future internet

MDPI

Review

Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management

In Lee

School of Computer Sciences, College of Business and Technology, Western Illinois University, Macomb, IL 61455, USA; I-Lee@wiu.edu

Received: 21 July 2020; Accepted: 16 September 2020; Published: 18 September 2020

check for updates

Abstract: Along with the growing threat of cyberattacks, cybersecurity has become one of the most important areas of the Internet of Things (IoT). The purpose of IoT cybersecurity is to reduce cybersecurity risk for organizations and users through the protection of IoT assets and privacy. New cybersecurity technologies and tools provide potential for better IoT security management. However, there is a lack of effective IoT cyber risk management frameworks for managers. This paper reviews IoT cybersecurity technologies and cyber risk management frameworks. Then, this paper presents a four-layer IoT cyber risk management framework. This paper also applies a linear programming method for the allocation of financial resources to multiple IoT cybersecurity projects. An illustration is provided as a proof of concept.

Keywords: Internet of Things; cybersecurity; risk management; linear programming; IT assets; cyberattack; vulnerabilities; cyber threat; risk assessment

1. Introduction

The Internet of Things (IoT) has created a new paradigm in which a network of machines and devices capable of communicating and collaborating with each other are driving new process innovations in enterprises [1]. Pervasive and ever-increasing cybersecurity attacks to IoT systems have caused people and organizations a wide range of issues in reputation, compliance, finance, and business operations. The rapid increase of cyberattacks is in part due to the phenomenal growth of IoT devices in such areas as smart grids, environmental monitoring, patient monitoring systems, smart manufacturing, and logistics. Security management of the IoT is challenging due to the dynamic and transient nature of the connection between devices [2], the diversity of actors capable of interacting within IoT systems [3], and resource constraints [4].

The worldwide IoT security market is expected to expand at a Compound Annual Growth Rate of 33.7% from 2018 to 2023 due to the increasing number of cyberattacks on IoT devices, growing IoT security regulations, and rising security concerns [5]. A recent survey reports that IoT-based threats will become more widespread and impactful, and senior management will need to pay more attention to IoT-related risks when developing organization-level cyber risk management [6]. However, only 35% of survey participants report that they have an IoT security strategy in place and, of those, only 28% report that they implemented it. Another survey shows that 80% of organizations experienced cyberattacks on their IoT devices in the past year [7]. However, it finds that 26% of the organizations did not use security protection technologies. These two surveys demonstrate the security limitations many IoT devices have and the need for organizations to move proactively to invest in IoT cybersecurity.

Despite weak security measures, existing risk assessment methods are not appropriate for dynamic systems such as the IoT [8]. For example, existing risk assessment methods are not sufficiently designed for cybersecurity risk assessment of medical IoT systems whose complexity exposes wide attack points to adversaries [9]. Developing IoT systems around a standard platform may help organizations develop IoT security measures without inadvertently raising cyber risks [10].

The purpose of IoT cybersecurity is to reduce cybersecurity risk for organizations and users through the protection of IoT assets and privacy. New cybersecurity technologies are constantly emerging and provide opportunities and challenges for IoT cybersecurity management. Most previous studies focus on the technological aspects of IoT cybersecurity. However, there is a lack of comprehensive risk management frameworks to address the complex cybersecurity issues in IoT systems. Against the backdrop of the gap in the IoT cybersecurity risk management, this paper presents a literature review on IoT security technologies and cyber risk management frameworks and develops a four-layer IoT cyber risk management framework. Then, this paper introduces a linear programming method to optimally allocate financial resources to different IoT cybersecurity projects. Finally, an illustration of the IoT cyber risk management for a hotel smart room provides the proof of concept of the risk assessment.

2. Literature Review

Given the unique nature of cyber threats and vulnerabilities of the IoT systems, developing a new IoT cyber risk management framework requires understanding both IoT cybersecurity technologies and existing cyber risk management frameworks.

2.1. Cybersecurity in IoT Architecture

Since each layer of the IoT architecture has unique security issues and interacts with other layers, security measures should be considered for the entire architecture [11]. A literature review of cybersecurity technologies through the lens of the IoT architecture helps us have a systematic and integrative view of the IoT cybersecurity. The following is based on Lee's five-layer architecture of enterprise IoT [1] and focuses on the layer-level cybersecurity issues and solutions.

2.1.1. Cybersecurity at the Perception Layer

While many IoT devices are designed to be low energy and lightweight, they often collect enormous amounts of data from the environment in real time and therefore apply various energy-saving methods. Technologies such as machine learning are often used to make reliable inferences from the data generated [12]. However, due to the resource-constrained capacity of devices, embedding computation-intensive security and privacy measures into lightweight IoT devices has been challenging [13–16].

One of the major security issues at the perception layer is the cloning of device chips for cyberattacks. For example, clones of RFID tags may be used to launch distributed denial-of-service (DDoS) attacks. Physical unclonable functions (PUFs) have been used for authentication and identification as well as cryptographic key generation for a chip [17]. PUFs chips enhance security through tamper resistance, device identification, authentication, and the prevention of cloned devices [18]. Since the components of IoT devices are often implemented on resource-constrained ones, lightweight PUF designs are required [19]. While PUFs are not cloneable, it is possible to clone a PUF key once it is extracted. Hence, a number of authentication protocols are proposed based on PUFs [11,20–22]. For example, Xu et al.'s protocol is based on PUFs and the lightweight cryptography to carry out an efficient verification of a single tag [21].

The enhancement of IoT cybersecurity requires doing tasks manually, expanding staff knowledge and tools, and addressing risks with manufacturers and other third parties [23]. IoT cybersecurity needs to take into account device security, data security, and individuals' privacy [23]. Certifying the security level of IoT devices is instrumental in achieving the acceptance of IoT devices, but the dynamic and heterogeneous nature of the IoT devices makes the development of a cybersecurity certification framework complicated from both technical and legal perspectives [24].

2.1.2. Cybersecurity at the Network Layer

In the IoT system, the network layer plays a critical role for the overall IoT security performance, since secure data transmission over the network is essential for the function of devices, processing stations, and the entire IoT system. An intrusion detection system (IDS) is used to detect attacks, take corrective measures, and monitor packets [25]. The IDS deploys various intrusion detection techniques: statistical analysis for anomaly detection [26]; evolutionary algorithm for classifying intrusions based on error conditions, behavior, and attempted intrusions [27]; protocol verification for classifying suspicious behaviors; data mining techniques such as random forest method [28]; and deep learning for classifying network breach patterns [29].

Deep learning models show promising results for the detection of DDoS attacks with the highest accuracy at 97.16% [29]. Hybrid methods using dimension reduction and classification techniques for detecting malicious activities on the IoT networks also show promising results [30]. The network security segment of the cybersecurity market is estimated to constitute the highest component of cybersecurity between 2018 and 2023, and the rising adoption of IoT applications is a key contributing factor to the growth [5].

2.1.3. Cybersecurity at the Processing Layer

Cloud computing and fog computing have become a standard technology at the processing layer for storing and processing large-size data streams generated from large numbers of IoT devices concurrently. Fog computing uses network devices for latency-aware processing of collected data [31]. In fog computing, IDS can be used on a fog node to detect intrusion [32]. A hybrid method using IDS, Virtual Honeypot Devices (VHD), and Markov models in fog computing shows promising results in identifying malicious devices as well as decreasing the false alarm rate [31].

The processing layer can utilize blockchain by publishing and storing data as a public ledger of every user or node in the system [33]. Some of the promising application areas of blockchain for the IoT include supply chains, smarter energy, and healthcare [34]. Blockchain can also be used to generate IoT security certificates for IoT devices to be deployed securely and automatically [35].

2.1.4. Cybersecurity at the Application Layer

Monitoring and control, big data and business analytics, and information sharing and collaboration are widely used enterprise IoT applications [36]. Different application areas such as smart homes, smart transportation, smart health, and smart grids require different security management approaches [37]. For example, smart health deals with highly personalized data and requires high-level security and privacy protection [38]. Since many IoT applications may be owned by third-party service providers, cyberattacks on these applications may affect the security of other interrelated applications [39].

Some security issues include the security of protocols such as CoAP, MQTT, and XMPP [40], improper patch management [41], inadequate authentication [42], and insufficient audit mechanisms [43]. The above-mentioned security issues have been addressed with various solutions such as key management, access control, heterogeneous network authentication, private information protection, and data security protection [37].

