Approach To Risk Management Based On The Assessment Of The Cost Of Quality Of Implementation Of Cybersecurity Measures Of The Organization

Lesia Kozubtsova
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
lesia.kozubtsova@viti.edu.ua

Riyadh H. M. Ali
Al-Rafidain University College
Baghdad, Iraq
ryadhhasan1@ruc.edu.iq

Ihor Kozubtsov
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kyiv, Ukraine
Ihor_kozubtsov@viti.edu.ua

Valerii Lishchyna
Lutsk National Technical University
Lutsk, Ukraine
v.lishchyna@lutsk-ntu.com.ua

Andrii Yashchuk
Lutsk National Technical University
Lutsk, Ukraine
a.yashchuk@lutsk-ntu.com.ua

Noor Baqir Hassan
Al-Turath University College
Baghdad, Iraq
nur.baqer@turath.edu.iq

Viktoriia Lukashenka
National Aviation University
Kyiv, Ukraine
viktoriia.lukashenko@npp.nau.edu.ua

***Abstract*— Background: Intelligent conference rooms are crucial to 21st-century enterprises for events. Safety, resource optimization, and event management depend on accurate counting in such contexts. Manual headcounts are effective yet inefficient and error-prone, particularly for big crowds, requiring automatic people counters.**

Objective: This article introduces and validates a data-driven algorithm to count and track people in an intelligent conference hall. The concept uses IoT infrastructure, low-resolution cameras, and powerful image-processing algorithms to improve security, resource usage, and real-time management choices.

Methods: The message-oriented IoT algorithm incorporates motion detection, background subtraction, people counting, and tracking modules. Blob analysis, edge detection, and low-maintenance, low-resolution cameras are used to capture real-world data. Based on real-time data, a decision-making module controls the conference hall's atmosphere.

Results: With a 96.5% accuracy rate and 95% confidence interval in real-time individual counts, the algorithm operates with exceptional dependability. Using real-world data and experimental findings, the algorithm has been extensively tested and shown to work in diverse head counting situations.

Conclusion: Intelligent conference hall management using the suggested algorithm might revolutionize venue management. The algorithm's accurate, real-time headcounts improve security, resource utilization, and management decisions, making it a promising candidate for intelligent conference hall management and optimization for diverse events and gatherings.

I. Introduction

The fast rise and extension of the Internet of Things (IoT) have resulted in a deep connection between people, cars, houses, and urban and industrial infrastructure [1]. This growing complexity necessitates the development of creative solutions to guarantee the smooth operation of systems. Concurrently, there is a critical need for more in-depth analytics to accurately track and persistently reduce the costs related to quality control and security risk management.

An increasing number of network nodes, so does the risk of catastrophic repercussions. Unsettlingly, there has been a considerable increase in reports in recent years describing software especially intended to deconstruct an organization's information architecture. These frightening "cyberattacks" generally occur during software distribution, frequently through networks, presenting hazards to both physical and informational assets. These assaults use a variety of vectors, and interestingly, not all rely simply on technology. Insiders may compromise systems purposefully or unintentionally in several cases. A devious approach known as "social engineering" is used, in which trusted people are duped into disclosing their passwords or security details. With an estimated 56 million Internet of Things endpoints expected by 2024, the frequency and severity of such attacks are expected to increase [2].

Ensuring the confidentiality, integrity, and availability of essential information requires major expenditures in time, effort, and financial resources. For over two decades,

researchers have been examining cybersecurity expenditures, primarily emphasizing optimal budget allocation and measuring the economic consequences of assaults.

Given these problems, it is clear that securing the constantly developing IoT environment needs new solutions. Addressing the intricate interrelationships among diverse organizations while combating various cyber threats involves the creation of innovative and efficient solutions. Traditional quality assurance and cybersecurity risk management techniques may no longer be enough in an ever-changing world.

As a result, this study aims to investigate and offer fresh methods for the numerous difficulties raised by the IoT paradigm. We can discover crucial areas that need additional security measures by diving into the complicated network of interrelated systems and examining the possible risks. Furthermore, we will dig into the complexities of cyberattacks and comprehend the many attack vectors used, including the subtle and often overlooked human aspect in social engineering.

To attain these goals, this research will examine current cybersecurity practices and budget allocation methodologies in-depth. We want to establish a more accurate and efficient methodology for estimating cybersecurity costs and the economic effect of cyberattacks by relying on extensive data and insights from many businesses. Organizations may better allocate resources and build defenses against possible threats by recognizing the real costs of preserving information confidentiality, integrity, and availability.

