside containing attacks on sensors and actuation, modifications may be needed to capture all threats that could be high risk. To overcome this, Shivraj et al. [71] simulate their proposed framework using STRIDE, DREAD, and LINDDUN, using LINDDUN to focus on privacy risks. Tseng et al. [73] use the STRIDE and DREAD models to find threats and attack potentials of wearable Internet of Medical Things devices, while Andrade et al. [44] use both models in the context of smart cities.

There are various methodologies available for identifying and mitigating cyber threats, and one such approach is the OCTAVE Allegro methodology as discussed by Ali and Awad in their study [41]. This methodology includes a dedicated phase for identifying potential threats, which involves identifying areas of concern and creating threat scenarios to better understand the various cyber threats that could target smart home data. Meanwhile, Echeverria et al. [51] perform threat modelling using analysis from the OWASP IoT Top 10 project as a way to identify the threats.

Pacheco et al. [66] use anomaly behaviour analysis to identify behaviours that deviate from normal operations, with anomaly behaviour being a threat to IoT systems, with this behaviour being characterised by variables such as hardware configuration and system memory. Abbass et al. [38] propose ASRAaaS (an ArchiMate-based security risk assessment as a service model), which uses the ArchiMate modelling language. The model analyses the potential threats for IoT systems using vulnerabilities which are assessed within attack scenarios.

Zahra and Abdelhamid [76] use EBIOS which includes assessing the context, feared events, and threat scenarios used to study risks. The authors use an example of a IoT threat scenario based on an attacker taking control of IoT processes. Chehida et al. [47] also use EBIOS to formulate a threat list, which classifies eight main categories, for example, threats that cause physical damage (e.g., fires and damage to hardware), unauthorised actions (e.g., the corruption of data), and the compromise of functions (e.g., the abuse of privileges).

Threat classifications can be used to categorise threats in simple or complex ways, with authors defining classifications based on several different factors. For example, threats may be categorised based on the types of impact they cause, such as the impact on confidentiality, integrity, and availability [58]. Threat classification can be based on attacker characteristics and the skills required to perform an attack [43,74], as well as the types of attackers that would target IoT systems [43].

Wangyal et al. [75] consider high-level risk factors that describe how threats may manifest. These factors are categorised in *cyber*, *physical*, and *psychological* groups. Mohsin et al. [62,63] classify IoT threats by core IoT components. *Context threats* are non-malicious imperfections associated with processing communicating information. *Trigger threats* are based on decision making, with triggers for actuation being blocked or incomplete where a decision cannot be made. *Actuation threats* are based on the anomalous behaviours that can cause denied or delayed actuation.

Attack surfaces can be used to define the threat landscape for IoT systems in its entirety. Lally and Sgandurra [61] utilise multiple threat models that relate to an attacker's access type, for example, physical, remote or application access. Rizvi et al. [68] define a threat environment for IoT network to uncover attacks on smart pacemakers, IP cameras, and radio frequency identification devices, using vulnerabilities which could be exploited on these device types. Additionally, James [56] defines two main types of attack surfaces based on attacks associated with local networks, public networks, users and how devices interact. Nakamura and Ribeiro [64] use threat mapping to display all possible security issues that may arise and how these may have been caused, for example, a threat being accidental, malicious, or natural. Pacheco et al. [65] define threat models for each architectural layer of IoT, with each threat model defining the attack surface and the associated entry points.

Finally, rather than providing a method that could be used to identify threats, papers may focus more on specific use cases and attack types. In the work of Arfaoui et al. [46], the authors formulate a threat model based on IoT wireless body area networks, where attacks (impersonation attacks, false data injection, false log-in attempts, sniffing, and eavesdropping) can be dynamic. Ksibi et al. [60] assess tampering attacks targeting a smart insulin pump and Christensen et al. [48] uncover threats towards distributed energy resources. In contrast, Parsons et al. [67] use tactics from Mitre's IoT ATT&CK matrix to formulate an example attack scenario, where an attacker acquires personal credentials to gain unauthorised access to a smart camera account; once access has been gained, the attacker uses the smart camera's functionalities to phish home residents into paying a ransom. As part of their security assessment of knowledge within smart homes, Aiken et al. [39] focus on common attacks that smart home residents need to know, questioning users about social engineering, spoofing, ransomware, denial of service, and man-in-the-middle attacks. Finally, James [57] and Anisetti et al. [45] spotlight the identification of attacks towards IoT sensors and actuators.

While existing threats are well documented, a major problem for IoT threat modelling is the consideration of unknown threats that may quickly emerge due to new technologies and improved attacker skills. For IoT, the new attack surface due to new functionalities and vast number of devices is unpredictable, with unexplored attack techniques and unknown attacks that may emerge [62]. Danielis et al. [49] suggest that new attack scenarios that were previously unknown are entered into a threat database, including attacks on specific IoT systems. IoT intrusion detection systems can aid in uncovering new attacks, with James [56] taking an anomaly detection approach to detect attacks. Here, a baseline model of system behaviour is formed through off-line training, with this model being used to detect anomalous behaviours that deviate from the baseline, which triggers an alert. The author suggests that the proposed system can detect any attack as well as configuration and misuse with fewer false alarms. Meanwhile, the IDS from Pacheco et al. [65,66] also carries the ability to detect known and unknown attacks. Flooding and replay attacks are used to train the system, then two new attacks not used in training, PulseDoS and HTTP GET, are used to test the detection ability [66]. The authors find that the framework can detect known and unknown IoT attacks with high detection rates and low false alarms [65,66].

Insight 3: Another factor of RQ1 relates to identifying potential threats that exist for an IoT domain in an accurate fashion. The most common way to model IoT threats is using STRIDE [42,44,49,59,69,70]. While effective, the use of well-known threat models may not allow for all threats to be uncovered, for example, STRIDE requires other models like DREAD and LINDDUN to uncover privacy risks, like within the work of Shivraj et al. [71]. STRIDE and other well-known models are not explicitly for IoT, which may be an issue when finding an exhaustive set of threats within an IoT domain. However, with the influx of new technologies that benefit attackers and users, emerging and unknown IoT attacks make it near impossible for an exhaustive list of threats to stay the same. Such new threats need to fit into threat models easily to facilitate dynamic decision making despite the unpredictable new threats. Uncovering threats requires a good understanding of assets, users, and the needs they possess, where it is important to ensure that all potential threats towards assets and users are accounted for, with critical threats not being forgotten.

4.1.4. Identification of Vulnerabilities

Vulnerabilities are the weaknesses in "information systems, system security procedures, internal controls, or implementation" that could be exploited by a threat source [16]. Within an overwhelming number of IoT cyber risk management papers, the identification of vulnerabilities is simply a phase within the framework and is not often expanded on [38,41,43–45,47,52,55,60,65,66,70,74,76], with more emphasis on using vulnerabilities for threat modelling. For example, the use of a threat modelling phase requires exploitable vulnerabilities and how these link to threat actors [40]. In other papers, vulnerability identification is undertaken by using various knowledge bases and methodologies that may also be used for threats, such as OWASP [51,64], NVD [50], CRAMM (CCTA Risk Analysis and Management Method) [49], the MITRE CVE list [53,54], and STRIDE [42,59,71].

Risk-related attributes can be used to indicate vulnerabilities [69] as well as contextual information gathered by monitoring an IoT system [46] that could make it easier to find weaknesses. Lally and Sgandurra [61] link vulnerabilities to IoT security requirements, tools for testing vulnerabilities, and threat models to formulate an attack surface. Not only this but vulnerabilities can be linked to attributes like external entities, trust boundaries, data flows, and entry points [73]. Part of this information may relate to the prioritisation of vulnerabilities due to their criticality based on the potential impact [68] or an increased likelihood of being targeted [56,62]. The commonality of vulnerabilities may also be prioritised due to the potential ease of exploit [48].

Vulnerabilities may be simplified into classifications based on risk-related attributes. For example, George and Thampi [53,54] categorise vulnerabilities into software weaknesses and insecure configurations for devices and networks, while Garcia et al. [52] propose eight vulnerability types for general IoT domains. Within the work of James [57], vulnerabilities are associated within a single or multi-state state attack, where more complex attacks exploit vulnerabilities to have multiple outcomes. In contrast, Rizvi et al. [68] uncover vulnerabilities for several devices, these being smart pacemakers, IP cameras, and radio frequency identification devices (RFIDs).

Wangyal et al. [75] propose a classification approach for identifying and assessing cyber risks in IoT systems. The approach categorises threats and vulnerabilities into different risk categories based on attacker factors, such as cyber, physical, and psychological. In addition, the approach also considers the specific IoT components that an attacker might target, such as software or hardware, and breaks down vulnerabilities based on these targets. An attacker's capabilities may also play a part in identifying vulnerabilities [63].

One subset of IoT vulnerabilities relates to human vulnerability/human weaknesses in relation to IoT systems. Human vulnerabilities express the ways that humans can be vulnerable to IoT attacks, which is increasingly more concerning with the large amount of personal information and increased attack surface brought by IoT technology [83]. While an IoT device's software can be updated and patched, humans are not as simple. Humans may be susceptible to psychological attacks or simply not be aware that their actions could lead to an attack. For example, if a user were to fall victim to social engineering, the reason may be a lack of training and awareness of what social engineering is and how it can compromise a system. This notable increase is due to there being more mediums for social engineering than before [84], with IoT devices carrying more capabilities than traditional IT.

Risky user actions can pose as IoT weaknesses, where users with a higher risk appetite can increase the likelihood of an attack happening due to the lack of cyber hygiene. Cyber hygiene refers to the regular good practices and mitigation methods that help maintain security, with the lack of cyber hygiene hampering an IoT domain's ability to respond to attacks [85,86]. Examples of high-risk actions include not changing passwords/usernames [72], the use of unknown public networks [57], and not receiving training when it comes to IoT security [75]. The lack of security knowledge and awareness [39,60,67] refers to the potential lack of security knowledge and awareness of a user about IoT security. Users may become vulnerable to cyber threats due to a lack of training, which can prevent them from understanding how to prevent or respond to such threats. This vulnerability also increases the risk of falling prey to social engineering attacks [41,43,67], such as phishing, which exploit personal factors to gain access to sensitive information. For instance, a user's emotional state and lack of knowledge regarding social engineering attacks can make them more susceptible to such attacks.

Another common high-risk action is the misconfiguration of IoT systems [43,54,56,66], where users configure an IoT system incorrectly or in a fashion that is not secure, for example, not setting up two-factor authentication. Finally, we have the potential misuse of systems [41,48,56,66], which may be intentional with users using a system to perform an attack (e.g., spying or eavesdropping) or unintentional, where users choose to ignore some security mechanisms, e.g., bypassing security processes when using their devices.

Insight 4: The main objective of uncovering IoT vulnerabilities is to clearly define exploitable weaknesses that may become an IoT threat event and dealing with these. Within RQ1, we stated that IoT cyber risk management frameworks need to extend existing threats and vulnerabilities to factor in specific IoT elements. A common theme within the surveyed papers is the consideration of human vulnerabilities due to a lack of cyber hygiene. The main benefit of identifying human vulnerabilities is the understanding of human to asset weaknesses that could affect security, something that is especially important in IoT domains with little to no regulations. Discovering the types of high-risk user actions puts focus on basic IoT practises and easy fixes that can reduce risk, for example, encouraging the use of different passwords/usernames from other accounts [72]. Cyber IoT vulnerabilities can be gathered from knowledge bases, with OWASP, NVD, and the MITRE CVE list being some of the most common. However, these bases are not always applicable to all IoT domains; works like those of George and Thampi [53,54] and Garcia et al. [52] use proposed classifications to overcome this. Moreover, IoT knowledge bases need to be consciously updated due to new vulnerabilities, with unknown vulnerabilities [62] making it difficult to predict the next IoT weakness. Within the work of Echeverria et al. [51], the authors define an attack surface as the sum of all exposures to risks, being the set of known, unknown and potential vulnerabilities as explored by Rizvi et al. [87]. The issue is that unlike traditional IT systems, IoT vulnerabilities (and by extension threats) need to consider non-traditional weaknesses, for example sensor-based attacks and insecure sensor hardware.

4.1.5. Identification of Controls

Security controls are “management, operational, and technical controls” [88] that are used to protect assets and users in different ways. A limited number of papers consider the identification of security controls to facilitate IoT risk assessment. In the context of smart homes, Parsons et al. [67] consider the efficiency of safeguard measures that already exist within a smart home, assessing the quality of awareness-based and practical defences in addition to how these can influence the IoT risk score.

Within the SKIP (self-assessment, knowledge, infrastructure, and practices) survey framework from Aiken et al. [39], knowledge-based questions consider IoT-specific cyber security areas, collecting information about a smart home’s infrastructure and practices. Details about IoT controls are collected here, examining the existing security systems in place, and establishing the network within the home. On the other side, practice-centred questions relate to the self-reporting of best security practices and the extent implemented.

In the context of security, readiness refers to how prepared users are to identify, prevent, and respond to cyber attacks. Within the work of Alsubaei et al. [43], readiness is used to understand the ease of an IoT attack based on the extent to which an IoT domain is prepared to detect, report, and respond when an attack occurs. Expanding this, Ksibi et al. [60] also represent the readiness of a device to detect and react, considering IoT security functions, like encryption and intrusion prevention mechanisms, embedded within the device or controller (like smart phones). These authors also use the lack of security knowledge of the users, which reflects an increased probability of successful attacks. In addition, the authors address the cyber risks at the network level, storage, and processing level, which both incorporate control-based risk factors. Since IoT devices are limited in security capabilities, device readiness may be weaker than expected, with readiness relying on uses to carry IoT cyber security knowledge and training.

Insight 5: Another factor of RQ1 is to identify pre-existing controls that reduce risk and the effectiveness in doing so. Surveyed papers involving control identification are limited, which is an issue for IoT domains that do not have clearly defined controls. In turn, controls that already reduce risk need to be factored into the risk assessment phase to ensure that the risk results are accurate. Overcoming this, the readiness of an IoT domain could be studied by assessing the ability to detect and react to threats from an asset and user perspective much like within the works of Ksibi et al. [60] and Alsubaei et al. [43].

