Telecommunication Systems (2023) 84:533–548
https://doi.org/10.1007/s11235-023-01039-9

# RONSI: a framework for calculating return on network security investment

**Kousik Barik[1] · Sanjay Misra[2] · Luis Fernandez-Sanz[1] · Murat Koyuncu[3]**

Accepted: 25 June 2023 / Published online: 14 October 2023


**Abstract**
This competitive environment is rapidly driving technological modernization. Sophisticated cyber security attacks are expanding exponentially, inflicting reputation damage and financial and economic loss. Since security investments may take time to generate revenues, organizations need more time to convince top management to support them. Even though several ROSI techniques have been put out, they still need to address network-related infrastructure. By addressing gaps in existing techniques, this study delivers a comprehensive framework for calculating Return on Network Security Investment (RONSI). The proposed framework uses a statistical prediction model based on Bayes' theorem to calculate the RONSI. It is validated by Common Vulnerability Security Systems (CVSS) datasets and compared to existing studies. The results demonstrate that the annual loss is reduced to 75% with the proposed RONSI model after implementing a security strategy, and the proposed model is compared with existing studies. An organization can effectively justify investments in network-related infrastructure while enhancing its credibility and dependability in the cutthroat marketplace.

**Keywords** Return on network security investment (ROSI) · Cyberattack · Network security · Bayesian approach · Investment decisions

## 1 Introduction

Users connect to the internet because of the rapid development of internet technology. Unfortunately, cyber-attacks directly target both public and private entities [1]. Cyber-attacks are growing exponentially from internet-connected devices like mobile phones; laptops are essential to daily life. While a single attack may have little to no impact, repeated attacks can cost financial loss to an organization. Data breaches exceeded 17% in September 2021, the same as the previous year, according to ITRC data [2]. Data loss in 2021 includes Comcast 1.5 billion, Facebook 533 billion, LinkedIn 500 billion, and Bykea 400 billion [3]. 83 security incidents affecting 5,127,241 records were officially disclosed in February 2022 [4]. By 2025, cybercrime will reach 10.5 trillion annually [5]. To minimize losses, business organizations need proactive approaches to security measures.

The proliferation and sophistication of cyber-breaks render preventive efforts ineffective [6]. Cyber threat protection techniques by themselves cannot identify threats. Consequently, cyber events present two critical questions to private and public sector enterprises: What kind of cyber investment is the best, and how much money should be devoted to safeguarding corporate entities? They link to public education research well [7–9]. The value of detection and containment procedures is jeopardized by the reluctance of many organizations to discuss their exposures. For instance, an email is the first step in 75% of targeted attacks; In 86% of organizations, users try to link to fraudulent websites, and 86% of attacks aim to bring in money [10]. Further, some businesses spend six months than necessary to discover a data breach [11].

The network architecture of a business may appeal to dishonest competitors. There have been known cyber-attacks on these systems, which have disrupted customer service

✉ Sanjay Misra
sanjay.misra@ife.no

Kousik Barik
kousik.kousik@edu.uah.es

[1] Department of Computer Science, University of Alcala, Madrid, Spain

[2] Department of Applied Data Science, Institute for Energy Technology, Halden, Norway

[3] Department of Information System Engineering, Atilim University, Ankara, Turkey

and cost the corporation money [12]. A corporate network can be attacked for several reasons, from employees' careless online behaviour to a delay in patching vulnerabilities [13]. The under-investment and lifetime management of cyber security investments presents additional challenges for enterprises. Before making a financial choice, senior management wants to support the investment concerning returns. The effects of security breaches across the entire organization are what they are worried about, not the security apparatus. Educating the board about the effects of crucial network infrastructures is a massive task for the security manager. Funding security does not equate to financial advantages but can significantly reduce corporate losses [14]. The under-investment and lifetime management of cyber security investments presents additional challenges for enterprises. Before making a financial choice, senior management wants to support the investment concerning returns. The effects of security breaches across the entire organization are what they are worried about, not the security apparatus. Educating the board about the effects of crucial network infrastructures is a considerable task for the security manager. Funding security does not equate to financial advantages but can significantly reduce corporate losses.

Different ROSI techniques support making decisions; however, cyber security still has challenges [14]. Existing frameworks do not estimate the likelihood of Specific exposure. Employee exposure and experience, instead of attack probability, determine an attack. Since businesses frequently get mixed results under the same circumstances, it is difficult to accurately estimate risk using the same methods [15]. Further, conventional methods enable concerned professionals to approximate budget advantages to a particular situation.

Investments in network security can either directly or indirectly shield essential assets from various threats. Maintaining a complete view of the network security budget is crucial for defence against various attacks. Several studies have been conducted on calculating ROSI, but only a few on computing RONSI. We developed a framework to compute ROSI in network systems and calculate the impact of an attack on essential network resources throughout the enterprise. With a g great certainty, the likelihood of a cyberattack is estimated on network resources using the Bayesian theorem [16]. The significant contribution of the work is as follows.

1. Instead of approximation and user experience, the traditional approach of computing return on investment, the proposed Return on Network Security Investment (RONSI), is based on the Bayesian theorem.
2. To validate the proposed RONSI framework, the CVSS dataset, two scenarios, and a comparison to prior work are utilized.
3. The findings demonstrate that the yearly loss without applying a security plan is relatively significant ($7548). The loss is decreased to $1887 using the analytical technique to calculate the RONSI.
4. An organization can persuasively explain investments in network-related infrastructure using the proposed RONSI framework, which promotes confidence, trust, and reputation.

