frontiers | Frontiers in Big Data

TYPE Review
PUBLISHED 10 October 2024
DOI 10.3389/fdata.2024.1402745

OPEN ACCESS

EDITED BY
Hai Dong,
RMIT University, Australia

REVIEWED BY
Amna Qureshi,
University of Bradford, United Kingdom
Wenxiu Ding,
Xidian University, China

*CORRESPONDENCE
Petar Radanliev
petar.radanliev@cs.ox.ac.uk

RECEIVED 25 March 2024
ACCEPTED 16 September 2024
PUBLISHED 10 October 2024

CITATION
Radanliev P, De Roure D, Maple C, Nurse JRC, Nicolescu R and Ani U (2024) AI security and cyber risk in IoT systems.
Front. Big Data 7:1402745.
doi: 10.3389/fdata.2024.1402745

AI security and cyber risk in IoT systems

Petar Radanliev[1,2]*, David De Roure[3], Carsten Maple[4], Jason R. C. Nurse[5], Razvan Nicolescu[6] and Uchenna Ani[7]

[1]Department of Computer Science, University of Oxford, Oxford, United Kingdom, [2]Department of Computer Science, School of Computing and Engineering, Huddersfield University, Huddersfield, United Kingdom, [3]Department of Engineering Science, Oxford e-Research Centre, University of Oxford, Oxford, United Kingdom, [4]WMG Cyber Security Centre, University of Warwick, Coventry, United Kingdom, [5]School of Computing, University of Kent, Kent, United Kingdom, [6]Digital Anthropology, University College London, London, United Kingdom, [7]School of Computer Science and Mathematics, Keele University, Keele, United Kingdom

Internet-of-Things (IoT) refers to low-memory connected devices used in various new technologies, including drones, autonomous machines, and robotics. The article aims to understand better cyber risks in low-memory devices and the challenges in IoT risk management. The article includes a critical reflection on current risk methods and their level of appropriateness for IoT. We present a dependency model tailored in context toward current challenges in data strategies and make recommendations for the cybersecurity community. The model can be used for cyber risk estimation and assessment and generic risk impact assessment. The model is developed for cyber risk insurance for new technologies (e.g., drones, robots). Still, practitioners can apply it to estimate and assess cyber risks in organizations and enterprises. Furthermore, this paper critically discusses why risk assessment and management are crucial in this domain and what open questions on IoT risk assessment and risk management remain areas for further research. The paper then presents a more holistic understanding of cyber risks in the IoT. We explain how the industry can use new risk assessment, and management approaches to deal with the challenges posed by emerging IoT cyber risks. We explain how these approaches influence policy on cyber risk and data strategy. We also present a new approach for cyber risk assessment that incorporates IoT risks through dependency modeling. The paper describes why this approach is well suited to estimate IoT risks.

KEYWORDS

artificial intelligence, Internet-of-Things (IoT), cyber risk management, cyber risk assessment, cyber risk estimation, cyber risk insurance, risk impact assessment, AI security

1 Introduction—Defining the Internet of Things (IoT)

The fast Internet of Things (IoT) adoption has transformed modern industries and daily life, creating interconnected environments that deliver unprecedented efficiency and convenience. However, this extensive integration of IoT devices has also introduced significant cybersecurity risks. The Internet of Things (IoT) has attracted the attention of cybersecurity professionals after cyber-attackers started using IoT devices as botnets (Palekar and Radhika, 2022). IoT devices are often vulnerable to various cyber threats, including distributed denial-of-service (DDoS) attacks, botnet exploitation, and data breaches, all of which can compromise critical systems' integrity, confidentiality, and availability. Understanding and mitigating the risks associated with IoT deployments is crucial in this evolving landscape, especially given the interdependencies between IoT components and systems.

1.1 Motivation

The primary motivation for this research arises from the pressing need to develop a comprehensive framework for assessing cyber risks in IoT environments. While several risk assessment models have been developed, only some fully capture the unique dependencies and interactions between IoT devices, networks, and services. These dependencies introduce cascading risks, where vulnerabilities in one component can propagate through the entire system, amplifying the impact of an attack.

Additionally, existing risk models often need more real-time adaptability and need to consider the heterogeneity of IoT systems, where devices from different manufacturers and platforms interact in dynamic and unpredictable ways. Given the increasing reliance on IoT in critical sectors such as healthcare, industrial automation, and smart cities, a more robust, adaptable, and scalable risk assessment model is urgently needed.

The research also addresses the gap in effectively utilizing AI/ML techniques for real-time risk assessment in IoT environments while ensuring these models are explainable and transparent to decision-makers. This is particularly important for building trust in AI-driven cybersecurity solutions and ensuring their alignment with organizational goals.

1.2 Contributions

This paper makes the following key contributions:

1. **A dependency-based cyber risk model for IoT systems**: we propose a novel dependency-based risk assessment framework that captures the interdependencies between IoT components and their cascading effects on overall system security. The model systematically quantifies and mitigates risks based on the interaction between devices, networks, and services.
2. **Incorporation of AI/ML for dynamic risk estimation**: the proposed model integrates AI/ML techniques to enable real-time risk assessment. The machine learning models are trained on diverse data sources, including network traffic, vulnerability databases, and incident logs, to predict and prioritize risks in dynamic IoT environments. Explainable AI (XAI) ensures that these predictions are transparent and interpretable to cybersecurity professionals.
3. **Generalization of the risk framework across IoT domains**: we demonstrate the applicability of the proposed model across various IoT domains, including smart cities, healthcare, and industrial IoT. The framework is adaptable to different types of IoT systems, regardless of device heterogeneity or scale, making it a versatile tool for risk assessment in diverse settings.
4. **Integration of risk transference strategies**: this research explores risk transference mechanisms, such as cyber insurance and third-party liability agreements, to mitigate IoT cyber risks' financial and operational impact. We discuss how these strategies can be effectively implemented within the proposed framework.
5. **Empirical validation using the BoT-IoT dataset**: the proposed model is validated using the BoT-IoT dataset, a comprehensive and realistic representation of IoT network traffic and attack scenarios. We provide an in-depth analysis of the model's performance in detecting and mitigating risks, and we compare it with alternative risk assessment frameworks to highlight its effectiveness.

IoT-based cyber-attacks often take the form of distributed denial of service (DDoS) attacks, where the attacker uses the hacked IoT devices as clones to infect or stop operations in other parts of the network. Various cybersecurity solutions have been proposed, including *"deep learning based malicious behavior detection in cloud computing"* (Bhingarkar et al., 2022), *"sensing and detection algorithms"* (Zhang, 2021) and the *"intelligent warehouse monitoring based on distributed system and edge computing"* (Lin et al., 2021). IoT is defined as networked objects communicating data between networks and humans (The PETRAS National Centre of Excellence – PETRAS, 2022). The development of IoT has provided opportunities for social and economic interaction in many areas, such as supply chain management, social media, medicine, and energy consumption (for example, smart health devices). IoT employs sensors and actuators and applies to various protocols, domains, and applications, e.g. cyber-physical systems, technologies related to smart grids, smart homes, intelligent transportation and smart cities. Some technologies used daily are currently not connected to the Internet, such as gas meters, house lights, healthcare devices, water distribution systems, cars, and other road transport vehicles. However, such devices are increasingly becoming digitally connected and can communicate through mobile (or wireless) networks, e.g., connected spaces, smart meters and autonomous cars. Ultimately, IoT may revolutionize the existing business ecosystem because connected objects can reduce costs, optimize processes, and enable new business models by automating data flow, centralized processing of data, and intelligent use of the data.

With the increased relevance of IoT for business, cyber security importance is growing (Pigman, 2019) and there are increasing security and privacy challenges (Maras and Wandt, 2019). New technologies also come with new risks (Constance, 2017) that traditional risk assessment/management methods have not anticipated or predicted (Crawford and Sherman, 2018). It has been argued that quantitative risk assessments do not necessarily offer a unique rationality that pinpoints a single right course of action but rather probabilities that require moral assessment for action (Adams, 1995). This kind of assessment can vary across domains and populations. For example, in financial markets, the complexity aspect of risk is of major importance. In contrast, in consumer markets, people are increasingly trained and habituated to act in the present regarding future risks (Caplan, 2000).

Different cyber risk valuation models have emerged recently, including a model based on *"computationally efficient solution.. operating under the probable impact of typed cyber-physical attacks"* (Kovtun et al., 2022), or applying deep learning to detect *"Trojan malware in bio-cyber attacks"* (Islam et al., 2022). However, in evaluating the impact of risk, conventionally, it is considered, essentially, that Risk = Likelihood × Consequences. However, we do not have probabilistic data on the likelihood or consequences, and without such data, the industry's understanding of IoT cyber risk is still in its infancy (Aggarwal and Reddie, 2018). Empirical

results have found that the aggregate frequency of data breaches is stable over time (Edwards et al., 2016; Wheatley et al., 2016). Still, future attacks are expected to increase (Leverett and Kaplan, 2017) with IoT systems and other digital infrastructure. Digital expansion also changes the cyber risk profile, making it difficult to quantify with historical measures. In addition, there are no standards, regulations, or policies on risk assessment that measure the impact, cost, and probabilities of cyber-attacks in specific IoT systems (Srinivas et al., 2019). For example, if we consider cyber risk in general, the estimates of impact range from 300 bn and $1 tn (Biener et al., 2014), $400 bn to over $575 bn (DiMase et al., 2015), or $400 bn to over $2 tn (Shackelford, 2016). Although these figures could be correct in the parameters of the assessments, the difference presents a rationale for some literature to argue that the real impact of cyber risk is unknown (Shackelford, 2016). This motivates our attempt to define a process for standardizing a unified cyber risk assessment approach.

In an IoT context, the most challenging aspects are risk's dynamic and complex aspects, including assessment of safety and security, co-existing of different producers and vintages, common cause failures and cascading risks. Although, like cyber risk in general, IoT risk can be decomposed into different risk verticals. For example, because of the low cost of IoT devices, it is generally assumed that IoT devices cannot be adequately secured and, therefore, logical placement of security capability is in the communications network (Anthi et al., 2018). To emphasize these differences, this paper articulates some of the possible security risks in the communications network, particularly the risk from distributed ownership and control of IoT systems. To develop and test the new approach for cyber risk estimation and assessment, in this study we used the *"BoT-IoT"* dataset[1], designed by the Cyber Range Lab of UNSW Canberra Cyber.

1.3 Justification for the use of the BoT-IoT dataset

The BoT-IoT dataset was chosen for this study due to its comprehensive and realistic representation of IoT network traffic, which includes a wide range of attack scenarios. Developed by the Cyber Range Lab of UNSW Canberra, this dataset is designed explicitly for IoT environments. It includes various simulated attacks such as distributed denial-of-service (DDoS), keylogging, data theft, and information gathering. The dataset's diversity in attack types and network traffic allows for a holistic analysis of IoT-related cyber risks, particularly in botnet-driven attacks, which are among the most prevalent in IoT systems.

Moreover, the BoT-IoT dataset offers the following advantages:

- **Realistic traffic simulation**: the dataset captures real-world IoT traffic patterns, making it highly suitable for testing intrusion detection and risk assessment methods in heterogeneous IoT environments.
- **Diverse attack vectors**: it includes multiple attacks, such as DDoS, brute force, and OS and service scanning, relevant to understanding a wide array of IoT cyber risks.
- **Detailed labeling**: the dataset is labeled, allowing for supervised machine learning approaches in identifying and mitigating threats, which is crucial for assessing the effectiveness of AI-based risk assessment models.

2 Alternative datasets

Several alternative datasets could have been considered for this study, though they have certain limitations compared to BoT-IoT. These include:

1. **Kitsune dataset**: this dataset focuses on the network traffic of IoT devices and has been widely used in anomaly detection. However, it is more limited in terms of attack variety and lacks certain botnet-specific data that is crucial for understanding large-scale distributed IoT attacks.
2. **TON_IoT dataset**: another comprehensive dataset developed by UNSW Canberra, the TON_IoT dataset contains IoT telemetry data, network traffic, and operating system logs. While useful, it is geared more toward industrial IoT (IIoT) environments and does not focus as heavily on botnet behavior, which is the primary threat discussed in this paper.
3. **IoT-23 dataset**: this dataset provides labeled IoT traffic data with malware analysis, but it is more focused on malware rather than the broad spectrum of cyber risks in IoT environments, making it less suitable for this study's goals.

While other datasets exist, the BoT-IoT dataset was chosen for its relevance to the focus of this study (evaluating the risks of IoT-based botnet attacks) and for its detailed attack scenarios that allow for robust risk estimation and assessment.

2.1 Organization of the paper

The rest of this paper is organized as follows:

- **Section 2: Background and related work**: this section reviews the current state of IoT cybersecurity, including existing risk assessment models and their limitations. We also discuss the use of AI/ML in cybersecurity and highlight the gap that this research addresses.
- **Section 3: Proposed dependency-based risk assessment model**: in this section, we detail the proposed model, explaining the methodology behind dependency analysis, the incorporation of AI/ML, and the use of explainable AI techniques. We also provide a formal definition of the risk estimation process.
- **Section 4: Data sources and AI/ML implementation**: this section describes the data sources used for training the machine learning models, including network traffic, device telemetry, vulnerability databases, and external threat intelligence. We explain the model's architecture and the machine-learning techniques employed.

1 https://ieee-dataport.org/documents/bot-iot-dataset

- **Section 5: Empirical evaluation and results**: here, we present the results of the empirical validation using the BoT-IoT dataset. We compare the performance of the proposed model against existing frameworks and discuss its effectiveness in detecting and mitigating IoT-related cyber risks.
- **Section 6: Discussion and generalization**: this section discusses the generalisability of the proposed model across various IoT domains. We provide case studies in healthcare, smart cities, and industrial IoT to demonstrate its broad applicability.
- **Section 7: Conclusion and future work**: we conclude the paper by summarizing the key findings and outlining potential areas for future research, particularly in refining the AI/ML techniques and further validating the model in live IoT environments.

3 Artificial intelligence and the Internet of Things (IoT)

The merging of Artificial Intelligence (AI) with Internet of Things (IoT) technology brings about a new era in cyber risk. This is marked by a complex interweaving of sophisticated threats that require an equally advanced approach to manage and mitigate them. This chapter delves into specific, technologically advanced examples that highlight the unique cyber risks brought about by AI in IoT environments, drawing from the foundational concepts in "Cyber Risk in IoT Systems."

One of the challenges posed by the use of AI in IoT is autonomous decision-making, which can amplify cyber risk. For example, AI-driven IoT devices in smart cities could autonomously manage traffic flow based on real-time data. However, a compromised AI algorithm could create chaotic traffic patterns, causing widespread disruption.

Data integrity is vital in AI-IoT systems, and data manipulation poses a risk. For instance, in healthcare IoT devices, AI algorithms process patient data for predictive diagnostics. The AI's predictive outcomes could be dangerously inaccurate if these data streams are manipulated—say through a man-in-the-middle attack intercepting and altering data from IoT health monitors. Similarly, AI model poisoning, where the AI's learning inputs are subtly tainted, could lead to erroneous learning, echoing the data integrity and manipulation concerns highlighted in the article.

Integrating AI into IoT brings unique AI-specific risks, such as adversarial machine learning. For example, in a network of interconnected smart home devices, an adversary could manipulate input data to an AI-powered security camera, causing it to misidentify or overlook intrusions. These AI-specific threats necessitate a novel approach to cybersecurity, diverging from traditional risk management strategies.

Addressing these enhanced risks requires a multifaceted and advanced approach. There is a need for risk assessment frameworks that specifically account for AI components in IoT ecosystems. This would involve understanding not only physical and data flow dependencies but also the AI algorithmic dependencies. Leveraging AI's capabilities for security in IoT networks presents a proactive defense mechanism. However, the implementation of such AI-driven security measures must be carefully managed to ensure they do not introduce new vulnerabilities. The integration of AI into IoT amplifies the need for comprehensive regulatory and ethical frameworks, addressing not only data privacy and security concerns but also the ethical implications of AI decisions, particularly in areas where these decisions impact human safety.

Given the complexity of AI in IoT, collaboration across disciplines is essential. Cybersecurity experts, AI researchers, IoT developers, and policymakers must work together to create advanced and resilient cybersecurity solutions that address the unique challenges posed by the AI-IoT convergence. In conclusion, the combination of AI and IoT presents a complex array of cyber risks that require advanced, specific, and comprehensive management strategies. Future research and practical approaches should focus on developing sophisticated AI-resilient security frameworks, enhancing regulatory standards, and promoting interdisciplinary collaborations, thus ensuring the secure advancement of AI within IoT systems.