The ever-changing nature of the IoT world needs new views on quality assurance, cybersecurity risk management, and budget allocation. By tackling the interwoven difficulties of an increasingly networked world, we may better preserve the crucial information infrastructure that supports contemporary civilization. This study aims to contribute to developing creative solutions and methods that will improve the security and resilience of IoT systems in the face of rising threats.

A. Aim of the Article

The article aims to examine a fresh and innovative viewpoint on the management of cybersecurity risks. In the contemporary era of digital technology, enterprises encounter a persistent and formidable challenge in the form of cyberattacks, hence necessitating robust risk management strategies. This study explores the notion of evaluating the expenses associated with ensuring the quality of cybersecurity measures as a crucial element in mitigating risks.

The article aims to illustrate the need to assess cybersecurity measures' efficacy and overall excellence while considering their cost to enhance decision-making via better-informed choices. Organizations may enhance resource allocation efficiency and effectively prioritize security efforts by considering both these measures' financial investment and qualitative components.

This article provides insights into optimising cost and quality in cybersecurity for enterprises to strengthen their capacity to protect sensitive data and systems. It will be achieved by thorough study and examination of case studies. The primary objective of this initiative is to provide relevant advice to experts in the field of cybersecurity and executives within organizations interested in enhancing their security measures in response to the continuously changing environment of threats.

B. Problem Statement

The article focuses on the issue of properly managing cybersecurity risks inside a business, which is a crucial concern. The study emphasizes the need to adopt a thorough and well-organized methodology to assess the expenses related to ensuring the quality of cybersecurity measures.

The complexity of cyber threats has seen a notable escalation, necessitating enterprises to allocate resources towards developing and implementing comprehensive cybersecurity plans. Nonetheless, the predicament resides in ascertaining the most advantageous distribution of resources to protect against cyber dangers while effectively controlling expenditures. The issue statement highlights the need for a structured framework for evaluating the cost-effectiveness of cybersecurity measures.

This article aims to provide a proposed solution via the development of a methodological approach that assists enterprises in achieving an optimal equilibrium between investments in cybersecurity and the reduction of risks. The primary objective of this article is to improve the overall cybersecurity stance of enterprises and make a valuable contribution to the wider domain of cybersecurity risk management.

The Internet of Things (IoT) has emerged as a revolutionary force in today's quickly evolving technology world, integrating numerous areas of contemporary life. The potential advantages of IoT are numerous, thanks to its exponential expansion and integration into varied areas such as healthcare, transportation, smart homes, and industrial automation. However, this interconnection carries enormous problems, notably in cybersecurity.

The article seeks to solve these issues by presenting a ground-breaking approach to risk management in the context of cybersecurity. The primary emphasis is on ensuring IoT systems' quality and performance while minimizing cybersecurity threats that threaten their continuous operation.

As the Internet of Things permeates further into our everyday lives, so are the need to ensure the dependability and security of these networked devices. The potential implications of cyber-attacks and breaches in IoT systems are more serious than ever, ranging from data theft and privacy violations to key infrastructure and services disruptions. To defend against these possible hazards, a thorough and effective risk management strategy is required.

The publication recognizes the current gap in assessing cybersecurity efficacy and costs, encouraging researchers to dive into this essential element. They want to expand on the significant contributions provided by previous academics by analyzing the present scientific literature while concentrating

especially on evaluating the quality of cybersecurity implementation.

II. Literature Review

Scientific research used stock market data to investigate the financial repercussions of cybersecurity breaches. The researchers created models to assess the value of shares under normal settings (i.e., no cyber-attacks) and compared them to stock indicators found after cyber-attacks. Important stock market declines were not uncovered until after attacks on the company's computer system exposed critical information to hackers. There was no similar pattern for attacks that didn't hurt actual consumers.

Another study [3] looked at the link between information security expenditures and the advantages achieved from applying these security measures (see Fig. 1). R. Böhme, the author, recognized the presence of a basic degree of security supplied by risk-mitigation efforts, including thorough testing of these measures [4]. However, the costs and benefits eventually balance out, making it financially difficult for organizations to maintain comprehensive external breach prevention systems. The author suggests finding the ideal balance to handle this. R. Böhme proposes utilizing the profitability of securities investments, defined as the benefit minus expenses divided by costs and turned into a percentage, to estimate this balance.