4.1.6. Identification of Impact

Simply put, impact is the “consequential magnitude of harm” from an attack [16]. Users and assets can be impacted by attacks in different ways. Providing specific details about the potential types of impact can help to ensure that a risk model accurately predicts the number and severity of potential losses. The CIA triad, which includes confidentiality, integrity, and availability, has been widely adopted as a suitable model for traditional IT systems and is integral to ensuring information security.

Regarding cyber risk, papers measure the impact of a threat event as the level or amount of CIA (confidentiality, integrity, and availability) loss [43,45,47,49–52,67,68]. For IoT systems, it is crucial to consider the impact on network performance and how security controls may affect network functionality, given the trade-off between security level and impact on network performance [46]. One significant difference between IoT and traditional systems is the extensive use of automation, which poses new threats that may impact the cyber–physical operation of devices. Therefore, cyber security measures should prioritise privacy, trust, and accountability to mitigate the risks of cyber–physical impacts that can be both cyber- and physical based.

The concept of cyber–physical impacts involves understanding the potential physical impacts that users may experience because of a cyber attack, which can lead to real-world consequences. For the use of IoT within organisations, 10 papers consider impact factors that affect organisational operations [41,43,44,52,60,65,67,70,71,76]. First, three of the frameworks refer to "business impact" to describe the cumulative impact on a business, with factors that could vary depending on the business's practices [52,70,71].

One specific type of impact on a business is the decline in reputation for an IoT domain, company/provider [65], with attacks causing negative press. In turn, a loss of reputation could also mean the reduced value of a company/provider's worth [41,60], with Alsubaei et al. [43] defining that the brand value loss is any tangible or intangible losses caused by an attack which can affect an organisation's integrity (reputation), which then leads to a loss of a brand's worth [43]. In contrast, attacks may cause operational impacts [44], meaning that a system no longer functions in the required way, which could then negatively impact enterprise/vocational activities [67,76].

The direct impact of an attack on users contains several factors that affect day-to-day lives. However, the most extreme relates to human autonomy. The impact to life refers to the user's health being put at risk (especially in the case of IoMT environments), as an attack could be life threatening, [60,76] which puts a user in physical danger [43], makes them unsafe [65–67], or leads to loss of life [64,74]. From a more psychological angle, one paper targets the emotional impact on individuals [67]. This explores the emotions, attitudes and behavioural changes that are seen within the user once an attack has occurred, with these feelings being dependent on how serious an attack is and the personality of the individual.

The impact of a cyber attack on a user's well-being can affect how they use other devices and their level of trust in them. In turn, attacks may lead to losses of important services, e.g., taking away essential services (such as water and power) [44]. This is reflected within the work of Pacheco et al. [65], where there is a potential loss or wasting of energy, which costs an individual or organisation extra money, taking away invaluable resources needed to power a city. Other impact types relating to the loss of time [66], resilience, security, and reliability [64] of IoT services, can be considered, with typing being dependent on an IoT domain's needs. One of the most common IoT impacts towards both individuals and organisations is financial loss due to a successful attack [41,43,53,60,65,67]. When an IoT system is compromised, both individuals and organisations will need to recover and control the ongoing damage, requiring a significant budget [43].

Meanwhile, another notable impact type is the loss of privacy that could be inflicted on users [41,43,64,67]. Researchers may consider the direct invasion of personal privacy, which leads to the loss or disclosure of personal information [41,43,49,60,68] and physical privacy because of an attack. This loss of privacy could also propagate to individuals and organisations suffering a loss of control over a system [41,66], which results in unauthorised access and the unauthorised execution of device operations [41]. This may occur when an attacker hijacks a system and takes full or partial control of a system, leaving users unable to use a device correctly and decreasing the amount of control they have over a system. While an attacker could inhibit the functions of a system, an attacker could use their enhanced control to conduct other attacks, such as spying and social engineering.

Insight 6: As discussed within RQ1, determining the value of impact and the types of impact that assets and users may suffer is an integral component of IoT risk. Impact needs to be estimated and defined to ensure meaningful results when used within risk assessment. Different types of IoT impact depend on the priorities of the IoT domain and its context, for example, the functionality of devices. While CIA is an important cyber impact for IoT, it does not encompass the physical, real-world damages that could occur. Overcoming this requires frameworks to focus on the domestic life and business impacts depending on the IoT setting. On one hand, impacts like privacy and monetary losses correlate to well-known traditional IT consequences, while other IoT impacts, such as the loss of essential services [44], also need to be considered. It is also notable that an attack on a supporting asset may affect primary assets, with primary assets possibly being dependent on multiple supporting assets [49]. This link between assets shows the potential for a threat to cascade and impact more than one asset, meaning that one attack could impact multiple assets in different ways. For example, if a smart hub was to be hijacked and an attacker could gain access to other devices, more than one asset would be affected by the attack.

4.1.7. Identification of Likelihood

In risk management, likelihood simply refers to the "chance of something happening" [7]. Likelihood can be represented in a qualitative, quantitative, or semi-qualitative way, with IoT cyber risk management frameworks commonly using numerical scales [45,46,49,50,53,54,58] and quantitative scales [64,75,76].

In the IoT cyber risk management literature, the most used likelihood parameter is the probability of an attack occurring [40,57,63] to predict the change of an attack happening; given the configuration of a device, different attack capabilities can be used, which affects the likelihood of exploitation. This probability can be used to predict the likelihood of an attack happening, given the specific configuration of a device.

Andrade et al. [44] utilise the likelihood of an IoT vulnerability being used to trigger a successful attack while also monitoring maintained behaviour over time, considering the probability that a node would be violated again based on prior behaviour. Echeverria et al. [51] use the OWASP IoT Top 10 to predict the probability of an IoT threat occurring, while Shivraj et al. [71] present the likelihood of attacks on each specific IoT network node.

Rather than estimating the probability of an attack occurring, Tseng et al. [73] focus on the probability of an IoT vulnerability causing damage due to threat exploitation. Meanwhile, Arfaoui et al. [46] consider the frequency of an IoT system being targeted to better understand the number of times an attack may occur, and Kavallieratos et al. [59] consider the probability that a vulnerable IoT node can be infected, recover, and become vulnerable again.

Several factors can influence the probability of an IoT attack occurring. In some cases, researchers target IoT attributes that would allow an attacker to conduct an attack. Christensen et al. [48] use a methodology which assesses the skills, physical accessibility, logical accessibility, attack vector, and vulnerabilities that an IoT attacker would need to uncover the likelihood of potential threats. Vakhter et al. [74] define the probability of an attack based on the IoT attacker's expertise, equipment, physical proximity to a system, device access time, and IoT device information.

Ksibi et al. [60], Alsubaei et al. [43] and Garcia et al. [52] assess the attacker capabilities (ease of attack) and motivation as well as the readiness of a healthcare provider to defend against attacks. Within the work of Alsubaei et al. [43], readiness is represented as a user's lack of training and knowledge as well as the degree to which a healthcare provider is prepared to ″detect, report, and respond“ to an attack. In turn, Parsons et al. [67] consider the risk appetite of users, referring to how high-risk behaviours can affect the likelihood of an attack happening and gauging whether users can effectively prevent and respond to attacks.

Insight 7: In line with RQ1, the probabilities surrounding threat events need to be identified. The IoT likelihood needs to be clearly defined, for example, the probability of an attack occurring [40,57,63] or the frequency of an IoT system being targeted [46]. Predicting attacker attributes allows for a better understanding of how easy an attack may be, with attributes such as accessibility, skills, and equipment being common themes within the surveyed papers. Overall, an IoT likelihood scale needs to be suitable for the assessed environment based on the types of attacks that can be faced; this also means identifying the factors which can affect the likelihood.

4.2. IoT Cyber Risk Calculation

The level of cyber risk is the "magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood" [7], with this phase using the identified risk parameters. Risk calculation is often expressed in a qualitative, quantitative, or semi quantitative way, depending on how comprehensible a risk level needs to be. The most common method of calculating risk is to use "risk equals likelihood multiplied by impact", a simple formula that forms the basis of how risk can be defined. However, within IoT cyber risk management frameworks, risk calculations can be used in different ways. We establish that common ways to calculate risk involve graph modelling, risk matrices, existing threat knowledge bases, and the use of weighted risk formulas. In the following subsections, we discuss the surveyed papers in the context of IoT risk calculation methods. Figure 5 provides insight into the number of papers that will be explored within each subsection.

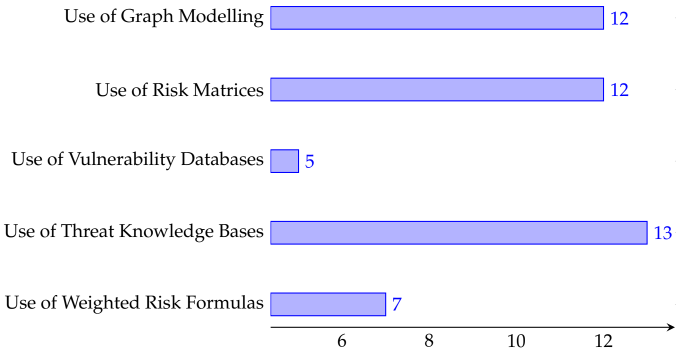

Figure 5. A visual breakdown of the number of papers per IoT risk ? concept. For example, of the 39 collected papers, 12 of them fit into our survey's use of graph modelling category.

4.2.1. Use of Graph Modelling

Within cyber risk management, graph modelling represents how an attacker can infiltrate a network using graphical models to show the potential attack paths that could be used, using such concepts as nodes, edges, and dependencies. It is very common to model data flow and interaction within networks to better understand the areas with high risk, and how a risk could propagate to other nodes. As an example, Mohsin et al. [62,63] formulate IoT network topologies using network mapping to form a connected graph to show the relationships between nodes. Not only this, but the authors also use plotted comparative graphs to show risk exposure scores to different attacks [63].

Bayesian networks are acyclic graph models that are probabilistic, depending on random variables and dependency. Due to IoT data not always been completely known, Bayesian networks can be used to infer the posterior probability distribution of unobserved variables, given evidence, or observed values for other variables in the network [44]. Andrade et al. [44] use Bayesian networks to visualise smart city states and connections of the nodes and estimate probabilities that may not be known. To account for changes over time, dynamic Bayesian networks can be used as a temporal extension to better model probabilities, which can help in providing updated estimates for IoT systems.

In connection, Shivraj et al. [71] propose a generic IoT risk assessment model using a weighted acyclic graph upon modelling information flow within an IoT network. The weighting system signifies priority paths and high impact, accounting for the increased risk in more vulnerable parts of an IoT network. The links between nodes reflect the dependency of one node or another depending on link direction, with nodes also being able to control other links. To demonstrate attack scenarios, an attack vector is formed which consists of aggregated likelihood and cumulative business impact at an IoT node.

This allows the risk of a directly attacked node/edge to be computed using the aggregated risk of a node due to other nodes of differing dependency.

A flow network is a directed graph where a flow starts from a source node and reaches a sink node with no dispersion. Anisetti et al. [45] use these graphs to solve the question of how much IoT risk an organisation can mitigate. The risk value of each IoT asset can be used to find the total maximum flow, given the degree of risk mitigation for a mechanism. In contrast, Ivanov et al. [55] use oriented graphs (directed graphs with no symmetric pair of directed edges) with arc identification representing compromised IoT nodes alongside the possibility of exploiting the vulnerability of the node. The criticality of compromise is computed for each node with the sum of criticality values to reflect the total risk.

Kavallieratos et al. [59] propose an IoT algorithm that can model and visualise the dynamic changes that occur in a smart home network topology. The algorithm also includes a study of the propagation of infection using attack graphs. A smart home network topology is simulated, generating a vector for a risk input parameter, which is followed by the IoT node and edge generation. The algorithm then visualises a smart home network topology with the given IoT risk metrics while considering malfunctioning or intermittent availability out of a user's control. To find IoT risk, the algorithm uses a conditional probability function which determines the state of risk, describing these states as vulnerable, infected, quarantined, healthy and intermittent.

George and Thampi [53] propose an IoT graphical model that captures multi-stage and multi-host IoT attacks through the linking of vulnerabilities found within networks, using graph modelling to uncover vulnerability patterns. Here, a probabilistic metric is applied to the corresponding edge nodes in the graph, and this enables the computation of a cumulative risk corresponding to each attack path. Here, IoT Vulnerabilities are assessed based on their ease of exploitability, by analysing the set of all vulnerabilities that can be exploited on each device within an Industrial IoT (IIoT) network. This provides a better understanding of the overall security posture and exploitable vulnerabilities in the network.

George and Thampi [54] focus on a multi-attacker and multi-target graphical model aimed at showing attack paths to target nodes within IoT edge computing networks. Vulnerability graphs can be created to better understand the potential attack paths that an attacker may use to exploit vulnerabilities in a system. These graphs can help to identify potential entry points and types of vulnerabilities that can be exploited. This is done by estimating the likelihood of an edge device being targeted, which can then be used to find the cumulative likelihood of all attack paths from attackers.

Duan et al. [50] use a Hierarchical Attack Representation Model (HARM) [89] for IoT. This is a two-layer hierarchy model which is used to separate network topology information and vulnerability data from each node. IoT risk is calculated using the probability of a successful attack on each node, with multiple vulnerabilities being represented by AND and OR logic gates, where AND shows that all IoT vulnerabilities must be exploited to compromise the node and OR means that an attack can gain control by exploiting even only one of them. Finally, the IoT risk of different attack paths is represented as the accumulation of all node risk values, which allows for the highest risk paths to be assessed.

James [56,57] proposes the use of finite state automata to demonstrate state transitions as an attacker exploits vulnerabilities in IoT systems, rather than focusing on data flow. This approach can be used to determine the potential success of an attack by analysing the various states an attacker would go through when attempting to exploit vulnerabilities in the system. Attack transition flow can be represented visually in transition graph showing the requirements needed to reach the next state. This transition could be simple, for example a single state or multi state attack with states that are in succession to one another. In the case of a more complex IoT attack, there may be multiple state transition pathways, making it non-deterministic, and providing the attacker with several options to take.