2.1.5. Cybersecurity at the Service Management Layer

Unlike the technological risks of the other layers, cybersecurity at the service management layer focuses on human and organizational aspects of cybersecurity. Trust and privacy issues are relevant to IoT service management, since these issues affect the usage of the IoT services and applications. A study on farmers' perceptions of agricultural technology shows that trust affects perceived value and perceived risk, and in turn, those affect IoT adoption [44]. Security and privacy threats become prevalent in the use of cloud services [45].

It is imperative to protect individuals' privacy impacted by personally identifiable information (PII) processing through the protection of device and data [23]. Incorporating privacy protection measures in the early stage of IoT development is critical for building trust and promoting the adoption of IoT systems [46]. However, since most IoT devices are low energy and lightweight, the task of protecting security and privacy is quite challenging [47]. To protect the privacy of patients in IoT-based healthcare systems, Luo et al. [48] propose a framework called PrivacyProtector with the aim of defending against sophisticated cyberattacks such as collusion attacks and data leakage.

2.2. Literature Review on Cybersecurity Risk Management

There is a paucity of studies on IoT cybersecurity risk management in academia and in the industry. Therefore, this literature review is not limited to cybersecurity risk management in the IoT. Previous studies are broadly categorized into qualitative and quantitative approaches to cybersecurity risk management.

2.2.1. Qualitative Approaches to Cybersecurity Risk Management

There are multiple competing and complimenting risk management frameworks. One of the most popular cybersecurity frameworks is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This is a high-level and easy-to-read guidance created for organizations to be able to customize [49]. The framework consists of the framework core, the implementation tiers, and the framework profile. The framework core describes five functions of the cybersecurity program. The implementation tiers describe the degree to which an organization's cybersecurity management practices exhibit the specific capabilities of cybersecurity defined in the tiers. An organization can use the framework profile to identify opportunities for improving its cybersecurity status by comparing a "Current" Profile with a "Target" Profile. While the NIST Cybersecurity Framework explicitly recognizes that the activities associated with managing cybersecurity risk are organization-specific, risk management issues are marginally addressed.

ISO/IEC 27005 is a set of standards developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides managers with guidelines and techniques for implementing and managing information security risks [50]. While ISO/IEC 27005 provides a structured sequence of activities, it does not directly employ any specific risk management method, and the organization is expected to define their own approach to risk management, depending on the type of information security management system, state of risk management, and/or industry-specific security issues.

The seven stages/chains Cyber Kill Chain® (CKC) framework is a risk management framework developed by Lockheed Martin [51]. The model analyzes what the cyber attacker would do in order to achieve their objectives and proposes countermeasures the defender must take to break the chain at an early stage as well as in later stages. The framework focuses mainly on the technological side of cybersecurity involving attackers and defenders, but it did not fully address the human and organizational issues in cyber risk such as human mistakes and internal threats. Furthermore, it does not provide any specific guide to cybersecurity investment decisions.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a security evaluation framework developed at the CERT(R) Coordination Center (Pittsburgh, PA, USA) [52]. OCTAVE helps an organization identify and rank key IT assets, weigh threats to those assets, analyze their vulnerabilities and impacts, and develop security priorities to reduce the risk to the IT assets. At the core of OCTAVE is the concept of self-direction with which a small, interdisciplinary team drawn from an organization's own departments leads the organization's evaluation process. The original OCTAVE was updated to OCTAVE Allegro to make the framework easier to implement in an organization [53]. OCTAVE Allegro allows for a broad assessment of an organization's operational risk environment in a workshop-style collaborative setting without the need for extensive risk assessment knowledge.

The CMMI Institute's Cybermaturity Platform shares a similar risk management approach with OCTAVE. However, one unique feature of the Cybermaturity Platform is a risk-based roadmap, which is a customized list of action items prioritized based on the risks most relevant to the organization [54]. To develop the risk-based roadmap, the Cybermaturity Platform conducts security gap analysis to measure current maturity versus target maturity and prioritizes security projects based on the organization's cybersecurity risk profiles.

The Center for Internet Security (CIS) publishes Consensus Audit Guidelines (CAG) consisting of 20 key actions, which are called critical security controls (CSC), that organizations should implement to prevent or mitigate cyberattacks [55]. Goals of the CAG include leveraging cyber offense to inform cyber defense, focusing on high payoff areas, ensuring that security investments are focused to counter the highest threats, maximizing the use of automation to enforce security controls, and using a consensus process to collect the best ideas. CAG includes Implementation Groups (IGs), which are similar to the implementation tiers of the NIST Cybersecurity Framework. IG 1 is the least mature, and IG 3 is the most mature in terms of resources and cybersecurity experience. The IGs are designed to help organizations classify themselves according to their cybersecurity maturity level, prioritize controls utilization, and develop an effective cybersecurity program.

2.2.2. Quantitative Approaches to Cybersecurity Risk Management

This section reviews a few studies that focus on quantitative approaches to cybersecurity risk management. The quantitative approaches tend to narrow down the scope of the studies to the cyber risk assessment. A Bayesian decision network (BDN) was applied to a framework for network security risk management [56]. The framework consists of several essential processes: risk assessment, risk mitigation, and risk validation and monitoring, which should be done accurately to improve the security level of a network. BDN models information needed for managing security risks, such as information about vulnerabilities, risk-reducing countermeasures, and the effects of implementing them on vulnerabilities. During the risk mitigation process, a cost–benefit analysis of the risk mitigation is conducted with modified Bayesian inference algorithms. Their experiments show that their framework helps improve network security significantly due to the accurate risk assessment and appropriate risk mitigation.

Another risk assessment framework, called AVARCIBER, extends the specific parameters of ISO 27005 [57]. The implementation of the framework follows a series of activities: launch the risk assessment, identify and assess assets, identify cybersecurity threats, assess the damage level for the vulnerability-asset (dimension) tuples, measure the risk, and perform countermeasures. The whole process is not unique compared to ISO 27005. However, more detailed activities and practical guides are provided. A case study was used to validate the implementation of the framework.

Realizing the NIST Cybersecurity Framework lacks a financial method useful for the justification of cybersecurity projects, a cost–benefit analysis was integrated into the framework [58]. The study demonstrates how cost–benefit analysis can help organizations select the most appropriate NIST Implementation Tier level and illustrates the relationship between the NIST Implementation Tier levels and a firm's appropriate level of spending on cybersecurity activities. However, this study does not provide operational details for the spending decisions nor explains how financial resources can be allocated among multiple cybersecurity projects.

2.3. Evaluation of the Literature

The literature review of both the qualitative and quantitative approaches to cybersecurity risk management shows that the qualitative approaches focus on high-level frameworks. These qualitative frameworks recognize the relevance of other frameworks and share a similar cybersecurity risk management process. For example, much of the NIST Cybersecurity Framework includes standards of ISO 27001 geared to certify information security requirements. The CMMI Cybermaturity Platform is aligned with leading frameworks such as ISO 27001 and the NIST Cybersecurity Framework.

However, none of the frameworks explicitly address the IoT cybersecurity ecosystem and its impacts on risk management. Furthermore, the frameworks do not provide any guide on how cybersecurity investment can be made for each cybersecurity project and how financial resources can be allocated among multiple cybersecurity projects. For example, the NIST Cybersecurity Framework provides no details of how a firm should conduct cost–benefit analysis when deciding on the organization's implementation tier [58]. Organizations are left with investing in cybersecurity projects by gut feeling.

The quantitative approaches to cybersecurity risk management focus on the risk assessment and the quantification of cyberattacks and impacts. There are only a few studies applying the quantification approaches. They do not explain how the quantification process can be integrated into the entire risk management process. They also do not provide a detailed cost–benefit analysis nor allocation of financial resources to multiple cybersecurity projects.

Based on the literature review, it has been determined that IoT cyber risk management did not receive proper attention. The current risk assessment approaches are inadequate in dealing with the complex array of connections among the wide range of devices and actors [3]. The review of the previous studies motivates us to develop an IoT cyber risk management framework that improves on the existing frameworks and quantitative approaches to risk assessment. This study integrates the qualitative and quantitative approaches and proposes a four-layer IoT cyber risk management framework that provides an essential guide for effective risk management.

3. The Four-Layer IoT Cyber Risk Management Framework

The four-layer IoT cyber risk management framework is proposed to help IoT security managers develop a cost-effective cybersecurity risk management plan. The proposed framework identifies major factors affecting cybersecurity risks and structures these factors into the four layers, so that risk management activities are organized and evaluated layer by layer without losing sight of the big picture cybersecurity issues. Figure 1 shows the proposed four-layer IoT cyber risk management framework, which consists of an IoT cyber ecosystem layer, an IoT cyber infrastructure layer, an IoT cyber risk assessment layer, and an IoT cyber performance layer.