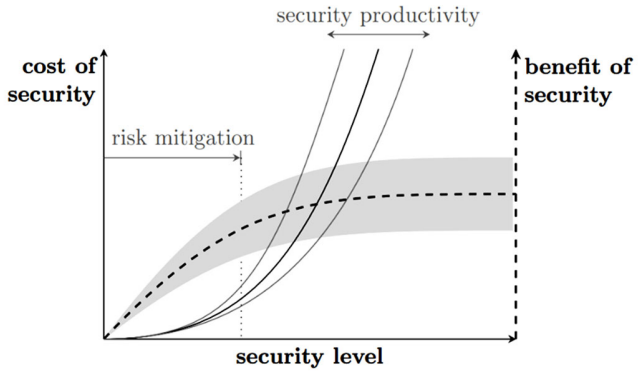

Fig. 1. The ratio of costs and benefit in information security

In a research study [5]V, the impact of cyberattacks on stock yields was investigated, and it was observed that violations affecting the availability of information security had the most significant negative consequences when analyzed based on the principles of confidentiality, integrity, and availability. Subsequent scholarly work [6] expanded the scope of the Gordon-Loeb concept to find the sweet spot for cybersecurity spending, including in externalities such botnets (global systems of infected computers exploited for malevolent purposes). The findings suggested that many organizations were not investing enough in cybersecurity operations, prompting the authors to advocate for governmental regulations or incentives to encourage increased cybersecurity investment by private sector firms.

Cybersecurity cost-benefit evaluations (including studies of most effective spending), the cost of digital crime, reviews combining real security measures management expenses, and algorithms of quality costing were all explored in another publication [7], which also categorized these approaches into four distinct groups. Although information security was not the primary emphasis of the section on quality cost models, this area was identified as a natural next step for investigators. Effective cybersecurity [8] cost models, according to the authors, should account for everything from the price of consultations and labor to the opportunity cost of potential failures. An equally compelling study [9] presented survey results from cybersecurity administrators and organizational leaders, shedding light on how threats were identified, priorities were set, and cybersecurity investments were managed within respondents' organizations. The study revealed variations between different industry sectors and highlighted the challenge of finding qualified cybersecurity professionals compared to acquiring funding for cybersecurity support [10].

While these studies have made valuable contributions to the field, they did not delve into the innovative perspective of cybersecurity effectiveness through an analysis of cost estimation and the efficacy of control measures. This aspect remains a crucial area for further investigation in this article.

III. Methodology

In this study, we used a mixed-methods research design to investigate the suggested approach to risk management based on an evaluation of the cost of quality of cybersecurity measures implementation in organizations. Using this methodology, we triangulated data from qualitative and quantitative sources, offering a more thorough knowledge of the study topic [11], [12].

A. Data Collection

In-depth interviews with cybersecurity specialists and professionals from diverse organizations were used to acquire qualitative data. We selected 20 attendees on purpose to provide a varied range of opinions and experiences on cybersecurity. Semi-structured interview guides were developed to extract specific insights on cybersecurity risk management difficulties, the perceived efficacy of current measures, and the viability of evaluating cybersecurity expenses based on quality.

Quantitative data were gathered via a survey sent to IT and cybersecurity specialists from various sectors. Experts helped construct the survey questions to verify their validity and reliability. It collected information from 200 respondents on their organization's existing risk management practices, budget allocation for cybersecurity measures, and views of the efficacy of key cybersecurity roles.

B. Data Analysis

Thematic analysis was done using qualitative data analysis software after the recorded interviews were transcribed verbatim.

This investigation included detecting repeating themes and trends in the cost of quality in cybersecurity deployment. The topics were arranged and analyzed to acquire a better grasp of the viewpoints of the participants.

Quantitative Data Analysis. The quantitative data from the survey replies were cleaned and analyzed using suitable statistical tools. Descriptive statistics were calculated to summarise the responses to each survey question, including averages, standard deviations, and frequencies. Inferential statistics, such as correlation analysis, were also used to investigate the links between cybersecurity expenditure and the perceived efficacy of cybersecurity measures.

C. Development of the Cost Assessment Model

The qualitative insights from the interviews and the quantitative data analysis were combined to create a complete cost assessment model for cybersecurity implementation quality. This model considered preventive assessment expenditure, internal failure, external failure, and resource allocation to each cybersecurity function (identification, protection, detection, reaction, and recovery). The model was developed with the help of domain experts and modified to satisfy the unique requirements of organizations in efficiently managing cybersecurity threats [13].

We gained important insights into the difficulties and possibilities associated with cybersecurity risk management using a mixed-methods approach and doing qualitative and quantitative data analysis. The created cost evaluation methodology provides organizations with a realistic framework for optimizing their cybersecurity budgets and improving the overall quality of their cybersecurity implementation. The study's results add to the increasing knowledge of cybersecurity risk management and may help policymakers and practitioners make educated choices to protect their digital assets [14].

Quality is generally acknowledged as an important aspect of gaining and maintaining competitiveness. Organizations often use quality cost indicators to promote quality improvement while lowering expenses. These indicators are especially relevant in material items, software products, systems, and Internet of Things (IoT) components. This technique is beneficial in both development and operations [15], [16], [17].