The remaining paper is formulated as follows. The related works and the current ROSI methodologies are discussed in Sect. 2. A proposed technique for RONSI computation is illustrated in Sect. 3, which facilitates senior management to justify investment decisions for network systems. The evaluation of the framework and the comparison with existing studies are conferred in Sect. 4. The discussion and the limitations of the work are presented in Sect. 5. Finally, the paper is concluded in Sect. 6 with the future research direction.

## 2 Related works

In this section, the existing ROSI frameworks are studied, deviated, and analyzed to demonstrate the most valuable techniques for developing an enhanced ROSI framework [17]. The NIST article [18] described the evaluation process for initiatives ROI, and the ENSA study [19] designed a ROSI metric using risk elements. Despite this, there are some restrictions in the report. Since the computation is based on static data, a particular threat may impact assets. Attack maps and Bayesian networks are combined in the study to show how cyber threats can be misunderstood [20]. Bistarelli et al. [21] evaluated the information technology security budget, employed defense trees, and placed countermeasures on each leaf. They determine the defenders' return on investment, security benefit, and single and annual loss probabilities. To evaluate attack strategies and preventive security techniques, Roy et al. [22] provided trees of defense in depth. Attack-countermeasure trees and prevention techniques, such as detection and mitigation, are included on each node.

Ji et al. [23] proposed trees of defence countermeasures, like identification and mitigation, on each node. The graphical security models evaluate network-based protection in terms of success or failure. A list of countermeasures can be used to prioritize security measures. Shawn [27] presented a security attribute-based technique that weighs potential investments against one another to choose the best investment. The model produces quantitative cost estimates but only calculates annual losses. Pontes et al. [28] proposed a model for calculating ROSI based on the Fibonacci sequence. It is possible to acquire security-related notifications, but they do not address the likelihood of the events they concern.

Aguiar et al. [29] presented a survey technique that underlined the importance of analysis using ROSI and estimations despite the lack of mathematical processes. Huang et al. [30] discussed the relationship between security spending and hazards while disseminating health information based on economic studies. The research employed a network-based methodology to analyze the financial considerations when investing. The proposed model uses the prior matching returns on security investment ideas. Using game theory, Yonge et al. [31] calculated security investments for carefully planned affiliate invasions. According to the findings, the amount spent on security should rise in direct correlation with the probability of lost gains, and collective investments can boost security while reducing expenses. Sonnenreich et al. [32], based on past knowledge, interviews, and assumptions, a method for assessing return on investment was proposed.

Fielder et al. [33] suggested a choice of three paths, and a combination of game theory and combinatorial optimization determines their viability in the investment decision. Yaqoob et al. [34] presented framework organizations emphasizing security that can use to calculate Bayesian ROSI. Despite providing a thorough mathematical analysis to calculate ROI and annual loss, the authors of this paper place a disproportionate amount of emphasis on the recovered CVVS dataset while mostly ignoring the penetration test findings. Skoufis et al. [44] proposed a techno-economic model to assess the project's cost viability via the prism of three possible migration routes.

Mamane et al. [45] presented a multi-criteria scheduler for 5G enhanced Mobile Broad Band (eMBB) communications transmission in a busy metropolitan environment. The method combines perceptron weight management with weighted sum multi-objective optimization employed in neural networks. Eswaran et al. [46] covered private 5G networks, deployment scenarios, spectrum considerations, and security issues. Vajanapoom et al. [47] presented a risk-based method for designing resilient networks. The fundamental design challenge is allocating funds for implementing a survivability approach in various network segments based on risk management, given a functioning network and a fixed budget. Kliks et al. [48] summarised discussions between scientific researchers and network device builders to determine a model's most likely effective operation in such a complex network environment. In cooperation with a skilled network architect, these suggestions were created. Gardikis et al. [49] examined how Software Defined Networking (SDN) as well as Network Functions Virtualisation (NFV) technologies might be applied to satcom platforms and identified. They identified and difficulties of integrating satellite infrastructures into future software-based networks. Zghaibeh et al. [50] proposed a lottery-based pricing system to improve the degree of sharing in peer-to-peer (P2P) networks and aid in the spread of more objects. A comparison of the existing ROSI frameworks is illustrated in Table 1. This study further aids in developing an enhanced RONSI framework by covering the gaps in the existing study.

## 3 The proposed framework of return on network security investment

This section proposes a redesigned ROSI framework, return on network security investment (RONSI), based on conventional ROSI methodologies to encourage monetary investments in network security**.** It is assumed that an organization's network would regularly receive patches from a cybersecurity vendor. With justification, our framework and method for estimating investment in network systems estimate the best methods. Figure 1 depicts the eight crucial phases of the proposed framework.