4 Cyber risk from distributed ownership and control of IoT systems

The distributed ownership and control of IoT systems is considered the one factor contributing to the number of zero-day exploits exacerbated by IoT (Meakins, 2019). Although there are many different cybersecurity approaches, they seem insufficient or not targeted at the right areas. This leads to a lack of security that creates unnecessary difficulty for IoT-connected producers and customers. The growth of the IoT market could increase significantly if policymakers have the methodology to assess, predict, analyze, and address the risks of IoT-related cyber-attacks in the communications network.

Without the appropriate risk assessment methodology, cyber risk could have costly consequences. Connecting cyber risk with IoT through impact models can provide feedback sensors and real-time data mechanisms to assist and enable industries and policymakers to understand and visualize the problem and address the risk created by IoT-related cyber-attacks.

4.1 Defining cyber risk

IoT risk and the risk of cyber-attacks can be explained by established methods for calculating risk. Risk = Likelihood × Consequences, and cyber-risk can be defined as a function of:

$$R = \{si, pi, xi\}, i = 1, 2, ..., N,$$

Where R—risk; s—the description of a scenario (undesirable event); p—the probability of a scenario; x—the measure of consequences or damage caused by a scenario; N—the number of possible scenarios that may cause damage to a system.

The model above for calculating risk is classical (DoD, 2017), but the question remains how IoT risk and cyber-attack risk can be estimated. Since we do not have the precise measurements and concrete number of IoT cyber risks, an answer is difficult to present and justify with a desirable degree of certainty that the

estimation is correct. Therefore, we discuss how IoT risk and the risk of cyber-attacks can be estimated assuming possession of the required data.

Businesses face strategic, compliance, operational, financial, and reputational risks regularly, all of which could affect their profitability or ability to function. Many businesses are looking to adopt new forms of technology (such as IoT, Blockchain and Artificial Intelligence) to increase the efficiency and effectiveness of their services. This exposes them to the risks that accompany these technologies. While these technologies have the potential to improve their productivity, there is also the potential for the business to become increasingly susceptible to a series of security risks—this is the aspect of focus in this paper.

In the following table, we explore the main cyber risks that many businesses face, and we define definitions for different types of cyber risks. We use the term *"cyber risk"* in line with the Institute for Risk Management definition of: *"Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems."* (Institute of Risk Management, 2019). In Table 1, we provide insights on how companies can manage the IoT cyber risk, and we include real world examples in each risk category.

Table 1 summarizes and explores the ethical, privacy, security, and technical aspects of cyber risk. To relate the findings, an IoT-based example of this is the probability of a phishing attack on a connected corporate device occurring, like a company laptop or a smart phone, which then leads to the infection of that device. This infection could propagate to other IoT sensors in the company and consequently cause the disruption of their manufacturing plant's production line. While there are many application domains for IoT, for organizations to consider cyber security risk solely in the context of their domain would give misinformed results, since IoT is an ecosystem with platforms and services shared by different application domains.

4.2 IoT risk assessment

Understanding what is meant by risk is only the first step when we are considering the potential risks in IoT. The next step is to be able to assess the risk, which involves the tasks of: (1) identifying (or defining) the risk—the action of developing a clear understanding of what organizational IoT assets are targeted by which threats and what harm could happen if those attacks are successful (Tanczer et al., 2018).

(2) Estimating the risk—this task aims to measure IoT risk based on the likelihood of the threat occurring and the impact on the organization's infrastructure if it does occur. These measures can be qualitative (e.g., ratings using the levels, high, medium, and low) or quantitative (e.g., based on mathematical estimations and calculations).

(3) Prioritizing the risk; once we have a list of the risks and each one has been estimated, the next task is for a company to prioritize the risks. This essentially provides a ranking of the risks based on their estimated levels. We interpreted that identifying the risk, estimating the risk, and prioritizing the risk are three tasks of IoT risk assessment. Figure 1, below, sets this out, and demonstrates that this is a continuous process.

4.3 IoT risk management

The risk assessment process described above is part of risk management. While risk management techniques are well developed and used in various IT areas, there remains a significant challenge in managing IoT risk. Here, we include our findings in the form of four basic ways to resolve IoT risk:

IoT risk mitigation involves either reducing the likelihood of the risk happening or reducing the impact of the risk. In IoT risk management, this might include implementing IoT risk controls.

IoT risk transfer—this involves outsourcing the risk to a third party. In this instance, via cyber insurance for example;

IoT risk avoidance—this involves removing the risk. An example would be to remove IoT asset where the risk has originated; and IoT risk acceptance—this involves accepting the risk as it stands, due to either the risk falling within the organizational risk appetite or the aggregated risk being sufficiently within the accepted risk levels.

The type of treatment selected for each risk is based on its estimated level, the costs associated with the treatment, and the organization's overall tolerance for risk. In IoT, these factors are constantly changing, and this aspect represents one of the unique challenges when managing risks in dynamic IoT environments.

5 How IoT transforms the nature of risk

IoT represents interconnected technologies continuously communicating and sharing data. This technology creates serious safety risks and ethical concerns. For example, IoT incorporated into autonomous vehicles introduces safety risk, however, the device owner and the data owner are not necessarily the same (Anthonysamy et al., 2017), because there is no legal basis to actually own data. The data owner is the data curator or controller. Here we are making the point about the legal impossibility to own data. Because there is no owner of data, but rather an entity that has the legal right to control and steward the data. In following sections, we discuss how the existing risk assessment approaches can be adapted to assess the nature of IoT risk.

These designs need data to support, and the data is very sensitive and private. There has been a number of suggestions on how to resolve this concern. Back in 2014, the original "Cyber Supply Chain Management and Transparency Act of 2014" (Royce, 2014) was proposed and suggested that that US government agencies obtain a software bill of materials' (SBOMs) for all new software. This led to the "Internet of Things Cybersecurity Improvement Act of 2017" (Howard, 2017), and more recently, "The US Executive Order on Improving the Nation's Cybersecurity of May 12, 2021, (Biden, 2021) ordered The National Institute of Standards and Technology (NIST) to issue guidance on "*providing a purchaser a Software Bill of Materials (SBOM) for each product.*" These efforts in the US are related to resolving the specific issue of sharing sensitive and private company data on cyber vulnerabilities, exploits, threats, and this has been a very sensitive topic for a long time. The most recent effort that we are making to resolve these issues is the new the **Vulnerability Exploitability eXchange** (VEX) (NTIA, 2021), which has already been adopted as a profile in the Common Security Advisory

TABLE 1 Defining the types of cyber risk from IoT systems.

Types of cyber risk	Definition	Key words	Example
Ethical	An action that falls short of what is considered morally right or outside of a professional standard. So, an ethical risk for an institution is the unintended harm caused by an unethical action.	Integrity, honesty, fraud, moral, standards, compliance, misconduct	Volkswagen develop and install software to cheat diesel emissions tests. This compromises organization and industry standards and results in massive reputational and financial losses (Fracarolli Nunes and Lee Park, 2016).
Privacy	Most information about people is digitized. Keeping this private and confidential is important. So, a privacy risk is when there is a temporary or permanent loss of control over data that may causes some form of harm to the individual and the business, organization or government that holds the data.	Trust, transparency, data, confidentiality, cyberattack, hacking, data breach, phishing, pharming, ransomware, spam	In May 2014 145 million eBay customers have their names, addresses, date of birth and passwords accessed (Ranganthan et al., 2018). Yahoo was the victim of a massive data breach in 2013–2014. In 2017 they finally admitted that all 3 billion user accounts had been compromised (Gupta, 2018).
Security	This is to do with vulnerabilities and gaps in security programmes and systems. These vulnerabilities can be exploited in order to gain access to assets causing damage, harm or loss. Types of attack include physical, network, software and encryption attacks.	Vulnerability, weakness, protection, attacks, breaches, DDoS (distributed denial of service), botnets, malware, virus	In October 2016 the Mirai Botnet launched a DDoS attack on DYN which led to parts of the internet going down and affected Twitter, Netflix, CNN, Reddit (along with many others) (Dubois, 2018; Payton, 2018). Building management systems were attacked in a Finnish town of Lappeenranta, causing the heating in two buildings to fail (Scott and Winter, 2016).
Technical	The failure of hardware or software due to poor design, construction, or evaluation.	Compliance, regulation, testing, evaluation	It was recently discovered that computer chips produced in the last 20 years all contain fundamental security flaws (Conte et al., 2018), some related to the chip variation, e.g., Specter and Meltdown.
Interoperability	Refers to the challenges in ensuring that IoT devices, software platforms, or services can communicate effectively with each other. Interoperability risks can lead to system miscommunications or data integration failures, especially in environments with heterogeneous devices and platforms.	Compatibility, integration, communication breakdown, data silos	A healthcare system relying on IoT medical devices that operate on different protocols fails to integrate data from wearable sensors and in-hospital monitors, leading to incomplete or inaccurate patient health records.
Safety	Risks that directly affect the physical well-being of individuals or groups due to IoT device misuse, malfunction, or cyber-attacks. These risks include bodily harm or fatalities resulting from compromised safety-critical systems.	Physical harm, injury, malfunction, cyber-physical systems, personal safety	A compromised autonomous vehicle causes accidents due to failure in its IoT control systems, leading to injuries and potential fatalities. Similarly, hacked smart home devices such as IoT-connected thermostats cause fires or unsafe temperature regulation.

Framework (CSAF) (OASIS, 2022). This article however, is more closely related to the updated version of the Common Vulnerability Scoring System Calculator (CVSS) (NIST, 2022), which is the Stakeholder-Specific Vulnerability Categorization (CISA-SSVC) (CISA, 2022) and it relates to the SSVC decision threes.

5.1 Security risk assessment for IoT systems

One of the main problems with IoT is that this technology is developing at a fast rate and in multiple directions so that governments and national and international institutions face difficulties to standardize and enforce regulations in this field. These difficulties are related, for example, with the continuing changing environment of IoT (Brass et al., 2018) or with the relatively much slower legislative and standardization processes (e.g., Schindler et al., 2013; Brass et al., 2019). We found that there are currently no risk assessment standards to govern companies in assessing the new types of risk before implementing IoT technologies and solutions. In the present climate, given the lack of unified global standards and regulations, businesses are pursuing economic profits from IoT solutions, but as it pertains to understanding the risk to their operations, businesses are often lacking in their approach to security.

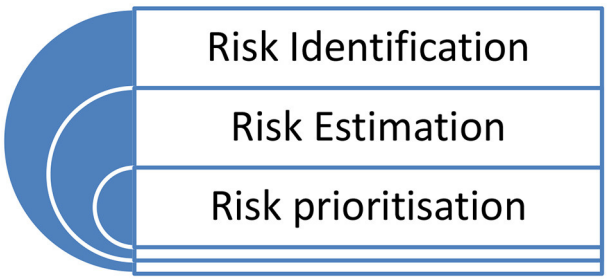


FIGURE 1
The IoT risk assessment process.

5.2 Analysis of cyber risk assessment approaches

As part of our research, we conducted an analysis of the existing cyber risk assessment approaches to enable us to provide basic guidance on how to develop a unified approach to risk assessment. Most cyber risk assessment approaches represent some similarities and after reviewing one we tend to get the general feeling that they all seem familiar. Hence, for differentiating these frameworks, for the reader and for our own research, in the Table 2 we tried

to define the main differences between the cyber risk assessment frameworks that we reviewed in this article. In Table 2, we also include references to all of the frameworks as a source for further information on these frameworks. The selection process involved firstly conducting a literature review on the topic of "most used" and "most prominent" cyber risk assessment approaches.

5.2.1 Secondary data: "most used" and "most prominent"

The selection of the "most used" and "most prominent" cyber risk assessment frameworks for this study was based on a combination of several key criteria that ensured relevance, industry adoption, and scholarly significance. These criteria were established following a comprehensive literature review and consultation with experts in cybersecurity, including those from Cisco Systems. The following criteria guided our framework selection:

1. **Industry adoption and standardization**: one of the primary indicators of prominence was the degree of adoption within industry sectors and standardization by international bodies. Frameworks such as **NIST Cybersecurity Framework** and **ISO/IEC 27001** were included because they are widely recognized and applied across various industries and sectors as global standards for cybersecurity risk management. Their extensive use across governmental, industrial, and private sectors made them foundational to this study.
2. **Scholarly citations and academic relevance**: frameworks that have been heavily cited in academic research and peer-reviewed journals were also prioritized. For example, frameworks like **OCTAVE** and **FAIR** have been the focus of numerous scholarly articles, making them prominent in the research community. The high citation count, particularly in the context of IoT cybersecurity and risk assessment, reinforced their relevance to this study's objectives.
3. **Expert recommendations**: insights from cybersecurity professionals and experts consulted during the research process, particularly those from Cisco Systems, played a crucial role in identifying frameworks that are "most used" in practice. These experts, with hands-on experience in cyber risk management, highlighted which frameworks they relied on in real-world scenarios, giving us a practical understanding of which frameworks are most relevant and widely applied across various sectors.
4. **Diversity of application**: frameworks that demonstrated applicability across a wide range of environments, including traditional IT infrastructures, IoT systems, and cloud computing, were considered more prominent. Frameworks such as **FAIR** (Factor Analysis of Information Risk) and **CVSS** (Common Vulnerability Scoring System) were selected because they are adaptable to different risk environments, including both qualitative and quantitative risk assessment contexts.
5. **Ease of use and implementation**: in practice, the complexity of a framework can influence its adoption. Frameworks that are well-documented, easy to use, and backed by automated tools or platforms were considered more prominent. For instance, **CVSS**, which provides a widely accessible scoring system for vulnerabilities, and **RiskLens**, which integrates FAIR for quantitative risk analysis, were selected for their ease of implementation in enterprise and IoT environments.
6. **Comprehensive risk coverage**: finally, frameworks that cover a broad spectrum of risk factors, including technical, operational, strategic, and reputational risks, were included. The **NIST Cybersecurity Framework**, for example, is notable for its comprehensive approach, addressing everything from threat identification to incident response, which aligns with the holistic perspective of this study on IoT cyber risks.

The selection of frameworks was based on a multifaceted approach combining:

- Industry recognition and standardization,
- Scholarly citation and academic significance,
- Expert recommendations from cybersecurity practitioners,
- Diversity and applicability across environments,
- Ease of implementation,
- Comprehensive risk coverage.

This selection process ensured that the frameworks chosen for analysis and inclusion in the study were not only theoretically sound but also practically relevant and widely used in the real world.

5.2.2 Primary data: expert consultations

Secondly, we consulted a number of experts in the field from Cisco Systems that are responsible for this function. This consultation was conducted in the period between year 2018 and 2023, initiated with a scoping workshop in June 2018 and concluded with a closing workshop in January 2023. The consultation was conducted as case study action research, and included personal interviews with 43 cybersecurity experts, 13 workshops, two demonstration projects for gathering feedback, and 6 months long action research at Cisco locations.

The resulting list of approaches is not complete, but its representative of the "most used" and "most prominent" cyber risk assessment frameworks, models, and methodologies—as determined in literature and by the experts from Cisco Systems.

The Cisco Systems experts consulted during this study represented a broad range of cybersecurity specialties, including, but not limited to, cyber risk assessment frameworks. Their involvement was crucial in providing a comprehensive and multi-faceted view of IoT cyber risks and the development of robust risk assessment methodologies.

Specifically, a subset of the consulted experts specialized directly in **cyber risk assessment**, focusing on frameworks such as CVSS, CoSAI, OCTAVE, FAIR, and NIST Cybersecurity Framework, which were critical for refining the dependency model presented in this study. These experts were responsible for implementing and managing cyber risk strategies within Cisco's cybersecurity operations, making their insights particularly valuable in aligning the proposed model with industry practices and standards.

TABLE 2 Analysis of cyber risk assessment approaches.