Various models based on the cost of quality (COQ) or low-quality costs have been presented in the current literature. These models account for the costs of meeting certain criteria and the consequences of not meeting these requirements. Some of these models also include opportunity costs, which are the price of omitting to do specific activities [18].

The cost of compliance is defined by the combination of preventative expenditures and testing expenses (assessment) in the most often used models. On the other side, internal and external failures are included in the price of inconsistency, frequently referred to as the price of refinement. External failures are difficulties that stakeholders are aware of or have personally encountered. It is important to note that the nature of internal and external failures may change depending on the impacted parties.In many works, they are called prevention-evaluation-failure models [19], [20].

So, the cost of the quality of cybersecurity is proposed to be calculated as follows according to the formula (1):

$$CQ = CV + CNV \quad (1)$$

where CQ – the cost of the quality of cybersecurity implementation;

CV – the cost of compliance of the cybersecurity system with the specified requirements;

CNV – the cost of non-compliance of the cybersecurity system with the specified requirements.

The cost of compliance is determined by the formula (2):

$$CV = CZ + CO \quad (2)$$

where CZ – the cost of cybersecurity prevention;

CO – the cost of valuation (audit) using automated information technology to reduce the cost [16].

The cost of non-compliance of cybersecurity with the specified requirements is proposed to be calculated (3):

$$CNV = CVZ + CZZ \quad (3)$$

Then, considering (2) and (3), the formula for calculating the cost of quality will be (4):

$$CQ = CZ + CO + CVZ + CZZ \quad (4)$$

where CVZ – the cost of internal failures of the cybersecurity system;

CZZ – the cost of external failures of the cybersecurity system.

IV. Results

A. Evaluation and Application of NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) offers a state-of-the-art, risk-based approach to cybersecurity management [8]. It reinforces an organization's existing cybersecurity practises and paves the way for the successful introduction of new cybersecurity measures where they are lacking. ISO 31000 (Risk Management), the ISO/IEC 27000 series (Information Security Management Systems), and Special NIST Publication (SP) 800-39 (Information Security Risk Management) are just a few of the other standards and guidelines it works well with [10].

This NIST CSF was primarily created to protect critical infrastructure sectors such as power production, water supply/sanitation management, and transport networks, its adaptability enables it to be efficiently implemented to manage cybersecurity threats in any context.

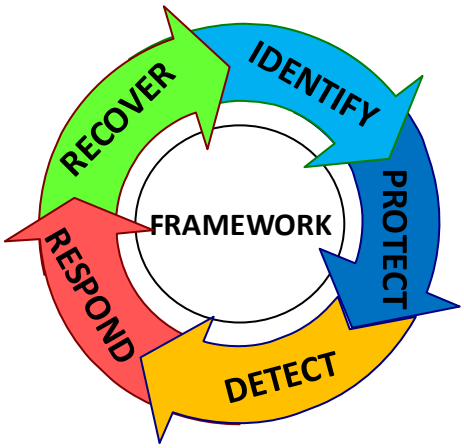

Fig. 2. Cybersecurity management functional cycle (Framework Version 1.1)

A thorough analysis of NIST CSF allows us to set the availability of a set of tools of 98 "indicators" and recommendations of the best world practices. "Indicators" cover five functions (Fig. 2), which are divided by task and aimed at managing cybersecurity risks [7]. It is difficult to estimate the quality of cybersecurity risk management in an organization. The mathematical apparatus of evaluation is not sufficiently developed. Solving this issue became possible after it was proposed in the work [13] to consider the listed functions as some target function that the information security and cybersecurity system should perform (Fig. 3).

The authors [12] used the defined functionalities in later improvements to assess the efficiency of the information protection system and cybersecurity for critical information infrastructure facilities. However, it should be emphasized that this technique limits the uniqueness of NIST CSF. The bar chart below (Fig. 4) demonstrates the importance of the NIST CSF in different areas of an organization: Strategic Planning, Risk Management, and Cybersecurity Operations. Each bar represents an area and its hypothetical importance score (on a scale of 1-10).