Identification of assets is the first phase. In an organization, there may be thousands of networks and related resources. Identification of assets and network inventory preparation is a thus crucial process. The classification of network assets is the next phase. Finally, the worth of an asset is determined by its severity, which also activates all of the organization's critical network assets. The third phase of the framework includes a vulnerability scan to look for weaknesses. A listing of vulnerabilities found by internal and external experts using the tool and their subject-matter expertise is produced by the framework's fourth phase, which involves internal and external penetration testing. Bayes' statistical theorem determines the probability of a connected threat in the fifth phase [20]. An invasion's probability is determined using datasets derived from actual cases [35]. Besides, if the vulnerability is exploited, the annual loss is calculated. By mapping the defects, the sixth phase documents potential defences to reduce the risks. It maps the significance of preventative countermeasures to align with the organization's business objectives and priorities. In the next phase, the cost–benefit analysis is determined. The final phase offers practical RONSI recommendations. The RONSI methodology predicts the likelihood of an attack on all critical network resources within an organization using a vulnerability scan report as input, validating the model. The model's practical importance can only be widely applied with a validation procedure. Using a dataset comprised of CVSS results from a vulnerability assessment and threat modelling, the proposed method can predict the frequency of attacks on an organization's critical network assets. To fully comprehend the phases of the proposed framework, this study combines methods for conducting threat investigations and attack mitigation strategies described in [36].

**Table 1** Study of existing approaches

| Title | Techniques | Observations | Gap |
|---|---|---|---|
| The ROI Initiative Draft [18] | ROI | The research provided the basic approach but did not offer particular information to show the effect | It may be difficult to accurately compare ROIs since certain investments will take longer to turn a profit than others, and ROI does not account for the time worth of money |
| ENSA [19] | Cost–benefit study | Cost projections and evaluation information should have been included in the study | A cost–benefit analysis could overlook significant monetary considerations, including inflation, interest rates, fluctuating cash flows, and the present value of money |
| Calculating return on security[21] | Defence trees | The method disregards computer problem instances | The organizations' general reluctance to share attack information with the public because of the potential harm to their image, it may be difficult to quantify the impact of an attack |
| The optimal security investment [22] | Attack trees | Impact analysis and vulnerability analysis results are not considered in the study | Despite not addressing model scalability difficulties, dynamic intrusion response |
| The cybersecurity analysis for cyber-physical systems [23] | Attack defense trees | The study did not consider asset identification based on practical implementation or vulnerability assessment, so the study emphasized calculating attack costs, ROI, and impact | Defenders should focus on concerns related to potential assaults that hackers can use maliciously to undermine network security while discovering system vulnerabilities |
| The security investment analysis [25] | T-HARM | This approach dealt with patterns while utilizing data | If the network is dynamic, it is challenging to analyze such investments |
| Cost–benefit evaluation based on security [27] | Cost–benefit study | Financial information and cost estimations are not evaluated in the study | Assessing security technology without considering an organization's information system environment is difficult |
| The ROSI calculation framework uses risk management. [28] | Fibonacci sequence | This study does not consider the risk management framework | Many traders have difficulty understanding the findings due to the intricacy of the data for reading |
| The optimal security investment in healthcare [30] | Economic analysis | Instead of using actual data, the study makes use of mathematical models that are based on hypotheses | It is predicated on the notion that rational economic actors and only economic equilibrium exist |
| Using decision support systems, invest in cybersecurity [32] | Game Theory, Combinatorial Optimization, and Hybrid approach | Practicing the techniques suggested in this study in organizations is challenging | That we could enter a Nash equilibrium in certain circumstances cannot be explained by it |
| Framework for calculating ROSI [33] | Bayesian approach | The study focused on annual loss estimation using CVVS data, ROI calculation, and vulnerability assessment as inputs, but it lacked live data and penetration test report specifics | There is no way to build a network from widely acknowledged data |