Name	References to author(s) or Institution	What is it	Type
OCTAVE	(Caralli et al., 2007)	This is a standardized questionnaire that can be applied to investigate and categorize recovery impact areas. However, the OCTAVE method is complex and takes time to understand	Qualitative
TARA	(Wynn et al., 2011)	This is a predictive framework that enables targeting of the most crucial exposures, as opposed to promoting the defense of all possible vulnerabilities	Qualitative
CVSS (Common Vulnerability Scoring System)	(CVSS, 2019)	A scoring system "that provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity". It is relatively easy to use and translate results although, the calculator is based on experts' opinion and do not represent an ultimate precision, the calculator represents a guiding point.	Qualitative
Exostar System	(Shaw et al., 2017)	This system enables enterprises to assess, measure, and mitigate risk across multi-tier partner and supplier networks and determines the gaps between cybersecurity posture and regulatory compliance.	Qualitative
Capability Maturity Model Integration (CMMI)	(CMMI, 2017)	This combines a set of best practices in the disciplines of systems analysis and design, software engineering and management. CMMI can simultaneously address multiple as opposed to stand alone improvements. This enables improvement in the entire enterprise risk and the full product development life cycle risk.	Qualitative
NIST Cybersecurity Framework	(NIST, 2014)	This is a framework based on an extensive use of acronyms, which can be confusing and require a detailed understanding of the standards referred to in the acronyms. At present, the NIST framework is documented, not an automated tool.	Qualitative
ISO/IEC 27001	(ISO, 2017)	This risk management framework promotes standardization of cyber risk and reflects international experience and knowledge. It is based on voluntary shared knowledge and is consensus based.	Qualitative
RiskLens	(FAIR, 2020)	This is a quantitative assessment method based on FAIR (Factor Analysis of Information Risk) and "provides a model for understanding, analyzing and quantifying information risk in financial terms".	Quantitative
CyVaR (Cyber Value at Risk)	(Erola et al., 2022)	This presents a method to quantitatively assess risk with Monte Carlo simulations. CyVaR needs to be adapted and modified to include units of measurement for IoT cyber risk vectors.	Quantitative
FAIR	(FAIR, 2017)	This model promotes a quantitative, risk based, acceptable level of loss exposure.	Quantitative

Additionally, the consultation involved professionals with expertise in **IoT security, network infrastructure vulnerabilities, and incident response frameworks**. Their contributions ensured that the proposed model incorporated a holistic understanding of the various layers of IoT ecosystems, including the unique challenges posed by real-time data flows, network management, and preventing cascading failures in IoT systems.

By engaging with a diverse group of experts, the study benefited from a broad spectrum of knowledge across different cybersecurity domains, ensuring that the proposed model focused on risk assessment and addressed practical implementation concerns, such as real-time threat detection, system recovery, and mitigation strategies. This interdisciplinary consultation strengthened the model's applicability to real-world IoT environments and enhanced its generalization to diverse risk scenarios.

The analysis in Table 2 provides guidance and concludes that most of the cyber security frameworks today apply qualitative approaches to measuring cyber risk, while quantitative approaches are mostly present in the cyber security models. The analysis in Table 2 also confirms that none of these approaches resolves adequately the cyber risk assessment in IoT, at least not individually or in isolation. Presented with the diversity of cyber risk assessment approaches analyzed in Table 2 and given that existing risk methods do not address entirely the cyber risk from IoT, questions emerge on: (a). how can these approaches be combined into a unified model, and (b). how can we be certain that a unified model addresses IoT context. We try to address these questions in Section 4.2 through a dependency model that presents a unified approach for improved standards, governance, and policy on data strategies.

6 Dependency modeling for creating a unified model

In this section, a unified cyber risk assessment approach for IoT risk is explored via dependency modeling (DM) approach and a step-by-step process is included, enabling other companies to replicate this cyber risk assessment process. Dependency modeling (DM) is a goal-oriented method of representing the interactions and inter-reliance amongst system components or elements using same to reason about the scope of risk feasible (Cherdantseva et al., 2022). DM works on the assumption that risks emerge from interactions and interdependencies which need to be recognized in order to effectively manage and guard against the impacts of the risks (Alpcan and Bambos, 2009). DM for security risk assessment can work through analyzing the vulnerabilities that can be found in IoT network/system components—evaluating the interactions and service flow amongst connected components including hardware infrastructure, software platforms (applications), processes, services, users, etc., and how these threats and vulnerabilities affect both the target components and others connected. Generally, these are explored considering how the entire system functions and objectives are impacted. Security threats and vulnerabilities can emerge or exist in diverse forms, ranging from design flaws

in hardware, software, and processes, as well as competency limitation in users, which can easily be exploited by malware, social engineering, etc. Thus, the service or functional dependencies amongst IoT system components can be used to design a unified approach for IoT risk assessment. In doing this, we consider contexts from IoT literature and use cases in the model definition and verification.

Interactions within IoT can be seen as complex, tightly coupled relationship structures amongst the systems, sub-systems, and components. This means that IoT subsystems and components inter-cooperate to fulfill desired service objectives, which each sub-system or components is unable to achieve in isolation. To function appropriately, one or more sub-systems rely considerably on the appropriate functions of another system or sub-system they connect to and receive command or instruction input. Thus, a dependency relationship (shown in Figure 2) exists between connected systems with a mechanism characterized by the transfer of data or control from one component to another (Callo Arias et al., 2011), and which can either be direct (a first order) or indirect (a higher order) (Laugé et al., 2015), physical or non-physical (O'Neill, 2013), and involve any constituent of the wider IoT System operational ecosystem.

Graph theoretical approach can be used to represent dependencies in IoT networks as shown in Figure 2. This presents a directed graph structure G as an ordered pair (C, T), where C represents a finite set of vertices referring to IoT components, T representing a binary relation on C. T imply edges which represent *"context transfer or flow"* along successive IoT components. These edges form an ordered pair $t = (c_i, c_k)$, where $c_i, c_k \in C$ represent interacting or cooperating IoT components on specific functional objective. t can represent the dependency flow of data, service, or functionality from an originating IoT component c_i to a destination IoT component c_k (see Figure 2).

This dependency relationship could apply to different types of cyber risks. Since our efforts are focused on different types of risk assessment, including cyber risk assessment in general, we have used examples specific to IoT risk. Firstly, take, for example, an industrial Internet-of-Things (IIoT) production line involving a robotic arm and a conveyor belt system for product identification, transfer, and packing, following the analogy. To optimize packing performance, desired analytics functions by cloud-based components and services such as HMI and performance dashboard on the application layer (AL), which can represent c_i of C in an IIoT system, would typically depend on the appropriate functioning of transmitted data t_i, $t_j \in T$ through the network layer (NL) components such as communication switches and Programmable Logic Controllers (c_j). Dependency could also extend to perception layer (PL) components such as the Photoelectric sensors that detect items and actuator switches that move conveyor belts (c_k).

Like in other digital systems, IoT security risks typically depend on the existence/exploitation of vulnerabilities in system components at any layers of the architecture. Exploiting vulnerable components can cause them to malfunction or fail to deliver the desired processes initially configured. If an attacker gains control of sensing and/or actuating service functions and flow t_j on a PL, wrong data could be transmitted to and through N, and worse, data flow could be completely stopped. The impact on process data can reach AL components such as HMI and performance analytics dashboard system, and can in turn impact on the functions or outputs (t_i) desired from components in AL. The impacts can include a failure to reach the final goal of passing down correct item processing data for analysis and optimisation functions to support decision-making. If a vulnerability on a host IoT component is exploited, potential functional dependency-based impact can be estimated quantitative as a proportion of an overall flow of component functional dependencies along the part of compromise. A functional dependency index can be evaluated by analyzing the number of components that are included along a path following the edges from the originating component. Depending on the existence or otherwise of a functional dependency link, initial impact(s) of the attack is typically expressed in the origin and flows through to other connected components along the same path.

A logical switch function $\varphi(v)$ can be used to evaluate the conditional existence of a functional dependency between any two nodes on the network, a logical 0 (FALSE) to indicate "connection not configured", and a 1 (TRUE) to indicated connection configured as shown in Equation 1. For a tree network structure for IoT, the functional dependency index fd_v of a component v can be evaluated by summing the functional dependency indices of components connected to component v with a "connection configured" settings, as shown in Equation 2.

The proportion of impact dependency can be evaluated in relations to the highest possible dependency, which represents worse case impact of a vulnerability exploitation max (fd_v). A worst-case scenario can involve a dependency that runs through all the components in IoT network, enabling negative impacts to also flow along the same path when a certain vulnerability is exploited. Here, the impact dependency proportion would be 1. A 0 would mean no component is affected. An impact dependency proportion, (P_{fd_v}) can be estimated as the degree of dependency impact which can occur when a certain vulnerability is exploited relative to the worst-case dependency impact (see Equation 3).

Thus, an IoT security risk landscape need not consider the failure of a single IoT component alone, but the failure of other IoT components (devices or services) due to abnormal events and/or impacts on a component they rely on. Functional dependency relationships amongst IoT sub-systems can also cause impacts or failures to cascade from one affected system or component onto another; aggravating the impacts (Bloomfield et al., 2010).

Depending on the evaluation approach, security and safety-critical impacts typically vary amongst assets, their functionalities (services), placement positions, and configurations within industrial networked systems, including IoT. However, to support effective decision-making from both security and safety perspectives, IoT adopters need to adopt risk assessment methods that goes beyond considering vulnerability/risk scenarios one-by-one, qualitatively or statically, to considering the relationship between the risk factors. This can provide a more thoughtful understanding of the scale of impacts involved and drive appropriate prioritization of security controls and responses. The dependency relationships are indicated by the directional arrows (in Figure 2), where the expressed dependencies describe a model for addressing IoT security risks.

The process of measuring the probability of things breaking down or dependencies is well understood in cyber economics

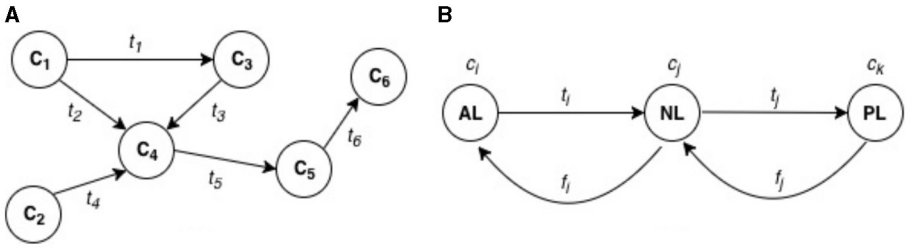


FIGURE 2
Dependency modeling for IoT risk assessment. **(A)** Dependency relationships among IoT components (C_1, C_2, C_3, C_4, C_5, C_6). The circles (C_1, C_2, C_3, etc.) represent different IoT components. The directional arrows (t_1, t_2, t_3, etc.) represent dependency flows between components. For example: t_1 is the dependency flow from component C_1 to component C_3. t_2 is the dependency flow from component C_1 to C_4. t_4 represents a dependency from C_2 to C_4. This structure shows how the functioning of one IoT component is dependent on the successful function of another connected component. **(B)** Layer-based dependencies in an IoT system. AL (Application Layer), Represents higher-level software components and services (e.g., analytics functions or cloud services); NL (Network Layer), Represents components such as communication switches or Programmable Logic Controllers (PLCs), through which data (t_1, f_1, etc.) is transmitted; PL (Perception Layer), Represents sensors or actuators, such as photoelectric sensors or conveyor belt switches, which interact with the physical world. The arrows in this part show how dependencies flow through these layers, with t_1 and f_1 representing different types of functional or data dependencies between the layers.

(Figure 3), and many papers have made an effort to calculate these numbers and provide ROI. Although some would argue that they are limited (Figure 4), but the evidence of such publication confirms that the lack of probabilistic data has not stopped either firms or researchers to make an effort. Hence, in this paper we try to relate similar efforts toward the assessment of IoT risk, by repeating similar thoughts throughout the paper.

To be impactful, risk assessment method needs to consider intrinsic capabilities as well as the more general characteristics of the IoT system which enable security risks. Capabilities can range from sensing, processing, actuating, interfacing, storage, and usage management. Characteristics can range from component heterogeneity, scale variability, connection temporality, low power retention, and intelligence generation/fusion.

This way, they can achieve the quantification of security-related dependencies that can help provide deeper and better security insights. Some of these insights include understanding how the impact of exploiting certain security vulnerability(ies) in an IoT infrastructure component or subsystem prevents it from delivering the relevant and required service(s), and how such affects the performance of other connected sub-systems that connect to, require data/service flows from, and rely on an affected target.

This can help in the development and adoption of effective security incident response and recovery (Laugé et al., 2015), as well as help reduce and manage the effects of IoT disruptions.

7 Cyber risk acceptance and transference—Response and recovery

The argument for using the dependency model to assess risk in IoT sub-systems is that we can also assess the impacts caused by failures that cascade through the system and understand the scale of such impact in relation to the fulfillment of operation objectives. Depending on the outcome of evaluating functional dependencies, after all possible states have been considered, often, there is a possibility of a "no-win" incidents, where each scenario leads to a risk that cannot be totally controlled or eliminated. The

$$\varphi(v) = \begin{cases} 1 & \rightarrow \text{connection configured} \\ 0 & \rightarrow \text{connection not configured} \end{cases} \quad (1)$$

$$fd_v = \sum_{u \epsilon T_v} (fd_u \times \varphi(v)) \quad (2)$$

where, T_v represents the subset of components reachable directly from v.

FIGURE 3
Connection configured.

next states would be risk acceptance and risk transference. In the following section, we give an overview of the steps involved in risk acceptance—which includes incident response, recovery (Van Kleek et al., 2018), and we end this section with a discussion of cyber insurance, which represents a method for risk transference.

7.1 Risk acceptance—Incident response and recovery

In this section, we provide insights on how companies can manage risk through their incident response and recovery. One form to describe risk acceptance is a state where adding additional defenses becomes too expensive within a certain dependency model. In such a state, it could be rational to accept that future attacks will happen. Then, an initial zero defense configuration is supported with a reactive defense that is activated when a vulnerability is exploited (Woods and Simpson, 2018). Incident response and recovery for IoT can follow similar approaches already common to digital and computing systems. Key phases of an incident response and recovery procedure for IoT systems include planning, detection, analysis and response formulation, containment, eradication, recovery, and post-incident activity. The diagram in Figure 5 (below) illustrates this process.

Companies can use the Planning phase or Incident Response (IR) Preparation, which involves activities that ensure IoT-user

$$P_{fd_v} = \frac{fd_v}{max(fd_v)} \quad (3)$$

FIGURE 4
Worst-case dependency impact.

FIGURE 5
The new emerging security incident response approach.

organizations are in a state of readiness for the prompt handling of incidents. Example activities include:

- Setting and training IoT incident response teams;
- Defining appropriate security response and escalation policies;
- Forensic evidence management in line with relevant security guidelines and practices;
- Awareness and response strategies to common security threats such as Denial of Service, Worms/Trojans, Phishing, web-based and web application attacks, insider threats, exploit kits, information leakage, and identity theft.

However, the scope and number of questions that need consideration and answers have only increased in planning for an effective response to IoT security incidents compared to traditional IT systems. For example, a self-driving vehicle relies on radar sensors to detect obstacles, which evidently can fail (Breza et al., 2018), resulting in a crash. This is a complex human-machine system relying on many different systems owned by a variety of enterprises. A good solution path would include viewing IoT incident response considering the mission process of IoT devices and system. This can support understanding of how malicious actors might exploit the normal infrastructure (device or system) functionality failures and impacts to hide malicious actions. Greater understanding can be achieved through ensuring that security experts responsible for securing the operations of IoT systems clearly understand the threat models that drive the systems (Russell and Van Duren, 2016). Security experts also need to be conscious and responsive to the dynamic states of the security threats to provide effective response actions.

Several conventional IR methodologies and frameworks can be adapted for IoT. While it may not be feasible to prevent all security compromises in IoT, effective threat response and management are needed. These must be built on well-structured and holistic incident response plans and procedures and on the respective dependency models assumed/used.

Companies can also use the Detection phase of IR, which emphasizes the importance of promptly recognizing the beginning of what is considered a "threat" in an IoT system for which critical decisions and actions are required. Since IoT relies on cloud-hosted infrastructures and often includes limited-functionality devices (from an events and log management perspective), it is necessary to include in the infrastructure monitoring design a capacity to capture instrumentation data directly from IoT devices, as well as from supporting cloud service providers. IoT devices use trusted credentials for exchanges, which, when compromised, can result in significant impacts across the system. As described above, only complex monitoring can provide the visibility necessary to spur timely decisions and responses. There is an increasingly significant role for computational intelligence in supporting risk assessment through identifying risk, capitalizing on opportunities, and gaining a deep understanding of a business through reports, dashboards, visualizations, and information analysis.

Traditional security information and event management (SIEM) systems, although powerful and well-advanced for standard networks, are unable to handle the complexities involved in IoT, where massive numbers of nodes and millions of data are involved. Hence, the need for newer, more tailored IoT-centric systems.

Instead, Companies can use the Analysis and Response formulation phase, which focuses on understanding the characteristics of security threats or incidents to learn the most suitable strategy or method for handling future incidents; again, traditional systems struggle, and IoT-specific digital forensic and incident response tools are necessary. In IoT, analysis of threats should consider both system-wide and component-specific perspectives. Using effective threat intelligence tools and processes that relate to IoT application sector is a good place to start, as threat indicators and protective patterns are often shared and made available on threat intelligence platforms.