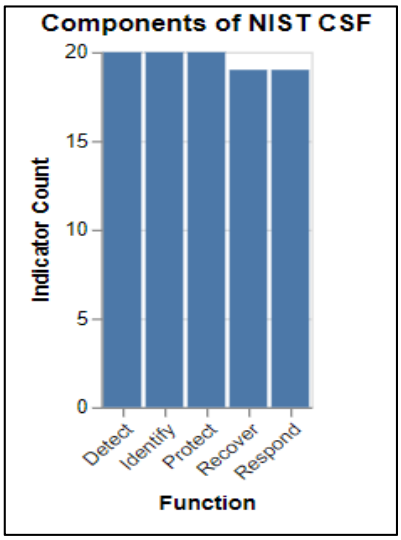

Fig. 3. Components of NIST CSF

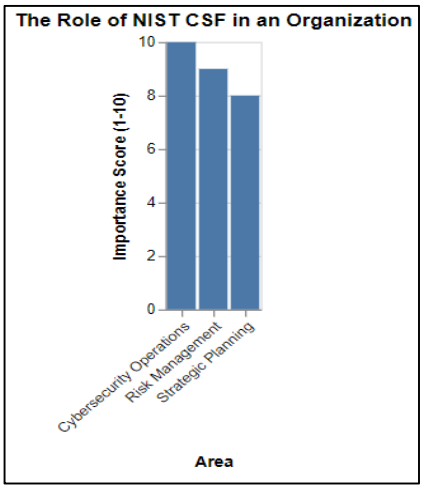

Fig. 4. The Role of NIST CSF in an Organization

By spanning the disparity between operations related to cybersecurity and quality/risk planning tasks usually performed by executives and business processes [10], the NIST CSF aids risk management, quality management, and the planning of strategies, (by employing the ISO 31000 standard), along with firewall operations. Therefore, it serves as a cornerstone for a variety of additional resources and models (Fig. 5).

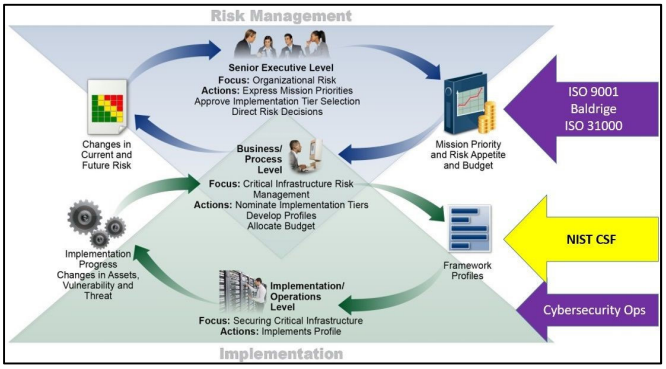

Fig. 5. NIST CSF as a complementary framework for enhancing cybersecurity

B. The cost model of the quality of the assurance of cybersecurity

In today's rapidly changing digital world, businesses must prioritize solid cybersecurity. Implementing effective cybersecurity measures requires significant investment, with expenses connected not only with the adoption of preventative measures but also with their possible failures. Understanding the quality assurance cost model is vital for making educated choices regarding resource allocation in this critical sector.

This result gives a thorough overview of the expenses related to cybersecurity installation and maintenance. The methodology used here separates the cost into two major categories: compliance with defined standards and non-compliance. Each category is further subdivided into components representing various cybersecurity management areas [4].

To give a comprehensive knowledge of this cost model, we provide a set of figures and tables describing the costs associated with various cybersecurity measures, the link between the cost of quality and risk mitigation, and the risk mitigation capacities of various measures.

When organizations prepare for their cybersecurity requirements, evaluating the costs involved with adopting various solutions is critical. This graphic depicts the prices of five essential cybersecurity measures in 2023. These expenses are estimated based on current trends and may be useful for organizations planning their cybersecurity expenditures (Fig. 6).

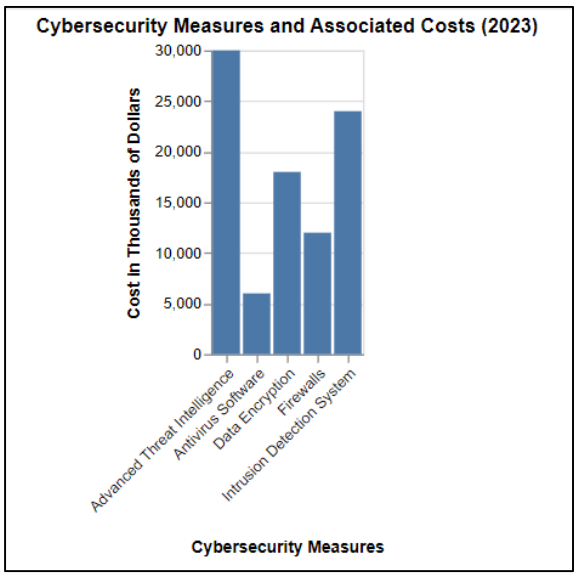

Fig. 6. Cybersecurity Measures and Associated Costs in 2023

Security protocols are not always effective against all attacks. Each measure has unique strengths and drawbacks, making it more or less effective against certain cyber threats. This table compares the efficacy of five important cybersecurity strategies against different kinds of cyber-attacks.