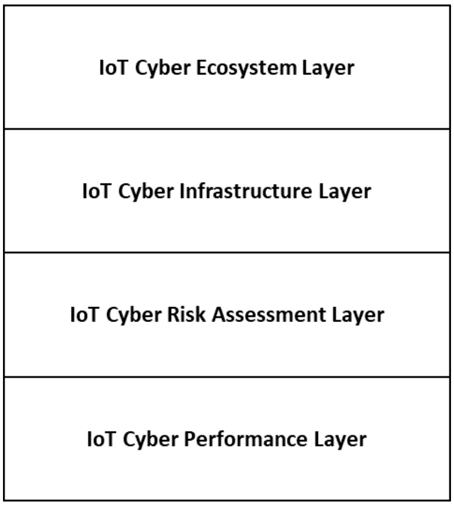
IoT Cyber Ecosystem Layer
IoT Cyber Infrastructure Layer
IoT Cyber Risk Assessment Layer
IoT Cyber Performance Layer

Figure 1. Internet of Things (IoT) cyber risk management framework.

The risk management framework starts with the IoT cyber ecosystem layer. From the assessment of the ecosystem elements, an organization identifies and understands the dynamics and roles of its stakeholders. The IoT cyber ecosystem layer periodically and/or continuously monitors and evaluates the environment and communicates findings to the other relevant layers. At the IoT cyber infrastructure layer, the organization analyzes the current state of the cybersecurity infrastructure by analyzing people's roles and responsibilities, organizational policies, and deployment of the IoT cybersecurity technologies. The IoT cyber risk assessment layer identifies IoT assets and services, vulnerabilities, and cyber threats, quantifies and prioritizes cyber threats and impacts, and makes a resource allocation to various IoT cybersecurity projects. At the IoT cyber performance layer, the cyber technologies are developed, monitoring and control activities are conducted, and continuous improvement activities are performed. Each layer is discussed below in detail.

3.1. IoT Cyber Ecosystem Layer

The IoT cyber ecosystem consists of stakeholders interacting with IoT systems collaboratively and competitively. The stakeholders of the IoT cyber ecosystem include IoT cybersecurity technology developers, external users/customers, adversaries, governments, and the standardization organizations. A change in the IoT cyber ecosystem needs swift attention from cybersecurity managers to formulate proper security responses for the protection of the IoT systems.

3.1.1. IoT Cybersecurity Technology Developers

Many IoT managers do not have sufficient expertise to develop IoT cybersecurity solutions. Hence, IoT managers need to be aware of the trends of IoT cyber technology developers' communities. As the IoT market grows, so does the market for the IoT cybersecurity technology developers. Cybersecurity technology developers are outfitting IoT devices with the latest tools in order to secure the transfer of data, prevent hacking, and keep privacy standards [59].

New technology developments such as 5G, serverless, and edge/fog computing IoT systems should be able to provide better protection against various security cyberattacks. Machine learning and AI will also show great potential for providing real-time prevention, detection, and recovery measures for IoT systems with higher accuracies than traditional methods. The IoT security platforms need to provide end-to-end solutions to deliver secure IoT systems unifying heterogeneous devices and applications from multiple vendors.

3.1.2. External Users and Customers

External users and customers enable IoT innovations to realize their full benefits. The users' and customers' acceptance of IoT services is critical for the success of IoT applications. A study shows that the perceived enjoyment and perceived usefulness of IoT applications positively affect usage behavior, but perceived privacy risk negatively affects IoT adoption [60]. Hence, it is imperative for IoT managers to identify the external IoT users and customers, understand their usage preferences and concerns about security and privacy, and develop an IoT usage model that focuses on security and privacy factors.

3.1.3. Adversaries

The cyber ecosystem takes into account adversaries such as intruders and hackers who pose cyber threats for economic gains or other nefarious purposes. Adversaries with higher cybersecurity knowledge remain a challenge, even with the use of advanced wireless security protocols and cryptography [61]. The adversaries are continuously developing new techniques, and it is critical for the organization to identify new intruders/hackers, understand their motivations to penetrate the systems, and analyze how they penetrate the system, steal data, install malware, and/or intercept operations.

3.1.4. Governments

Government cybersecurity regulations are imposed on organizations to make the necessary investments to meet the minimum regulatory requirements. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the security and privacy of healthcare information by creating national standards [62], and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 expanded the scope of privacy and security protections available under HIPAA [63]. These regulations significantly affect hospital data-sharing practices and potentially mobile healthcare operations.

In the US, as of July 2020, various cybersecurity regulations have been enacted to safeguard organizations' computer systems and protect data from cyberattacks. For example, the Internet of Medical Things Resilience Partnership Act of 2017 (the Medical Things Act) (H.R. 3985, 115 Cong. (2017)) establishes a working group of private and public entities to develop voluntary guidelines and frameworks for the security of Internet of Medical Things devices [64]. The Internet of Things Cybersecurity Improvement Act of 2019 would require a supplier of IoT devices to meet specified criteria before a U.S. government agency buys devices [65].

In Europe, the General Data Protection Regulation (GDPR) 2016/679 sets minimum levels of cybersecurity requirements for organizations to safeguard personal data they collect [66]. On June 7, 2019, the EU Cybersecurity Act was published in the Official Journal of the European Union [67]. This regulation proposes that the EU Cybersecurity Act establish a new mandate for the European Union Agency for Network and Information Security ("ENISA"), the EU Agency for Cybersecurity, and a European cybersecurity certification framework.

As discussed, governments address security concerns related to the use of IoT services by enacting regulations and incentivizing security technology investments with various taxes. Organizations involved in IoT cybersecurity technologies, IoT products, services, or processes should monitor the evolution of the various government regulations, assess their impacts on their IoT systems development, and consider necessary investments.

3.1.5. Standardization Organizations

Despite a significant amount of investment made on information assurance, there were no standards to assist cybersecurity managers in choosing the most appropriate cybersecurity technologies [68]. Recently, the need for the effective development of secured IoT products and services has led to standardization efforts for IoT security. Three standardization organizations' efforts for IoT cybersecurity standardization are discussed below.

The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) developed ITU-T Recommendations that define elements in the global infrastructure of ICTs [69]. The Global Standards Initiative on Internet of Things (IoT-GSI) of ITU-T promoted a unified approach for the development of technical standards to enable the global operations of the IoT and wrapped up its activities in July 2015 with the establishment of the Study Group 20 on "IoT and its applications including smart cities and communities." Their IoT-related series of recommendations were made from Y.4000 to Y.4999.

The ISO/IEC JTC 1 Special Working Group (SWG) 5 Internet of Things (IoT) was established in 2012 to develop standards relevant to the IoT and encourage them to be recognized and utilized by industry and other standards-setting organizations. Their preliminary report was made in 2014 [70]. Relevant to IoT cybersecurity standards is ISO/IEC TR 29181-5:2014 Information technology–Future Network–Problem statement and requirements–Part 5: Security (https://www.iso.org/standard/57487.html).

The European Telecommunications Standards Institute (ETSI) released its first globally applicable standard for consumer IoT security, TS 103 645, to specify high-level provisions for the security of Internet-connected consumer devices and their associated services [71]. TS 103 645 requires implementers not to use universal default passwords and to include a vulnerability disclosure policy.

3.2. IoT Cyber Infrastructure Layer

In developing a future-oriented cyber risk management plan, organizations must evaluate their current IoT cyber infrastructure from both technological and managerial perspectives. Many studies focus on the technical aspects of risk management to protect IT assets and services. However, a lack of organizational and users' support for cybersecurity is as detrimental to cybersecurity as a lack of cybersecurity technologies. Supporting a holistic approach to cyber risk management, the IoT cyber infrastructure layer consists of employees/internal users, the organization, and cybersecurity technologies.

3.2.1. Employees/Internal Users

The employees/internal users provide the behavioral element of the system. The focus of this element is on factors affecting user satisfaction, attitude, intention, and actual behavior on the use of cybersecurity technologies and compliance with security and privacy policies.