From these, further analysis can be explored evaluating the scope of compromise, activities, timelines, and attacker identities related to certain breaches. However, recognition of the potential for attacks to employ anonymity and other anti-forensic capabilities characterized in the IoT domain is required. Since IoT systems are data-intensive, data compromise analysis with respect to confidentiality, integrity, and availability is also crucial. These mechanisms for assuring integrity and availability can be complemented with IoT devices and gateway forensic analysis to provide acceptable proof of the breach of IoT devices and systems.

Alternatively, companies can use the Containment phase, which aims to ensure prompt, interim resolution to a security incident by engaging in attempts to restrict further damage to the system. Typical actions in traditional IT systems may include disabling affected services, disconnecting or swapping out compromised devices and systems with new ones, revising access credential values such as passwords, disabling affected accounts or,

at worst, initiating a temporary shut-down. Some of these activities do not translate to incidents in IoT systems; here we list them as descriptive examples. The main task in this phase is for affected devices, services, or systems to be isolated from the operations IoT network as quickly as possible while allowing for forensic analysis of affected systems.

Companies can also use the Eradication phase, which leads from the containment phase, focuses on the long-term removal of threats, and ensures that the system is no longer vulnerable to the threat. Typical activities in this phase include policy updates and independent security audits. This can be achieved in IoT systems by evaluating whether existing security policies can sufficiently address any threats that have been identified; if not, security policy upgrades need to be adopted and implemented. For example, automated software/firmware updates and patching are challenging in today's IoT. It is necessary to devise and adopt policies and approaches for security patching that would provide the necessary security without disrupting operations and functionality. With reference to the need to support forensic analysis, it is desirable to track the activities of a malicious actor in a network. IoT can benefit from gateway devices that support the establishment of logical rules for automated isolation of compromised infrastructure based on monitored commands or traffic flow patterns without alerting an active attacker on the network (Craggs and Rashid, 2017). In this way, the attacker's actions and activities can be observed and studied to inform decisions for necessary security improvements.

Companies can use the Recovery phase to restore the system to normal working order. Typical actions may include restoring systems using backups, system re-configurations, or fresh installations. These must be considered for both cloud and on-premises infrastructure, and restoration must be initiated in a way that does not cause significant delays or disruptions to the normal operation of the IoT system.

Companies can use the Post-Incident Activity phase, which includes a combined process of drawing lessons from breaches and reporting these lessons in a structured way that helps to form capability for future occurrences. Typically, this should be conducted through reflective meetings that bring together senior executives and technical experts (Falco et al., 2019). In the reflective reviews, privacy checks, root cause analysis, and after-incident forensics can be performed in relation to the compromised system. Using root cause analysis, organizations can easily understand the failure of their security and determine how to strengthen the weaknesses as well as produce true assessments of what happened, how it happened, how well or poor the response went and why, and what a better response may look like in the future. Overall, lessons learned should be evaluated and amended as required, including the incident response plan, the network access control (NAC) plan, existing tools and resources to enhance security, deficiencies in cloud service providers and the on-premises incident response process.

IoT brings inherent cyber risks spanning multiple functional sectors with varied dependencies. Further, IoT systems often operate on platforms that cut across geographical boundaries for which appropriate cyber incident response and recovery plans and strategies are required. Collaborative Incident Response and Recovery (IR&R) utilizes shared threat intelligence and should evolve based on this intelligence. This is required since the security risk landscape is continually evolving, so an incident response plan which was appropriate yesterday might not be today; a plan that seems effective today could also be ineffective tomorrow. Effective IR&R should (1) be designed to fit the dependency model chosen to assess risk in the respective IoT environment or service, and (2) be characterized by continuous refinements of processes and procedures. This represents a move from a reactive response to the management of security incidents in a way that fosters cooperation through the exchange and sharing of incident management information among several distinct IoT-adopter organizations. Such an approach should enable both proactive and reactive capacities and enforce and assure trust and privacy among IoT infrastructures and cooperating organizations.

These findings represent a key insight that refers to a wide variety of enterprises, and it addresses a missing discussion of the impact of IoT cyber risk on liability and insurance risk ownership. The answer must be partially addressed by virtual reality cyber assessment (Furfaro et al., 2017) and cost and frequency analysis of cyber-attacks. Such analysis would complement building frameworks and methodologies for mitigating the impact of cyber risk and assessing cyber risk in IoT-connected products and services. This would resolve the previously discussed lack of standardized methods for measuring the cost and probabilities of cyber-attacks in IoT systems and the impact of such (IoT product, service or platform-related) cyber risk. The lack of empirical data to construct actuarial tables applies to cyber risk in general. Adding to this, the growth of IoT cyber risk markets in the finance and insurance sectors is impeded by the lack of empirical data to construct actuarial tables (Egan et al., 2019). We could also argue that actuarial tables are irrelevant in many emergent risk markets—for example, cyber insurance creates what is called "reliance"—that is, reliance that insurance companies take care of possible risks or financial risk depends not necessarily on actuarial tables, but rather on specific mechanisms such as how the markets price the potential hazards and price the consequences.

Nevertheless, the highly dynamic systems in these sectors make it difficult for businesses to formulate significant assumptions on the nature of risk, as even the possible knowledge of risks can further affect them. Despite the development of models related to the impact of cyber risk (Jalali et al., 2019; Evans, 2019), there is a lack of such models related to specific IoT verticals. Hence, banks and insurers cannot price IoT cyber risk with the same precision as in traditional insurance lines (Camillo, 2017).

8 Case study discussion on estimation and valuation of IoT cyber risk

While conducting this research, we used the case study and action research methods to apply our research findings in practice. Since this research was co-funded by Cisco Systems, one of the main benefits of this research was the access and engagement with their cyber risk management. We used their risk management tools as a platform to test, verify and advance our understanding of the role IoT is playing in their risk management operations. One of the first case study discoveries was related to risk transference and how companies are dealing with such unpredictable risks. Cyber risk insurance represents risk transference and is categorized as a

risk management operation. IoT technologies are becoming more prevalent, and we can observe cyber risks worldwide, increasingly impacting physical property and challenging present notions of accountability and liability.

Consequently, cyber insurance has often been investigated as a possible market-based solution to cyber security problems. For example, in dynamic systems, cyber insurance is meant to control financial risk and thus depends on how the markets price the possible hazards and the consequences. However, the cyber insurance market needs help in measuring and assessing risks and designing and managing cyber risks efficiently. Some of the major problems cyber insurers face is the lack of historical data on risks, a lack of claims data, the volatility of the rather immature IoT technology and markets and the increased scope for cyber security risks. From a broader perspective, governments and the insurance industry are far from a working public-private partnership for cyber insurance.

- To identify how a company can deal with such risk scenarios, we conducted action research with Cisco Systems. From our case study research, we identified that our model for risk assessment could be applied if we had the probabilistic data we do not have. Therefore, in our action research, we focused on the data strategy. We have worked with Cisco Systems for three years and developed a data strategy to deliver the probabilistic data needed for risk assessment. This data strategy was presented to the FAIR Institute webinars, and we gathered further feedback from other companies. The advantage of participating with the FAIR Institute was that we gained access to many different companies' specific cyber risk departments. In Figure 6, we include a snapshot of the simulation of the proposed goal-oriented approach. The original table is a much larger document, and the image we see in Figure 6 is just a small sample to demonstrate the process. What we can see in the demonstration is a unique code for each risk category (on the left side), where each risk category is allocated to a specific principle, and principles are categorized in areas of focus. Individual principles are allocated weights from 0 to 3, and the weight is determined by the risk exploitability of the vulnerabilities allocated to the specific principle. Applying the design to the previously described goal-oriented approach is necessary, which also operates as a decision three in this scenario.

In Figure 6, we can visualize the process of applying the proposed goal-oriented approach. The unique code is also a unique reference to a specific vulnerability that is found in the National Vulnerability Database (NVD), which are stored as JSON files. The unique code is included to resolve the product naming problem, which is one of the most difficult issues to solve in the new software bill of materials (SBOM) and the proposed integration with the vulnerability exploitability exchange (VEX). This work relates to the ongoing efforts of the Common Security Advisory Framework (CSAF) and the new Stakeholder-Specific Vulnerability Categorization (SSVC), which is an updated version of the Common Vulnerability Scoring System Calculator (CVSS). Still, it's based on a decision threes and qualitative data.

8.1 Advantages of SSVC's decision trees and qualitative data for prioritizing vulnerabilities

The Stakeholder-Specific Vulnerability Categorization (SSVC) applies decision trees and qualitative data, and offers several key advantages for prioritizing vulnerabilities in a goal-oriented approach to IoT cyber risk management. While traditional risk assessment methods often rely heavily on quantitative data, the inclusion of qualitative assessments through SSVC enhances flexibility, adaptability, and relevance to real-world IoT systems, where data may not always be complete or measurable in a purely quantitative form. Below are the primary advantages of SSVC in this context:

1. Tailored decision-making process

One of the strengths of SSVC's reliance on decision trees is that it enables the prioritization of vulnerabilities based on context-specific factors relevant to each organization's risk tolerance and operational environment. The decision tree methodology provides clear decision points, such as whether a vulnerability needs immediate patching or whether it can be delayed based on factors like:

- The potential impact on critical services,
- The presence of mitigations, or
- The likelihood of exploitation.

By guiding stakeholders through a structured series of questions, the decision tree helps ensure that the decision to prioritize or defer mitigation efforts aligns with the organization's overall goals and resource constraints. In goal-oriented approaches, this helps organizations avoid "one-size-fits-all" risk assessments and instead tailor their responses based on unique operational needs and priorities.

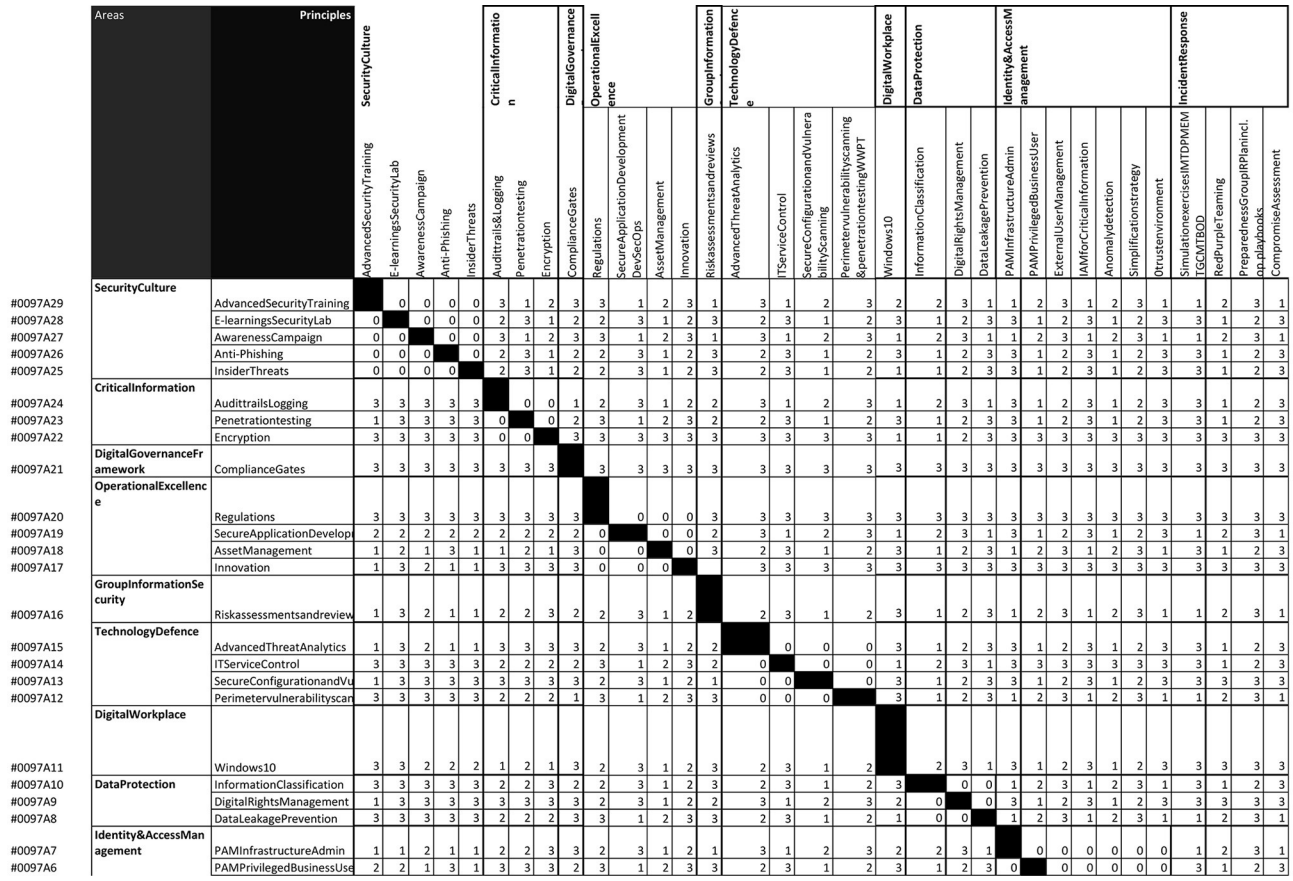
2. Handling of uncertain or incomplete data

In IoT environments, there are often scenarios where precise quantitative data about vulnerabilities, likelihoods, or impacts are unavailable. SSVC's use of qualitative data offers a practical solution for addressing these uncertainties. By enabling decision-makers to categorize risks using qualitative descriptors, such as high, medium, or low impact,the SSVC framework facilitates risk prioritization even when probabilistic data may be lacking or incomplete. This flexibility is particularly useful in dynamic IoT ecosystems, where new vulnerabilities may emerge faster than they can be quantified through traditional metrics.

For example, in a situation where a vulnerability is known to exist, but the exploitability is unclear due to a lack of historical data, SSVC allows stakeholders to make informed decisions based on qualitative assessments (e.g., whether the vulnerability is in a critical system or whether mitigations are already in place), rather than waiting for complete quantitative data.

3. Enhanced collaboration and communication

SSVC's decision tree structure simplifies the communication of risk decisions across multidisciplinary teams, including cybersecurity professionals, management, and other stakeholders. The step-by-step nature of the decision trees makes the reasoning behind prioritization decisions more transparent and accessible,