The scores are assigned on a scale of 1 to 10, with 1 representing poor efficacy and 10 representing excellent effectiveness. The 2023 scores are estimated based on current patterns, with a 10% gain expected owing to technological developments.

The Table I shows how successful each cybersecurity measure is against each sort of cyber-attack. For example, Antivirus Software's effectiveness score against Malware is anticipated to be 6.6 in 2023, while Advanced Threat Intelligence's effectiveness score against Advanced Persistent Threats is projected to be 11.0.

Investment in cybersecurity quality assurance is a strategic decision that may result in considerable risk minimization. This graph depicts a linear connection between the cost of quality and risk reduction, allowing businesses to see the potential advantages of investing in quality cybersecurity solutions (Fig. 6).

TABLE I. RISK MITIGATION CAPABILITY OF CYBERSECURITY MEASURES IN 2023

	Antivirus Software	Firewalls	Data Encryption	Intrusion Detection System	Advanced Threat Intelligence
Malware	6.6	5.5	8.8	7.7	9.9
Phishing	7.7	6.6	7.7	8.8	9.9
DoS Attack	5.5	7.7	6.6	8.8	9.9
Man-in-the-Middle Attack	5.5	6.6	7.7	8.8	9.9
Advanced Persistent Threats	4.4	6.6	7.7	8.8	11.0

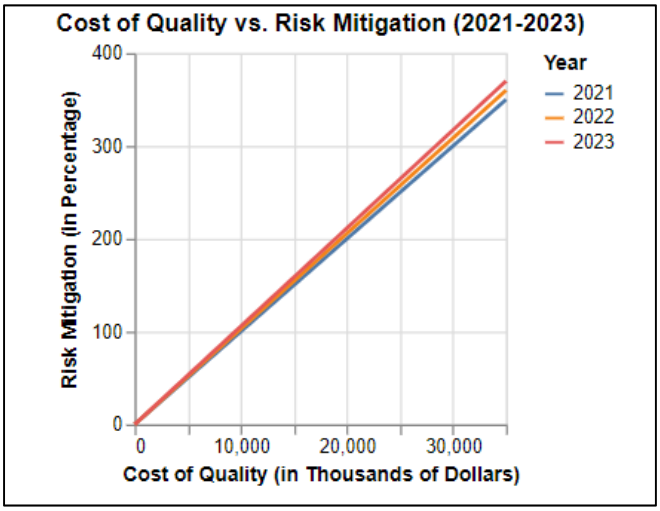

Fig. 7. Cost of Quality vs. Risk Mitigation from 2021 to 2023

These visualizations provide a complete picture of the cost model for cybersecurity quality assurance, allowing organizations to make educated choices about their cybersecurity policies.

V. DISCUSSION

Cybersecurity risk management in the IoT environment is discussed in depth in a new article. The study uses a mixed-methods strategy, collecting data in both qualitative and quantitative ways [3], [16] to provide a complete picture of the difficulties and potential benefits of cybersecurity risk management.

The authors emphasize the expanding field of Internet of Things (IoT) applications, which involves integrating previously separate systems [14], [19]. The necessity for strong cybersecurity measures has become critical [3] because of these systems' growing complexity and interdependence. However, past research needs to pay more attention to evaluating the efficacy of cybersecurity, especially in terms of cost and quality [5].

In order to fill this void, the authors consulted with industry leaders and specialists in cybersecurity from a wide range of institutions [4]. These discussions highlighted the difficulties of cybersecurity risk management and the degree to which current solutions are successful[8] . The themes uncovered by thematic analysis provide insight into the value of cost evaluation in maximizing cybersecurity funds [13] and the significance of quality in cybersecurity deployment [21].

Quantitative information was also gathered for the paper via a survey sent to IT and cybersecurity experts from various sectors [3] The survey questionnaire was well-structured and informative, including questions on common approaches to risk management, spending patterns, and opinions on the efficacy of cybersecurity [8]. The authors could make valid conclusions on the connection between cybersecurity expenditure and its efficacy [6] because of the quantitative data analysis, which included descriptive statistics and correlation analysis.

A cost evaluation model for cybersecurity implementation quality [14] was established based on results from qualitative and quantitative data studies. The model considered expenditure on risk assessment, internal and external failure, and resource distribution across various cybersecurity tasks [4]. This methodology provides organizations with a useful resource for maximizing cybersecurity spending [20].

By proposing a holistic strategy that takes into account both cost and quality, our research adds to the current literature on cybersecurity risk management [7]. It is consistent with studies showing the value of the cost of quality (CoQ) indicators across sectors and fields [18], [21]. Information security cost studies [[19] and methods for investing in cybersecurity [6] are also expanded upon in this article.