Insight 8: Within RQ2, we stated that we want to know the ways in which IoT risk is calculated. Graph modelling provides a holistic view of an IoT network's relationship between nodes and dependencies, modelling data flow and interaction visually using directed graph types [55]. IoT networks and attacks can be simulated, displaying the paths of single and multi-state attacks [56,57] and entry points that an attack could use [54]. IoT risk formulas and values can be integrated onto graphs to show risk, for example criticality of compromise [55], which allows for a thorough risk evaluation. Noticeably, Bayesian network graphs are most used within cyber risk assessment papers due to a lack of known data and uncertainty around impact and likelihood values. A dynamic modelling approach that can re-calculate risk upon changes is needed for IoT networks to ensure that risk result is correct, which also allows for the calculation of risk mitigation when a control is implemented [45]. Consequently, the surveyed papers do not seem to consider a user's relationship to an asset within an IoT network, which negates the analysis of good cyber hygiene. It is easy to see how graph models can display IoT dependencies and threat propagation within a network. Within Shivraj et al. [71], more edges means more dependencies, being able to represent a highly dependent network. Not only this, but the authors can simply show the dependency or control of one node on another node (and vice versa) by the direction of the link. Meanwhile, Kavallieratos et al. [59] consider dynamic dependencies of a network when a malware infection is propagated. To do this, dependencies are analysed using a smart home network topology modelling algorithm based on functional, physical and communication mappings. As we have discussed, threat propagation can cause a cascade in impact on more than one asset with dependencies, making it extremely important to assess within the calculation of IoT cyber risk.

4.2.2. Use of Risk Matrices

A risk matrix is a well-known method used to describe the probability and impact associated with an attack [90] which can be used to produce a risk value in a qualitative or semi-quantitative way. Wangyal et al. [75] analyses IoT risk using a matrix that describes risk probability and impact, resulting in a qualitative result based on the risk response: avoidance, mitigation, transference, and acceptance. Meanwhile, Shivraj et al. [71] represent the impact at a IoT network's node using an impact matrix, with this then being integrated to show the cumulative impact for an attack vector. In contrast, George et al. [53,54] utilise an adjacency matrix to indicate IoT hot spots in a network and how they are connected within the system In addition, to define IoT risk, George et al. [53] finds the cumulative IoT risk of an attack pathway and represents it as a threat score matrix, mapping the nodes and links of a pathway with the calculated score.

Vakhter et al. [74] use risk matrices as part of a three-tiered scoring system based on IoT threat characteristics that affect impact severity and probability of an attack occurring. Upon the creation of a risk matrix, different colours are used to represent the various levels of risk from very low to very high, allowing for risks to be prioritised, with the authors suggesting the modification of a risk matrix to prioritise impact in cases were an IoT attack could threaten life.

Nakamura and Ribeiro [64] express the probability and impact of IoT attacks using a measurement criterion of low, medium, and high, which is then utilised in a risk matrix to evaluate different attack scenarios. For example, a low-impact and probable IoT attack scenario would be considered low risk. The risk matrix provides a basic calculation to express the risk value associated with each attack scenario, making it easier to identify and prioritise potential risks. Unlike prior papers, the Common Vulnerability Scoring System is used by Ali and Awad [42] to formulate a threat score matrix for smart thermostat components using STRIDE, where each STRIDE attack group is mapped to various system components (e.g., firmware and credentials) by threat scores (such as high and critical levels of threats). Danielis et al. [49] use a STRIDE-per-element matrix that shows attacks based on STRIDE mapped to system components. However, the STRIDE-per-Element matrix often excludes threats that were relevant, such as all data flows being affected by spoofing attacks rather than others like man-in-the-middle attacks.

Wangyal et al. [75] have adopted a project management approach to assess IoT risks, which includes a three-step process for formulating the risk assessment process. The first step involves gathering risk specifications through a literature survey. By reviewing existing literature, the authors can identify potential risks and develop a better understanding of the overall risk landscape for IoT systems. Upon finding 28 risk factors, these are analysed using and risk matrix, mapping the risk probability and impact of risks, classifying them based on risk avoidance, risk mitigation, risk transference, and risk acceptance. Finally, is the risk evaluation phase which evaluates proposed countermeasures and quantifies the risks using a risk formula. The formula first finds a risk value based on the approximated asset value, value of threat, and value of vulnerability, with the second using impact, probability, and value of vulnerability.

Within Echeverria et al. [51] proposed a risk assessment model that considers hardening processes, which is aimed at minimising the attack surface. The authors use compliance class scores based on CIA impact, For example, class one reflects a limited impact on the IoT system where a low potential impact on confidentiality, a medium potential impact on integrity, and a medium potential impact on availability. The risk matrix describes the compliance class score and an attack's probability of occurrence, shown within a scale of 1 to 10, which reflects critical, high, medium, low, and null risk levels.

Since IoT and attacker behaviour are non-deterministic in nature, Mohsin et al. [63] use a Markov Decision Process model to represent system states. The authors use a transition probability matrix which represents the transition probabilities of all states, since moving from one state to another within an IoT system is probabilistic based on the current state and the action that triggered the transition. This non-deterministic and dynamic nature is also reflected within Andrade et al. [44] who use dynamic Bayesian networks to model the dynamic nature of IoT and produce probability of attack matrix is also used to express the conditional probability.

Chehida et al. [47] propose a methodology for assessing cyber security risks in water management systems. After uncovering the assets in the system and creating a threat list using EBIOS, the authors use a threat-asset matrix to map potential threats to each asset. This mapping allows each threat to be linked to specific security objectives and the countermeasures needed to achieve those objectives.

Insight 9: Another method for RQ2 is the use of a well-defined IoT risk matrix, which can be an easy way to show risk. It is integral for a risk matrix to have a defined set of risk values that allow for the evaluation of risk. A basic IoT risk matrix displays risk by mapping a threat by its impact and likelihood value, for example, Vakhter et al. [74] denote risk on a very low to very high scale depending on impact severity and probability of an attack occurring. Interestingly, IoT risk matrices are often used alongside other methods, for example a risk matrix can be used alongside graph modelling, with George et al. [53,54] using graphs and a corresponding adjacency matrix. The non-deterministic nature of IoT and attackers needs to be considered when assessing risk, with an IoT risk matrix potentially being used to model dynamic system nature, for example producing probability of attack matrix from a Bayesian network model [44] or using a Markov Decision Process model to produce a transition probability matrix [63].

4.2.3. Use of Threat Knowledge Bases

According to NIST, threat intelligence is the information that has been "aggregated, transformed, analysed, interpreted, or enriched" [91] to provide context for decision-making. In the context of IoT, this means collecting applicable IoT threat information from various sources to form a threat knowledge base that can be used within IoT cyber risk management frameworks. Creating an IoT threat knowledge base allows an organisation or individual to assess threats and vulnerabilities that may not be considered in traditional IT system knowledge bases, for example sensor and actuator threats.

Zahra and Abdelhamid [76] build a knowledge base for estimating security needs and sources of IoT threats by using attacks found within EBIOS. They attribute baseline values of severity and likelihood to each attack and uncover sources for these attacks. This knowledge base can be used to carry out risk assessments by estimating the risk associated with different threat scenarios, where one or more attacks may take place. The associated risk values can then be combined to find the total risk of these scenarios. In contrast, Chehida et al. [47] also use EBIOS attacks to form a threat list, which is then used to map threats to threat classifications and assess their potential impact on systems based on the CIA model. However, they do not provide direct impact values for the attacks.

Alsubaei et al. [43] use current IoT literature to develop a taxonomy for the security and privacy of medical IoT. This taxonomy is used to determine the architectural layers of IoMT and identify potential attacks that may target these layers.

To expand the threat knowledge, attack properties such as the difficulty of attack, CIA impact applicability, the method of carrying out each attack, the level of compromise, and the origin of the attack can be associated with each attack. This approach is used in various works, such as Ali and Awad [41], who curate smart home threats and link impact types, assets, and risk scores to them.

The use of a defined criteria to estimate impact and likelihood can be easily applied to vulnerabilities as shown within Nakamura and Ribeiro [64]. Here, the authors categorise low, medium, and high values using strict definitions. For example, a vulnerability with a high likelihood of exploitation would typically have a history of malicious incidents, motivated threat agents who can exploit the vulnerability, and assets that contain the vulnerability.

In turn, each risk value uses a simple impact multiplied by likelihood calculation that produces a risk score, which is linked to a multidimensional matrix that displays the attack pathway, threat agent, associated assets, and threat that represent each risk. Tseng et al. [73] utilise DREAD as part of the criteria to estimate the potential of attacks. They produce a table of threats ranked by potential damage, reproducibility, exploitability, the number of affected users, and discoverability. The authors use a scale of high (3), medium (2), and low (1) to rank each of these criteria. As an example, an attacker that performs a man-in-the-middle attack targeting an IoT mobile application is rated as a medium risk as the total DREAD score is 8 out of 15, with reproducibility being the highest rating due to the ease of attack.

Within Pacheco et al. [66], a smart water security development framework is presented which reflects a 2-D architecture that can be used to assess risks within a smart water system. This framework focuses on capturing the attack surface, impact, and priority planes at different architectural layers (end device, communications, services, and application layers). The threat knowledge bases are formed by focusing on attack surfaces within each layer and associating impact types and priorities within each. For example, at the communications layer one attack surface is protocols, which can impact control, human safety, time, money, and energy are identified as high level priority.

Threat knowledge may require IoT cyber risk management frameworks gather data from users to better understand human vulnerability. Parsons et al. [67] take this into consideration and assess various parameters that could affect impact and likelihood of attacks based on user actions. Here, high risk behaviours, security familiarity, the ability to perceive and prevent attacks, as well as the impact and efficiency level of each user are used to curate risk profiles and analyse the effect of user action on how risk can be predicted.

Insight 10: In reference to RQ2, IoT threat knowledge bases are repositories containing all the risk knowledge needed to calculate risk and the calculated total risk given a threat event. A new IoT threat knowledge base can prioritise a particular IoT domain and allow for threat event ranking based on risk scores, However, there is no single knowledge base that exists for IoT, which requires new bases to be created. Since there is no agreed upon knowledge base method, different approaches can be used to ensure that risks values are evaluated. It is notable that works such as Zahra and Abdelhamid [76], use existing IoT works to form knowledge bases, such as the use of traditional IT bases like CVE and EBIOS. The creation of an IoT threat knowledge base allows for many risk totals based on simple likelihood multiplied by impact scores per threat event, which could be used to calculate risk in a matrix. Given that a new repository may need to be formed, user cyber hygiene can also easily be considered and assessed [67].

4.2.4. Use of Weighted Risk Formulas

Weighted risk calculations can be used to adjust the importance of a given risk parameter. Rather than simply using multiplying likelihood by impact, weighted formulas prioritise certain likelihood and impact metrics. As an example, Andrade et al. [44] form a quantitative assessment of IoT using security weightings for different IoT areas within smart cities, such as the economy, environment, and society, to be prioritised. The process of defining weighting provides freedom for users to easily modify risk scores. This allows the authors to consider the different needs of each smart city and the areas of security that city officials may want to prioritise. Therefore, the weighted sum of a smart city's security is the sum of all assigned weights of each factor. Meanwhile, Alsubaei et al. [43] states that a user needs to define the weights using a specific 1 to 10 scale, with worst-case scenarios being assigned a 10.

An IoT cyber risk management framework may use different impact types to show how a smart domain is affected by an attack. For Parsons et al. [67], impact is defined as the weighted impact sum that represents types of impact for a smart home, such as the impact domestic lives of the smart home inhabitants and cyber impact on systems. Correspondingly, Ksibi et al. [60] define weights as a scale from 1 to 10, with these weights reflect different impact types of financial risk, brand value loss, data theft, and threat to life. Here, risk is evaluated depending on the related vulnerabilities, threats, likelihood, and the impact of an attack, with risk impact using weights to associate classes of impacts.

Unlike other papers, Aiken et al. [39] propose an initial attempt at an IoT-based smart home security assessment named SKIP (Self-assessment, Knowledge, Infrastructure, and Practices). They use self-assessment questionnaires (related to understanding IoT terminology, and assessing the understanding of IoT information systems, security, and cyber-attacks), knowledge (questioning the user on security systems, attack scenarios, legal issues and general IoT knowledge), details into the smart home infrastructure, and IoT practices (e.g., questioning users about how they use security systems). All this data is used to form a weighted composite score to estimate risk, with the weightings used to prioritise practices over knowledge and infrastructure, as the actions that users take are more important and better express high risk actions a user may be taking.

Weighting can also work alongside graph modelling, with Shivraj et al. [71] suggesting that users can signify paths of priority by factors like impact, generating weighted attack trees. Weighted graphs have assigned values that represent some form of cost, such as impact and likelihood. Finally, George and Thampi [54] use weighted and directed graphs with weights representing the risk likelihood assigned to network pathways, with the total risk likelihood of a path being the product of all weights on all links.

Insight 11: Another solution for RQ2 is the use of IoT risk weighting which helps to prioritise impact, certain assets, and users etc. Weighting signifies that a given risk value is deemed as critical over other values, for example, an IoT domain may prioritise the potential impact to life within threat events over cyber impacts. This allows for an IoT cyber risk framework to assess risk based on criticality, as the weights will likely change the value of risk. Weighted scoring is also useful in assessing the security of users, with Aiken et al. [39] using weights to estimate risk using a questionnaire based approach. Not only this, but other methods of risk calculation (such as graphs and risk matrices) can use weightings, making this easy to implement to increase prioritisation on selected risk components.

5. Cyber Risk Treatment For IoT Survey Results

Upon IoT cyber risk management strategies assessing and determining IoT risk based on risk *assessment*, results are used to establish risk *treatment*, which allows for the implementation and evaluation of security controls to mitigate risk. Upon the completion of a risk assessment, processes to modify risk can be introduced, taking risk assessment results into account [18], with risks being monitored to ensure risk treatment is effective. As defined by ISO, risk treatment involves a mirage of processes, for example, the selection of risk treatments, implementation of required actions and determining whether an acceptable level of risk has been met [92].