Promoting cybersecurity awareness and best practices is critical for the success of cybersecurity management [72]. According to a study conducted by Shred-it, more than 85% of senior executives believe that employee negligence is one of their biggest information security risks [73]. An empirical study shows that one of the reasons that cyberattacks occur at a rapid rate in the IoT systems is the poor compliance to information security policies that arises from behavioral issues and the lack of security awareness [74]. Another empirical study shows that there is a low level of IoT cybersecurity awareness by employees and proposes a cybersecurity e-brochure playbook as a possible solution [75].

3.2.2. Organization

The organization element focuses on senior management support, security policy, investment in security, security training, and other organizational activities. These activities are significant for the enhancement of IoT cybersecurity performances, since these activities are known to positively affect the attitudes and behaviors of internal users and employees as well as external users and customers of IoT services. Organizational preparedness to handle cyberattacks has become an integral part of enterprise risk management [76]. Strong support from senior management is crucial to developing and implementing successful security plans [72].

As the landscape of cyber threats shifts, organizations need to update their cybersecurity strategies. They need to establish cybersecurity governance and operations strategies and align their IoT cyber risk management with IT risk management and enterprise risk management. The NIST Cybersecurity Framework suggests four Implementation Tiers related to organizations' cybersecurity capabilities [49]. Depending on the organization's existing cybersecurity capabilities, they need to decide the desired level of Implementation Tier and develop their security strategies accordingly.

3.2.3. Cybersecurity Technologies

The cybersecurity technologies at this layer refer to internal cyber technology assets. The IoT cybersecurity technology developers at the IoT cyber ecosystem are highly relevant and may help the organization find and establish strong IoT cybersecurity technologies. Internal cybersecurity technologies should support the organization's overall cybersecurity goals as well as the IoT cybersecurity goals.

Hildebrandt distinguishes three main classes of cybersecurity technologies [77]: technologies that ensure the confidentiality of information; technologies that detect and counter online threats and vulnerabilities; and technologies that detect and counter cybercrime. Cybersecurity technologies are accompanied by authentication, which involves certification and the management of credentials [78]. Common IoT cybersecurity technologies include intrusion detection systems/intrusion prevention systems, device authentication and management, secure communications, data encryption and tokenization, secure software and firmware, Public Key Infrastructure (PKI) technology, firewalls, DDoS protection, security analytics, and incidence response systems [5].

3.3. IoT Cyber Risk Assessment Layer

Once the organization identifies their current IoT cyber infrastructure, they need to assess their current and future cyber risk. The IoT cyber risk assessment layer consists of three major activities: risk identification, risk quantification, and resource allocation.

3.3.1. Risk Identification

The risk identification stage identifies IoT assets, vulnerabilities, and cyber threats [57]. For each IoT asset, its vulnerabilities and threat types are identified (e.g., IoT device 1–vulnerability 1–threat type 1, IoT device 1–vulnerability 2–threat type 2, IoT device 2–vulnerability 1–threat type 2, etc.). The IoT risk identification involves understanding how intruders launch cyberattacks. Intruders have two different mindsets: explorative and exploitative [72]. In the explorative stages, intruders typically use deliberate and intuitive thinking and rely on intensive experimentation. Once access to a system is successful, they rely on an exploitative mindset to achieve their goals. Another useful tool for risk identification is the CKC framework [51]. The CKC framework is widely used to prevent and spot cyberattacks. Breaking the chain at an early stage is more effective in defending against the adversary's malicious activities. Specific risks can be identified through the analysis of the seven stages of the CKC framework.

3.3.2. Risk Quantification

At the risk quantification stage, the impact, frequencies, and defense probability of each IoT–asset–vulnerabilities–cyber threat grouping is estimated. The following techniques and tools are utilized to quantify risks.

For risk quantification, the frequency of cyberattacks refers to the expected number of cyberattacks in a given period. The expected impact of a cybersecurity attack in a given period can be estimated with selected metrics such as the number of compromised data records and/or financial loss. A defense probability of each attack is also estimated (e.g., a defense probability of 0.9 for threat type A). As the first activity of the risk quantification, the frequency of cyberattacks can be modeled as a random process of arrival with a Poisson probability density function, which is commonly used for a variety of arrival applications, including cyberattacks [79].

Secondly, a risk matrix is developed to understand the risk standing of all IoT asset–vulnerabilities–threats. The risk matrix has two dimensions. One dimension is the frequency of penetrated attacks of each IoT asset–vulnerabilities–threat and the other dimension is the expected financial loss per penetrated attack. Penetrated attacks are a failure of defense. Through the construction of the risk matrix, high priority IT asset–vulnerabilities–threats can be identified.

The risk matrix in Figure 2 shows an example. For illustrative purposes, dotted lines are arbitrarily drawn to divide a high, medium, and low risk area. In the figure, IoT asset–vulnerabilities–threat–1 and IoT asset–vulnerabilities–threat–2 are high risk, IoT asset–vulnerabilities–threat–3 and IoT asset–vulnerabilities–threat–4 are medium risk. IoT asset–vulnerabilities–threat–5 is low risk. The risk matrix can help managers prioritize the asset–vulnerabilities–threats and allocate resources for proper risk management. Though it is not a trivial task, the risk matrix should be updated periodically to protect an organization from evolving attack patterns as much as possible.

3.3.3. Resource Allocation

As discussed above, cyberattacks arrive in certain probability distributions (e.g., Poisson probability distribution), and the frequency of penetrated attacks per period is an essential parameter of the resource allocation model. From the defender's side, the defender's goal to increase defense probability will be achieved with a matching investment. The defense probability is binomial (i.e., either success or no success). The defense probability of each IoT asset–vulnerabilities–threat type and the frequency of penetrated attacks together determine the total financial loss of each IoT asset–vulnerabilities–threat type. The frequency of the penetrated attacks (i.e., unsuccessful defense) is measured as $n * (1 - p)$, where n is the frequency of attacks in a given period and p is the defense probability. $n * (1 - p) * m$ is the total financial loss where m is financial loss per penetrated attack. As an example, assume that the current defense probability of the IoT asset–vulnerabilities–threat–1 is estimated to be 0.9. Assuming that the current frequency of attacks for the IoT asset–vulnerabilities–threat–1 is 5000/period, and each penetrated attack costs $1000. Then, the total financial loss from the IoT asset–vulnerabilities–threat–1 is estimated to be $500,000 (i.e., 5000 * (1 − 0.9) * ($1000).

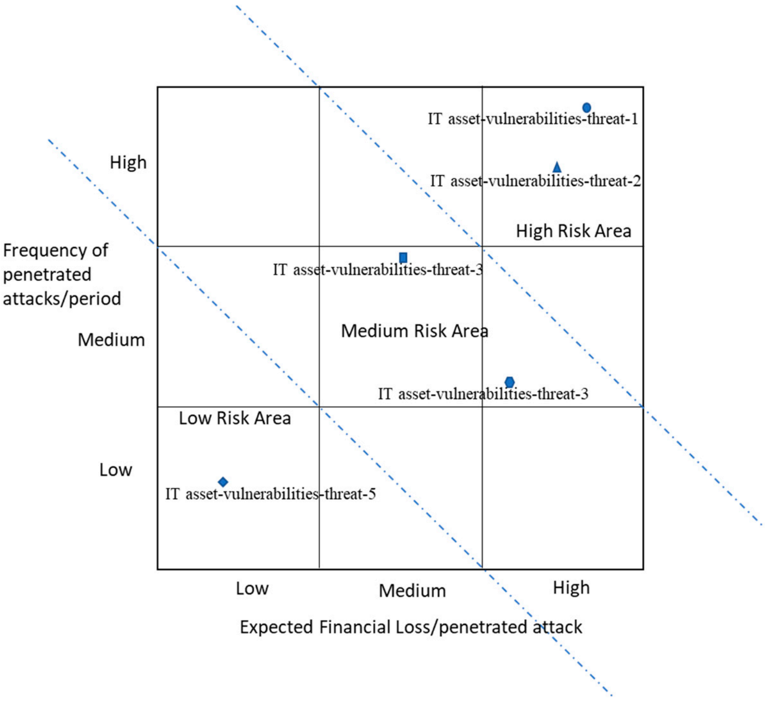
High
Frequency of penetrated attacks/period
Medium
Low
IT asset-vulnerabilities-threat-1
IT asset-vulnerabilities-threat-2
High Risk Area
IT asset-vulnerabilities-threat-3
Medium Risk Area
IT asset-vulnerabilities-threat-3
Low Risk Area
IT asset-vulnerabilities-threat-5
Low
Medium
High
Expected Financial Loss/penetrated attack

Figure 2. Example risk matrix.