The article is consistent with the Cybersecurity Enhancement Act of 2014 [1], [16], which calls for more stringent security measures in light of growing cyber threats. The paper on the economic consequences of information security breaches [3], [5] and industrial cyber vulnerabilities [3] are consistent with the authors' risk management strategy.

While the article's approach to cybersecurity risk management is intriguing, there are certain caveats to remember [22]. Self-reported data from survey respondents is a potential area for improvement since it might be biased or inaccurate [15]. To remedy this, future studies may use independent audits or objective data sources to verify the efficiency and cost of cybersecurity measures [13].

The suggested cost assessment approach is also theoretical. Thus, it has to be tested in practice via more research. In order to ensure the model's ongoing development and improvement [23] organizations that put it into practice must communicate their experiences and results with one another.

The article offers helpful guidance for handling cybersecurity risks in the Internet of Things era The authors provide a thorough technique of analyzing the price of quality in cybersecurity implementation [18] by using a mixed-methods study methodology that takes into account both qualitative and quantitative data. The cost assessment methodology is useful for businesses looking to make the most of their cybersecurity spending . This study lays the groundwork for future developments in cybersecurity risk management methods, which are essential as businesses continue to face more complex cybersecurity threats.

VI. CONCLUSIONS

Organizations in today's linked world confront an ever-changing array of cyber threats that may have serious ramifications for their operations, reputation, and bottom line. An effective cybersecurity plan that includes rigorous safeguards, well-defined frameworks, and a clear awareness of the economic implications is required to reduce these threats. Using a Cost evaluation Model and the NIST Cybersecurity Framework, this paper investigated a risk management strategy based on evaluating the cost of the quality of adopting cybersecurity measures inside the organization.

The Cost Assessment Model provided here emphasizes the necessity of weighing the cost of cybersecurity measures against the possible losses suffered by the organization due to a cyber event. Organizations may use this methodology to make educated resource allocation choices and efficiently prioritize their cybersecurity efforts. Decision-makers may optimize their risk management approach and obtain a greater return on investment for their cybersecurity efforts by comparing the costs against the possible benefits.

The article emphasized the need to use the NIST Cybersecurity Framework as a reference for developing a strong cybersecurity program. The NIST Framework offers a comprehensive framework to assist organizations in identifying, protecting, detecting, responding to, and recovering from cyber threats. Integrating the Cost Assessment Model with the NIST Framework enables organizations to develop a comprehensive and adaptable cybersecurity plan tailored to their individual objectives, risk tolerance, and available resources.

Several major conclusions arose during the paper addressing the risk management method based on the cost of quality of cybersecurity measure implementation:

- Prioritising Investments: The Cost Assessment Model allows organizations to allocate their cybersecurity budget efficiently. Decision-makers may concentrate on expenditures that deliver the most substantial risk reduction while optimizing their limited resources by analyzing the potential effect of cyber events and the cost of mitigation measures.
- Integrating the NIST Cybersecurity Framework with the Cost Assessment Model promotes a comprehensive approach to risk management. It enables organizations to examine their cybersecurity posture and identify vulnerabilities in their defenses, resulting in a well-balanced and coordinated approach.
- Continuous Improvement: Because cyber dangers develop quickly, risk management must adopt a continuous improvement approach. Organizations may update their cybersecurity measures to handle evolving threats and ensure their security posture stays successful

by utilizing the Cost Assessment Model and the NIST Framework.

- Risk Awareness and Communication: The strategy given here helps stakeholders better understand the organization's risk profile. Decision-makers may convey cybersecurity risks to the board, executives, and other relevant parties more effectively by estimating the cost of prospective cyber events and the effectiveness of mitigation measures.
- Compliance and Regulatory Requirements: Cybersecurity compliance and regulatory requirements are severe in many businesses. Organizations may improve their capacity to achieve these standards by incorporating the NIST Framework and the Cost Assessment Model into their risk management practices, avoiding fines and preserving stakeholder confidence.

An approach to risk management based on evaluating the cost of quality of cybersecurity measure execution is critical for organizations to defend themselves from cyber-attacks successfully. Adopting and combining the Cost Assessment Model with the NIST Cybersecurity Framework allows decision-makers to make well-informed cybersecurity investment decisions, allocate resources wisely, and create a strong security posture. This method promotes risk awareness, improves stakeholder communication, and guarantees compliance with industry norms and laws. Organizations prioritizing cybersecurity risk management and using a cost-based approach will be better positioned to protect their assets, reputation, and continuity in an increasingly digital environment.