On the surface, treating risk requires risk responses to be assessed, with NIST referring to risk response as the decision to accept, avoid, mitigate, share, or transfer risk to decrease risk to tolerable levels [15]. However, further analysis into mitigation methods is needed to ensure that mitigation controls are effective. Despite well-crafted risk treatment phases of cyber risk frameworks, IoT carries significant challenges when treating risk that differ from traditional IT, for example the lack of device hardware and software capacity for security and limited resources (money etc). Not only this, but in private IoT domains like smart homes, security relies on user's carrying out good practices due to the lack of required standardisation. It is notable that IoT risk treatment categories contain significantly less papers, as shown within Table 2.

Table 2. A breakdown of the various papers showing elements of IoT risk control and IoT risk monitoring. A tick symbol (✓) represents a paper's inclusion to a category, while a dash symbol (-) represents a paper that is non-applicable to a category.

	IoT Risk Control				IoT Risk Monitoring	
Reference	**IoT Control Strategies**	**IoT Security Requirements**	**IoT Risk Resources**	**Optimise IoT Control Strategies**	**Continuous Monitoring**	**Residual IoT Risk**
Abbass et al. [38]	✓	✓	-	-	✓	-
Aiken et al. [39]	-	-	-	-	-	-
Al et al. [40]	✓	-	✓	-	✓	✓
Ali and Awad [41]	✓	✓	-	-	-	-
Ali et al. [42]	-	-	-	-	-	-
Alsubaei et al. [43]	✓	-	-	-	-	-
Andrade et al. [44]	✓	✓	✓	-	✓	✓
Anisetti et al. [45]	✓	-	-	✓	✓	✓
Arfaoui et al. [46]	✓	✓	-	✓	✓	-
Chehida et al. [47]	✓	✓	-	-	✓	-
Christensen et al. [48]	✓	✓	-	-	-	-
Danielis et al. [49]	✓	-	-	✓	-	-
Duan et al. [50]	-	-	-	-	-	-
Echeverria et al. [51]	✓	✓	-	-	✓	-
Garcia et al. [52]	-	-	-	-	✓	-
George and Thampi [53]	✓	-	-	✓	-	-
George and Thampi [54]	✓	✓	-	-	-	-
Ivanov et al. [55]	✓	-	✓	✓	-	-
James [56]	✓	✓	-	-	-	-
James [57]	✓	✓	✓	-	-	-
Kalinin et al. [58]	-	-	-	-	✓	-
Kavallieratos et al. [59]	-	-	-	-	-	-
Ksibi et al. [60]	-	✓	-	✓	✓	-
Lally and Sgandurra [61]	-	-	-	-	-	-
Mohsin et al. [62]	✓	✓	-	-	-	-
Mohsin et al. [63]	✓	✓	-	-	-	-
Nakamura and Ribeiro [64]	✓	✓	-	✓	-	-
Pacheco et al. [65]	✓	✓	-	-	-	-
Pacheco et al. [66]	✓	✓	-	-	-	-
Parsons et al. [67]	✓	-	✓	✓	-	-
Rizvi et al. [68]	✓	✓	-	✓	✓	-
Ryoo et al. [69]	-	-	-	-	✓	✓
Seeam et al. [70]	✓	✓	-	-	✓	-
Shivraj et al. [71]	-	-	-	-	-	-
Shokeen et al. [72]	✓	✓	✓	-	-	-
Tseng et al. [73]	✓	✓	-	-	-	-
Vakhter et al. [74]	✓	-	-	✓	✓	-
Wangyal et al. [75]	✓	✓	-	-	-	-
Zahra and Abdelhamid [76]	✓	✓	-	-	✓	✓

5.1. IoT Risk Control

Security controls are the "means of managing risk" referring to all mechanisms that can reduce risk, such as good practices, policies, and physical controls [16]. In the case of mitigation, risks need to be treated appropriately by the most suitable yet effective controls which takes further evaluation, implementation, and prioritisation [15]. IoT Cyber risk management frameworks must contain a phase that forms strategies to combat risk, for example a risk mitigation phase where risk assessment results are evaluated and security controls or risk response are applied to reduce risk to an acceptable level [38,40,60,74,76]. On a surface level, implementing IoT control strategies based on the prioritisation of critical risks is a simple view of combating risk in an effective way, for example, the elimination of the top five most critical IoT vulnerabilities [55] or use of NIST's frameworks [44]. IoT risk assessment results show critical areas of concern that should be responded to [43] and security controls can be used to ensure that security requirements are achieved [64,65]. For Shokeen et al. [72] vulnerabilities that can impact IoT data are assessed, with risk control focusing on whether vulnerabilities are controlled and if IoT data is secure. However, the effectiveness of an IoT security control also needs to be considered, For example Parsons et al. [67] explore the effectiveness of IoT security controls for smart home environments, assessing if controls are effective enough to reach an acceptable level of risk.

Within the surveyed papers, the selection of risk controls are driven by literature and applied to IoT domains by means of discussion, exploring how these controls can be applied to reduce IoT risk [41,47,68,70,75]. For example, Tseng et al. [73] discuss controls that combat spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege in the context of IoT, while Danielis et al. [49] build a IoT risk catalogue using Deutsche Telekom's ISO/IEC 27001 certified privacy and security assessment document [93]. Controlling risks can support cyber resiliency, which is the ability to "anticipate, withstand, recover from, and adapt to adverse conditions". Mohsin et al. [62,63] focus on building IoT resiliency against attacks and assess how attacks can impact resiliency, for example, the number of services per actuator opens more entry points for attackers and can reduce actuation resiliency. One of the common suggestions within the surveyed papers is the use of hardening, which is a process that eliminates attacks by patching vulnerabilities and "turning off non-essential services" [94]. Despite IoT vulnerabilities often not being patchable, there associated IoT components that can be hardened, like mobile operating systems and physical access [48]. For IoT, Echeverria et al. [51], focus on implementing hardening controls where possible, with IoT vulnerabilities being patched and ports being switched off to shrink a system's attack surface. George and Thampi [53,54] use graph modelling to propose algorithms uncover strategies to eliminate risk. These algorithms aim to reduce threats within network pathways by removing high threat paths, low hop paths, and the detection of high risk nodes [53] which can lead to the isolation of high risk devices [54].

Security control decision making is integral for IoT as it helps to select security controls based on control properties like strength and the degree risk is mitigated [45], for example security controls used to prevent risk occurrence [38]. Within Pacheco et al. [66], an action Handling unit for security control decisions is used, which picks security actions based on the amount of risk that can be reduced. Ivanov et al. [55] use a countermeasure selection module which implements vulnerability search algorithms to find intruders and prompt action to be taken, when an intruder is removed from the system, the risk level is minimised. Within Arfaoui et al. [46], dynamic decisions are used to adjust security levels to an acceptable level. The framework uses sensor behavioural patterns that have an associated risk thresholds (accepted level of risk) decided by security admins, where if a level is higher than the risk threshold for a device, it should switch on more effective security controls.

In contrast, an Intrusion Prevention System (IPS) that can detect an intrusive activity and attempt to stop an attack from happening [95] is proposed by James [56], which can be used to choose risk control strategies based on the causes of risk, with the system performing preventive actions once a strategy has been formed. IoT mitigation strategies are chosen using several distinct factors, e.g., the root of risks that have been evaluated, the common causes, suitability, and the required resources needed. Based on these factors, mitigation solutions are created based on the selection of controls [56,57] An IoT strategy can be accepted, allowing for the control be implemented, or rejected, where evaluation will need to take place again [57].

Insight 12: Within our discussion, we have shown that IoT risk control greatly relies on risk assessment results and the need to reduce risk to an acceptable level, thus a robust IoT risk control strategy needs to prioritise critical risks using reliable controls. When answering RQ3, one of the main pitfalls of IoT cyber risk management papers is the lack of risk control processes that are discussed. Due to the nature of IoT, a framework that simply states to implement a control to reduce risk may not always be applicable or may be hard to implement. Papers such as Chehida et al. [47], contain a IoT risk control phase, but do not provide insight into controlling risk to an acceptable level. In turn, there is no agreed upon set of controls for IoT, with papers often using threat attributes (such as suggesting controls that combat STRIDE threats [73]). However, CIS controls can be applied to IoT domains, with CIS publishing an IoT companion guide [96] that explores how each control may or may not be suitable for an IoT domain.

Assessing the literature brought to light three common themes that expand IoT risk control beyond papers that simply state to apply controls. Firstly, is the need to establish security requirements for emerging IoT domains like smart homes, to better understand acceptable risk. Second is the consideration of resources needed to facilitate risk control processes. Finally, is the ability to optimise IoT risk control by considering various factors like resources. In the next subsections, we discuss the surveyed papers in the context of these IoT risk control themes. Figure 6 provides insight into the number of papers that will be explored within each subsection.

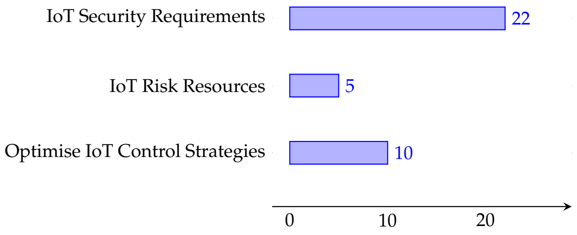

Figure 6. A visual breakdown of the number of papers per IoT risk control concept. For example, of the 39 collected papers, 22 of them fit into our survey's IoT security requirements category.

5.1.1. Establish Security Requirements

One of the first risk control processes within the work of Zahra and Abdelhamid [76] is to identify the security objectives that relate to identified risk and choose the controls that reduce the effect of attack or ensure prevention. According to NIST, security requirements specify "the functional, assurance, and strength characteristics for a mechanism, system, or system element" [7] which are derived from systems such as laws, policies, standards, to ensure the confidentiality, integrity, and availability of a system [15]. Within the work of Chehida et al. [47], IoT controls are based on the security requirements of an IoT system using the CIA model, with security requirements leading to the implementation of technical controls, which are then justified by how or what the objective aims to protect. Christensen et al. [48] suggest that IoT security requirements should be specified at a development level to better understand the parts of the system that need increased security, the security goals that should be achieved, and how controls should be implemented. These requirements need to be clearly defined, for instance, within smart cities, security requirements need to ensure that only secure IoT services and devices are created and implemented [70]. To accomplish clarity, an IoT security assessment checklist could be used to ensure that security requirements are met [72].

Security policies provide a criterion that facilitates security services [15], with IoT risk assessment results also being used to facilitate security policies and requirements by ensuring they are up to date to maintain security [38,46,65,66]. Using security policies relating to authentication and access control can serve as preventive measures that decrease the likelihood of easy attacks, as well-known vulnerabilities within IoT often relate to weak, guessable, or hard coded passwords with attacks that can be avoided. For example, password policies can be used to lock-out attackers that try to brute force access, while controller policies avoid false requests. These measures make brute force attacks impractical. Therefore, IoT security policies need to be implemented as effectively as possible to prevent attacks. Poor password policies negate password length and complexity, which can lead to brute force attacks [44,68], and access control policies not being implemented correctly makes it very easy for an attacker to gain access [54], Therefore, IoT security policies need to be reviewed [54], with Ksibi et al. [60] considering security policy issues, such as non-conformity and misconfigurations that can affect policies from operating as intended and need to be tighten. Within the work of Wangyal et al. [75], a risk that is of a low likelihood but high impact reflects a lack of enforced security requirements, which can be transferred with the help of a policy or insurance adoption. Nakamura and Ribeiro [64] suggest that stakeholders of the OCARIoT platform should build a security policy that ensures security objectives, such as smart applications and devices being coded and transported securely. Such policies need to focus on the authors' risk assessment results, and the safety of the operational aspects of the OCARIoT platform pertaining to its safety, security, reliability, resilience, and privacy.

Smart homes are often not regulated with the same rigour that an organisation can provide, with risk assessments needing to be used to define security requirements [57]. By extension, Ali and Awad [41] suggest that risk assessment is one of the steps to understanding smart home security and facilitating the establishment of appropriate security requirements to ensure that they are improving. Given the nature of smart homes, Mohsin et al. [63] build functional and environmental requirements based on operational policies to reflect how sensor data are processed and actuation is triggered, with these policies being mapped to IoT controllers. Despite traditional security requirements relating to confidentiality, integrity, and availability being used for IoT security policies [51], IoT risk management frameworks have shown the need for tighter security requirements due to the increased physical damages and domestic impact that an attack may have. Due to this, Mohsin et al. [62,63] establish user-defined policies to act as satisfying conditions that trigger actuator actions by using a "if this then that" methodology, where a precondition is needed to command an action. Such policies are used to govern the behaviour of smart home services, for example, a functional requirement of a smart fire alarm is to detect smoke and for the controller to open doors. By doing this, the authors use risk assessment results to assess policies that may need to be protected in the case of an attack.

Insight 13: From the literature, IoT security relies on meeting a defined set of security objectives to reduce risk to acceptable levels, with RQ3 referring to how the IoT risk management paper defines security objectives. Despite its importance, most papers do not discuss security objectives. Forming security objectives carries the benefit of justifying controls in an easier way. IoT security policies use security objectives, with security policies (such as passwords policies) using a criterion that needs to be adhered to prevent attacks. For all IoT domains, traditional objectives like CIA may not encompass all the security objectives needed for IoT, thus affecting security policies. Overcoming this issue, the approach within the work of Mohsin et al. [62,63] utilises user-defined policies based on what a user should be doing and how a device's function is used safely. Interaction and communication can be depicted using the "if this then that" method, for example, if a user initiates a trigger, then the expected outcome is for a smart bulb to turn on.

5.1.2. Consider Resources for Risk Control

Various resources are needed to implement security controls, with resources including time, money, people, device capabilities, etc. Within the work of James [56], the most suitable mitigation strategies are not only those that decrease risk but strategies that are feasible based on the available resources. Concerning this, Ivanov et al. [55] characterise the security of a smart infrastructure by using integral security indicators that can be used to choose security controls based on risk scores and the resources that are available.