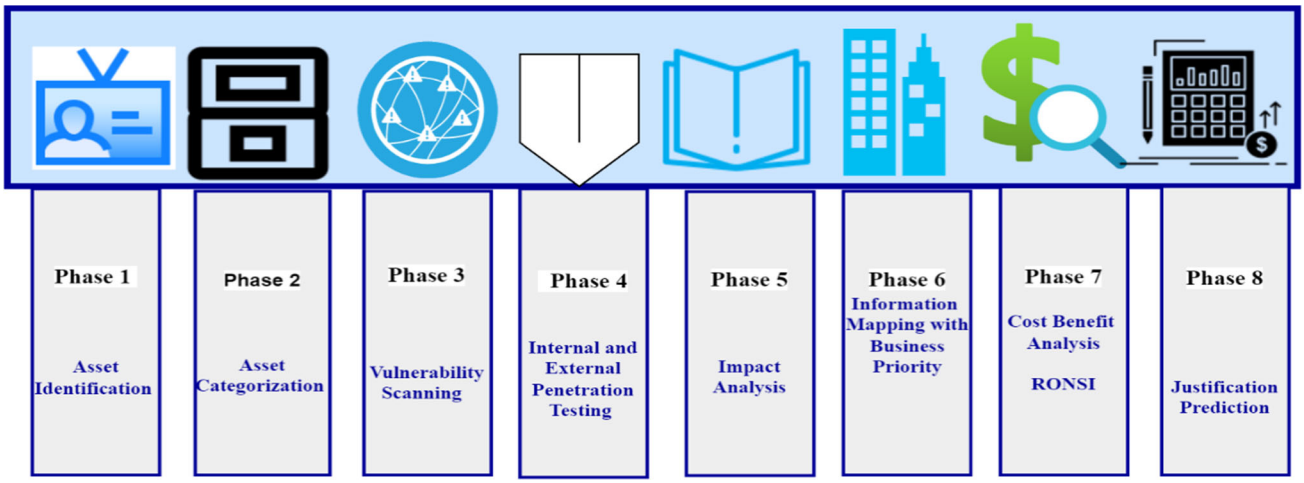


**Fig. 1** Proposed RONSI framework

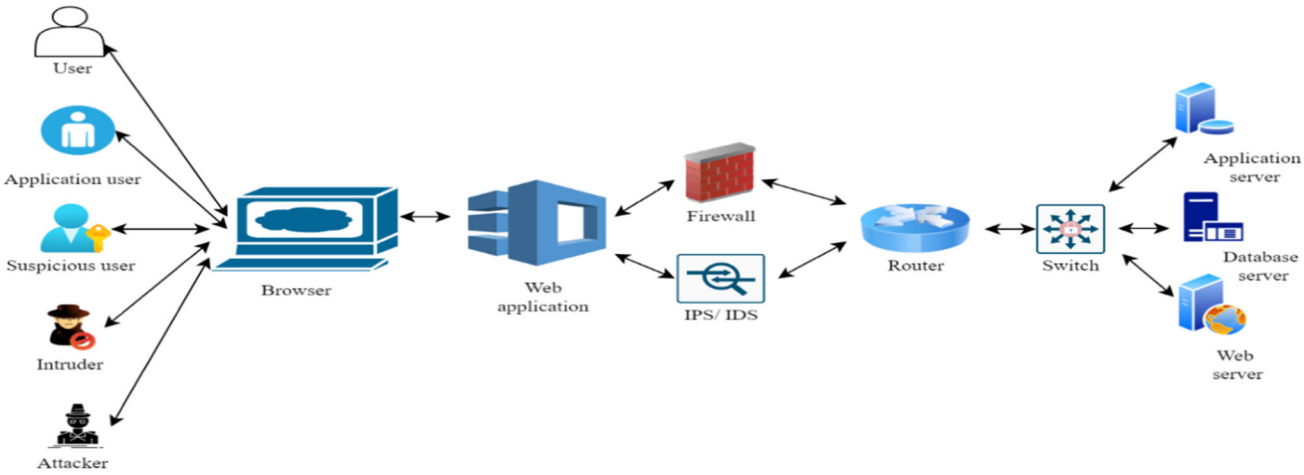


**Fig. 2** The context for penetration testing case

A hypothetical penetration testing scenario has been used as the test case in Fig. 2 to comprehend the phases of the proposed framework. A secure web application running over the internet is available. Firewalls, routers, switches, and intrusion detection systems verify user credentials before granting them access to restricted resources. The various invaders and attackers flood the network with traffic, implant malware, and monitor user activities like successful and unsuccessful logins to gather information on the system's operation. This process investigated significant assets, accompanying exposures, and related hazards. The countermeasures are examined, and RONSI is calculated using this analysis. The sections that follow each phase's components are illustrated.

### 3.1 Phase 1: asset identification

To purchase connected vital assets that could significantly impact the business if compromised. Identifying networks and other related assets in operating the business is crucial at this point. The ISO 27001 Framework is applied [38]. Table 2 illustrates the asset identification step of our method.

### 3.2 Phase 2: asset categorization

This step determines the criticality of assets in terms of confidentiality (C), integrity (I), and availability (A) using Eq. 1.

$$\text{Criticality} = C + I + A \tag{1}$$

C, A have, and I value ranging from 1 to 5. The higher critical value denotes the asset's need for critical protection. We have labeled the router, firewall, IDS, and database server as critical assets in the diagram, as shown in Table 1. The monetary cost of assets can be calculated using Eq. 2.

$$\text{Monetary value} = \text{Critical value} \times \text{Physical cost of asset} \tag{2}$$

**Table 2** Asset recognition

| Asset identification | C | I | A | Criticality |
|---|---|---|---|---|
| Switch | 4.0 | 2.0 | 4.0 | 10.0 |
| Firewall | 5.0 | 3.0 | 5 | 13.0 |
| IDS | 5.0 | 4.0 | 5.0 | 14.0 |
| Nodes | 4.0 | 3.0 | 1.0 | 8.0 |
| Web Server | 4.0 | 3.0 | 4.0 | 11.0 |
| Database Server | 5.0 | 5.0 | 3.0 | 13.0 |
| Application Server | 3.0 | 3.0 | 3.0 | 9.0 |
| Router | 5.0 | 4.0 | 5.0 | 14.0 |

### 3.3 Phase 3: vulnerability scanning

This stage locates user privacy occurrences, also known as vulnerabilities [39]. It can be accomplished using technologies for protection, readily available resources, skilled security professionals, and advisory services. Figure 3 displays how traffic flooding, scanning, and the injection of malicious software in the given context might cause DDoS and information theft attacks. The man in the middle, phishing and getting access, is the assault target. The three methods used are user action, injection, and input verification.

This step outlines all operational and security procedures and system configuration flaws that could lead to successful security violations, as shown in scenario 1. In the hypothetical situation, DDoS assaults are simulated, and systems are tested by being inundated with network traffic. Attackers looking to steal information employ numerous systems, including servers, routers, firewalls, intrusion detection systems, and user behaviour, to uncover gaps in the infrastructure. The attacker gathers relevant data. Table 3 illustrates the target, tactics, and attack simulation details.