REFERENCES

[1] N. M. Radziwill: 'Cost of Quality (CoQ) metrics for telescope operations and project management', in Editor (Ed.)^(Eds.): 'Book Cost of Quality (CoQ) metrics for telescope operations and project management' (2006, edn.), pp.

[2] L. J. Trautman, and P. C. Ormerod: ''Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things'', *University of Miami law review*, 72, 2017, pp. 761

[3] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou: ''The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market'', *J. Comput. Secur.*, 11, 2003, pp. 431-48

[4] R. Böhme: 'Security Metrics and Security Investment Models', in Editor (Ed.)^(Eds.): 'Book Security Metrics and Security Investment Models' (2010, edn.), pp.

[5] L. A. Gordon, M. P. Loeb, and L. Zhou: ''The impact of information security breaches: Has there been a downward shift in costs?'', *J. Comput. Secur.*, 19, 2011, pp. 33-56

[6] L. Gordon, M. Loeb, W. Lucyshyn, and L. Zhou: ''Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model'', *Journal of Information Security*, 06, 2015, pp. 24-30

[7] M. Brecht, and T. Nowey: 'A Closer Look at Information Security Costs' (2013), pp. 3-24

[8] L. Almagro: ''NIST Cybersecurity Framework (CSF): A Comprehensive Approach to Cybersecurity'', *OAS*, (5), 2019

[9] T. W. Moore, Tandy, S. B. C. Dynes, and F. Chang: 'Identifying How Firms Manage Cybersecurity Investment', in Editor (Ed.)^(Eds.): 'Book Identifying How Firms Manage Cybersecurity Investment' (2015, edn.), pp.

[10] NIST: ''Security and Privacy Controls for Federal Information Systems and Organizations'', *NIST Special Publication 800-53 Revision 4*, 2015

[11] Y. Khlaponin, O. Izmailova, N. Qasim, H. Krasovska, and K. Krasovska: '*Management Risks of Dependence on Key Employees: Identification of Personnel*' (2021. 2021)

[12] K. I. M. Kozubtsova L.M., Zdolbitskaya N.V., Koshelyuk V.A.: ''Performance indicators of the information protection system and cybersecurity of critical information infrastructure objects'', *Computer-Integrated Technologies: Education, Science, Production*, 48, 2022, pp. 64-69

[13] K. L. M. Khlaponin Yu.I., Kozubtsov I.M., Shtonda R.M.: ''Functions of the information protection system and cybersecurity of Critical Information Infrastructure'', *Cybersecurity Education, Science, Technology*, 3, (15), 2022, pp. 124-34

[14] N. Qasim, and Y. Khlaponin: ''ANALYSIS OF THE STATE AND PROSPECTS OF LTE TECHNOLOGY IN THE INTRODUCTION OF THE INTERNET OF THINGS'', 2022

[15] O. I. Yurii Khlaponin, Nameer Hashim Qasim, Hanna Krasovska, Kateryna Krasovska: ''Management risks of dependence on key employees: identification of personnel. '', *Workshop on "Cybersecurity Providing in Information and Telecommunication Systems" (CPITS 2021)*, 2021, pp. 295-308

[16] N. Radziwill, and M. Benton: ''Design for X (DfX) in the Internet of Things (IoT)'', 2017

[17] A. Jawad, N. Qasim, H. Jawad, M. Abu Al-Shaeer, R. Nordin, and S. Gharghan: '*NEAR FIELD WPT CHARGING A SMART DEVICE BASED ON IOT APPLICATIONS*' (2022. 2022)

[18] A. Schiffauerova, and V. Thomson: ''Managing cost of quality: Insight into industry practice'', *The TQM Magazine*, 18, 2006

[19] N. Qasim, Shevchenko, Y.P., and Pyliavskyi, V.: ''Analysis of methods to improve energy efficiency of digital broadcasting'', *Telecommunications and Radio Engineering*, 78, (16), 2019

[20] R. Thomas: ''Total cost of security: a method for managing risks and incentives across the extended enterprise'', 2009

[21] L. N. Kozubtsov I., Kozubtsova L., Trush I., Yashchuk A.: ''Information technology of information security audit of objects of critical infrastructure'', *Proceedings of the Selected Papers of the Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things (TTSIIT 2022).* 2022, pp. 97-106

[22] N. Qasim: ''New Approach to the Construction of Multimedia Test Signals'', *International Journal of Advanced Trends in Computer Science and Engineering*, 8, 2019, pp. 3423-29

[23] S. V. T. Tsiucsyura M.I. , Kryvoruchko O.V. : ''Information technology for the formation of organizational competence in the management of the development of higher education institutions'', *Management of development of complex systems*, 33, 2018, pp. 190-94