Shokeen et al. [72] consider the number of resources that need to ensure that a risk is minimised as much as possible based on the nature of the associated vulnerability. The number of available resources for IoT will greatly differ depending on the environment. For an organisation that uses IoT, it is likely that a group of employees would carry the responsibility for cyber risk management, having a designated budget and mitigation mechanisms. However, IoT domains like smart homes will not have the same people power, budget, and mitigation mechanisms that an organisation has. Parsons et al. [67] consider that there are fewer resources within smart homes, which means that other assessments and controls would be needed to accommodate this. Not only this but IoT devices in general have a limited set of security capabilities. An assessment that Al et al. [40] suggest before controls are implemented is a cost–benefit analysis that is used to understand the cost of implementation and impact. When it comes to financial resources for organisations, the estimated value of an IoT control can be determined by the cost of implementation, threat event occurrence rate and expected losses. Considering the cheapness of IoT devices, some controls may not be suitable with the control cost, outweighing the risk [44].

Insight 14: IoT risk responses need to be determined based on accessible resources, with money being the most discussed resource. As part of answering RQ3, the consideration of resources is limited within the surveyed papers. For unregulated personal IoT domains, the types of controls may be limited, for example, smart home residents may not want to learn about and buy an intrusion detection system due to the amount of money and time required to use this control. This means that there needs to be an assessment of control benefits and drawbacks, with no access to certain controls affecting the acceptable risk threshold or requiring another control.

5.1.3. Optimise Control Strategies

As defined by NIST, the optimisation of controls refers to the process of minimising negative and maximising positive consequences and probabilities depending on risks, costs, and legal obligations [35]. In practice, optimal decision making for cyber security involves a trade-off between available resources for risk control and the minimisation of risk [97,98], which poses several issues when finding the best set of security controls. While the effectiveness of a control can be estimated in a probabilistic way [97,98], controls do not always maintain maximum effectiveness [99] and may not always be an attack-preventive measure [97]. The analysis of how a control performs at different levels of implementation can aid in making long-term optimal decisions by estimating the amount of time for which maximum effectiveness can be maintained [99]. In turn, different controls can be used for different actions, such as prevention, detection, and recovery [97], with control classifications helping to distinguish between these. The optimisation of controls within IoT is integral to ensure a balance between resource spending and the minimisation of risk, based on context information and the need to prioritise security controls [64]. However, IoT domains can carry the burden of lacking resources and the potential negative cost benefits due to how cheap IoT devices are, with [45] concluding that to reach the optimal solution for IoT decision making, a cost model needs to be integrated into their framework to balance risk and costs. In turn, the implementation and modification of security controls need to be carried out quickly for controls to be the most optimal, given emerging risks and risk assessment results [49].

According to Ksibi et al. [60], contextual information is required to optimise IoT decision making accuracy, alongside adaptive risk assessment. For Ksibi et al. [60], an initial risk threshold is set by a security administrator to reflect anomalous scenarios, which is used to generate a risk value. Vakhter et al. [74] suggest that IoT engineers need to assign weights to security controls to achieve the best trade-off between safety, reliability, resilience, and privacy. Here, this trade-off ensures that optimal controls are implemented based on a defined value, for example, the effectiveness of a control and the amount of money needed to implement it. When an IoT risk is to be mitigated, the trade-off between security effectiveness and network performance is integral to ensure safe usage, with little impact on performance, which is explicitly important within wireless body area networks.

To optimise security controls, Arfaoui et al. [46] use a game theoretic approach based on IoT device capabilities and the quality of survive objectives to find the Nash equilibrium. This equilibrium reflects the most desirable IoT security outcome by following a strategy, being optimal based on decisions from other players. The authors define such a strategy via the use of adaptive risk assessment that assesses contextual information and a threat model, using a Markov decision process that is defined by the finite set of states, possible actions, probability, and reward obtained from the execution of an action. From this process, payoff functions can be determined to show increases in security versus performance degradation.

Using graph modelling, George and Thampi [53] consider the optimal set of vulnerabilities that should be healed while considering the constrains of IIoT networks, such as the lack of vulnerability patches and the cost of patching. To integrate this, the authors suggest risk mitigation strategies based on finding the number of vulnerabilities that can be patched considering constraints to improve IIoT security. Cost modelling within IIoT networks is circumstantial, with a lack of accepted standards to aid security administrators. To this end, a security administrator needs to set risk threshold values (the maximum cumulative threat value in any attack path) in a way that allows for the optimal set of vulnerabilities to be patched. Meanwhile, Ivanov et al. [55] use a developed software toolkit to formulate attack graphs that allow for an iterative search of optimal countermeasures based on the number of vulnerabilities that need to be eliminated and priority. By using criticality indicators that characterise IoT security, the model selects security measures based on reducing risk levels based on resources that can be used during an intrusion. However, recalculating indicators to select the most optimal security measure takes a large amount of time, then more connected components than there are, which the authors suggest need to be further optimised to reduce the operating time expense. Finally, Parsons et al. [67] consider the optimal smart home security practices that need to be implemented by users, with controls being selected based on the reduction in high risk behaviours, increasing a user’s ability to perceive and prevent attacks, as well as ensuring security familiarity. For example, in an optimal scenario, users should be risk averse and be highly familiar with security practises, showing the requirements of a secure smart home. The authors suggest that optimising the awareness towards and knowledge of good security practices allows for enhanced IoT security and the assurance that basic good practices are being enforced.

Insight 15: Optimisation for IoT control within the surveyed papers is limited, despite its importance to the implementation of controls and the justification of doing so. Within RQ3 and prior sections, we discussed the need for resources and security objectives when choosing controls. Finding the best controls for IoT depends on several factors defined by the IoT domain, with resources and security objectives being some of the most common. The key component of optimisation for IoT is the balance and trade-off between identified factors and the effectiveness of each control. Different types of IoT controls (e.g., prevention, detection, and recovery [97]) mitigate risks in different ways, with varying degrees of effectiveness that may degrade over time. While not specific to IoT, game theory approaches attempt to find the best strategies with the most beneficial outcome, considering the trade-offs. However, of the surveyed papers, few use this approach. One challenge that optimisation solves is the estimation of security control effectiveness alongside many attack paths and resource requirements [97] to achieve an equilibrium strategy.

5.2. Risk Monitoring

According to NIST [7], monitoring is the process of ”maintaining ongoing awareness“ into threats, vulnerabilities, and controls to support risk management decisions. This means that risk management processes, such as risk assessment, are not definitive once conducted, with cyber risk management systems often being continuous to ensure that risks can be reviewed and updated. In the following subsections, we discuss the surveyed papers in the context of IoT risk-monitoring methods. Figure 7 provides insight into the number of papers that will be explored within each subsection.

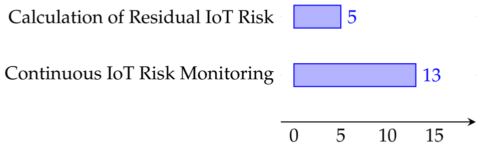

Figure 7. A visual breakdown of the number of papers per IoT risk control concept. For example, of the 39 collected papers, 13 of them fit into our survey's continuous risk management section.

5.2.1. Ensure Continuous Risk Monitoring

For IoT, risk monitoring involves observing key risks to find vulnerabilities that may arise, for example systems that monitor authentication attempts [68]. The regular monitoring of IoT networks also allows for suspicious behaviours to be uncovered [70] and the anticipation of future risks, given the development of IoT technology, with new vulnerabilities being discovered [74]. Not only this but well-known cyber risk management frameworks use continuous risk monitoring, with Andrade et al. [44] exploring the NIST cyber framework and ISO 3100 in the context of smart cities.

Monitoring IoT risks can be process that IoT cyber risk management frameworks use to ensure dynamic decision making and continuous risk management. As part of managing risks, Vakhter et al. [74] specify that risk factors (like threats, vulnerabilities, device capabilities, and attacker motivations) should be monitored for changes that could affect security, which can then be used to update risk assessments. Meanwhile, Al et al. [40] propose a monitor and anticipate risks step within their model with the goal of ensuring that the risk response is correctly implemented, determining the effectiveness of responses, and uncovering changes that cause the risk parameter to transpose. In doing this, the authors ensure that IoT devices are as up to date as possible to maintain a satisfactory level of security. Ksibi et al. [60] suggest the use of a risk-adaptation phase, which monitors risk rates, allowing for the adjustment of security controls depending on the risks. Rather than being a phase within a model, monitoring could be seen as a security objective, where processes, infrastructures, and logs must be monitored to ensure that unauthorised actions are detected [47]. In contrast, monitoring can be viewed as a type of security control, with Echeverria et al. [51] suggesting the use of the network monitoring and defence control from CIS controls to ensure IoT audit log management by the use of maintenance, monitoring, and analysis.

Within the work of Garcia et al. [52], monitoring and reviewing risks is considered an additional support activity to ensure that risk management is continuously ”controlling, reacting, and improving“ [52] the information needed by the risk management process. Considering that IoT risks can change quickly, continuous risk management processes that work dynamically are important. Abbass et al. [38] suggest that the ASRAaaS responsive IoT risk assessment allows for continual monitoring based on preventive risk analysis, with this not being in real time. Regardless, the monitoring and reviewing of IoT risks dynamically in real time may require supplementary data and an increased set of computing resources. For example, Kalinin et al. [58] require supplementary training samples based on IoT scenarios within dynamic networks to ensure high accuracy for risk assessment. Ryoo et al. [69] envision the use of a smart phone application within the smart home, which allows users to quickly monitor IoT devices and view the security state of the home.

Arfaoui et al. [46] apply the continuous monitoring of device channel attributes, such as traffic nature and device capability, to continuously estimate risk to find the best security controls dynamically. Monitoring IoT behaviour is key to finding security risks that may develop over time. In the context of smart grids, operations are monitored by the National Control Centre (NCC) and the Regional Control Centre (RCC), with servers monitoring and managing consumption patterns, which allows for differences in behaviours to be spotted [76]. In the same vein, Anisetti et al. [45] use assurance techniques to monitor the behaviour of devices to ensure that device behaviour is legitimate with all mechanisms implemented acting as expected.

Insight 16: Monitoring IoT risks is integral to ensuring that IoT controls are implemented, functioning as required, and replaced when risk results change. Therefore, monitoring works in tandem with dynamic decision making to be as updated as possible. RQ4 questions how risk monitoring takes place, with the above papers using a risk-monitoring phase as part of their framework, with monitoring also being considered as a type of control [51] or a security objective [60], The most common theme in IoT risk-monitoring papers is IoT networking monitoring, for example, Arfaoui et al. [46] monitor IoT networks and devices behaviour to update risk results. However, a notable missing piece from the surveyed papers is the monitoring and discovery of new threats and vulnerabilities that were previously unknown. Without monitoring emerging threats and vulnerabilities, there is potential for critical risks to be overlooked. This questions how an effective IoT cyber risk management framework can capture new risks to ensure that risks are prevented or mitigated. Part of the solution requires networking monitoring and the use of intrusion detection systems; however, such systems can be unsuitable for certain IoT domains, like smart homes, where resource consumption (such as time and money) outweighs the benefits. Overall, the discussion of IoT risk monitoring to ensure dynamic risk management in the current literature is limited, not appearing in many of the surveyed papers.

5.2.2. Calculate Residual IoT Risk

Residual risk refers to the portion of risk that remains once security measures are implemented [15]. An organisation may assume that implemented security controls will be used to their full potential all the time, which is not always the case; this issue causes risk to be underestimated, for example, the uncertainty for a trained user to still fall for a social engineering attack.

To combat this problem, Anisetti et al. [45] identify the amount of risk an organisation cannot control based on the difference between the assets' total risk and the total mitigated risk. In doing this, an organisation can identify the amount of risk that can be controlled and if the level remaining can be deemed as acceptable or if controls need to be adjusted.

For IoT domains like smart homes, a baseline of risk acceptance needs to be determined. Ryoo et al. [69] conceptualise this by asking users a series of questions when the proposed risk assessment application is first used. Despite not having a deep analysis of the vulnerabilities, Andrade et al. [44] discuss the use of a tool called MAGERIT applied within the context of a smart city. MAGERIT, which focuses on the analysis of assets and control effectiveness, allows for residual risk to be calculated from the remaining impact value when controls are applied.

Monitoring the remaining risk allows for the anticipation of future attacks that may have been deemed acceptable. Al et al. [40] utilise residual risks within a risk monitor stage, where risks that are not fully controlled are monitored in case they become worse. Good practices for IoT need to be continuous, with practices such as devices patches and training being updated to remain up to date with future risks. However, some risks may never be fully controlled, as it may not be feasible, resource wise, when considering how much IoT devices cost [40]. Unlike Al et al. [40], Zahra and Abdelhamid [76] dedicate a phase to analyse residual risks to ensure that risks are acceptable. The authors assess groups of IoT mitigation controls, like access control mechanisms and cryptography, by mapping controls to risks and the extent to which they do so.

Insight 17: To further answer RQ4, residual IoT risks show the amount of remaining IoT risk upon the implementation of controls. The number of papers discussing residual risk is limited, which raises questions about how acceptable risk for an IoT domain is determined and how residual risk can be calculated. Despite Ryoo et al. [69] asking users a series of questions upon the first use of a risk management application to gauge risk, the authors do not explore how these questions lead to the discovery of an acceptable risk threshold and do not provide examples. For the calculation of residual IoT risk, risk assessments could be performed again, or an equation could be used, as within the works of Anisetti et al. [45] and Andrade et al. [44]. The value of residual IoT risk should also be monitored since controls may degrade over time [36].

6. Recommendations

As we explored in the introduction, the implementation of IoT technologies provides a multitude of capabilities that assist in the automation of work and life. Reporting on cyber incidents and breaches for 2023, Verizon [100] provides a statistical analysis of 21 industry groups, such as retail, accommodation, and healthcare. Each industry group's analysed statistics shows how different each group is, with different attacker motivations and threat patterns. Mirroring this, applications of IoT technologies have differences in requirements, functionalities, and motivations for attackers. Within Verizon [100], personal and medical information are the most compromised data types within the healthcare industry, while payment and credential data are the most common within retail. Numerous domains are mentioned within our survey; however, we find that authors concentrate particularly on smart homes, organisations, healthcare, smart grids and smart cities. To expand our recommendations for future work, we explore how such guidance can be applied to different IoT domains, showing the distinctions between them. In the remainder of this section, we use our literature findings and make recommendations for future researchers to consider when creating a IoT cyber risk management framework for a chosen IoT domain.