**Table 3** Simulation of attack

| | |
|---|---|
| Attack target | Man in the middle, phishing, and gaining access |
| Techniques | Verifying input, injecting malware, and user activity |
| Attack vectors | DDoS, theft of information |

### 3.4 Phase 4: penetration testing

Vulnerability scanning warns organizations of their code's pre-existing defects. Penetration tests exploit a system's exposures to determine whether unauthorized entry or other adversary action is achievable and which weaknesses jeopardize the application. Penetration testing is carried out both internally and externally at this phase. Internal penetration testing is carried out inside a company while considering the surroundings. External penetration testing, on the other hand, is carried out by a different organization. Figure 3 represents the goal: to identify open ports that should not be utilized,

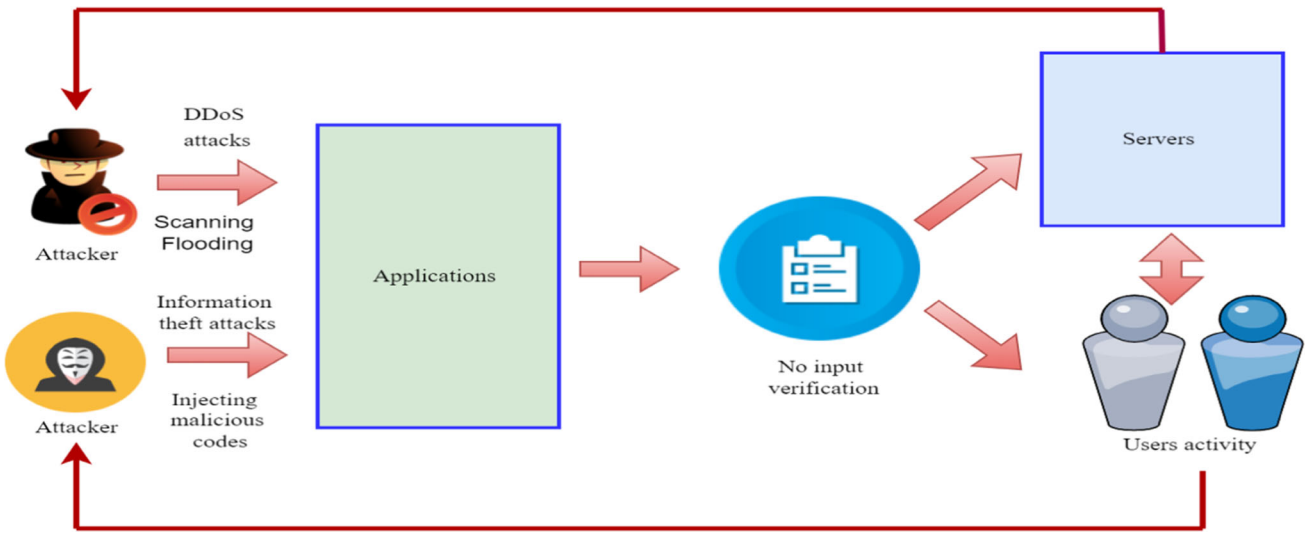


**Fig. 3** Example scenario of penetration testing

**Table 4** Report on penetration testing

| Asset details | Unwanted ports open | Vulnerable running service | Updated patches not applied |
|---|---|---|---|
| Router | 1.0 | 1.0 | 1.0 |
| Application server | 3.0 | 1.0 | 2.0 |
| Database server | 4.0 | 2.0 | 1.0 |
| Web server | 5.0 | 3.0 | 3.0 |

active apps that can be attacked, and the status of brings with it several updates and threats to the program and systems.

Figure 3 depicts how to attack modelling using a quantitative design analysis method to identify pertinent weaknesses early in the design process. Such techniques offer comprehensive information on how to attack a specific application or system by identifying critical data flows, vulnerabilities, and access points, as illustrated in Figure and a penetration testing report exhibited in Table 4.

Input verification contributes to up to 65% of attacks, according to vulnerability and penetration scanning, which reveals that unnecessary network ports, operating services, and new patches are not deployed. According to a scan, user activity and the introduction of malware account for 25% and 10% of online application vulnerabilities, respectively. A scan shows that because of unintentional open ports in networks, attackers can delay network activity and consume large amounts of bandwidth. The events' exemplification could result in severe financial and identity loss if realized.

### 3.5 Phase 5: impact analysis

This phase estimates the likelihood and consequences of an effective violation concerning the asset's severity. The limitation of the current approaches is that since they rely on the employee's knowledge, assessments of the chance that a threat will materialize cannot make an objective claim. As a result, different values will be obtained using the same methodology when RONSI is calculated under identical conditions. The proposed methodology overcomes these constraints by including a robust statistical prediction model based on the Bayesian theorem to systematically analyze the likelihood of assaults on network systems [34]. The dataset includes the following components of the fictitious scenario that assisted in foreseeing the threat's appearance.

For specific servers, the number of unpatched and known vulnerabilities.

- Criticality of devices in terms of ratings.
- The vulnerabilities disclosure rate.

The Bayesian theorem explains how to calculate the odds that the general population will test and accept a sample's hypotheses. There are many advantages to applying mathematical procedures and uncertainty estimates correctly. The Bayesian probability is calculated using Eq. 3.

$$P(A|B)\frac{P(A) * P(A|B)}{P(B) + P(A^{\sim}|B) * P(A^{\sim})} \tag{3}$$

A and B are events.

P(A|B) give the probability that A will happen given B.

P(B) demonstrates the probability that event B will take place.

P(A˜) shows the probability that event A would not happen.

P (A˜|B) denotes the absence of the event B with the conditional probability.