One of the challenges in cybersecurity management is the optimal allocation of limited resources among competing IoT asset–vulnerabilities–threats. A cost–benefit model is adopted to determine resource allocation to various IoT asset–vulnerabilities–threats. Organizational resources include labor, IoT assets, and financial resources, and these are translated into monetary terms. This paper uses a linear programming model to optimally allocate financial resources to each IoT asset–vulnerabilities–threat. It is noted that there have not been any resource allocation methods used for cybersecurity investment decisions. The linear programming is an intuitive and logical mathematical modeling technique, and it guarantees optimal solutions under certain financial and operational constraints for many business problems such as budgeting, transportation routing, production scheduling, and investment portfolio management. Given the limited financial resources for cybersecurity management and multiple cybersecurity projects, the linear programming method can serve as an effective decision-making technique.

Figure 3 illustrates that more financial resource allocation will increase the defense probability from the starting defense probability of 0.9. The horizontal axis represents the defense probability from 0.9 to 0.99. The greater the financial resource allocation, the lower the financial loss will be from the IoT asset–vulnerabilities–threat–1 due to the increase of the defense probability. The total cost is the sum of the financial loss from the penetrated attacks and the allocated cyber investment cost for the target defense probability. In this example, linear curves are assumed for both the financial loss and the cyber investment cost within the range of 0.9 and 0.99. An exponential increase of the cyber investment cost is expected from a defense probability of 0.99 and greater due to the rapid increase of the marginal cost of cyber technologies. In this example, the formula for the financial loss is FL = $500,000 − $5,000,000 * ($x$ − 0.9), where x is the defense probability. The formula for the investment cost is IC = $3,000,000 * ($x$ − 0.9). The formula for the total cost is the sum of FL and IC: $TC = FL + IC$ = $500,000 − $2,000,000 * ($x$ − 0.9).

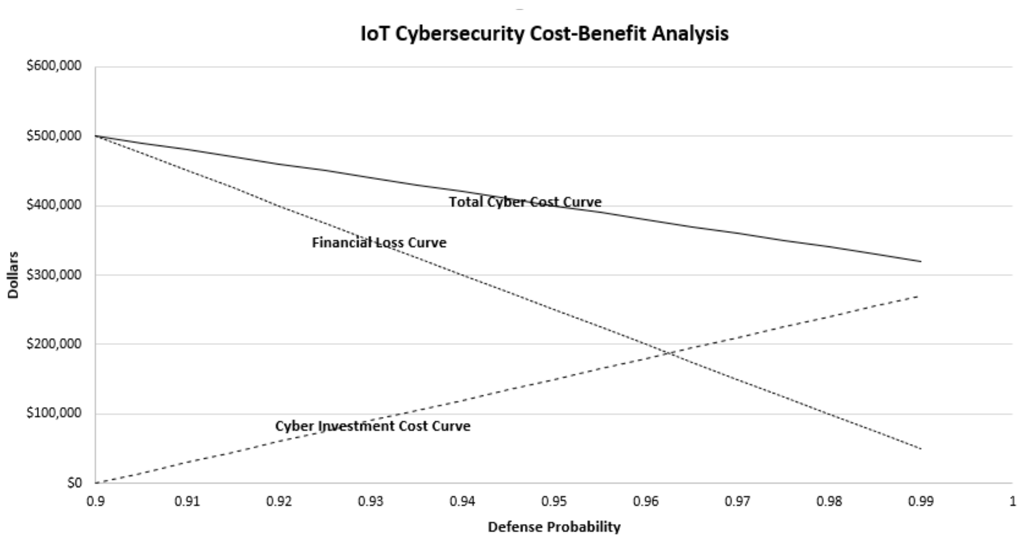

Figure 3. IoT cybersecurity cost–benefit analysis.

3.3.4. Multiple IoT Asset–Vulnerabilities–Threats with Constraints

Figure 3 shows that the total cost decreases up to the defense probability of 0.99 for IoT asset–vulnerabilities–threat–1. Since the investment is subject to many financial and operational constraints and limited organizational resources, one challenging question is how an organization should allocate limited resources to multiple IoT cybersecurity projects. To make decisions further complicated, each organization is in a different stage of the NIST's four Implementation Tiers, and each IoT asset–vulnerabilities–threat is likely to be subject to different operational and financial constraints.

To minimize the total cyber cost of the entire IoT asset–vulnerabilities–threats under these constraints, this paper proposes a linear programming (LP) model with financial and operational constraints. The LP model has three major components: decision variables, which represent the defense probabilities of IT asset–vulnerabilities–threats; an objective function, which is a mathematical function of the decision variables for the minimization of the total cyber cost; and constraints, which are a set of functional equalities or inequalities that represent financial, technological, and operational restrictions on what numerical values can be assigned to the decision variables. All formulas for the objective function and constraints are in a linear form. The algorithmic discussion of the LP model is outside the scope of this paper, and readers interested in the details can refer to Chakraborty, Chandru, and Rao [80].

Constraints ensure the defense probability of each IoT asset–vulnerabilities–threat to have an upper limit. For example, they may believe the organization does not have the staffing or experience necessary to develop a security solution with a high defense probability. A lack of experience or personnel may also force the organization not to adopt a highly complicated technology. All of these constraints will affect the optimality of the defense probabilities and investment costs.

3.3.5. LP-Based IoT Cyber Cost–Benefit Model

The IoT cyber investment LP model is expressed in canonical form as

$$\text{Minimize } c^T x$$

$$\text{Subject to } Ax \leq b$$

$$\text{And } 1 \geq x \geq 0$$

where x represents the vector of decision variables for defense probabilities for IoT asset–vulnerabilities–threat types, c and b are vectors of known coefficients, A is a matrix of coefficients, and $(\cdot)^T$ is the matrix transpose. The inequalities $Ax \leq b$ and $1 \geq x \geq 0$ are the constraints that specify a convex polytope over which the objective function is to be minimized for the total cyber cost. With the previous example of the five IoT asset–vulnerabilities–threat types, there will be five decision variables, a set of functional constraints, and a set of nonnegativity constraints. Later in the illustration section, the use of the LP model will be illustrated with a hypothetical case of a hotel smart room.

3.4. IoT Cyber Performance Layer

Once a cyber solution is identified and a resource allocation decision is made at the IoT cyber assessment layer, the IoT cyber performance activities kick in. While this layer is important for the whole of risk management, the discussion will be brief, as the activities mostly follow the decisions made at the risk assessment layer. The three major activities at the IoT cyber performance layer are implementation, monitoring and control, and continuous improvement.

3.4.1. Implementation

The implementation of the new IoT cyber infrastructure includes IoT cyber technology development, testing, deployment, new policy development, training, and user acceptance. Organizations need to develop selection criteria to evaluate and choose among commercially available cybersecurity technologies identified in the IoT cyber ecosystem layer. The implementation must take into account the ease, usability, and usefulness of cyber monitoring and control systems. While commercially available cybersecurity platforms facilitate the development of monitoring and control systems, these platforms can limit the developer in terms of customization of the solution [81]. The decision on the new IoT cyber infrastructure also needs to take into account the types of IoT applications and devices; e.g., some of the IoT devices are too small to implement computation-intensive cybersecurity algorithms directly on their devices, so a gateway-based architecture may be used to protect the entire IoT network as well as devices [82].

3.4.2. Monitoring and Control

Prevention, detection, and recovery are the core activities of the monitoring and control stage and are conducted concurrently to respond to various cyberattacks. Prevention and detection activities collect data on equipment performance, abnormal user activities, and illegal access to data and applications. Recovery activities deliver a solution in real time.

3.4.3. Continuous Improvement

For continuous improvement, the organization needs to measure key performance metrics, which include frequencies and sources of cyberattacks, impacts of penetrations (e.g., amount of data stolen, penalty, lost sales, and ransom paid), and recovery time. One difference between monitoring and control and continuous improvement is the timing of the activities and the data in which they are interested. Continuous improvement utilizes historical data to identify trends and analyze long-term performance. However, monitoring and control collect data in real time in order track cyberattacks and responds to them in real time. Continuous improvement activities need to establish measurable performance goals and generate periodic performance reports. It is important to establish performance goals of the various IoT security projects with benchmark data from the industry/sector and competitors, and prioritize the performance goals for continuous improvement.

4. Illustration of the Risk Assessment with Smart Room Scenario

This section focuses on the illustration of the IoT cyber risk assessment with a realistic smart room scenario.