6.1. Recommendations for IoT Cyber Risk Identification

Being the first part of IoT cyber risk assessment, identifying IoT risk parameters accurately is integral to assessing risk. Our work shows that IoT assets, users, threats, vulnerabilities, controls, impact, and likelihood all need to be identified within an IoT cyber risk management framework. RQ1 provides insight into how identification processes may take place, which shows a number of areas that need to be considered within future IoT cyber risk management frameworks. Below, we suggest questions for future works and recommend ways to overcome problems within IoT cyber risk identification processes.

How can IoT assets be defined, given the constraints of an IoT domain? IoT is intertwined with traditional IT assets, with devices using conventional hardware like routers, and notably deviate in functionality and data use, for example sensors and actuators, as well as the data produced by them. Furthermore, researchers need to consider how IoT assets are classified and how this helps IoT cyber risk management, with the main point of contention being IoT devices. In this case, an IoT device can be targeted at various system components, with the most important being sensors and actuators; thus, we recommend that researchers at the very least consider sensors and actuators as individual assets from a device. By defining IoT assets, associated attributes and priorities can then be established, such as identifying the capabilities and limitations of IoT devices. Asset classifications need to be dynamic and suitable for IoT, challenging researchers to find a fitting method of classification for an IoT domain. Organisations may use IoT to assist business operations, with IoT devices becoming assets owned by the organisation. However for a smart home, assets may be personal belongings that dwell within a place of residence, with personal information assets being accessed on a daily basis, such as payment and account credentials. IoT devices serve as daily conveniences [22] (such as smart cameras, locks and fridges) that may produce private data, for example, a smart camera's visual and audio information. Within healthcare, medical records are lucrative assets for attackers to steal due to the increasingly high payoff [101]. IoT medical equipment assets are used to help patients, with devices like pacemakers helping patients to live. Complexly, IoT medical technologies may be taken home by a patient, which may produce private data about a patient's medical state. Alternatively, assets within smart cities and grids are heavily relied on and must be available to ensure operation. For a smart grid, the energy produced may be an asset, as well as the industrial control system (ICS) equipment used to create it, while smart city assets can include devices used for traffic and building management.

How influential are users to IoT risk? Asset classifications may define users as assets; however, consider that users are not assets and should be treated differently due to the potential lack of IoT cyber hygiene. In unregulated IoT domains like smart homes, users could be viewed as having a high influence on risk values. We find that most researchers do not focus on users in regards to how they influence risk and the increased complexity of user interactions towards smart technology. For IoT users within an IoT domain, consider profiling users based on the risk actions and associated assets that they may use; this makes it easier to understand the links between users and assets, as well as users and security. Furthermore, researchers could pinpoint how users interact with device capabilities to better uncover threats. Users within IoT domains are culpable and accountable for ensuring that security is maintained. The importance of user interactions with device security as explored by Andrade et al. [44] can be applied to all IoT domains to comprehend complex relationships. For example, within organisations, healthcare, and smart grid domains, employees are held accountable for their security responsibilities, but insider threats could prevail due to employee attitude, intention and/or behaviour [102]. Meanwhile, smart homes do not contain the same vigorous regulation and training due to being private residential accommodations with increased freedoms. This means that user's have more choice in whether they ensure security and the extent to which they do so. For example, within an organisation, though two-factor authentication is not a option that must be used, it might be within a home. The approach within the work of Parsons et al. [67] identifies users that pose as a human vulnerability by identifying cyber hygiene components, such as high-risk behaviours and prevention abilities. Such freedoms make it harder for IoT domains to be secured, not being limited to smart homes, as smart cities rely on users to not misuse technology.

How can suitable IoT threats be determined? The core difference between each IoT domain is the attack surface and type of threats that may be faced. An attack on one industry may not affect another, which is partly due to the motivations of attackers and the types of technologies typically used within them [100]. For example, within a smart home, the ease of successfully phishing and/or gaining system access [100] due to lacking cyber hygiene poses an easy reward for an attacker. In contrast, exploiting information from smart meters to smart grid operators can allow an attacker to steal energy for personal gain [103] When it comes to IoT threats, the commonly used threat modelling method is STRIDE, which is not IoT specific. The issue is that not all IoT threats are covered within the STRIDE model, thus researchers need to use additional methods to ensure that all threats are captured to fulfil the security objectives. Furthermore, applicable threats may vary within different IoT domains, which raises the question of *how suitable IoT threats can be determined*. While Shjivraj et al. [71] and Tseng et al. [73] use STRIDE combined with other threat models (DREAD and LINDDUN), another solution is the adoption of an existing taxonomy or threat repository that has been created for a specific IoT domain. A taxonomy useful for smart homes is given by Heartfield et al. [22], who outline domain-specific threats, technologies, and impacts. Meanwhile, Kumar et al. [104] provide a taxonomy of attacks towards different types of smart grid networks. For healthcare, Affia et al. [105] provide insight into the types of security risks faced by IoT health devices using layered architecture as leverage. In the context of smart cities, Izrailov et al. [106] propose a method to classify smart city transport infrastructure threats since the implementation of smart cities is relatively new. Using taxonomies like the ones above, researchers could also assign threat attributes to explain how threats manifest, for example, threats that could propagate within an IoT domain.

How can suitable IoT vulnerabilities be determined? Similar to IoT threats, IoT vulnerabilities vary within different IoT domains. IoT devices are subject to numerous weaknesses depending on manufacturing, exploits, and functionality. While vulnerabilities databases like CVE can aid in uncovering exploits, they are not IoT specific, making it a lengthy process to find and filter out suitable IoT vulnerabilities. However, vulnerability databases provide extensive data into threats, with new threats being quickly documented, thus being easy to monitor. To avoid lengthy processes, an IoT vulnerability and exploit database could be used, for example, VARIoT [107], which relies on existing databases and is not necessarily exhaustive but does allow for vendor and device model searches. Due to this, vulnerability classifications could also be used, which allows researchers to group applicable vulnerabilities for an IoT domain. Vulnerability classifications should be specific yet leave ample room for unknown vulnerabilities to emerge. Significantly, IoT threat taxonomies are likely to identify common IoT vulnerabilities, for example, within the work of Kumar et al. [104] In tandem, we suggest that human vulnerabilities should be a primary focus within IoT cyber risk management frameworks to target preventable risks, with OWASP showing preventable vulnerabilities, such as the use of guessable or hardcoded passwords. We encourage researchers to focus on how human vulnerabilities can affect risk, given high-risk actions, security knowledge and awareness, susceptibility to social engineering, and misuse/misconfiguration. Part of this involves the question of how behaviour analysis can be integrated into models, and how this behaviour can affect risk factors like impact. This would require researchers to add behaviour analysis to each aspect of risk management, identifying risk factors and meaningful values as well as the assessment of risk with behaviour in mind. In turn, assessing the risk of a user and the potential increase in risk allows for the targeting of risk mitigation and training based on the user's security profile.

The focus on human vulnerability is applicable to any IoT domain, with regulated IoT domains likely already having training schemes in place to ensure a secure workforce. In healthcare and smart grid domains, user responsibility of security is increasingly important due to the potential threat to life. For a smart home, users with a lack of cyber hygiene are especially vulnerable, which heightens the need to assess user behaviours since an attacker will want to exploit them. If a user at home has optimal cyber hygiene at work, it does not directly translate into smart home cyber hygiene.

How can existing IoT controls be used to assess risk more accurately? Both regulated and unregulated IoT domains are likely to contain several existing controls that can impact the likelihood of risk. We find that papers do not always consider control-based risk assessment, meaning that security controls are not explicitly factored into the risk assessment phase. Notably, in cases where an IoT risk assessment is taking place for the first time, uncovering existing controls is a necessary process to ensure that risk is assessed accurately, given an existing risk landscape. Such a process is applicable to all IoT domains, as traditional IT controls can partly control IoT risk, for example, firewalls and antivirus software. To include a process that finds existing controls, researchers could consider assessing the readiness of an IoT domain, which filters practical cyber controls and good practises, and estimating how effective these are. As an example, readiness within a smart home could refer to the use of good cyber hygiene practices.

How can the impact of an IoT threat event be defined? For the impact on IoT assets, CIA, as well as privacy, trust, accountability, and nonrepudiation, are all important factors that can be affected by an attack. However, cyber impact does not encompass the myriad of ways in which users can be impacted by an IoT attack. An IoT user may be directly affected by an attack, thus showing an impact of IoT risk in daily life. As an example, a medical IoT device may be exploited to cause physical harm to a user because of an attack on account access. Upon identifying impact types, researchers can map assets and users to the relevant impact types and prioritise the most important impact types within the IoT domain. Then, researchers can identify crucial impact types within an IoT domain and define a meaningful severity scale. For domains such as healthcare, smart grids, and smart cities, researchers could consider an impact scale of physical harm from no risk, harm, to life-threatening harm. In contrast, within a smart home, the loss of privacy and control could be more crucial. In cases of monetary loss within an organisation using IoT, asset valuation could be used to better understand the potential value loss when a threat event is successful, while for other impact types, a questionnaire could be used. Moreover, it is integral for researchers to consider the worst-case impact, including how threats can cascade to multiple assets for a greater loss.

How can the likelihood of an IoT threat event be defined? When it comes to likelihood, one problem researchers may find is the lack of coherent data that suggests the likelihood of an attack occurring within different IoT domains, making it difficult to value the occurrence of an attack. If controlled effectively, the likelihood of an attack being successful can be drastically lowered, As an example, it is commonly known in research that social engineering can use diverse mediums, with attackers exploiting users unaware of such attacks. If a user is informed of social engineering methods, and does not provide information to the attacker, the likelihood of attack success drops. However, attacker motivations can cause persistence risks. For example, lucrative information assets like medical records and trade secrets can be sold for high prices. Semi-quantitative scales can easily represent meaningful values to determine likelihood. Such values rely on using prior works as justification for likelihood as well as the cyber hygiene and controls used within the specific IoT setting that combat attacker attributes (accessibility, skills, equipment, etc.). Given this, the link between existing controls and cyber hygiene to likelihood should not be unnoticed within future works.

6.2. Recommendations for IoT Cyber Risk Calculation

Being the second component to IoT cyber risk assessment, the identified risk parameters are used to calculate risk in a meaningful way to determine risk. We explored multiple ways that risk can be assessed; however, risk parameters and results must be meaningful and easy to understand, aiding in risk decision making. Risk calculations can represent risk in a semi-quantitative, quantitative, or qualitative way, with researchers potentially using well-established risk calculation methods by adapting them to better suit IoT domains or using a brand-new system, which facilities cyber security standards. The common methods within the surveyed IoT cyber risk management frameworks are the uses of graph modelling, risk matrices, threat knowledge bases, and risk weighting, methods that researchers could use to determine risk within an IoT domain. Below, we suggest questions for future works and recommend ways to overcome problems within IoT cyber risk calculation processes.

How can future works use graph modelling to effectively calculate IoT risk? When it comes to calculating risk, graph modelling allows researchers to easily visualise risks within a network by displaying entry points, attack paths, data flow, threat propagation, and dependencies. Within our survey, there are a number of examples of graph modelling within varying IoT domains, and it is notable that different graphical models can be used in several different ways as discussed within our literature review. For example, Andrade et al. [44] use dynamic Bayesian networks to to visualise smart city nodes and links, while Kavallieratos et al. [59] visualise dynamic changes within a smart home network. Researchers may consider using graph modelling and assess the benefits and drawbacks to using different types of graph models, dependent on available resources and functionality of IoT risk management tools. As an example, Bayesian networks are a common way to predict likelihood, showing probabilistic relationships between nodes based on conditional dependencies. A major advantage of Bayesian networks is seen when information is not fully known, which, as we described, is an issue that affects likelihood estimation. For IoT, it is integral to model the dynamic nature of IoT devices; however, like other graph-modelling methods, the more nodes and updates required, the greater the computational effort. While graph modelling is commonly used to capture risk on various parts of a network, human interactions are not represented by the works we surveyed. To combat this, researchers may need to integrate human-to-IoT interactions to assess the dependencies that users have within an IoT domain.

How can future works use risk matrices to effectively calculate IoT risk? Alternative to graph modelling, future works can examine the use of risk matrices to effectively calculate IoT risk, as a risk matrix provides a simpler way to visualise risk in a semi-quantitative chart format. Risk matrices need to have well-defined risk categories that are accurately comparable to one another, making different levels of risk clear. An issue surrounding risk matrices is the potential for unreliable views of impact/likelihood values and the oversimplification of risk values. In the context of healthcare devices, Vakhter et al. [74] utilise a simple risk matrix that measures impact severity and probability, which aids in the prioritisation of critical risks. Alternatively, for smart grids, Chehida et al. [47] use a matrix that reflects the relationships between threats and assets. While simple IoT risk matrices are useful, researchers could consider a more complex route. For example, an adjacency matrix can be used to represent a graph, as seen by George et al. [53,54]. Notably, an increasingly complex risk matrix can be used to model a dynamic system nature, which is prominent within IoT, and could also be used to emulate user interaction.

How can future works use IoT threat knowledge bases to effectively calculate IoT risk? An IoT threat knowledge base is a great method to store threat data in a structured way, with simple risk calculations using likelihood and impact to define the risk of a threat. Future works need to consider the lack of existing knowledge bases for IoT, meaning that a threat knowledge base will need to be created. Despite this, another issue is the potential to neglect critical threat events and the difficulty in estimating likelihood and impact. Forming a knowledge base takes time, but threat models, existing papers, and reports of cyber incidents can justify the values used. For example, within the healthcare-focused work of Alsubaei et al. [43], the literature is used to curate a base of threat knowledge. Another example from Zahra and Abdelhamid [76] is to use existing bases, like CVE, that contain vulnerability records and scores. However, these are not always IoT specific, which requires researchers to filter out non-IoT records. One pitfall with the surveyed papers, is that we did not see an example of a threat base that contains values that could be used in other instances. Overcoming these issues requires threat, vulnerability, likelihood, and impact identification processes to be streamlined. In turn, the current uses of IoT threat knowledge bases do not necessarily consider human vulnerabilities, which should not be overlooked. In turn, researchers may benefit from using risk matrices or graph modelling alongside a threat knowledge base.