The likelihood in the given scenarios with the support of some prior statistics. The Bayesian approach is practical and only responds to some individual estimates. Uncertainty in the prophecies is logically confounded by a trustworthy predictive measure [41]. In the sample, using a web server to launch a DDoS assault that displays all the files in a requested directory but leaves out the default base file to gain access, introduce malware, or provoke attacks. Attack data shows that the input verification method changes 35% of events. Malware injection allows for unauthorized access to 45% of systems, which are then attacked by opening unauthorized network ports, while user login-related problems attack 20% of systems.

In contrast to attacks that steal information, 40% of systems are hacked because of problems with input validation, 50% because of problems getting access through malware injection, and 10% because of human activity. According to the findings of the network scans, which were previously detailed in Sect. 2, there is a 65%, 25%, and 10% likelihood that an asset will be vulnerable to penetration testing, input verification, malware insertion, and user activity. How likely are DDoS and data heist attempts to hit our system due to these flaws? The likelihood of a DDoS attack and the likelihood of data theft is calculated using Eq. 4.

P(A) = possibility that input verification was not thorough enough.

P(B) = Possibility of introducing malware.

P(C) = Potential for user activity.

P (A|D) = likelihood of a DDoS attack because of inadequate input verification.

P(D|B) = DDoS likelihood in the event that the input verification phase is skipped.

P (D|P) = likelihood of DDoS should problems with user activity continue.

$$P(A|D) = \frac{P(A) * P(D|A)}{P(A)*P(D|A) + P(B)*P(D|B) + P(C) * P(D|C) + P(D^{\sim}|A)*P(A^{\sim})} = \frac{0.35*0.65}{0.35*0.65 + 0.50*0.25 + 0.10*0.10 + 0.35*0.60} = 0.398 \quad (4)$$

Similar estimates are made for the likelihood that inserting malicious code will result in a DDoS attack using Eq. 5.

P(A) = Probability of insufficiency of input verification.

P(B) = likelihood of introducing malware.

P(C) = likelihood of user activity.

P(A|D) = likelihood of a DDoS attack due to inadequate input verification.

P (D|B) = DDoS likelihood in the event that the input verification phase is skipped.

P (D|P) = likelihood of DDoS should problems with user activity continue.

As a result of input verification, we estimate the probability of information theft.

P(A) = likelihood of inadequate input verification.

P(B) = likelihood of introducing malware.

P(C) = likelihood of user activity.

P(A|D) = likelihood of information theft owing to inadequate input verification.

P(D|B) = The likelihood of information theft in the case of the input verification process is disregarded.

P(D|U) = Probability of information theft in the event of malware injection.

$$P(A|D) = \frac{P(A) * P(D|A)}{P(A) * P(D|A) + P(B) * P(D|B) + P(C) * P(D|C) + P(D^{\sim}|A) * P(A^{\sim})} = \frac{0.50 * 0.25}{0.50 * 0.25 + 0.40 * 0.65 + 0.10 * 0.10 + 0.50 * 0.75} = 0.162 \quad (5)$$

Similarly, Eq. 5 determines the likelihood that a DDOS attack would occur due to a code execution vulnerability. Therefore, the earlier method is used to evaluate the risk that a DDoS attack may happen due to user behaviour.

P(A) = likelihood of inadequate input verification.

P(B) = likelihood of introducing malware.

P(C) = likelihood of user activity.

P(A|D) = likelihood of a DDoS attack due to inadequate input verification.

P(D|B) = likelihood of a DDoS attack should the input validation process go unchecked.

P(D|P) = likelihood of DDoS should problems with user activity continue.

$$= \frac{0.10 * 0.10}{0.10 * 0.10 + 0.40 * 0.65 + 0.50 * 0.10 + 0.90 * 0.90} = 0.0085$$

By adding up specific vulnerabilities aimed at the successful attack realization, the chance of an information theft assault can be estimated.

$$\text{Probability of attack} = 0.398 + 0.162 + 0.0085 = 0.568$$

P(D|P) = Probability of information theft in the event that user activity problems continue.

$$= \frac{0.40 * 0.65}{0.40 * 0.65 + 0.25 * 0.50 + 0.10 * 0.10 + 0.60 * 0.60} = 0.344$$

Calculations are made to determine how likely it is that information will be stolen as a result of malware injection.

P(A) = likelihood of inadequate input verification.

P(B) = likelihood of introducing malware.

P(C) = likelihood of user activity.

P(A|D) = likelihood of information theft owing to inadequate input verification.

P(D|B) = likelihood of information theft owing to inadequate input verification.

P(D|U) = likelihood of information theft in the event of malware injection.

P(D|P) = likelihood of information theft should user activity issues persist.

$$= \frac{0.10 * 0.10}{0.10 * 0.10 + 0.40 * 0.65 + 0.25 * 0.40 + 0.90 * 0.90} = 0.0084$$

**Table 5** The DDoS attack's effects

| Inventory | Exposure factor | Asset value ($) | Recovery cost($) |
|---|---|---|---|
| Database server | 65/100 | 4000 | 628 |
| Firewall | 25/100 | 3750 | 560 |
| Router | 25/100 | 2500 | 375 |

The likelihood of an information theft attack by user behaviour is calculated using the earlier method.

P(A) = likelihood of inadequate input verification.

P(B) = likelihood of introducing malware.

P(C) = likelihood of user activity.

P(A|D) = likelihood of information theft owing to inadequate input verification.