4.1. IoT-Based Smart Room

IoT-based smart rooms have become highly popular in hotels, hospitals, individual houses, and various types of buildings. An IoT-based smart room is appropriate for the illustration of the IoT risk assessment, since multiple complex IoT asset–vulnerabilities–threats exist in smart rooms where multiple heterogeneous devices and technology platforms interact with each other. In the hotel industry, a smart hotel room has become a norm due to the declining price of IoT systems and competition in the hotel industry. Some of the expected benefits of the smart hotel room include customers' integrated experience with access to their own data and information, accessible voice and mobile-optimized controls, and improved personalized service. However, invasion of privacy is still a concern to users of a smart hotel room.

As a proof of concept, the proposed LP model is applied to the scenario of a hypothetical smart room. While this scenario is realistic and is likely to occur in any smart hotel room, this illustration does not imply that any actual hotel organization is involved in this scenario development. To facilitate the discussion, assume that there are five major IoT asset–vulnerabilities–threats for the smart hotel room as discussed in the previous section. Table 1 shows the hypothetical IoT architecture and the IoT asset–vulnerabilities–threats (Sources: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/customers/vmware-marriott-17q1-casestudy.pdf; http://serve360.marriott.com/wp-content/uploads/2018/10/2018_Serve_360_Highlights.pdf; https://www.energy.gov/sites/prod/files/2018/06/f52/cyber_security_lighting.pdf.). Table 2 shows the risk quantification of the IoT asset–vulnerabilities–threats.

Table 1. IoT architecture and IoT asset–vulnerabilities–threats.

Layers	IoT Asset and Services	Vulnerabilities and Threats
Application Layer	Mobile voice-enabled technology	IoT asset–vulnerabilities–threat–v: Recording of voice-enabled devices may be accessible by intruders and hotel employees or is accidentally sent to someone randomly and completely on its own.
Processing Layer	A virtualized, software-defined and automated data center	IoT asset–vulnerabilities–threat–w: Cybercriminals and insiders use techniques such as password cracking and email hacking in order to gain access to user accounts.
Network Layer	A distributed antenna system (DAS) with private LTE solutions	IoT asset–vulnerabilities–threat–x: An attacker gains access to a packet of unencrypted data in transmission. The attacker may change the content of the unencrypted data.
Perception Layer	Digital Lighting Management (DLM) sensors and switches with wireless sensor networks (WSNs) Heating, ventilation, and air conditioning (HVAC) with wireless sensor networks (WSNs)	IoT asset–vulnerabilities–threat–y: DLM sensors being used in DDoS attacks (e.g., WiFi-enabled light bulbs). IoT asset–vulnerabilities–threat–z: An attacker gains access to wireless sensor networks to send commands to malware placed inside the network and to launch malicious operations.

Table 2. Risk quantification parameters.

IoT Asset–Vulnerabilities–Threat	Financial Loss Function	Investment Cost Function	Total Cost Function (Financial Loss Function + Investment Cost Function)
Type v	$\text{FL} = \$480{,}000–\$4{,}000{,}000 * (u - 0.88)$	$\text{IC} = \$2{,}000{,}000 * (u - 0.88)$	$\text{TC} = \$480{,}000–\$2{,}000{,}000 * (u - 0.88)$
Type w	$\text{FL} = \$660{,}000–\$6{,}000{,}000 * (v - 0.89)$	$\text{IC} = \$2{,}500{,}000 * (v - 0.89)$	$\text{TC} = \$660{,}000–\$3{,}500{,}000 * (v - 0.89)$
Type x	$\text{FL} = \$500{,}000–\$5{,}000{,}000 * (x - 0.9)$	$\text{IC} = \$3{,}000{,}000 * (x - 0.9)$	$\text{TC} = \$500{,}000–\$2{,}000{,}000 * (x - 0.9)$
Type y	$\text{FL} = \$300{,}000–\$2{,}000{,}000 * (y - 0.85)$	$\text{IC} = \$500{,}000 * (y - 0.85)$	$\text{TC} = \$300{,}000–\$1{,}500{,}000 * (y - 0.85)$
Type z	$\text{FL} = \$700{,}000–\$5{,}000{,}000 * (\text{z} - 0.86)$	$\text{IC} = \$2{,}000{,}000 * (\text{z} - 0.86)$	$\text{TC} = \$700{,}000–\$3{,}000{,}000 * (\text{z} - 0.86)$

4.2. LP Formulation for IoT Cyber Resource Allocation

Assume that type v and w are independent and require a resource allocation decision separately, while type x, y, and z are network related, and the resource allocation of the three types needs to be optimized. Hence, an LP model for type x, y, and z is developed, and the result is discussed after the execution of the model.

Assumptions for the LP model

(1) Decision variables: Defense probability for type x, y, and z, respectively

(2) The minimum defense probability: $x = 0.90$; $y = 0.90$; $z = 0.90$

(3) The maximum defense probability (operational feasibility constraint): all $x, y, z = 0.99$

(4) Financial constraints to achieve the defense probability of 0.94:

$$\$3{,}000{,}000\, x + \$500{,}000\, y \leq \$3{,}290{,}000,$$

$$\$3{,}000{,}000\, x + \$500{,}000\, y \geq \$3{,}150{,}000,$$

$$\$500{,}000\, y + \$2{,}000{,}000\, z \leq \$2{,}350{,}000,$$

$$\$3{,}000{,}000\, x + \$2{,}000{,}000\, z \leq \$4{,}700{,}000,$$

$$\$3{,}000{,}000\, x + \$2{,}000{,}000\, z \geq \$4{,}500{,}000,$$

(5) Defense probability to an operational feasibility constraint between y and z: $y + z <= 1.91$.

Based on the assumptions, the following LP model is formulated:
Minimize GTC = $7{,}155{,}000 - 2{,}000{,}000\, x - 1{,}500{,}000\, y - 3{,}000{,}000\, z$
Subject to

$$3{,}000{,}000\, x + 500{,}000\, y \leq 3{,}290{,}000,$$

$$3{,}000{,}000\, x + 500{,}000\, y \geq 3{,}150{,}000,$$

$$500{,}000\, y + 2{,}000{,}000\, z \leq 2{,}350{,}000,$$

$$3{,}000{,}000\, x + 2{,}000{,}000\, z \leq 4{,}700{,}000,$$

$$3{,}000{,}000\, x + 2{,}000{,}000\, z \geq 4{,}500{,}000,$$

$$y + z \leq 1.91$$

This linear programming (LP) model was executed using a free online LP, and the result is discussed below. Source: https://www.wolframalpha.com/widgets/view.jsp?id=daa12bbf5e4daec7b363737d6d496120).

Table 3 shows that Option 3 is the lowest cost with type y assigned to the defense probability of 0.98, type x assigned to the defense probability of 0.933, and type z assigned to the defense probability of 0.93. The optimal total investment cost is $304,999. Using the LP model, Option 3 generates a lower total cost than Option 2, even with a smaller investment cost. This illustration shows the effectiveness of the LP model in complicated IoT cyber resource allocation decisions. A variety of sensitivity analyses can be conducted by changing the assumptions, which will help managers be more confident about using the LP model for resource allocation decisions. As the NIST's four Implementation Tiers model suggests [49], each organization is different in their cyber defense capability. The suggested LP model can effectively accommodate the unique situations of each organization.

Table 3. Results of three cyber investment options.

	Option 1	**Option 2**	**Option 3 (LP Solution)**
Defense Probability	x = 0.90 y = 0.90 z = 0.90	x = 0.94 y = 0.94 z = 0.94	x = 0.933333 y = 0.98 z = 0.93
Financial Loss	x = $500,000 y = $200,000 z = $500,000 Total Financial Loss: $1,200,000	x = $300,000 y = $120,000 z = $300,000 Total Financial Loss: $720,000	x = $333,335 y = $40,000 z = $350,000 Total Financial Loss: $723,335
Investment Cost	x = $0 y = $25,000 z = $80,000 Total Investment Cost: $105,000	x = $120,000 y = $45,000 z = $160,000 Total Investment Cost: $325,000	x = $99,999 y = $65,000 z = $140,000 Total Investment Cost: $304,999
Total Cost	x = $500,000 y = $225,000 z = $580,000	x = $420,000 y = $165,000 z = $460,000	x = $433,334 y = $105,000 z = $490,000
Grand Total Cost	$1,305,000	$ 1,045,000	$1,028,334

5. Conclusions

The IoT has been a foundational component for smart cities, smart grids, smart manufacturing, smart health, driverless cars, and drones, to name a few. As a growing number and variety of connected devices are introduced into the IoT networks, the potential security exposures grow exponentially. A lack of security in the IoT systems opens up opportunities for intruders and hackers to access critical infrastructure and sensitive data. However, the absence of an IoT cybersecurity risk management framework makes it very difficult for organizations to make effective decisions on IoT cyber risk management and investment.