How can future works use risk weighting to effectively calculate IoT risk? The use of weighted risk calculations focuses on the importance of various IoT risk parameters and how IoT critical components can be prioritised, which could also be implemented into graph models and risk matrices. IoT weighting is especially useful for prioritising crucial impact types, such as physical harm, where the potential consequences of an attack need to be eradicated. In our review, many impact types are suggested, and all IoT domains likely contain at least one critical consequence that needs to be focused on, for example, the potential threat to life within healthcare domains. However, risk weighting can also be applied to assets and users that could be affected by such an impact to further strengthen the prioritisation. For example, if within a healthcare setting, there is a potential threat to life, the patients and implanted medical devices that could cause or be deeply affected by such threats hold increased significance when assessing risk. It is notable that IoT user interaction and behaviours could also be assigned weights to signify critical cyber hygiene practices and the lack thereof.

6.3. Recommendations for IoT Cyber Risk Control

Risk assessment results facilitate the selection of appropriate risk responses to control risk. IoT risk response should not only consider the most suitable risk mitigation methods but also determine risk responses, such as transference, where possible. Future works need to consider how effectively security decision making can be performed to ensure that risk control is effective. Given the lack of in-depth IoT cyber risk control within the surveyed papers, there is also a need to pay attention to how IoT controls are chosen. Below, we suggest questions for future works and recommend ways to overcome problems within IoT cyber risk control processes.

What are the available IoT security controls and how effective are they? Risk assessment results facilitate the selection of appropriate risk responses that reduce risk to acceptable levels. To be appropriate, identified controls need to be viable for an IoT domain, meaning they effectively reduce risk, meet security requirements, and examine the resources needed to do so. IoT security capabilities are often extremely limited, relying on user interaction and configurations to ensure security. Existing IoT controls should already be known; however, the risk results will reveal how effective they are and if more controls are required. Much like identifying threats, various papers and guides have documented controls for various IoT domains. For organisations, the CIS controls IoT companion guide [96] can be used to apply CIS controls in the context of IoT. Meanwhile, The European Union Agency for Cybersecurity (ENISA) published a good practice guide for smart grids [108] as well as a cyber security and resilience guide for smart hospitals [109]. In turn, ENISA also produced a good practice web tool for smart infrastructures [110], which includes advice on smart cities, aviation, etc. Lastly, for smart homes, NIST published an article that underlines key mitigation methods that aid in ensuring smart home security [111]. For future works, identifying specific controls from the IoT literature will aid in understanding the available controls for an IoT domain, while also considering the upkeep of IoT cyber hygiene. The IoT literature may also aid in the estimation of control effectiveness and the rate at which effectiveness degrades to ensure the best controls are utilised.

What are the security requirements for an IoT domain and how can controls ensure security requirements are met? For organisations, security objectives are defined in line with regulations and law; however, in non-organisational IoT domains (like smart homes), requirements may not have been formed. We find that researchers often do not describe specific security objectives that need to be met for risk to be acceptable. This missing aspect challenges future works to uncover what the security requirements are for an IoT domain and the controls that are needed to meet security goals. To combat this, IoT security requirements need to be clearly defined first, an extra challenge for unregulated IoT domains like smart homes. Defined IoT security requirements are the goals to be achieved by an IoT control to satisfy a strong level of security and apply to all domains since establishing security goals can help to define unacceptable risk levels.

What are the IoT security resources that affect the selection of IoT controls? Another limited topic is the consideration of resources required to ensure effectiveness and usability. Resources can refer to more than money, like the time and effort needed to use IoT controls. Assessing control accessibility is integral to determine risk acceptance thresholds, as not all risks may be controlled due to a lack of resources for IoT controls. For IoT domains such as organisations, healthcare, smart cities and smart grids, the cost and time of a control's implementation and maintenance may outweigh the mitigation benefits. However, smart homes and small organisations may have significantly less access to costly and time-consuming IoT controls, making the implementation of an IDS, for example, unsuitable. In turn, smart home residents may not have the willingness to effectively implement and maintain controls, which downgrades a control's potential mitigation benefits.

How can IoT risk control find optimal control strategies? Overall, successful risk treatment needs to consider several factors to ensure risk is reduced. However, this can be optimised to uncover the best strategies for an IoT domain, with future work needing to facilitate optimal control strategies. To achieve this, future works need to assess resources and security goals by uncovering the trade-offs between different types of controls and resources. IoT controls could be classified by control functions, such as prevention, detection, and recovery, where controls eliminate, reduce, expose, and recuperate IoT risks. Trade-offs assess the benefits and drawbacks of using an IoT control to ensure a positive balance between reducing risk and maximising resources. All types of IoT domains should aim to meet identified security requirements in the most optimal way for reasonable trade-offs to the available resources. The optimisation process is key since IoT domains prioritise different resources. For example a smart home trade-off may be between a control's security benefits and the original cost of the devices it protects, personal willingness to implement the control as well as the cost of the control itself. Unlike smart homes, security requirements may hold jurisdiction within regulated IoT domains, meaning that there is an added set of legal issues that need to be considered.

6.4. Recommendations for IoT Cyber Risk Monitoring

IoT risk monitoring is a continuous process that allows for risk management processes to use up to date information that maintain acceptable risk levels. Much like IoT risk control, we find that discussions into IoT risk monitoring were limited, and often not part of IoT cyber risk management frameworks. Below, we suggest questions for future works and recommend ways to overcome problems within IoT cyber risk-monitoring processes.

How can IoT risk be dynamically monitored? Monitoring requires the observation of critical risks to find vulnerabilities that may manifest into threats. Such a process needs to be continuous to ensure that dynamic decisions for IoT control take place when risk becomes unacceptable. IoT risk management does not simply end once controls are implemented since new threats can materialise at a fast pace. In turn, adding a new device or user to a network can drastically change risk due to changes in control and dependencies. Within regulated IoT domains, (such as within organisations, healthcare, smart grids and smart cities), monitoring processes are likely to be easier to implement due to increased access to resources, for example the use of an intrusion detection system that monitors and detects unauthorised IoT system behaviours by users and devices at a network level. However, for smaller IoT domains, such as smart homes, monitoring needs to be easily manageable. By extension, regular users need to understand how to monitor security, in such cases, an IoT cyber risk management application may be helpful. It is notable that user and system behaviours should be monitored to ensure that actions performed are legitimate and that user actions are not of a high risk; however, preventing such risks from occurring will require additional IoT controls.

How can residual IoT risk be assessed to ensure risk is at an acceptable level? Residual risk is the amount of risk remaining once a set of controls have been implemented. Only a very limited number of works address residual risk, which is curious, as it is an important aspect of risk control. We suggest that future works focus on the consideration of residual risk and identifying the amount of risk remaining to ensure that risk is acceptable, as well as what this means to IoT risk management. This also requires dynamic risk monitoring where an organisation or user can update risk parameters to continuously assess risk, which can easily lead to quick preventive actions being implemented. To gain an accurate view of residual risk, updated risk assessment results are required. Within regulated IoT domains, such as smart grids and healthcare, governing bodies around the globe provide strict work regulations, for example, the Health and Safety Executive (HSE) states that risk assessments should be reviewed when major system changes are made [112]. However, smart homes are not held to the same standard, making acceptable residual risk harder to define due to uncertainty surrounding whether an resident will maintain cyber security controls and cyber hygiene.

7. Conclusions

In this paper, we presented a systematic review and taxonomy of works that aim to build IoT cyber risk management, risk assessment, risk analysis, and IoT threat modelling frameworks.

We introduced our research questions related to IoT cyber risk management concepts, the needs of IoT, and human vulnerabilities. Using our research questions, we reviewed the literature and used our results to propose a taxonomy. We then used the taxonomy to compare the surveyed works and critically analysed the collected literature. Finally, we made recommendations for future researchers to consider when they create a risk management system for IoT domains.

The biggest issue posed to IoT domains is that traditional cyber risk management systems may not be optimal for IoT due to the increasing needs, requirements, and capabilities of IoT technology. Overall, due to the increasing number of devices globally, it is integral to improve IoT cyber risk management and allow it to become optimal within all IoT domains. Therefore, our future work will be to use the recommendations we suggest and use them to create a new IoT cyber risk management for a specific IoT domain.

Author Contributions: Conceptualization, E.K.P. and E.P.; methodology, E.K.P.; validation, E.K.P., E.P., G.L. and G.S.; formal analysis, E.K.P.; investigation, E.K.P.; data curation, E.K.P.; writing—original draft preparation, E.K.P., E.P., G.L. and G.S.; writing—review and editing, E.K.P., E.P., G.L. and G.S.; visualization, E.K.P.; supervision, E.P., G.L. and G.S.; project administration, E.K.P., E.P., G.L. and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Herath, T.; Herath, H.S. Coping with the new normal imposed by the COVID-19 pandemic: Lessons for technology management and governance. *Inf. Syst. Manag.* **2020**, *37*, 277–283. [CrossRef]
2. Zikria, Y.B.; Ali, R.; Afzal, M.K.; Kim, S.W. Next-generation internet of things (iot): Opportunities, challenges, and solutions. *Sensors* **2021**, *21*, 1174. [CrossRef] [PubMed]
3. Baruah, P.D.; Dhir, S.; Hooda, M. Impact of IOT in current era. In Proceedings of the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 February 2019; pp. 334–339.
4. Lee, S.K.; Bae, M.; Kim, H. Future of IoT networks: A survey. *Appl. Sci.* **2017**, *7*, 1072. [CrossRef]
5. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
6. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*; Cengage Learning: Boston, MA, USA, 2017.
7. Ross, R.; Pillitteri, V.; Graubart, R.; Bodeau, D.J.; McQuaid, R.M. *NIST Special Publication 800–160. Volume 2 Revision 1: Developing Cyber Resilient Systems: A Systems Security Engineering Approach*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
8. Wunder, J.; Halbardier, A.; Waltermire, D. *Specification for Asset Identification 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
9. Mavropoulos, O.; Mouratidis, H.; Fish, A.; Panaousis, E. Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Netw.* **2019**, *92*, 101743. [CrossRef]
10. Mavropoulos, O.; Mouratidis, H.; Fish, A.; Panaousis, E. ASTo: A tool for security analysis of IoT systems. In Proceedings of the 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, UK, 7–9 June 2017; pp. 395–400.
11. Heartfield, R.; Loukas, G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Comput. Secur.* **2018**, *76*, 101–127. [CrossRef]
12. Bada, M.; Nurse, J.R. The social and psychological impact of cyberattacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 73–92.
13. Chatterjee, S.; Sarker, S.; Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *J. Manag. Inf. Syst.* **2015**, *31*, 49–87. [CrossRef]
14. Cullen, A.; Armitage, L. A Human Vulnerability Assessment Methodology. In Proceedings of the 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Scotland, UK, 11–12 June 2018; pp. 1–2.
15. Ross, R.S. *Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1*; US Department Commerce, NIST: Gaithersburg, MD, USA, 2012.
16. Joint Task Force Transformation Initiative. *NIST Special Publication 800-53 Revision 4-Security and Privacy Controls for Federal Information Systems and Organizations*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
17. National Institute of Standards and Technology. *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View*; Organization, Mission, and Information System View; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011; p. 88.
18. International Organization for Standardization. *Information Technology-Security Techniques-Information Security Management Systems-Requirements (ISO/IEC 27001:2013 Including Cor 1:2014 and Cor 2:2015)*; Ger. Version EN; International Organization for Standardization: Geneva, Switzerland, 2017; Volume 27001.

19. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
20. Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. *Introducing Octave Allegro: Improving the Information Security Risk Assessment Process*; Technical Report; Carnegie-Mellon Univ. Software Engineering Inst.: Pittsburgh, PA, USA, 2007.
21. Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R.; Graubart, R.; Clausen, L. *Threat Assessment & Remediation Analysis (TARA): Methodology Description Version 1.0*; Technical Report; MITRE CORP: Bedford, MA, USA, 2011.
22. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.; Filippoupolitis, A.; Roesch, E. A taxonomy of cyber-physical threats and impact in the smart home. *Comput. Secur.* **2018**, *78*, 398–428. [CrossRef]
23. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef]
24. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
25. Akinrolabu, O.; Nurse, J.R.; Martin, A.; New, S. Cyber risk assessment in cloud provider environments: Current models and future needs. *Comput. Secur.* **2019**, *87*, 101600. [CrossRef]
26. Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.Á.O.; Toval, A. Security and privacy in electronic health records: A systematic literature review. *J. Biomed. Inform.* **2013**, *46*, 541–562. [CrossRef] [PubMed]
27. Google Trends. 2023. Available online: https://trends.google.com/trends (accessed on 3 March 2023).
28. International Organization for Standardization. *Risk Management–Principles and Guidelines*; International Organization for Standardization: Geneva, Switzerland, 2009.
29. Zardari, S.; Nisar, N.; Fatima, Z.; Dhirani, L.L. IoT–Assets Taxonomy, Threats Assessment and Potential Solutions. In Proceedings of the 2023 Global Conference on Wireless and Optical Technologies (GCWOT), Malaga, Spain, 24–27 January 2023; pp. 1–8.
30. Booth, H.; Rike, D.; Witte, G.A. The National Vulnerability Database (nvd): Overview. Available online: https://nvd.nist.gov/ (accessed on 1 March 2023).
31. Mitre. 1999. Available online: https://cve.mitre.org/ (accessed on 22 July 2023).
32. Stine, K.; Quinn, S.; Witte, G.; Gardner, R. Integrating cybersecurity and enterprise risk management (ERM). *Natl. Inst. Stand. Technol.* **2020**, *10*.
33. Maner, J.K.; Gailliot, M.T.; Butz, D.A.; Peruche, B.M. Power, risk, and the status quo: Does power promote riskier or more conservative decision making? *Personal. Soc. Psychol. Bull.* **2007**, *33*, 451–462. [CrossRef] [PubMed]
34. Wolter, K.; Reinecke, P. Performance and security tradeoff. In *Formal Methods for Quantitative Aspects of Programming Languages, Proceedings of the 10th International School on Formal Methods for the Design of Computer, Communication and Software Systems, SFM 2010, Bertinoro, Italy, 21–26 June 2010*; Advanced Lectures; Springer: Berlin, Germany, 2010; pp. 135–167.
35. Quinn, S.; Barrett, M.; Witte, G.; Gardner, R.; Ivy, N. Prioritizing Cybersecurity Risk for Enterprise Risk Management. In *NIST Interagency/Internal Report (NISTIR)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
36. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. [CrossRef]
37. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the mirai botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 15–17 August 2017; pp. 1093–1110.
38. Abbass, W.; Baina, A.; Bellafkih, M. ArchiMate based Security Risk Assessment as a service: Preventing and responding to the cloud of things' risks. In Proceedings of the 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 29 October–1 November 2019; pp. 1–5.
39. Aiken, W.; Ryoo, J.; Rizvi, S. An Internet of Things (IoT) Security Assessment for Households. In Proceedings of the 2020 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, USA, 28–30 October 2020; pp. 53–59.
40. Al Mousa, A.; Al Qomri, M.; Al Hajri, S.; Zagrouba, R.; Chaabani, S. Environment based IoT security risks and vulnerabilities management. In Proceedings of the 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 9–10 September 2020; pp. 1–6.
41. Ali, B.; Awad, A.I. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817. [CrossRef]
42. Ali, O.; Ishak, M.K.; Bhatti, M.K.L. Internet of things security: Modelling smart industrial thermostat for threat vectors and common vulnerabilities. In *Intelligent Manufacturing and Mechatronics*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 175–186.
43. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9–12 October 2017; pp. 112–120.
44. Andrade, R.O.; Tello-Oquendo, L.; Ortiz, I. *Cybersecurity Risk of IoT on Smart Cities*; Springer: Berlin, Germany, 2021.
45. Anisetti, M.; Ardagna, C.A.; Bena, N.; Foppiani, A. An Assurance-Based Risk Management Framework for Distributed Systems. In Proceedings of the 2021 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 5–10 September 2021; pp. 482–492.
46. Arfaoui, A.; Kribeche, A.; Senouci, S.M.; Hamdi, M. Game-based adaptive risk management in wireless body area networks. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 1087–1093.