Areas	Principles	SecurityCulture					CriticalInformation			DigitalGovernance	OperationalExcellence					GroupInformation	TechnologyDefence				DigitalWorkplace	DataProtection			IdentityAccessManagement						IncidentResponse			
		AdvancedSecurityTraining	E-learningsSecurityLab	AwarenessCampaign	Anti-Phishing	InsiderThreats	AudittrailsLogging	Penetrationtesting	Encryption	ComplianceGates	Regulations	SecureApplicationDevelopment DevSecOps	AssetManagement	Innovation	Riskassessmentsandreviews	AdvancedThreatAnalytics	ITServiceControl	SecureConfigurationandVulnerabilityScanning	PerimetervulnerabilityscanningPenetrationtestingWWPT	Windows10	InformationClassification	DigitalRightsManagement	DataLeakagePrevention	PAMInfrastructureAdmin	PAMPrivilegedBusinessUser	ExternalUserManagement	IAMforCriticalInformation	Anomalydetection	Simplificationstrategy	Otrustenvironment	SimulationexercisesIMTDPMEMTGCMTBOD	RedPurpleTeaming	PreparednessGroupIRPlaninclplaybooks	CompromiseAssessment
#0097A29	SecurityCulture		0	0	0	0	3	1	2	3	3	1	2	3	1	3	1	2	3	2	2	3	1	1	2	3	1	2	3	1	1	2	3	1
#0097A28		0		0	0	0	2	3	1	2	2	3	1	2	3	2	3	1	2	3	1	2	3	3	1	2	3	1	2	3	3	1	2	3
#0097A27		0	0		0	0	3	1	2	3	3	1	2	3	1	3	1	2	3	1	2	3	1	1	2	3	1	2	3	1	1	2	3	1
#0097A26		0	0	0		0	2	3	1	2	2	3	1	2	3	2	3	1	2	3	1	2	3	3	1	2	3	1	2	3	3	1	2	3
#0097A25		0	0	0	0		2	3	1	2	2	3	1	2	3	2	3	1	2	1	1	2	3	3	1	2	3	1	2	3	3	1	2	3
#0097A24	CriticalInformation	3	3	3	3	3		0	0	1	2	3	1	2	2	3	1	2	3	1	2	3	1	3	1	2	3	1	2	3	3	1	2	3
#0097A23	AudittrailsLogging	1	3	3	3	3	0		0	2	3	1	2	3	2	2	3	1	2	3	1	2	3	3	1	2	3	1	2	3	3	1	2	3
#0097A22	Penetrationtesting	3	3	3	3	3	0	0		3	3	3	3	3	3	3	3	3	3	1	1	2	3	3	3	3	3	3	3	3	3	3	3	3
#0097A21	DigitalGovernanceFramework	3	3	3	3	3	3	3	3		3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
#0097A20	OperationalExcellence	3	3	3	3	3	3	3	3	3		0	0	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
#0097A19	Regulations	2	2	2	2	2	2	2	2	2	0		0	0	2	3	1	2	3	1	2	3	1	3	1	2	3	1	2	3	1	2	3	1
#0097A18	SecureApplicationDevelop	1	2	1	3	1	1	2	1	3	0	0		0	3	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	3	1	2	3
#0097A17	AssetManagement	1	3	2	1	1	3	3	3	3	0	0	0			3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
#0097A16	GroupInformationSecurity	1	3	2	1	1	2	2	3	2	2	3	1	2		2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	1	2	3	1
#0097A15	TechnologyDefence	1	3	2	1	1	3	3	3	3	2	3	1	2	2		0	0	0	3	1	2	3	3	1	2	3	1	2	3	3	1	2	3
#0097A14	AdvancedThreatAnalytics	3	3	3	3	3	2	2	2	2	3	1	2	3	2	0		0	0	1	2	3	1	3	3	3	3	3	3	3	3	1	2	3
#0097A13	ITServiceControl	1	3	3	3	3	3	3	3	3	2	3	1	2	1	0	0		0	3	1	2	3	3	1	2	3	1	2	3	3	3	3	3
#0097A12	SecureConfigurationandVu	3	3	3	3	3	2	2	2	1	3	1	2	3	3	0	0	0		3	1	2	3	1	2	3	1	2	3	1	1	2	3	1
#0097A11	DigitalWorkplace	3	3	2	2	2	1	2	1	3	2	3	1	2	3	2	3	1	2		2	3	1	3	1	2	3	1	2	3	3	3	3	3
#0097A10	DataProtection	3	3	3	3	3	2	2	3	2	2	3	1	2	3	2	3	1	2	3		0	0	1	2	3	1	2	3	1	3	1	2	3
#0097A9	DigitalRightsManagement	1	3	3	3	3	3	3	3	3	2	3	1	2	2	3	1	2	3	2	0		0	3	1	2	3	1	2	3	3	3	3	3
#0097A8	DataLeakagePrevention	3	3	3	3	3	2	2	2	3	3	1	2	3	3	2	3	1	2	1	0	0		1	2	3	1	2	3	1	1	2	3	1
#0097A7	Identity&AccessManagement	1	1	2	1	1	2	2	3	3	2	3	1	2	1	3	1	2	3	2	2	3	1		0	0	0	0	0	0	1	2	3	1
#0097A6	PAMPrivilegedBusinessUse	2	2	1	3	1	3	3	3	2	3	1	2	3	3	2	3	1	2	3	1	2	3	0		0	0	0	0	0	3	1	2	3

FIGURE 6
Simulation of the goal-oriented approach.

enabling better collaboration between technical and non-technical team members. In a goal-oriented approach, where aligning cybersecurity objectives with business and operational goals is crucial, the decision tree's clarity facilitates shared understanding and decision-making across different levels of the organization.

By providing clear rationales for prioritizing certain vulnerabilities over others, SSVC enhances the alignment between cybersecurity efforts and organizational goals, ensuring that resources are focused on the most critical vulnerabilities that pose the greatest threat to achieving those goals.

4. Rapid and adaptive response to emerging threats

Decision trees offer the advantage of enabling a more rapid and adaptive response to newly identified vulnerabilities. In fast-paced IoT environments, where new devices and technologies are frequently deployed, waiting for complete quantitative risk data may delay critical vulnerability mitigations. SSVC's decision trees provide an immediate framework for determining the severity of a vulnerability and the urgency of required action, allowing organizations to act quickly and adjust their strategies as new threats emerge.

For instance, if a new vulnerability in a widely used IoT device is discovered, the SSVC framework can quickly guide decision-makers through prioritization steps, such as assessing whether the vulnerability affects critical operations or whether there are feasible mitigations in place. This agility is crucial in dynamic IoT environments, where the rapid identification and prioritization of risks can prevent widespread system disruptions.

5. Alignment with existing risk management standards

SSVC's qualitative approach aligns well with existing cybersecurity standards, such as the **NIST Cybersecurity Framework** and **ISO/IEC 27001**, which also incorporate qualitative elements in their risk management processes. This makes SSVC compatible with widely used risk assessment methodologies, allowing organizations to integrate the SSVC decision tree approach into their broader cybersecurity management efforts seamlessly.

In a goal-oriented framework, this compatibility ensures that organizations can apply SSVC while still adhering to broader regulatory or compliance requirements, thus enhancing its practical application in both industry-standard and custom-tailored risk **management** strategies.

8.2 SSVC's in a goal-oriented approach

SSVC's reliance on decision trees and qualitative data offers significant advantages for prioritizing vulnerabilities in a goal-oriented approach. By allowing tailored decision-making, handling uncertainty, enhancing communication, and enabling

rapid response, SSVC helps organizations align their cybersecurity efforts with operational goals more effectively. Its flexibility and adaptability make it a valuable tool for IoT environments where risks are constantly evolving, and quantitative data may not always be immediately available. The integration of SSVC into the proposed goal-oriented model strengthens the model's ability to assess and mitigate IoT cyber risks in a comprehensive and practical manner.

8.3 Simulation of the goal-oriented approach

Figure 6 presents a critical simulation of the proposed goal-oriented approach to risk assessment, specifically focusing on the allocation of risk categories, principles, and their associated weightings. This table is an essential part of the research as it demonstrates how the proposed model can be applied in real-world settings for effective cyber risk assessment and mitigation in IoT environments. The following points elaborate on the significance and interpretation of Figure 6:

1. Categorization of risk principles

Figure 6 is structured to categorize risks based on specific principles that reflect different dimensions of IoT security. Each risk category is allocated a unique code, which corresponds to a specific vulnerability or risk scenario identified in IoT systems. These principles encompass a wide range of security concerns, from technical vulnerabilities (e.g., device compromise) to broader strategic risks (e.g., reputational damage from data breaches).

The inclusion of these principles allows for a comprehensive assessment that goes beyond individual technical vulnerabilities, offering a more holistic view of the organization's overall risk posture. This categorization enables organizations to prioritize risks based on their relevance and severity in different IoT environments, such as smart cities, industrial IoT, or healthcare.

2. Weighting system

Each risk category is assigned a weight ranging from 0 to 3, depending on the likelihood and impact of the associated vulnerability or threat. The weighting is determined by evaluating the **exploitability** of the vulnerability and its potential to cause cascading failures across interconnected IoT devices and systems.

- **Weight 0** indicates minimal risk or low likelihood of exploitation.
- **Weight 1** indicates a moderate level of risk that requires monitoring but may not necessitate immediate intervention.
- **Weight 2** reflects a higher probability of exploitation with potentially significant consequences, warranting proactive risk mitigation.
- **Weight 3** indicates a critical risk that requires immediate action due to its potential to cause widespread disruptions or severe financial and operational damage.

The weighting system allows organizations to focus resources on the most pressing risks, enabling efficient allocation of security budgets and efforts to mitigate IoT-related cyber threats.

Definition of Risk Exploitability and Weight Determination in Figure 6.

Risk exploitability refers to the likelihood that a vulnerability or risk in an IoT system can be successfully exploited by a threat actor. In the context of IoT cybersecurity, exploitability is a crucial factor because not all identified vulnerabilities carry the same probability of being exploited. For instance, certain vulnerabilities may require advanced skills, specific conditions, or access to specific network segments to be exploited, while others can be easily exploited with widely available tools.

In this work, risk exploitability is determined based on several key factors:

1. **Access complexity**: the ease or difficulty with which a threat actor can access the vulnerable component. This includes whether the vulnerability is exposed to the internet or resides behind secure layers like firewalls.
2. **Required privileges**: the level of privileges or access control required to exploit the vulnerability. For example, a vulnerability that requires administrative privileges is typically harder to exploit than one that can be exploited by a standard user.
3. **Publicly available exploits**: whether or not there are existing tools or scripts available to exploit the vulnerability. If an exploit is readily available and easy to use, the risk exploitability is higher.
4. **Attack vector**: the means through which the attack is executed. For instance, vulnerabilities that can be exploited remotely over a network generally have higher exploitability than those requiring physical access to the device.
5. **Patch availability and mitigation**: whether there are patches or mitigation strategies in place. A vulnerability with no available patch or limited mitigation options is more exploitable than one for which a patch exists and has been widely applied.

Further detail on the weight determination in Figure 6.

The weights assigned to vulnerabilities in Figure 6 are based on an estimation of risk exploitability. Each risk category is evaluated using the factors mentioned above, and a numerical weight (ranging from 0 to 3) is assigned to represent the likelihood of exploitation. The weights correspond to the following levels of exploitability:

- **Weight 0 (low exploitability)**: this weight is assigned to vulnerabilities that have extremely low risk of being exploited. This may include vulnerabilities that require highly specialized skills, physical access to the device, or complex conditions that are unlikely to occur. For example, vulnerabilities that exist only in closed networks or require multiple layers of compromise to access would receive this weighting.
- **Weight 1 (moderate exploitability)**: vulnerabilities with moderate risk of being exploited are assigned this weight. These might require some level of specialized knowledge or access but are feasible for an attacker to exploit under the right conditions. An example would be a vulnerability that requires privilege escalation within a network but does not have readily available public exploits.

- **Weight 2 (high exploitability)**: this weight is assigned to vulnerabilities that are relatively easy to exploit and are likely to be targeted by attackers. These may involve publicly available exploits, easily accessible devices, or remote attack vectors. For instance, a vulnerability in an IoT device exposed to the internet without sufficient patching or protective measures would typically fall into this category.
- **Weight 3 (critical exploitability)**: vulnerabilities that are extremely easy to exploit and carry severe consequences are assigned the highest weight. These include vulnerabilities for which widely used exploit kits are available, or where a remote attacker can easily gain control over a device or network segment. An example would be an unpatched zero-day vulnerability in an IoT system that is exposed to the public internet.

Example of weight assignment in Figure 6.

For example, in Figure 6, if a particular IoT vulnerability exists in a publicly accessible smart device that requires minimal technical knowledge to exploit and has a widely available exploit tool, it would be assigned a weight of **3 (critical exploitability)**. In contrast, a vulnerability in a back-end server that requires significant expertise and internal network access might be assigned a weight of **1 (moderate exploitability)**.

The weighting is also influenced by the **dependency relationships** in the IoT system. If a vulnerability in one device can cause a cascading effect across multiple interconnected devices, its exploitability may be weighted higher due to the broader system-wide impact. Conversely, isolated vulnerabilities with limited impact are weighted lower.

Integration with AI/ML models.

The exploitability weights are incorporated into the proposed AI/ML-based risk assessment framework to dynamically adjust the risk scores of IoT components. The AI model processes these weights along with other input data (e.g., network traffic patterns, device telemetry) to produce real-time risk assessments. The use of exploitability weights ensures that the model prioritizes the most severe and actionable risks, helping organizations focus their mitigation efforts on vulnerabilities that pose the highest threat.

By defining risk exploitability and assigning corresponding weights, this work introduces a structured and transparent method for prioritizing vulnerabilities within IoT systems. This approach ensures that both easily exploitable and high-impact vulnerabilities receive the attention they warrant, while lower-risk issues are deprioritized. This allows for more efficient allocation of resources in mitigating IoT cyber risks, enhancing the overall security posture of IoT deployments.

3. Vulnerability exploitability and decision trees

Figure 6 links each risk category to the concept of **vulnerability exploitability**. By incorporating the **Stakeholder-Specific Vulnerability Categorization (SSVC)** decision tree methodology, the table provides a dynamic assessment of risk scenarios. SSVC helps assess the decision points around patching vulnerabilities or applying other mitigation measures based on the risk's exploitability and the organization's tolerance for risk.

This approach allows organizations to decide whether to accept, mitigate, or transfer a specific risk. For instance, for highly exploitable vulnerabilities that pose significant risk (assigned a weight of 3), the organization might opt for immediate patching or enhanced monitoring. In contrast, less severe vulnerabilities with a lower weight might be mitigated over time or transferred via cyber insurance.

4. Real-world application of the goal-oriented approach

Figure 6 demonstrates the practical applicability of the goal-oriented approach by simulating real-world scenarios where organizations need to assess and prioritize IoT-related risks. For example, in industrial IoT (IIoT) environments, the risk of a compromised sensor leading to downtime in a production line would be assigned a high weight due to the potential cascading impact on production processes. Similarly, in smart cities, the failure of IoT-connected traffic control systems could lead to significant public safety risks, requiring immediate mitigation strategies.

This simulation shows how the proposed framework can be applied across different domains and provides a clear roadmap for decision-makers to follow when assessing IoT risks. It enables them to make informed choices about where to allocate resources, how to prioritize risks, and which mitigation strategies (e.g., risk acceptance, transference, or mitigation) to adopt.

5. Alignment with global standards

The principles and weightings in Figure 6 align with widely accepted cybersecurity frameworks, such as **ISO/IEC 27001** and **NIST Cybersecurity Framework**, making the table highly adaptable to different organizational contexts. The integration of global standards ensures that the approach is applicable not only to Cisco's operational environment but also to a wide range of industries and sectors, from healthcare to manufacturing and beyond.

6. Future refinements

Figure 6 provides a snapshot of the current state of the proposed goal-oriented approach, but it also points to potential areas for future refinement. For example, as new IoT vulnerabilities emerge or regulatory environments evolve, the weightings and principles in Figure 6 can be updated to reflect the latest threat landscape. The flexibility of this framework allows it to remain relevant in the face of rapid technological change, ensuring that it can accommodate new developments in IoT security.

Figure 6 illustrates the practical applicability and flexibility of the goal-oriented approach for IoT risk assessment. By categorizing risks, applying weightings based on vulnerability exploitability, and integrating decision trees, this table offers a structured and actionable framework for organizations to assess and prioritize cyber risks in their IoT ecosystems. The alignment with global standards and the potential for future refinements ensure that the approach remains adaptable and generalizable to a wide range of operational contexts.

This case study brought forward the limitations of current exchange mechanisms on vulnerability data, with the main concern being around the fact that sharing exploitability data on vulnerabilities that have not been patched, exposes the risk of this data being intersected by hackers, enabling them to use exploits in real time before cybersecurity experts had sufficient time to patch the vulnerability. This is the main concern in terms of cyber risk, and this concern has been in circulation since 1990s. VEX is the latest attempt to resolve this long-term issue in cyber risk assessment of third-party risk.

8.4 CSAF/VEX and cyber insurance

However, comparing our arguments of targeted data strategy for risk assessment, with the current model of cyber insurance works as a risk mitigation tool and covers the costs of losses caused by human malicious activity or natural disasters. In this context, many of the problems in the banking and financial sector and their failures of the past decade can be directly tied to model failure or overly optimistic judgments in the setting of assumptions or the parameterization of a model. Now, a new public policy has emerged in which insurance companies act as clearing houses for information, integrate different security services and provide guidance on appropriate security investments to businesses seeking liability coverage (Allodi and Massacci, 2017). For example, new and traditional insurers can outsource important parts of the forensic investigation to different consultancies such as software or networking companies. However, recent research shows that this view of cyber insurance as a delegated policy tool has limitations in producing the anticipated coordination benefits and indeed may erode the aggregate level of security investment undertaken by targets in different insurance markets (Allodi and Massacci, 2017). These limitations are reflective of the previously discussed issue that insurance markets are lacking empirical data to construct actuarial tables. Thus, resulting with banks and insurers being unable to price IoT cyber risk with the same precision as in traditional insurance lines. While new and recent quantitative models partially address this issue, it may still be some time before these new approaches are widely adapted in the banking and cyber insurance sectors.

It should be recognized that IoT represents a huge opportunity for insurers to harness and understand cyber risks. IoT can thus represent a part of the solution to improved coverage and liability of non-tangible digital assets and to the dynamic nature of cyber-attacks. IoT can provide a part of the response to the general agreement that there is not enough data to understand the risks and reduce resource allocation problems arising from incomplete information regarding parties' actions (e.g., moral hazard) and characteristics (e.g., adverse selection). However, the analysis and correlation of large IoT data sources and new digital forensics and methods might sometimes be insufficient. For example, even though algorithms used to calculate cyber-risk metrics can analyze and correlate vast amounts of data, the methodologies that inform actuarial models may still struggle to make sense of and integrate the real-time information available from IoT devices.