This paper reviewed IoT cybersecurity technologies and cyber risk management frameworks. Then, this paper presented the four-layer IoT cyber risk management framework: the IoT cyber ecosystem layer, the IoT cyber infrastructure layer, the IoT cyber risk assessment layer, and the IoT cyber performance layer. Specifically, the IoT cyber risk assessment layer identifies, quantifies, and prioritizes IoT cyber risks. An LP model was developed to make resource allocation decisions for multiple competing IoT security projects. Then, an illustration of the IoT cyber risk assessment with an LP model was presented as a proof of concept.

This study fills a gap in the IoT cybersecurity risk management and intends to promote further interest for anyone interested in IoT cybersecurity risk management. For example, existing frameworks did not provide any resource allocation methods to managers. Since there are no resource allocation methods, any cyber investment decisions were made based on gut feeling and poor justification. The proposed four-layer IoT cyber risk management framework addressed this deficiency. The LP model can be easily scalable to larger IoT systems involving hundreds of decision variables (e.g., smart manufacturing and smart transportation).

Organizations need to continuously monitor the development of technologies in order to quickly respond to cybersecurity breaches and attacks. For example, along with the advances of 5G and related 5G-enabled IoT developments, cyberattacks will also become more prevalent in 5G-enabled IoT services such as self-driving cars, augmented reality and virtual reality, and smart patient monitoring. Along with the rapid adoption of the IoT applications, managers need to understand cyber risk management processes to become better prepared for adversaries' evolving attacks. This study contributes to the literature by presenting an IoT risk management framework useful for developing and deploying secured IoT systems.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Lee, I. The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet Things Eng. Cyber Phys. Hum. Syst.* **2019**, *7*, 100078. [CrossRef]
2. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
3. Nurse, J.R.C.; Creese, S.; de Roure, D. Security risk assessment in Internet of Things systems. *IT Prof.* **2017**, *19*, 20–26. [CrossRef]
4. Malik, V.; Singh, S. Security risk management in IoT environment. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 697–709. [CrossRef]
5. MarketsandMarkets. IoT Security Market Worth $35.2 Billion by 2023. 2019. Available online: https://www.marketsandmarkets.com/PressReleases/iot-security.asp (accessed on 17 September 2020).
6. PwC. Managing Emerging Risks from the Internet of Things. 2016. Available online: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/managing-iot-risks.html (accessed on 17 September 2020).
7. Irdeto. New 2019 Global Survey: IoT-Focused Cyberattacks Are the New Normal. 2019. Available online: https://resources.irdeto.com/global-connected-industries-cybersecurity-survey/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal (accessed on 17 September 2020).
8. Aldmour, R.; Burnap, P.; Lakoju, M. Risk assessment methods for converged IoT and SCADA systems: Review and recommendations. In Proceedings of the Living in the Internet of Things (IoT 2019), London, UK, 1–2 May 2019; p. 6.
9. Rao, A.; Carreón, N.; Lysecky, R.; Rozenblit, J. Probabilistic threat detection for risk management in cyber-physical medical systems. *IEEE Softw.* **2018**, *35*, 38–43. [CrossRef]
10. Deloitte. Secure IoT by Design. 2018. Available online: https://www2.deloitte.com/us/en/pages/operations/articles/iot-platform-security.html (accessed on 17 September 2020).
11. Bendavid, Y.; Bagheri, N.; Safkhani, M.; Rostampour, S. IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function". *Sensors* **2018**, *18*, 4444. [CrossRef]
12. Hejazi, D.; Liu, S.; Farnoosh, A.; Ostadabbas, S.; Kar, S. Development of use-specific high-performance cyber-nanomaterial optical detectors by effective choice of machine learning algorithms. *Mach. Learn. Sci. Technol.* **2020**, *1*, 025007. [CrossRef]
13. Mollah, M.B.; Azad, M.A.; Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *J. Netw. Comput. Appl.* **2017**, *84*, 38–54. [CrossRef]
14. Sha, K.; Wei, W.; Yang, T.A.; Wang, Z.; Shi, W. On security challenges and open issues in Internet of Things. *Future Gener. Comput. Syst.* **2018**, *83*, 326–337. [CrossRef]
15. Yu, R.; Xue, G.; Kilari, V.T.; Zhang, X. Deploying Robust Security in Internet of Things. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9. [CrossRef]

16. Liu, W.; Zhang, L.; Zhang, Z.; Gu, C.; Wang, C.; O'neill, M.; Lombardi, F. XOR-based low-cost reconfigurable PUFs for IoT security. *ACM Trans. Embed. Comput. Syst.* **2019**, *18*, 1–21. [CrossRef]
17. Gao, Y.; Ranasinghe, D.C.; Al-Sarawi, S.F.; Kavehei, O.; Abbott, D. Emerging physical unclonable functions with nanotechnology. *IEEE Access* **2016**, *4*, 61–80. [CrossRef]
18. O'Neill, M. Insecurity by design: Today's IoT device security problem. *Engineering* **2016**, *2*, 48–49. [CrossRef]
19. Mukhopadhyay, D. PUFs as promising tools for security in Internet of Things. *IEEE Des. Test* **2016**, *33*, 103–115. [CrossRef]
20. Kulseng, L.; Yu, Z.; Wei, Y.; Guan, Y. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA, 15–19 March 2010; pp. 1–5.
21. Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors* **2018**, *18*, 760. [CrossRef]
22. Zhu, F.; Li, P.; Xu, H.; Wang, R. A lightweight RFID mutual authentication protocol with PUF. *Sensors* **2019**, *19*, 2957. [CrossRef] [PubMed]
23. Boeckl, K.R.; Fagan, M.J.; Fisher, W.J.; Lefkovitz, N.B.; Megas, K.N.; Nadeau, E.M.; Piccarreta, B.M.; O'Rourke, D.G.; Scarfone, K.A. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228. 2019. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (accessed on 17 September 2020).
24. Matheu, S.N.; Hernandez-Ramos, J.L.; Skarmeta, A.F. Toward a cybersecurity certification framework for the Internet of Things. *IEEE Secur. Priv.* **2019**, *17*, 66–76. [CrossRef]
25. Hodo, E.; Xavier Bellekens, X.; Hamilton, A.; Dubouilh, P.-L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System. In Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia, 11–13 May 2016; pp. 1–6.
26. Pacheco, J.; Benitez, V.; Félix, L. Anomaly Behavior Analysis for IoT Network Nodes. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–6.
27. Li, J.; Zhao, Z.; Li, R.; Zhang, H. AI-based two-stage intrusion detection for software defined IoT networks. *IEEE Internet Things J.* **2019**, *6*, 2093–2102. [CrossRef]
28. Subasi, A.; Al-Marwani, K.; Alghamdi, R.; Kwairanga, A.; Qaisar, S.M.; Al-Nory, M.; Rambo, K.A. Intrusion Detection in Smart Grid Using Data Mining Techniques. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6.
29. Roopak, M.; Tian, G.Y.; Chambers, J. Deep Learning Models for Cyber Security in IoT Networks. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 452–457.
30. Pajouh, H.H.; Javidan, R.; Khayami, R.; Dehghantanha, A.; Choo, K.R. A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. *IEEE Trans. Emerg. Top. Comput.* **2019**, *7*, 314–323. [CrossRef]
31. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [CrossRef]
32. Yi, S.; Qin, Z.; Li, Q. Security and Privacy Issues of Fog Computing: A Survey. In *Wireless Algorithms, Systems, and Applications, Proceedings of the WASA 2015, Qufu, China, 10–12 August 2015*; Xu, K., Zhu, H., Eds.; Springer: Cham, Switzerland, 2015; Volume 9204, pp. 685–695.
33. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Internet Things* **2018**, *1*, 1–13. [CrossRef]
34. Rao, A.R.; Clarke, D. Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet Things* **2020**, *10*, 100079. [CrossRef]
35. Neisse, R.; Hernández-Ramos, J.L.; Matheu, S.N.; Baldini, G.; Skarmeta, A. Toward a Blockchain-Based Platform to Manage Cybersecurity Certification of IoT devices. In Proceedings of the 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019; pp. 1–6.
36. Lee, I.; Lee, K. The Internet of things (IoT): Applications, investments and challenges for enterprises. *Bus. Horiz.* **2015**, *58*, 431–440. [CrossRef]
37. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 64–71. [CrossRef]