P(D|B) = The likelihood of information theft in the case of the input verification process is disregarded.

P(D|U) = Probability of information theft in the event of malware injection.

P(D|P) = Probability of information theft in the event that user activity problems continue.

$$= \frac{0.25 * 0.40}{0.25 * 0.40 + 0.40 * 0.65 + 0.10 * 0.10 + 0.75 * 0.90}$$
$$= 0.0956$$

It is feasible to calculate the probability of information theft or intrusion by compiling all of the vulnerabilities that led to assault realization.

$$Attack\ \ probability = 0.344 + 0.0084 + 0.0956 = 0.448$$

According to information in Table 5, three key assets—a router, a firewall, and a database server—make up the presented scenario's total number of DDoS attack losses ($). The following calculation can be used in the impact analysis [32] to determine the likely loss resulting from realizing significant asset risks using Eq. 6.

$$\text{Impact} = \sum_{a=1}^{n} \text{expose factor}_a * \text{value of asset}_a + \text{recovery cost}_a \quad (6)$$

where a = number of assets;$recoverycost_a$ is the price of recovery to restore an item to its initial condition.

$$\text{Impact} = \sum_{a=1}^{3} (25/100 * 2500 + 375) + (25/100 * 3750 + 560) + (65/100 * 4000 + 628)$$

**Table 6** Impact information on the information theft attack

| Inventory | Exposure factor | Asset value($) | Recovery cost($) |
|---|---|---|---|
| IDS | 40/100 | 3125 | 500 |
| Web Server | 50/100 | 1250 | 125 |
| Database Server | 50/100 | 4000 | 625 |
| Firewall | 40/100 | 3750 | 560 |
| Database Server | 50/100 | 4000 | 625 |
| Router | 40/100 | 2500 | 375 |

$$= \$1000 + \$1498 + \$3228 = \$5726$$

This economic loss ($) in the scenario that is being presented is calculated using the information in Table 6 [34]; there are six essential resources: a firewall, router, web server, database server, and application server.

$$\begin{aligned}\text{Impact} = \sum_{a=1}^{6} &(40/100 * 2500 + 375) \\ &+ (40/100 * 3750 + 560) \\ &+ (40/100 * 3125 + 500) \\ &+ (50/100 * 1250 + 125) \\ &+ (50/100 * 4000 + 625) \\ &+ (50/100 * 1560 + 250) \\ &= \$1375 + \$2060 + \$1750 + \$750 \\ &+ \$2625 + \$1030 = \$9590\end{aligned}$$

Equation 7 can be used to compute annual loss.

$$Annualloss = Impact * likehood \quad (7)$$

The annual loss due to DDoS attacks ($) is

$$\text{Annual loss} = 5726 \times 0.568 = \$3252$$

The annual loss due to theft of information attacks ($) is

$$\text{Annual loss} = 9590 * 0.448 = \$4296$$

Total annual loss can be calculated ($) using Eq. (8)

$$\text{Total annual loss} = AL\text{due to } DDoS \text{ attack} + AL\text{due to theft of information attack} \quad (8)$$

$$\text{Total annual loss} = \$3252 + \$4296 = \$7548$$

We estimate prevalent annual loss because our system realizes usable invasions using Eq. 9.

$$\text{Annual loss} = a_0 + \sum_{t=1}^{n} \text{loss}_t \times \text{likehood}_t \tag{9}$$

where $t$ is the number of threats, $loss_t$ is loss of assets due to t, $likehood_t$ is the occurrence of t threats.

### 3.6 Phase 6: information mapping and business priority alignment

This level involves identifying credible threats and connecting them to relevant information. The company's processes, goals, and priorities align with the dangers. This facilitates understanding of organizational threat scenarios for business owners.

### 3.7 Phase 7: cost–benefit analysis, RONSI

Since it estimates the annual loss before and after protective measures are implemented, the cost–benefit analysis aids in determining the significance of the countermanded. The case studies presented show a difference between the two annual losses. The loss is barely noticeable after the countermeasure.

We examine every factor affecting the estimation and cost, and budget justification are crucial. We evaluate gaps and the effects of investments on a company's core business function rather than utilizing traditional methodologies. Discussions with industry experts and a panel of subject matter experts have taken place to take other considerations into account when calculating the total investment cost. Based on the interview, critical parameters are included in this study: cost of implementation, advisory charges, installation, annual maintenance charges, and training. These five parameters are considered in this study while calculating the total cost of investments using Eq. 10.

$$\begin{aligned}\text{Total cost of investment} = \sum_{c=1}^{n} &\text{Cost of implemention} \\ &+ \text{Cost of advasiory charges} \\ &+ \text{Cost of installtion} \\ &+ \text{Cost of annual maintenece charges} \\ &+ \text{Cost of traning}\end{aligned} \tag{10}$$

j denotes the number of treatments to handle the occurrence of the event.

$$\begin{aligned}\text{Total cost of investment} &= \$3750 + \$30 + \$125 \\ &+ \$60 + \$30(20) = \$3995\end{aligned}$$

The RONSI calculation based on cost–benefit analysis is a concern of ours. Preventative actions were covered earlier. The likelihood of risk realization should be below after the preventative measures in the plot are put into practice. The likelihood of risk realization drops to 0.25 [42], demonstrating the benefit of preventative action for the organization. The cost–benefit analysis is essential in measuring the impact of preventative measures because it compares the annual loss before and after the distribution of preventative measures. We can tolerate a noticeable fluctuation in both annual losses in the figure. After precautions, the loss is reduced to \$7548*0.25 = \$1887 from \$7548, a rather significant loss.