Over-reliance on modeling in cyber insurance can also conceal difficult-to-detect processes, such as in the "normalization of deviance" case. The normalization of deviance defines the processes that socially organize and systematically reproduce mistakes related to complex technological solutions. In this context, IoT can help by making use of data to increase transparency and predictability of such processes, understand the limitations of computational modeling and techniques and improve the assumptions that these models are based on. The constant inspection of granular IoT data and the possibility of sharing aggregates of IoT data and increasing transparency between parties can help insurers and re-insurers understand strict liability and its sharing across complex ecosystems. Parties can collaborate to prevent risks from cascading and to investigate possible "black swan" events (an event that is unprecedented and unpredicted) in relation to the use of digital devices, which are likely to increase in number, at least in the short term. Formal methods for trustworthiness assessment may then help inform insurance models for complex IoT ecosystems. Such developments would temper the proliferation of false beliefs due to over-reliance on the "accuracy" of the outputs from computing models, which can lend an apparent objectivity to the results that can then justify inappropriate actions and policies.

From a risk management point of view, one important question is: what architectural improvements of a company's IT data system might increase resilience to cyber risk? We tend to think of cyber security as pertaining to IT companies, but digitalization is currently extending well beyond the existing IT systems to manufacturing floors and other production activities that only a few people normally associate with IT data strategy. Thus, the boundaries between IT systems and operational activities, such as manufacturing, may not be obvious. Then, data processing is mobile and is constrained by the environment where the system operates. For example, when complex systems interact, it is very difficult to predict the system's behavior and, in particular, the failure modes in operational conditions because of the emergent nature and the created feedback loops. This represents a particular challenge as, despite new investments in IoT and broad concerns with cyber risks, the manufacturing industry is still fragmented in its approach to managing cyber-related risks and having the organizational ownership to do so effectively (Van Wieren et al., 2016).

More general risks pertain to the vulnerability that IoT solutions currently have in relation to cyber-attacks and the capability of such solutions to establish and maintain different sorts of rights, such as the right to privacy. The relatively recent DDoS attacks that exploited simple, but poorly secured IoT end devices, such as baby monitors with immutable default passwords, show that: (a). the model of low-cost, low-security IoT solutions is not sustainable, and that (b). organizations and individuals need to protect themselves through collaborations, increased transparency, re-drawing of the current accountability and liability domains, and so forth. However, the mechanisms needed to implement these aspects need to work in a globalized context and across jurisdictions.

From a public policy point of view, insurers have become "de facto regulators" by establishing a minimum-security level to gain cyber coverage. This argument emerges from research that links security controls and cyber insurance proposal forms. In this context, IoT can help shape public policies that are beneficial for the insurance sector and the society at large. For example, one important opportunity is represented by businesses using IoT to demonstrate their compliance with both national and international industry standards as well as internal policies. The challenges facing organizations in standards compliance for IoT systems are significant (Christensen et al., 2019).

However, insurers can design dynamic insurance policies that would not only reflect the changes in behavior and characteristics of businesses and the contexts in which they operate but will also allow the creation of insured ecosystems where dynamic mechanisms such as double rewarding mechanisms and adaptive incentives can be operationalized. In such ecosystems, network-specific risks

could be transferred between businesses and insurers (or re-insurers) in near real time, e.g., by using smart contracts. However, there are important limitations here as these systems operate in environments that are too complex to manage, cannot be rationally understood and pose specific moral questions such as those around privacy and data protection. The difficulty is that each of these aspects helps the system to evolve but it can also change the a priori allocation of risks. Nevertheless, dynamic risk assessment and dynamic insurance policies can improve some of the current challenges in cyber risk mentioned in this paper and can represent opportunities to improve the existing regulation, public policies and government interventions in the cyber insurance market.

Current developments in IoT ecosystems allow innovative ways to design cyber insurance services that would utilize IoT data to:

- Design of a tailored data strategy for IoT and cyber risk assessment;
- Mitigate risk management and facilitate new developments in this area, such as risk engineering;
- Increase transparency and predictability of the cyber insurance processes, including near real-time evidence-based explanations meant to increase trust and reduce risks;
- Increase the flexibility and adaptability of the current business environments, including the correlation of multi-model information such as risk, anomaly scores and liability;
- Enable co-evolution of systems, where learning and knowledge are distributed between the insurance company and the insured parties toward a still more efficient allocation of risk and responsibility, and
- Investigate the use of Smart Contracts to manage cyber risks within the insured environment.

The use of Smart Contracts raises one critical question on how empirical data can be collected and used with the dependency model to provide quantitative assessments. More comprehensive and systematic understanding of this question will arise when AI/ML technologies are migrated to the periphery of the internet and into local IoT networks. By integrating AI/ML in the dependency risk analytics, we can anticipate that real time intelligence data would enable dependency systems to recover and become more robust. AI/ML in the dependency risk analytics would also enable an understanding how and when compromises happen and enable systems to adapt and continue to operate safely and securely when they have been compromised.

8.5 Data sources for gathering probabilistic information in the proposed data strategy

Given the complexity and dynamic nature of IoT systems, the data sources included in the data strategy are drawn from diverse domains to ensure robust probabilistic risk assessments. The data strategy integrates real-time and historical data from multiple layers of IoT infrastructure, allowing for more accurate predictions and risk estimations. The key data sources are outlined below:

a. **Network traffic data**: one of the primary data sources is real-time network traffic data generated by IoT devices and networks. This includes data on the types, frequency, and volume of communications between IoT devices, servers, and external systems. Analyzing network traffic enables the identification of anomalies, such as unusual patterns of data transmission, which could indicate cyber threats like botnet activity, distributed denial-of-service (DDoS) attacks, or data exfiltration. Tools such as **intrusion detection systems (IDS)** and **network monitoring platforms** provide raw traffic data, which is processed to extract probabilistic insights on attack likelihood and impact.
b. **Device telemetry data**: telemetry data from IoT devices includes metrics related to device health, performance, and operational status. This data is crucial for understanding the normal operational baseline of IoT devices and detecting deviations that could signal a cyber-attack or device malfunction. For example, abnormal energy consumption or processing delays could indicate that a device is compromised. Telemetry data is gathered through **device management platforms** and **cloud-based IoT hubs** that aggregate information from multiple devices in real-time.
c. **Incident logs and historical attack data**: historical incident logs from security breaches, cyber-attacks, and device failures serve as a valuable source of probabilistic information. These logs provide insights into attack vectors, timelines, and vulnerabilities exploited in past incidents. By examining patterns in historical data, the proposed model can estimate the likelihood of future attacks. Data sources such as **Security Information and Event Management (SIEM) systems**, **firewall logs**, and **threat intelligence platforms** are critical for gathering and analyzing this historical information.
d. **Vulnerability databases**: publicly available vulnerability databases, such as the **National Vulnerability Database (NVD)** and the **Common Vulnerability Scoring System (CVSS)**, provide critical data on known vulnerabilities in IoT devices, software, and protocols. These databases are constantly updated with information on newly discovered vulnerabilities, enabling organizations to assess the likelihood of exploitation based on the severity and type of vulnerability. These data sources are used to quantify the risk of unpatched vulnerabilities being exploited in a probabilistic framework.
e. **Threat intelligence feeds**: external threat intelligence feeds, such as those provided by **commercial security vendors** or open-source platforms, offer real-time information on emerging cyber threats, attack techniques, and indicators of compromise (IoCs). These feeds are crucial for staying updated on new attack patterns targeting IoT ecosystems. Integrating threat intelligence feeds allows the model to dynamically adjust its risk estimates based on real-time threat levels. Sources include **MITER ATT&CK**, **FireEye**, **Palo Alto Networks**, and **IBM X-Force**.
f. **IoT-specific sensor data**: in environments where IoT devices are deeply integrated with physical systems, such as smart cities, industrial automation, and healthcare, sensor data plays a key role in identifying risk scenarios. For example, sensor data from smart meters, connected vehicles, or industrial equipment can indicate when devices are behaving

abnormally, allowing for early detection of potential threats. **SCADA systems** and **IoT platforms** typically aggregate this data, which can then be used to estimate the likelihood of equipment failure or cyber-physical attacks.

g. **Third-party security audits and compliance reports**: organizations often conduct security audits and assessments of their IoT infrastructure to ensure compliance with industry standards such as **ISO/IEC 27001** or **NIST Cybersecurity Framework**. These audits provide valuable data on system weaknesses, compliance gaps, and potential threats. The results of these audits are included in the probabilistic model to help determine the organization's overall cyber risk posture and identify areas where additional mitigation measures are necessary.

h. **Cyber insurance claims data**: data from cyber insurance claims offers a unique perspective on the financial impact and frequency of cyber incidents. Claims data can provide insights into the types of attacks that lead to significant financial losses and the effectiveness of risk transfer mechanisms, such as insurance. This data can be aggregated from **insurance companies**, **brokers**, and **industry reports**, and can help calibrate the financial risk models in the proposed strategy.

8.6 Combining data sources for enhanced probabilistic assessment

The proposed data strategy leverages these multiple data sources to create a comprehensive dataset for probabilistic analysis. The data is processed using **machine learning algorithms** and **statistical models** to estimate the likelihood of various cyber threats and their potential impact. By integrating real-time data with historical trends and external threat intelligence, the model can dynamically adjust risk estimates and provide a more accurate and proactive assessment of IoT cyber risks.

This approach ensures that organizations can move beyond static, qualitative assessments and rely on data-driven, probabilistic insights to inform their IoT security strategies. The inclusion of diverse data sources also makes the model adaptable to different IoT environments and threat landscapes.

8.7 Adoption and impact of VEX on third-party cyber risk assessment

8.7.1 Current level of VEX adoption in the cybersecurity community

The **Vulnerability Exploitability eXchange (VEX)** has emerged as a relatively new but increasingly important tool in the cybersecurity community for improving the precision of vulnerability management and third-party risk assessments. Developed in response to the long-standing challenge of assessing the exploitability of known vulnerabilities in real-time, VEX is being gradually adopted, especially in industries where supply chain security and third-party risk are critical.

As of the time of writing, VEX adoption is still in its early stages but gaining traction, particularly in the following areas:

1. **Adoption in software supply chain security**: with growing concerns over supply chain vulnerabilities, VEX is being increasingly integrated into **Software Bill of Materials (SBOM)** frameworks to provide more granular and timely information about which vulnerabilities in a software component are exploitable. The U.S. **National Telecommunications and Information Administration (NTIA)** and **National Institute of Standards and Technology (NIST)** have both recognized the importance of VEX in their cybersecurity guidance, and its use is being advocated in sectors such as healthcare, critical infrastructure, and defense, where software supply chain risks are particularly high.
2. **Industry adoption**: several major vendors and cybersecurity providers, including those in cloud services and IT management, are beginning to incorporate VEX profiles into their vulnerability management tools. For example, leading providers of vulnerability assessment platforms and risk management solutions are adding support for VEX to improve the precision of vulnerability prioritization, particularly when assessing the security of third-party software and services.
3. **Regulatory push for adoption**: the inclusion of VEX in key U.S. government initiatives, such as **Executive Order 14028** on improving national cybersecurity, is driving broader adoption across critical industries. The Executive Order calls for improved transparency in software components through SBOMs, with VEX providing essential details on the real-world exploitability of vulnerabilities. This regulatory push is influencing sectors such as energy, finance, and telecommunications to adopt VEX as part of their vulnerability management and compliance efforts.

8.7.2 Assessment of VEX's impact on improving third-party cyber risk assessment

Although VEX is relatively new, initial assessments of its impact suggest that it has the potential to significantly improve the way third-party cyber risks are assessed and managed. Some of the key benefits and emerging impacts of VEX on third-party risk assessments are as follows:

1. **Precision in vulnerability prioritization**: one of the primary advantages of VEX is that it allows organizations to focus on vulnerabilities that are truly exploitable, rather than wasting resources on vulnerabilities that may not pose a real threat. In third-party risk assessments, this added precision helps organizations more effectively evaluate the security posture of their vendors and partners by identifying which vulnerabilities in third-party software are exploitable within their operational environment. This shift reduces false positives and minimizes the burden of patching non-critical vulnerabilities.
2. **Reduction of patch fatigue**: third-party vendors often release patches for vulnerabilities that may not be exploitable in all environments. With VEX, organizations can more effectively prioritize which patches to apply based on actual exploitability data, reducing "patch fatigue" among IT and security teams. This has been especially impactful in environments with

extensive vendor relationships and dependencies, such as **cloud computing** and **SaaS providers**, where constant updates and patches can be overwhelming.

3. **Improved supply chain risk management**: VEX improves transparency across the software supply chain by providing explicit, machine-readable information about whether a vulnerability in a software component is exploitable. This enhanced visibility allows organizations to better manage risks across their third-party ecosystem, which is crucial for mitigating supply chain attacks such as those seen in incidents like **SolarWinds** or **Log4j**. Initial industry feedback indicates that organizations using VEX-enabled SBOMs can more effectively respond to vulnerability disclosures and reduce their exposure to third-party risks.
4. **Integration with cyber insurance models**: another emerging impact of VEX is its potential role in cyber insurance underwriting. By providing more precise data on the exploitability of vulnerabilities in third-party software, VEX enables insurance providers to better assess the cyber risk posture of insured parties. This could lead to more accurate pricing of cyber insurance policies and incentivise better vulnerability management practices across the supply chain.
5. **Enhanced regulatory compliance**: VEX's machine-readable format aligns well with the increasing demands for transparency and accountability in cybersecurity regulations. In industries where compliance with security standards is essential (e.g., healthcare, financial services), VEX can help organizations demonstrate that they are addressing truly exploitable vulnerabilities, thereby enhancing compliance with frameworks like **NIST 800-53** or **ISO/IEC 27001**. This impact is particularly important in the context of third-party risk management, where regulatory bodies are increasingly requiring organizations to take greater responsibility for the security of their entire supply chain.

8.7.3 Challenges to VEX adoption and its future prospects

While VEX shows great promise, its adoption is still facing several challenges:

- **Standardization and Interoperability**: although VEX is being promoted as a standard, different vendors may interpret or implement it differently, leading to issues with interoperability between tools and platforms. Efforts are underway to establish more unified standards and guidelines to streamline VEX's use across the industry.
- **Education and awareness**: many organizations are still unfamiliar with VEX and its benefits. As with any new standard, significant efforts are required to educate both vendors and users on how to implement and leverage VEX for more effective vulnerability management.

Nevertheless, with the continued regulatory push for software transparency, the increasing complexity of supply chain attacks, and the growing emphasis on third-party risk management, VEX is likely to see broader adoption in the coming years. As more organizations incorporate VEX into their SBOMs and vulnerability management processes, its impact on improving third-party cyber risk assessments will become more evident, contributing to a more resilient cybersecurity ecosystem.

9 Discussion

9.1 Generalization of the proposed model to real-world scenarios

While the BoT-IoT dataset provides a valuable basis for developing and testing the proposed model for IoT cyber risk assessment, it is essential to acknowledge that the model is designed to be generalisable to a wide range of real-world IoT environments. The challenges posed by the BoT-IoT dataset, such as botnet attacks, DDoS scenarios, and other cyber threats, reflect a subset of the broader set of cyber risks faced by IoT systems. However, the proposed model is not limited to the specific characteristics of this dataset and can be applied to other real-world scenarios in various IoT ecosystems.

The key features of the model that enable its generalization include:

a. **Dependency modeling**: the use of dependency modeling in the proposed approach is highly flexible and can accommodate different types of IoT systems, from smart homes to industrial IoT (IIoT) environments. By focusing on the interactions and interdependencies between IoT components, such as devices, networks, and data flows,the model can be adapted to capture cyber risks in complex, real-world systems where threats arise from diverse sources. This is particularly important in real-world deployments where different vendors, protocols, and device architectures coexist, creating unique vulnerabilities.
b. **Scalability to heterogeneous IoT environments**: IoT systems in real-world scenarios often involve heterogeneous devices with varying levels of security and functionality. The proposed model, by abstracting key risk factors such as network topology, communication protocols, and device types, is well-suited for application in environments where these elements differ significantly. For example, in smart city infrastructure, the same dependency-based risk assessment methodology can be used to assess risks in traffic management systems, connected energy grids, or public safety networks, despite the differences in the nature of devices and data flows involved.
c. **Inclusion of multiple attack vectors**: the model is adaptable to multiple attack vectors, beyond the botnet attacks simulated in the BoT-IoT dataset. In real-world applications, IoT systems are susceptible to a wide range of attacks, such as malware infections, ransomware, zero-day vulnerabilities, and data breaches. The proposed model's flexible risk estimation framework can be extended to incorporate new attack vectors as they emerge, ensuring that it remains relevant in the ever-evolving threat landscape.
d. **Applicability to different IoT domains**: although this study focused on a dataset tailored to a specific subset of IoT risks, the model can be applied to other critical domains such as healthcare, industrial automation, and connected

transportation. For instance, in healthcare IoT, where safety and data integrity are paramount, the same risk estimation principles can be applied to assess the cyber risks posed by compromised medical devices or the failure of patient-monitoring systems. Similarly, in IIoT environments, the model can be adapted to assess risks in the context of supply chain disruptions or physical damage caused by cyber-physical system failures.

e. **Adaptability to emerging IoT cybersecurity standards**: the model's framework can also be integrated with evolving IoT cybersecurity standards and regulatory frameworks. For example, the NIST Cybersecurity Framework for IoT and ISO/IEC 27001 standards provide guidelines that can be mapped onto the proposed model's structure, ensuring that it remains aligned with industry best practices and can be easily adopted by organizations seeking compliance with these standards.