38. Almulhim, M.; Zaman, N. Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 481–487.
39. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber security threats to IoT applications and service domains. *Wirel. Pers. Commun. Int. J.* **2017**, *95*, 169–185. [CrossRef]
40. Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017; pp. 659–666.
41. Tekeoglu, A.; Tosun, A.S. A Testbed for Security and Privacy Analysis of IoT Devices. In Proceedings of the IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016; pp. 343–348.
42. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
43. Yang, K.; Forte, D.; Tehranipoor, M.M. Protecting Endpoint Devices in IoT Supply Chain. In Proceedings of the 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, 2–6 November 2015; pp. 351–356.
44. Jayashankar, P.; Nilakanta, S.; Johnston, W.J.; Gill, P.; Burres, R. IoT adoption in agriculture: The role of trust, perceived value and risk. *J. Bus. Ind. Mark.* **2018**, *33*, 804–821. [CrossRef]
45. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and privacy for cloud-based IoT: Challenges. *IEEE Commun. Mag.* **2017**, *55*, 26–33. [CrossRef]
46. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
47. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, Kona, HI, USA, 13–17 March 2017; pp. 618–623.
48. Luo, E.; Bhuiyan, M.Z.A.; Wang, G.; Rahman, M.A.; Wu, J.; Atiquzzaman, M. PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun. Mag.* **2018**, *56*, 163–168. [CrossRef]
49. NIST. Cybersecurity Framework. 2018. Available online: https://www.nist.gov/cyberframework (accessed on 17 September 2020).
50. ISO/IEC. ISO/IEC 27005:2018(en) Information Technology—Security Techniques—Information Security Risk Management. 2018. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en (accessed on 17 September 2020).
51. Lockheed Martin. Cyber Kill Chain®. 2009. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 13 August 2019).
52. Alberts, C.; Dorofee, A. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Managing Information Security Risks: The OCTAVESM Approach. Addison Wesley. 2002. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.7807&rep=rep1&type=pdf (accessed on 17 September 2020).
53. Caralli, R.A.; Stevens, J.F.; Young, L.R.; William R Wilson, W.R. TECHNICAL REPORT CMU/SEI-2007-TR-012 ESC-TR-2007-012 CERT Program. 2007. Available online: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf (accessed on 17 September 2020).
54. CMMI Institute LLC. Over 1/2 of Cyber Professionals Expect a Cyber Attack within 12 Months. 2020. Available online: https://cmmiinstitute.com/products/cybermaturity (accessed on 17 September 2020).
55. CIS. CIS Controls® V7.1. 2019. Available online: https://www.cisecurity.org/controls/ (accessed on 17 September 2020).
56. Khosravi-Farmad, M.; Ghaemi-Bafghi, A. Bayesian Decision Network-Based Security Risk Management Framework. *J. Netw. Syst. Manag.* **2020**. [CrossRef]
57. Rea-Guaman, A.M.; Mejía, J.; San Feliu, T.; Calvo-Manzano, J.A. AVARCIBER: A framework for assessing cybersecurity risks. *Clust. Comput.* **2020**. [CrossRef]
58. Gordon, L.A.; Loeb, M.P.; Zhou, L. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *J. Cybersecur.* **2020**, *6*, tyaa005. [CrossRef]

59. Thomas, M. 13 IOT security companies you should know. 2019. Available online: https://builtin.com/internet-things/iot-security-companies-startups (accessed on 17 September 2020).
60. Hsu, C.-L.; Lin, J.C.-C. Exploring factors affecting the adoption of Internet of Things services. *J. Comput. Inf. Syst.* **2018**, *58*, 49–57. [CrossRef]
61. Das, R.; Gadre, A.; Zhang, S.; Kumar, S.; Moura, J.M.F. A Deep Learning Approach to IoT Authentication. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
62. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996. 1996. Available online: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996 (accessed on 17 September 2020).
63. U.S. Department of Health & Human Services. HITECH Act Enforcement Interim Final Rule. 2009. Available online: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (accessed on 17 September 2020).
64. US Congress. H.R.3985—Internet of Medical Things Resilience Partnership Act of 2017. 2017. Available online: https://www.congress.gov/bill/115th-congress/house-bill/3985/text?format=txt (accessed on 17 September 2020).
65. US Congress. S.734—Internet of Things Cybersecurity Improvement Act of 2019. 2019. Available online: https://www.congress.gov/bill/116th-congress/senate-bill/734/text?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+ (accessed on 17 September 2020).
66. European Union. General Data Protection Regulation GDPR. 2016. Available online: https://gdpr-info.eu/ (accessed on 17 September 2020).
67. European Union. The EU Cybersecurity Act. 2019. Available online: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (accessed on 17 September 2020).
68. Romero-Mariona, J. DITEC (DoD-Centric and Independent Technology Evaluation Capability): A process for testing security. In Proceedings of the 2014 IEEE Seventh International Conference on Software Testing, Verification and Validation Workshops, Cleveland, OH, USA, 31 March–4 April 2014; pp. 24–25.
69. ITU. Internet of Things Global Standards Initiative. 2015. Available online: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx#:~{}:text=The%20Internet%20of%20Things%20(IoT,interoperable%20information%20and%20communication%20technologies (accessed on 17 September 2020).
70. ISO. ISO/IEC JTC 1 Internet of Things (IoT) Preliminary Report 2014. 2014. Available online: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf (accessed on 17 September 2020).
71. ETSI. Cyber Security for Consumer Internet of Things. 2019. Available online: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accessed on 17 September 2020).
72. Esteves, J.; Ramalho, E.; de Haro, G. To Improve cybersecurity, think like a hacker. *MIT Sloan Manag. Rev.* **2017**, *58*, 71–77.
73. Shred-it. Security Tracker 2018. 2018. Available online: https://www.shredit.com/en-us/resource-center/original-research/security-tracker-2018 (accessed on 17 September 2020).
74. Jeremiah, P.; Samy, G.N.; Shanmugam, B.; Ponkoodalingam, K.; Perumal, S. Potential Measures to Enhance Information Security Compliance in the Healthcare Internet of Things. In *Recent Trends in Data Science and Soft Computing, Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018), Kuala Lumpur, Malaysia, 23–24 July 2018*; Saeed, F., Gazem, N., Mohammed, F., Busalim, A., Eds.; Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2019; Volume 843, p. 843.
75. Dorasamy, M.; Joanis, G.C.; Jiun, L.W.; Jambulingam, M.; Samsudin, R.; Cheng, N.J. Cybersecurity Issues among Working Youths in an IoT Environment: A design Thinking Process for Solution. In Proceedings of the 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, 2–3 December 2019; pp. 1–6.
76. Bodeau, D.; Graubart, R. Cyber prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness. *Tech. Rep.* **2017**. Available online: https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf (accessed on 17 September 2020).
77. Hildebrandt, M. Balance or trade-off? Online security technologies and fundamental rights. *Philos. Tech.* **2013**, *26*, 357–379. [CrossRef]

78. Loi, M.; Christen, M. Ethical Frameworks for Cybersecurity. In *The Ethics of Cybersecurity*; Christen, M., Gordijn, B., Loi, M., Eds.; The International Library of Ethics, Law and Technology Book Series; Springer: Cham, Switzerland, 2020; Volume 21, pp. 73–95.
79. Kuypers, M.; Maillart, T. Designing Organizations for Cyber Security Resilience. In Proceedings of the 2018 The Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, 18–19 June 2018; Available online: https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2016/09/WEIS_2018_paper_50.pdf (accessed on 17 September 2020).
80. Chakraborty, A.; Chandru, V.; Rao, M.R. A linear programming primer: From Fourier to Karmarkar. *Ann. Oper. Res.* **2020**, *287*, 593–616. [CrossRef]
81. Georgescu, T.-M.; Iancu, B.; Zurini, M. Named-entity-recognition-based automated system for diagnosing cybersecurity situations in IoT networks. *Sensors* **2019**, *19*, 3380. [CrossRef]
82. Boja, C.; Zamfiroiu, A.; Iancu, B.; Georgescu, T.M.; Cartas, C.; Toma, C. *Avant-Garde Technology Hub for Advanced Security—Technical Study*; Military Technical Academy: Bucharest, Romania, 2018.