47. Chehida, S.; Baouya, A.; Alonso, D.F.; Brun, P.E.; Massot, G.; Bozga, M.; Bensalem, S. Asset-Driven Approach for Security Risk Assessment in IoT Systems. In Proceedings of the Risks and Security of Internet and Systems: 15th International Conference, CRiSIS, Paris, France, 4–6 November 2020; pp. 149–163.
48. Christensen, D.; Martin, M.; Gantumur, E.; Mendrick, B. Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources. *Electr. J.* **2019**, *32*, 50–57. [CrossRef]
49. Danielis, P.; Beckmann, M.; Skodzik, J. An ISO-Compliant Test Procedure for Technical Risk Analyses of IoT Systems Based on STRIDE. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 499–504.
50. Duan, X.; Ge, M.; Le, T.H.M.; Ullah, F.; Gao, S.; Lu, X.; Babar, M.A. Automated Security Assessment for the Internet of Things. In Proceedings of the 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC), Perth, Australia, 1–4 December 2021; pp. 47–56.
51. Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity model based on hardening for secure internet of things implementation. *Appl. Sci.* **2021**, *11*, 3260. [CrossRef]
52. García, S.N.M.; Hernandez-Ramos, J.L.; Skarmeta, A.F. Test-based risk assessment and security certification proposal for the Internet of Things. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 641–646.
53. George, G.; Thampi, S.M. A graph-based security framework for securing industrial IoT networks from vulnerability exploitations. *IEEE Access* **2018**, *6*, 43586–43601. [CrossRef]
54. George, G.; Thampi, S.M. Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive Mob. Comput.* **2019**, *59*, 101068. [CrossRef]
55. Ivanov, D.; Kalinin, M.; Krundyshev, V.; Orel, E. Automatic security management of smart infrastructures using attack graph and risk analysis. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 295–300.
56. James, F. IoT Cybersecurity based Smart Home Intrusion Prevention System. In Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, 23–25 October 2019; pp. 107–113.
57. James, F. A Risk Management Framework and A Generalized Attack Automata for IoT based Smart Home Environment. In Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, 23–25 October 2019; pp. 86–90.
58. Kalinin, M.; Krundyshev, V.; Zegzhda, P. Cybersecurity risk assessment in smart city infrastructures. *Machines* **2021**, *9*, 78. [CrossRef]
59. Kavallieratos, G.; Chowdhury, N.; Katsikas, S.; Gkioulos, V.; Wolthusen, S. Threat analysis for smart homes. *Future Internet* **2019**, *11*, 207. [CrossRef]
60. Ksibi, S.; Jaidi, F.; Bouhoula, A. Cyber-Risk Management within IoMT: A Context-aware Agent-based Framework for a Reliable e-Health System. In Proceedings of the 23rd International Conference on Information Integration and Web Intelligence, Linz, Austria, 29 November–1 December 2021; pp. 547–552.
61. Lally, G.; Sgandurra, D. Towards a framework for testing the security of IoT devices consistently. In Proceedings of the International Workshop on Emerging Technologies for Authorization and Authentication, Barcelona, Spain, 7 September 2018; pp. 88–102.
62. Mohsin, M.; Anwar, Z.; Husari, G.; Al-Shaer, E.; Rahman, M.A. IoTSAT: A formal framework for security analysis of the internet of things (IoT). In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 180–188.
63. Mohsin, M.; Sardar, M.U.; Hasan, O.; Anwar, Z. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things. *IEEE Access* **2017**, *5*, 5494–5505. [CrossRef]
64. Nakamura, E.T.; Ribeiro, S.L. A privacy, security, safety, resilience and reliability focused risk assessment in a health iot system: Results from ocariot project. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
65. Pacheco, J.; Zhu, X.; Badr, Y.; Hariri, S. Enabling risk management for smart infrastructures with an anomaly behavior analysis intrusion detection system. In Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W), Tucson, AZ, USA, 18–22 September 2017; pp. 324–328.
66. Pacheco, J.; Ibarra, D.; Vijay, A.; Hariri, S. IoT security framework for smart water system. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1285–1292.
67. Parsons, E.K.; Panaousis, E.; Loukas, G. How secure is home: Assessing human susceptibility to IoT threats. In Proceedings of the 24th Pan-Hellenic Conference on Informatics, Athens, Greece, 20–22 November 2020; pp. 64–71.
68. Rizvi, S.; Pipetti, R.; McIntyre, N.; Todd, J.; Williams, I. Threat model for securing internet of things (IoT) network at device-level. *Internet Things* **2020**, *11*, 100240. [CrossRef]
69. Ryoo, J.; Tjoa, S.; Ryoo, H. An IoT risk analysis approach for smart homes (work-in-progress). In Proceedings of the 2018 International Conference on Software Security and Assurance (ICSSA), Seoul, Republic of Korea, 26–27 July 2018; pp. 49–52.
70. Seeam, A.; Ogbeh, O.S.; Guness, S.; Bellekens, X. Threat modeling and security issues for the internet of things. In Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp), Balaclava, Mauritius, 19–21 September 2019; pp. 1–8.

71. Shivraj, V.; Rajan, M.; Balamuralidhar, P. A graph theory based generic risk assessment framework for internet of things (IoT). In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.
72. Shokeen, R.; Shanmugam, B.; Kannoorpatti, K.; Azam, S.; Jonkman, M.; Alazab, M. Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, Australia, 8–9 May 2019; pp. 22–29.
73. Tseng, T.W.; Wu, C.T.; Lai, F. Threat analysis for wearable health devices and environment monitoring internet of things integration system. *IEEE Access* **2019**, *7*, 144983–144994. [CrossRef]
74. Vakhter, V.; Soysal, B.; Schaumont, P.; Guler, U. Threat Modeling and Risk Analysis for Miniaturized Wireless Biomedical Devices. *IEEE Internet Things J.* **2022**, *9*, 13338–13352. [CrossRef]
75. Wangyal, S.; Dechen, T.; Tanimoto, S.; Sato, H.; Kanai, A. A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT). In Proceedings of the 2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI), Kitakyushu, Japan, 1–15 September 2020; pp. 639–644.
76. Zahra, B.F.; Abdelhamid, B. Risk analysis in Internet of Things using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–7.
77. de la Defense Nade la Defense Nationale, Secretariat General. EBIOS: Expression of Needs and Identification of Security Objectives. 2005. Available online: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html (accessed on 18 May 2023).
78. Breier, J.; Schindler, F. Assets dependencies model in information security risk management. In Proceedings of the Information and Communication Technology: Second IFIP TC5/8 International Conference, ICT-EurAsia 2014, Bali, Indonesia, 14–17 April 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 405–412.
79. Federal Information Processing Standards. *Minimum Security Requirements for Federal Information and Information Systems*; FIPS Publication: Gaithersburg, MD, USA, 2005.
80. Archiveddocs, M. The STRIDE Threat Model. 2009. Available online: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (accessed on 18 April 2023).
81. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *16*, 3–32. [CrossRef]
82. Michael, H.; David, L. *Writing Secure Code*; Pearson Education: London, UK, 2002.
83. Wang, Z.; Zhu, H.; Sun, L. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access* **2021**, *9*, 11895–11910. [CrossRef]
84. Gan, D.; Heartfield, R. Social engineering in the internet of everything. *Cut. IT J.* **2016**, *29*, 20–29.
85. Souppaya, M.; Stine, K.; Simos, M.; Sweeney, S.; Scarfone, K. *[Project Description] Critical Cybersecurity Hygiene: Patching the Enterprise*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
86. Maennel, K.; Mäses, S.; Maennel, O. Cyber hygiene: The big picture. In Proceedings of the Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, 28–30 November 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 291–305.
87. Rizvi, S.; Orr, R.; Cox, A.; Ashokkumar, P.; Rizvi, M.R. Identifying the attack surface for IoT network. *Internet Things* **2020**, *9*, 100162. [CrossRef]
88. Zevin, S. *Standards for Security Categorization of Federal Information and Information Systems*; DIANE Publishing: Collingdale, PA, USA, 2009.
89. Hong, J.; Kim, D.S. *Harms: Hierarchical Attack Representation Models for Network Security Analysis*; Edith Cowan University: Joondalup, WA, Australia, 2012.
90. ISO. *Medical Devices: Application of Risk Management to Medical Devices*; International Organization for Standardization: Geneva, Switzerland, 2019.
91. Johnson, C.; Badger, L.; Waltermire, D.; Snyder, J.; Skorupka, C. *NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
92. ISO. 31000: 2018 Risk Management. Guidelines. Suomen Standarditoimisliitto SFS ry. 2018. Available online: https://sfs.fi/ (accessed on 26 July 2023).
93. Deutsche Telekom. Privacy and Security Assessment Process. 2012. Available online: https://www.telekom.com/en/company/data-privacy-and-security/news/privacy-and-security-assessment-process-358312#:~:text=The%20PSA%20process%20guarantees%20for,(zip%2C%203.5%20MB) (accessed on 26 July 2023).
94. Barker, E.B.; Smid, M.; Branstad, D. *Profile for US Federal Cryptographic Key Management Systems*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.
95. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2011**, *800*, 16.
96. Center of Internet Security. CIS Controls v8 Internet of Things Companion Guide. 2021. Available online: https://www.cisecurity.org/white-papers/cis-controls-v8-internet-of-things-companion-guide/ (accessed on 22 July 2023).
97. Khouzani, M.; Liu, Z.; Malacaria, P. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *Eur. J. Oper. Res.* **2019**, *278*, 894–903. [CrossRef]
98. Zhang, Y.; Malacaria, P. Bayesian Stackelberg games for cyber-security decision support. *Decis. Support Syst.* **2021**, *148*, 113599. [CrossRef]

99. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cyber security investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
100. Verizon. 2023 Data Breach Investigations Report. 2023. Available online: https://www.verizon.com/business/resources/reports/dbir/ (accessed on 18 July 2023).
101. Motohashi, T.; Hirano, T.; Okumura, K.; Kashiyama, M.; Ichikawa, D.; Ueno, T. Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation. *J. Med. Internet Res.* **2019**, *21*, e13385. [CrossRef]
102. Safa, N.S.; Maple, C.; Watson, T.; Von Solms, R. Motivation and opportunity based model to reduce information security insider threats in organisations. *J. Inf. Secur. Appl.* **2018**, *40*, 247–257. [CrossRef]
103. Yao, D.; Wen, M.; Liang, X.; Fu, Z.; Zhang, K.; Yang, B. Energy theft detection with energy privacy preservation in the smart grid. *IEEE Internet Things J.* **2019**, *6*, 7659–7669. [CrossRef]
104. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
105. Affia, A.A.O.; Finch, H.; Jung, W.; Samori, I.A.; Potter, L.; Palmer, X.L. IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT* **2023**, *4*, 150–182. [CrossRef]
106. Izrailov, K.; Chechulin, A.; Vitkova, L. Threats classification method for the transport infrastructure of a smart city. In Proceedings of the 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT), Uzbekistan, Tashkent, 7–9 October 2020; pp. 1–6.
107. VARIoT. Variot Databases of IOT Exploits and Vulnerabilities. 2022. Available online: https://www.variotdbs.pl/ (accessed on 2 June 2023).
108. ENISA. Smart Grid Threat Landscape and Good Practice Guide. 2013. Available online: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide (accessed on 26 July 2023).
109. ENISA. Cyber Security and Resilience for Smart Hospitals. 2021. Available online: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (accessed on 26 July 2023).
110. ENISA. ENISA Good Practices for IoT and Smart Infrastructures Tool. 2021. Available online: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool (accessed on 22 July 2023).
111. Haney, J.M.; Furman, S.M.; Acar, Y. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In Proceedings of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, 19–24 July 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 393–411.
112. Health and Safety Executive. Managing Risks and Risk Assessment at Work. Available online: https://www.hse.gov.uk/simple-health-safety/risk/index.htm (accessed on 24 July 2023).

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.