9.1.1 Real-world application examples

To illustrate the potential for generalization, consider the following real-world examples where the model could be applied:

- **Smart cities**: the proposed model could assess the risks in smart traffic systems, where compromised IoT devices like traffic lights or surveillance cameras could lead to large-scale disruptions.
- **Healthcare IoT**: In a hospital setting, the model could help assess the risk of data breaches in IoT-connected medical devices, such as insulin pumps or heart monitors, which could have serious implications for patient safety.
- **Industrial IoT**: The model could be used in a factory setting to assess risks to connected machinery, where a failure in one system could cascade through others, disrupting the entire production line.

In these cases, the dependency-based risk assessment and mitigation strategies proposed in this model would be applicable even when faced with varying device types, communication protocols, and risk profiles.

While the BoT-IoT dataset served as a valuable starting point for evaluating the model's performance, the model is inherently designed to be adaptable to real-world IoT environments that extend beyond this dataset. Its flexibility, scalability, and ability to accommodate new attack vectors make it highly generalisable across a variety of sectors and use cases. Future work will focus on further testing and refinement of the model in live IoT environments to validate its effectiveness in mitigating cyber risks across different domains.

9.2 Generalizability of findings on IoT and risk transference

While this research benefited from substantial input and access to Cisco's cyber risk management environment, the findings on IoT cyber risks and risk transference are designed to be generalizable to a wide range of organizations beyond Cisco. Several factors support this generalizability:

a. **Common IoT risk factors**: the IoT-specific risks identified in this research, such as interoperability challenges, cascading failures, and vulnerabilities in connected devices, are common across many industries and sectors. These risks are not unique to Cisco's operational environment but reflect broader trends observed in IoT ecosystems worldwide, such as in healthcare, industrial automation, and smart cities. Therefore, the risk transference strategies proposed in this research can be applied to any organization facing similar challenges in managing interconnected IoT devices.

b. **Industry-agnostic risk transference strategies**: the concept of risk transference, particularly through mechanisms like **cyber insurance**, is not exclusive to Cisco's environment. Risk transference frameworks, such as the ones discussed in this study, apply universally to organizations that seek to mitigate the financial and operational risks posed by IoT-related cyber threats. For instance, cyber insurance policies, third-party liability agreements, and outsourcing of security functions are strategies used across multiple industries to shift risk exposure. As such, the recommendations made in this research can be adopted by a variety of organizations seeking to develop robust IoT risk management strategies.

c. **Framework applicability across diverse IoT environments**: the dependency modeling approach used in this research is flexible and adaptable, making it applicable to different types of IoT deployments and architectures beyond Cisco. By focusing on interdependencies between IoT devices, data flows, and cyber-physical systems, this model can be tailored to various operational environments, such as connected manufacturing lines, smart healthcare systems, and autonomous vehicle networks. The IoT risks and mitigation strategies discussed in this research therefore extend well beyond Cisco's specific use case and are relevant for organizations with similar IoT-driven infrastructures.

d. **Global cybersecurity standards and practices**: the findings of this research are grounded in widely accepted cybersecurity standards, such as the **NIST Cybersecurity Framework** and **ISO/IEC 27001**, which are globally applicable and not specific to Cisco's internal practices. These standards promote best practices in cyber risk management and can be adapted by organizations of all sizes and sectors. The alignment of this study's findings with these international frameworks further reinforces the generalisability of the results across different organizational contexts.

e. **Broader input from multiple experts**: although Cisco provided valuable insights, the research also incorporated feedback from a variety of cybersecurity experts, representing different specializations beyond Cisco's operational environment. This helped ensure that the findings, particularly those related to risk transference and IoT cyber risks, were not limited by the perspective of a single organization. The collaboration with experts in IoT security, network vulnerabilities, and cyber risk frameworks has made the findings more applicable to a broader range of organizations.

The findings of this research are designed to be applicable to organizations across various industries and sectors. The identified IoT risks, dependency modeling, and risk transference strategies reflect global trends and are supported by widely accepted cybersecurity standards, making them highly relevant to organizations seeking to mitigate IoT risks in diverse operational environments. Future research could explore additional case studies in different sectors to further validate the generalisability of these findings.

9.3 Ensuring explainability and transparency in AI/ML for dependency risk analysis

The integration of AI/ML in dependency risk analysis offers significant advantages, particularly in identifying complex relationships and patterns that may not be apparent through traditional risk assessment methods. However, one of the key challenges associated with AI/ML in cybersecurity, and specifically in IoT dependency risk analysis, is ensuring that the decision-making process remains explainable and transparent. Stakeholders, including cybersecurity professionals and decision-makers, must be able to understand how AI/ML systems arrive at their conclusions, especially in high-stakes environments like IoT, where decisions may affect safety and critical operations.

To address these challenges, several strategies and best practices can be implemented to improve explainability and transparency:

1. Use of explainable AI (XAI) techniques

Explainable AI (XAI) is an emerging field that focuses on making AI and ML models more interpretable without sacrificing performance. XAI techniques ensure that decisions made by AI models can be traced back to understandable factors. When applying XAI to dependency risk analysis in IoT systems, the following methods can be utilized:

- **Feature importance**: in dependency risk analysis, ML models typically analyze multiple features (e.g., network traffic, device telemetry, historical attack data). Feature importance techniques, such as **SHAP (SHapley Additive exPlanations)** or **LIME (Local Interpretable Model-agnostic Explanations)**, can help explain which features had the most significant impact on the model's decision. For example, if the model flags a specific IoT device as a high-risk point in the network, the feature importance analysis can show whether this is due to abnormal data traffic, historical vulnerabilities, or dependency with critical systems.
- **Model-agnostic approaches**: these approaches enable the analysis of complex models (e.g., deep learning or ensemble methods) by generating interpretable approximations. LIME, for instance, creates a locally interpretable linear model around the prediction, helping to clarify how a black-box model arrived at a specific conclusion regarding risk dependencies in IoT systems.

2. Interpretable ML models

In some cases, using inherently interpretable models can be an effective way to ensure transparency. While deep learning models or complex neural networks may offer high accuracy, they can be difficult to explain. Instead, opting for more interpretable models, such as **decision trees, random forests, or logistic regression**, can provide a clearer path from input data to decision output. These models, though potentially less complex, offer higher explainability in decision-making processes for dependency analysis.

For example, decision trees, which mimic human decision-making logic, can be used to illustrate how specific vulnerabilities or IoT device dependencies lead to a higher overall risk score. Each branching point in the tree reflects a critical decision, making the process transparent and easy to follow.

3. Traceability and auditability

For any AI/ML-based risk assessment model, it is crucial to ensure **traceability** and **auditability**. This involves maintaining logs and records that track every decision made by the AI/ML system. These records allow cybersecurity analysts to trace the steps leading to a specific risk prediction, ensuring that every decision can be reviewed and validated post-decision.

- **Traceable workflows**: implementing a workflow that tracks every action, from data ingestion to model training and prediction, ensures that the decision-making process remains transparent. These workflows can include detailed documentation of which models were used, the data they were trained on, and how predictions evolved over time.
- **Model audits**: regular audits of the AI/ML models used for dependency risk analysis should be conducted to ensure their outputs remain aligned with real-world data and organizational goals. This process can involve reviewing how new data affects predictions and making adjustments to the models as necessary to maintain accuracy and transparency.

4. Human-in-the-loop systems

To maintain a high level of trust and transparency, many AI/ML systems in cybersecurity integrate a **human-in-the-loop** approach. This method involves human analysts in critical decision points, allowing them to validate, refine, or override AI/ML-generated risk assessments. This hybrid approach combines the efficiency of automated analysis with the intuition and domain expertise of human cybersecurity professionals.

In dependency risk analysis, human experts can review key AI-driven decisions, particularly in cases where the model's output is uncertain or where the risks involve critical infrastructure. By keeping humans engaged in the decision-making process, organizations can ensure that all decisions are explainable and supported by both machine intelligence and human judgment.

5. Transparency in data sources and model inputs

Ensuring transparency begins with the **data inputs** used to train and operate AI/ML models. The types of data used for dependency risk analysis, such as network traffic logs, vulnerability databases, and IoT telemetry data, should be well-documented and made available for inspection. This transparency ensures that stakeholders understand the source of the model's knowledge and can assess whether the data used is relevant, up-to-date, and of sufficient quality.

- **Data provenance**: documenting the origin of data, such as which vulnerability feeds or IoT device logs were used, ensures

that all stakeholders can understand the foundation of the AI/ML model's decisions. This is particularly important when models incorporate third-party data, as the reliability of this data directly affects the model's output.

- **Open datasets**: wherever possible, using open datasets or sharing anonymized data sources improves transparency and allows third parties to verify the models. For instance, the use of datasets like **BoT-IoT** or open vulnerability databases ensures that the data sources can be scrutinized and understood by a wider audience.

6. Clear risk reporting and visualization

One of the key ways to ensure transparency in AI/ML models is to provide clear and understandable visualizations of the model's risk assessments. **Dashboards** that visualize key risk metrics, such as the likelihood of exploitability, device dependencies, and impact of failures, make AI/ML-driven decisions more interpretable for non-experts. These dashboards should offer:

- Visual representations of how different IoT devices are interconnected,
- Risk scores for individual devices or systems,
- Explanations of how changes in dependencies influence overall system risk.

By providing clear and detailed risk visualizations, organizations can help all stakeholders, from technical staff to decision-makers, understand and trust the AI/ML outputs.

7. Model testing and validation

To ensure that AI/ML models used in dependency risk analysis are both accurate and explainable, it is essential to rigorously test and validate the models against real-world data. This process involves:

- **Benchmarking against known outcomes**: testing the model against historical data to ensure it makes accurate predictions based on past incidents.
- **Cross-validation**: ensuring that the model's predictions generalize across different datasets and scenarios, helping to confirm that it is robust and transparent in different IoT environments.
- **Regular updates**: continuously updating the models with new data and testing their performance ensures that the AI/ML models stay relevant and interpretable as new IoT vulnerabilities emerge.

Ensuring explainability and transparency in AI/ML models for dependency risk analysis is crucial for maintaining trust in the decision-making process. By leveraging XAI techniques, using interpretable models, implementing human-in-the-loop systems, ensuring transparency in data sources, and providing clear risk visualizations, organizations can ensure that the AI/ML-driven decisions are understandable and actionable. These steps allow stakeholders to gain insight into how AI/ML models arrive at their conclusions, building confidence in the overall risk assessment process.

10 Conclusion

The findings of this research emphasize the critical need for a comprehensive risk assessment framework tailored to the unique challenges of IoT environments. Through the development of a dependency-based cyber risk model, this study highlights the significance of interdependencies among IoT components in understanding and mitigating cyber risks. The integration of AI/ML techniques enhances the model's adaptability, offering dynamic risk assessments based on real-time data, while ensuring transparency through explainable AI (XAI) methodologies. Furthermore, the exploration of risk transference strategies such as cyber insurance demonstrates practical approaches for mitigating financial and operational impacts. By empirically validating the model using the BoT-IoT dataset, the research provides a robust tool that can be generalized across diverse IoT domains, contributing to the development of a more secure and resilient IoT ecosystem. These contributions lay the groundwork for future advancements in IoT cybersecurity, particularly in refining AI-driven solutions and addressing the evolving landscape of IoT threats.

This article reviews existing literature on emerging trends in IoT risk assessment, including the emergence of the Software Bill of Materials (SBOM), the Vulnerability Exploitability eXchange (VEX) and the Common Security Advisory Framework (CSAF). Although there is a wealth of research on the values of a Bill of Materials in cyber risk assessment, there is very little work on the software components used in low-cost IoT devices. The Software Bill of Materials (SBOM) was developed to address this issue, but analyzing vulnerabilities from SBOMs usually results in a serious workload for cybersecurity professionals. Much of this process can be automated, and in this article, we reviewed some potential solutions for such automation. The article proposes a dependency model based on the goal-oriented approach, designed to be compliant and supportive of the new Stakeholder-Specific Vulnerability Categorization (SSVC) based on decision trees.

Through reviewing existing risk methods, in this paper, we determined that the existing models, individually, do not provide solutions for impact estimation of IoT cyber risk in autonomous systems. This research builds upon integrating the existing models and presents a unifying model incorporating IoT cyber risks in the impact estimation. The challenge in testing and verifying this new "combined/unified model" and ensuring that the new model addresses the IoT context is resolved with dependency modeling. To test and verify the new model, we designed dependency relationships. In Figure 2 we describe what the connections (arrows) mean, and how dependencies are expressed, and we give a description of dependency presented in the paper. The proposed cyber risk assessment with a unified model and dependency modeling is designed to estimate IoT risks, the impacts caused by failures that cascade and aggravate the impacts from one affected system or component to another. Since IoT risks are decentralized through networked objects, such risk is often invisible in the risk assessments with methodologies designed for general cyber risk assessment. Our approach is designed to advance the IoT risk assessment discipline. It considers the dependencies in "no-win"

scenarios, where each scenario leads to a risk we cannot protect from. The dependency states we considered are risk acceptance and risk transference.

This paper provides an overview of the current IoT cyber risk assessment research, with specific new models on this topic, such as dependency modeling and cyber risk mitigation and transference strategies (e.g., cyber risk insurance). The paper refers to several models and risk assessment articles and technical publications that have emerged recently in the research literature. This research is important because it covers the lack of specific standards to govern the assessment of IoT cyber risk. The paper contributes to the current efforts to advance the understanding of risk in IoT systems and to produce a standardized design and a holistic approach for IoT risk assessment. Although our unified approach though dependency modeling does not resolve all the issues we identified in this article, this work represents an important step forward for the discipline.

In this article, what we argue is that what is really needed to improve cyber risk assessment, are rigorous mathematical and verifiable experimental results. Hence, we have conducted this work in collaboration with the FAIR Institute (Factor Analysis of Information Risk), the North Carolina Chapter of FAIR (2023), and we applied the FAIR by design principles (Wilkinson et al., 2016). We are one of the leading protagonists in using quantitative methods, instead of the currently used qualitative and hybrid cyber risk assessment methods. That, however, needs confidence intervals, time bound ranges, frequency, distribution, and many other data inputs that we currently do not have. We argue that when AI/ML can be shifted to the IoT devices operating at the edge of the network, this data could be possible to collect autonomously, and that would enable moving on from qualitative and hybrid assessment, into a qualitative cyber risk assessment that uses rigorous mathematical reasoning to deliver verifiable experimental results.

10.1 Limitations of this study and opportunities for further research

Using the new design of a unified and holistic model for IoT risk assessment and risk management without the required probabilistic risk data remains a challenge. To test and verify the new design, this study applied the case study research method, conducted individual interviews, and conducted workshops with Cisco experts in cybersecurity. To prove the new design further, we also conducted 6-month long action research with Cisco and recorded the performance of the design, then made iterative improvements to ensure functionality in different real-world environments. The solution presented in this paper is the final version of the new design; multiple versions were tested in the process. However, most failed in the application stage, usually because they have proven challenging to implement or even to understand by experts who didn't build the method. The selection criteria were based on the experts' ability to understand and use the new process. The rationale behind this was that if a cybersecurity expert cannot use the system, it would be almost impossible to train a non-expert to use the system, and occasionally, we require different expertise in the risk assessment process.

Prior to attempting to use the new unified/holistic model, appropriate data strategies should be developed that would enable the collection of probabilistic data. Given the lack of standards and regulations on developing the required data strategies (for IoT cyber risk), it seems that private sector is leading these efforts rather than national statistical offices. However, without standards, regulations, and policies in place, it is hard to see how individual data strategies of private companies could be synchronized to enable sufficient probabilistic data for a comprehensive understanding of IoT cyber risks. To promote advancements in collection of probabilistic data through appropriate data strategies, further research should focus on the combination of regulations, standards, and policies on data collection of IoT risk, artificial intelligence for data collection from IoT sensor networks, IoT data safety, IoT cyber security and data collection from IoT equipment, along with ethics of machine learning in IoT cyber risk data collection. Interdisciplinary research such as this would benefit the process of identify a dynamic and self-adapting system supported with AI/ML and real-time intelligence for predictive cyber risk analytics for edge computing. The current state of our knowledge on this topic is that 'overcoming the alleged limitation of model-centric AI may well require paying extra attention to the alternative data-centric approach' (Hamid, 2022). In other words, the current position in existing literature is that to resolve the problem with absence of probabilistic data, we need to look at how we structure our data strategies, and then consider the algorithms we use, in combination with the data states and properties. We must note that applying the proposed holistic model for IoT risk assessment and risk management is a challenge in the absence of relevant probabilistic data. This in turn requires developing appropriate data strategies to enable the collection and processing of required probabilistic data. This links to the currently increasing demands on developing data-centric approaches in the development of AI technologies which, with machine learning (ML) techniques, forward to the development of the IoT. This would enhance our capacity for a comprehensive understanding of the opportunities and threats that arise when edge computing nodes are deployed, and when AI/ML technologies are migrated to the periphery of the internet and into local IoT networks.

Author contributions

PR: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. DD: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Supervision, Validation, Writing – original draft, Writing – review & editing. CM: Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing. JN: Conceptualization, Formal analysis, Funding acquisition, Methodology, Software, Validation, Writing – original draft, Writing – review & editing. RN: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. UA: Writing –

original draft, Writing – review & editing, Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. This work has been supported by UK EPSRC under grant number EP/S035362/1.

Acknowledgments

Eternal gratitude to the Fulbright Visiting Scholar Programme.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Adams, J. (1995). *Risk*. Chicago: Questia.

Aggarwal, V. K., and Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: a framework for analysis. *J. Cyber Policy* 3, 291–305. doi: 10.1080/23738871.2018.1553989

Allodi, L., and Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analy.* 37, 1606–1627. doi: 10.1111/risa.12864

Alpcan, T., and Bambos, N. (2009). "Modeling dependencies in security risk management," in *Post-Proceedings of the 4th International Conference on Risks and Security of Internet and Systems, CRiSIS 2009* (Toulouse, France: IEEE Xplore), 113–16.

Anthi, E., Williams, L., and Burnap, P. (2018). "Pulse: an adaptive intrusion detection for the internet of things," in *Living in the Internet of Things: Cybersecurity of the IoT* (London: Institution of Engineering and Technology).

Anthonysamy, P., Rashid, A., and Chitchyan, R. (2017). "Privacy requirements: present and future," in *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)* (Bueons Aires: IEEE), 13–22.

Bhingarkar, S., Thanga Revathi, S., Kolli, C. S., and Mewada, H. K. (2022). An effective optimization enabled deep learning based malicious behaviour detection in cloud computing. *Int. J. Intellig. Robot. Appl.* 9, 15796–15818. doi: 10.1007/s41315-022-00239-x

Biden, J. (2021). *Executive Order on Improving the Nation's Cybersecurit*. Washington, DC: The White House. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed May 12, 2021).

Biener, C., Eling, M., and Wirfs, J. H. (2014). *Insurability of Cyber Risk 1*. Zürich: Geneva Association.

Bloomfield, R., Buzna, L., Popov, P., Salako, K., and Wright, D. (2010). "Stochastic modelling of the effects of interdependencies between critical infrastructure," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, eds. E Rome and R Bloomfield (Berlin: Springer Berlin Heidelberg).

Brass, I., Pothong, K., Tanczer, L., and Carr, M. (2019). "Standards, governance and policy," in *Cybersecurity of the Internet of Things (IoT): PETRAS Stream Report* (London: University College London). doi: 10.13140/RG.2.2.15925.42729

Brass, I., Tanczer, L., Carr, M., Elsden, M., and Blackstock, J. (2018). "Standardising a moving target: the development and evolution of IoT security standards," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018* (London: Institution of Engineering and Technology).

Breza, M., Tomic, I., and McCann, J. (2018). Failures from the environment, a report on the first FAILSAFE workshop. *ACM SIGCOMM Comp. Commun. Rev.* 48, 40–45. doi: 10.1145/3213232.3213238

Callo Arias, T. B., Van Der Spek, P., and Avgeriou, P. (2011). A practice-driven systematic review of dependency analysis solutions. *Empir. Softw. Eng.* 16, 544–586. doi: 10.1007/s10664-011-9158-8

Camillo, M. (2017). Cyber risk and the changing role of insurance. *J. Cyber Policy* 2, 53–63. doi: 10.1080/23738871.2017.1296878

Caplan, P. (2000). *Risk Revisited*.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Middlesex, MA: Hansom AFB.

Cherdantseva, Y., Burnap, P., Nadjm-Tehrani, S., and Jones, K. (2022). A configurable dependency model of a SCADA system for goal-oriented risk assessment. *Appl. Sci.* 12, 1–29. doi: 10.3390/app12104880

Christensen, D., Martin, M., Gantumur, E., and Mendrick, B. (2019). Risk assessment at the edge: applying NERC CIP to aggregated grid-edge resources. *Electr. J.* 32, 50–57. doi: 10.1016/j.tej.2019.01.018

CISA (2022). *CISA Stakeholder-Specific Vulnerability Categorization Guide*. Washington, DC: Cybersecurity and Infrastructure Security Agency.

CMMI (2017). *What Is Capability Maturity Model Integration (CMMI)®?* Pittsburgh: CMMI Institute. CMMI Institute. Available at: http://cmmiinstitute.com/capability-maturity-model-integration

Constance, E. (2017). The internet of things: preparing for the revolution. *J. Cyber Policy* 2, 152–154. doi: 10.1080/23738871.2017.1361890

Conte, T. M., DeBenedictis, E. P., Mendelson, A., and Milojicic, D. (2018). Rebooting computers to avoid meltdown and spectre. *Computer* 51, 74–77. doi: 10.1109/MC.2018.2141022

Craggs, B., and Rashid, A. (2017). "Smart cyber-physical systems: beyond usable security to security ergonomics by design," in *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)* (Buenos Aires: IEEE), 22–25.

Crawford, D., and Sherman, J. (2018). Gaps in United States Federal Government IoT security and privacy policies. *J. Cyber Policy* 3, 187–200. doi: 10.1080/23738871.2018.1514061

CVSS (2019). *Common Vulnerability Scoring System SIG*. Available at: https://www.first.org/cvss/ (accessed July 1, 2024).

DiMase, D., Collier, Z. A., Heffner, K., and Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environm. Syst. Deci.* 35, 291–300. doi: 10.1007/s10669-015-9540-y

DoD (2017). *Risk, Defense. Issue, and Opportunity Management Guide for Defense Acquisition Programs* Washington, DC: Office of the Deputy Assistant Secretary of Defense for Systems Engineering. Available at: https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf

Dubois, E. (2018). *The Implementation of a Cybersecurity Testbed for Education and Research*. New York: Business/Business Administration.

Edwards, B., Hofmeyr, S., and Forrest, S. (2016). Hype and heavy tails: a closer look at data breaches. *J. Cybersecu.* 2, 3–14. doi: 10.1093/cybsec/tyw003

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., et al. (2019). Cyber operational risk scenarios for insurance companies. *Br. Actuarial J.* 24:e6. doi: 10.1017/S1357321718000284

Erola, A., Agrafiotis, I., Nurse, J. R. C., Axon, L., Goldsmith, M., and Creese, S. (2022). A system to calculate cyber value-at-risk. *Comput. Secur.* 113:102545.

Evans, A. (2019). "Managing cyber risk," in *Managing Cyber Risk*. Abingdon: Taylor and Francis. doi: 10.4324/9780429057632

FAIR (2017). *Quantitative Information Risk Management*. Spokane, WA: The FAIR Institute. Available at: http://www.fairinstitute.org/ (accessed July 1, 2024).

FAIR (2020). *FAIR Risk Analytics Platform Management. FAIR-U Model*. Available at: https://www.fairinstitute.org/fair-u (accessed July 1, 2024).

FAIR (2023). *North Carolina Chapter — FAIR Institute*. Available at: https://link.fairinstitute.org/group/8-north-carolina-chapter (accessed July 1, 2024).

Falco, G., Noriega, A., and Susskind, L. (2019). Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks. *J. Cyber Policy* 4, 90–116. doi: 10.1080/23738871.2019.1586969

Fracarolli Nunes, M., and Lee Park, C. (2016). Caught red-handed: the cost of the Volkswagen dieselgate. *J. Global Responsib.* 7, 288–302. doi: 10.1108/JGR-05-2016-0011

Furfaro, A., Argento, L., Parise, A., and Piccolo, A. (2017). Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simulat. Model. Pract. Theory* 73, 43–54. doi: 10.1016/j.simpat.2016.09.007

Gupta, A. (2018). "The evolution of fraud: ethical implications in the age of large-scale data breaches and widespread artificial intelligence solutions deployment," in *ITU Journal: ICT Discoveries, Special Issue.*

Hamid, Q. H. (2022). "From model-centric to data-centric AI: a paradigm shift or rather a complementary approach?," in *2022 8th International Conference on Information Technology Trends (ITT)* (IEEE), 196–199.

Howard, M. (2017). *Cybersecurity Improvement Act of 2017: The Ghost of Congress Past - DevOps.Com. Devops.Com*. Available at: https://devops.com/cybersecurity-improvement-act-2017-ghost-congress-past/

Institute of Risk Management (2019). *Cyber Risk*. Available at: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/ (accessed July 1, 2024).

Islam, M. S., Ivanov, S., Awan, H., Drohan, J., Balasubramaniam, S., Coffey, L., et al. (2022). Using deep learning to detect digitally encoded dna trigger for trojan malware in bio-cyber attacks. *Sci. Rep*. 12, 1–13. doi: 10.1038/s41598-022-13700-5

ISO (2017). *ISO - International Organization for Standardization*. Available at: https://www.iso.org/home.html (accessed July 1, 2024).

Jalali, M. S., Kaiser, J. P., Siegel, M., and Madnick, S. (2019). The internet of things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products. *IEEE Secur. Privacy* 17, 39–48. doi: 10.1109/MSEC.2018.2888780

Kovtun, V., Izonin, I., and Gregus, M. (2022). Reliability model of the security subsystem countering to the impact of typed cyber-physical attacks. *Sci. Rep*. (2022) 12, 1–14. doi: 10.1038/s41598-022-17254-4

Laugé, A., Hernantes, J., and Sarriegi, J. M. (2015). Critical infrastructure dependencies: a holistic, dynamic and quantitative approach. *Int. J. Crit. Infrastruct. Prot.* 8, 16–23. doi: 10.1016/j.ijcip.2014.12.004

Leverett, E., and Kaplan, A. (2017). Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate. *J. Cyber Policy* 2, 195–208. doi: 10.1080/23738871.2017.1362020

Lin, S., Huang, J., Chen, W., Zhou, W., Xu, J., Liu, Y., et al. (2021). Intelligent warehouse monitoring based on distributed system and edge computing. *Int. J. Intellig. Robot. Appl.* 5, 130–142. doi: 10.1007/s41315-021-00173-4

Maras, M. H., and Wandt, A. S. (2019). Enabling mass surveillance: data aggregation in the age of big data and the internet of things. *J. Cyber Policy* 2019, 1–18. doi: 10.1080/23738871.2019.1590437

Meakins, J. (2019). A zero-sum game: the zero-day market in 2018. *J. Cyber Policy* 4, 60–71. doi: 10.1080/23738871.2018.1546883

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity*.

NIST (2022). *NVD - CVSS v3 Calculator. CVSS Version 3.1*. Available at: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (accessed July 1, 2024).

NTIA (2021). *Vulnerability-Exploitability EXchange (VEX)*. United States Department of Commerce: National Telecommunications and Information Administration. Available at: https://www.ntia.gov/page/software-bill-materials (accessed July 1, 2024).

OASIS (2022). *OASIS Common Security Advisory Framework (CSAF) TC*. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf (accessed July 1, 2024).

O'Neill, P. (2013). Protecting critical infrastructure by identifying pathways of exposure to risk. *Technol. Innovat. Manage. Rev*. 2013, 34–40. doi: 10.22215/timreview/714

Palekar, S., and Radhika, Y. (2022). IoT authentication model with optimized deep Q network for attack detection and mitigation. *Int. J. Intellig. Robot. Appl.* 6, 350–364. doi: 10.1007/s41315-022-00227-1

Payton, T. (2018). Staying safe in an increasingly interconnected world: iot and cybersecurity. *Cyber Security* 2, 66–72. doi: 10.69554/HTTE6540

Pigman, L. (2019). Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion. *J. Cyber Policy* 4, 22–34. doi: 10.1080/23738871.2018.1546884

Ranganthan, V. P., Dantu, R., Paul, A., Mears, P., and Morozov, K. (2018). "A decentralized marketplace application on the ethereum blockchain," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)* (Philadelphia, PA: IEEE), 90–97.

Royce, E. R. (2014). "H.R.5793 - 113th congress (2013-2014): cyber supply chain management and transparency act of 2014," in *Congress.Gov*. Available at: http://www.congress.gov/

Russell, B., and Van Duren, D. (2016). *Practical Internet of Things Security: a Practical, Indispensable Security Guide That Will Navigate you Through the Complex Realm of Securely Building and Deploying Systems in our IoT-Connected World*. Birmingham: Packt Publishing. Available at: https://cir.nii.ac.jp/crid/1130282272636139008

Schindler, H. R., Cave, J. A. K., Robinson, N., Horvath, V., Hackett, P. J., Gunashekar, S., et al. (2013). *Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of Things: SMART 2012/0053*. RAND. Available at: https://op.europa.eu/en/publication-detail/-/publication/18e2ee38-75a8-4b61-aad5-97b1728d11ee

Scott, J., and Winter, S. (2016). *Rise of the Machines: The Dyn Attack was Just a Practice Run December 2016*. Washington, DC: Institute for Critical Infrastructure Technology.

Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Rev.* 19, 412–445. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/chlr19&div=26&id=&page=

Shaw, R., Takanti, V., and Zullo, T. (2017). *Best practices in cyber supply chain risk management, Boeing and Exostar Cyber Security Supply Chain Risk Management - Interviews*. Available at: https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf (accessed March 8, 2018).

Srinivas, J., Das, A. K., and Kumar, N. (2019). Government regulations in cyber security: framework, standards and recommendations. *Future Generat. Comp. Syst.* 92, 178–188. doi: 10.1016/j.future.2018.09.063

Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., and Carr, M. (2018). "Emerging risks in the iot ecosystem: who's afraid of the big bad smart fridge?," in *Living in the Internet of Things: Cybersecurity of the IoT* (London: Institution of Engineering and Technology).

The PETRAS National Centre of Excellence – PETRAS (2022). Available at: https://petras-iot.org/

Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., et al. (2018). "X-ray refine," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (New York: ACM Press), 1–13.

Van Wieren, M., Van Luit, E., Estourgie, R., Jacobs, V., and Bulters, J. (2016). *Cyber Value at Risk in The Netherlands*. London: Deloitte. Available at: https://securitydelta.nl/images/deloitte-nl-risk-cyber-value-at-Risk-in-the-Netherlands.pdf

Wheatley, S., Maillart, T., and Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *Eur. Phys. J. B* 89, 1–12. doi: 10.1140/epjb/e2015-60754-4

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., et al. (2016). The FAIR guiding principles for scientific data management and stewardship. *Scientific Data* 3, 1–9. doi: 10.1038/sdata.2016.18

Woods, D., and Simpson, A. C. (2018). "Monte carlo methods to investigate how aggregated cyber insurance claims data impacts security investments," in *Workshop on the Economics of Information Security (WEIS)*. Available at: https://www.danielwoods.info/assets/pdf/DW2018_IWLCSI_WEIS.pdf

Wynn, J., Whitmore, G., Upton, L., Spriggs, D., McKinnon, R., McInnes, R., et al. (2011). *Threat Assessment and Remediation Analysis (tara)*. Bedford, MA: MITRE Corporation. Available at: https://apps.dtic.mil/sti/tr/pdf/ADA576473.pdf

Zhang, X. (2021). Introduction to the focused section on new trends of autonomous robot navigation. *Int. J. Intellig. Robot. Appl.* 5, 101–103. doi: 10.1007/s41315-021-00182-3