### 3.8 Phase 8: justification procedure

The organizational loss can be computed using Eq. 11, and RONSI offers senior management a convincing defence of the purchase and its value.

$$RONSI = \sum_{n=1}^{\infty} 100 * \frac{ALE_{i,j} - mALE_{i,j}(j) - \text{cost of solution}}{\text{cost of solution}} \tag{11}$$

RONSI identifies the value of a potential investment. The effective yield indicates the financing decisions; otherwise, the investment is not worthwhile. Zero return, however, shows that the reason is the most useful.

## 4 Evaluation

Comparing the proposed method to the existing one provides better accuracy. Unlike conventional techniques, which mostly rely on hypotheses, we evaluate the possibility of an invasion using CVSS datasets and the expertise of subject matter experts. Traditional ROSI frameworks rely on prior information, contributor data, and the examination of false inferences. The suggested framework offers a mathematically based way of computing a single loss, in contrast to the conventional methodology. The annual loss is restricted using the Bayes' technique, even though traditional frameworks compute loss based on beliefs obtained from employees' experiences, comprehension, and consequences. This fills a gap in existing methodologies' inability to analyze the impact of network infrastructure expenditure. The study's findings show that the annual loss without a security plan is quite significant, at \$7548, and that the proposed RONSI model reduces it to \$1887. Table 6 summarizes the comparison between the standard and suggested procedures.

**Table 7** Analytical framework

| Specification | Proposed approach | ROSI for security organization [34] | Cost–benefit analysis [27] | Practical model [32] |
|---|---|---|---|---|
| The methodical approach of identifying the likelihood | The Bayesian approach is used to calculate probabilities | Yes | The attribute-based method was utilized | Likelihood of ARO is computed using previous learning, discussions and beliefs |
| Model validation | CVSS dataset used | CVSS dataset used | No, question ware | No |
| Approaches penetration testing | Internal and external penetration testing methods | No | No | No |
| A method for classifying assets using math | Asset prioritization = C + I + A | Yes | No | No |
| Methods for assessing risk and vulnerability | Vulnerability identification | Yes | No | It is lacking a procedure to determine asset exposures |
| Calculating the "Return Of Network Security Investment" (RONSI) | Yes | No | No | No |

The proposed RONSI method is evaluated by comparison and evaluation of the results. This model's performance in calculating network security investment shows that the suggested methodology is effective and efficient compared to other methods and approaches like Return on Network Security Investment (RONSI). A comparison to the existing methods Security Attribute Evaluation Method (SAME), Return on Security Investment (ROSI), and Volatile Transaction Authentication Insurance Method (VTAIM). The pictorial exhibits the accuracy (%) rate the recommended approach applies for a false rate and complexity. The process of choosing the most beneficial features based on the outputs of models and forecasts is known as feature engineering. Table 7 summarizes the comparison between the standard and proposed procedures.

The accuracy is calculated using Eq. 12, the corrected prediction divided by the total number of forecasts. Figure 4 illustrates the accuracy of the proposed system. The consumption prediction of accuracy in existing systems and the proposed system is denoted. SAEM has attained 52%, ROSI has acquired 73%, VTAIM has reached 89%, and the proposed system has attained 98% accuracy. The proposed approach is more effective, illustrated in Table 8.

$$\text{Accuracy} = \frac{\text{Correct prediction}}{\text{Total number of prediction}} \tag{12}$$

The false Rate technique computes the false rate detection and transaction information analysis to build volatile insurance and safety features at various time intervals and prevent false rates. Figure 5 portrays the false rate of the proposed system. SAEM has achieved 92%, ROSI has acquired 72%,

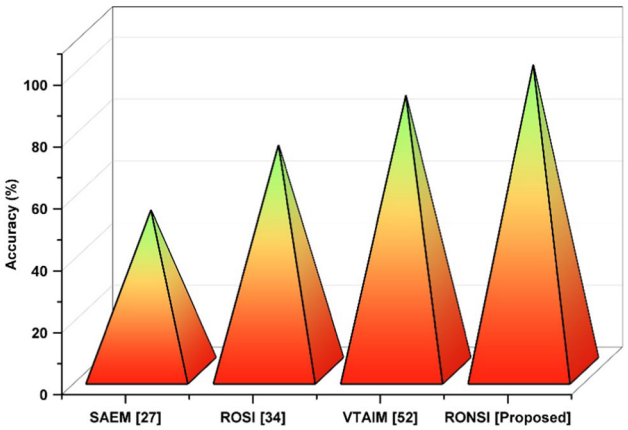


**Fig. 4** Accuracy

**Table 8** Accuracy

| Methods | Accuracy |
|---|---|
| SAEM [27] | 52 |
| ROSI [34] | 73 |
| VTAIM [51] | 89 |
| RONSI(Proposed) | 98 |

VTAIM has attained 63%, and the proposed system attained a 43% false rate. It shows that the proposed method is high compared to the current work, presented in Table 9.

Complexity risk mitigation in the final product depends on user transaction interest verification for volatile insurance authenticity, which does not make suggestions through

**Table 9** False rate

| Methods | False rate |
|---|---|
| SAEM [27] | 92 |
| ROSI [34] | 72 |
| VTAIM [51] | 63 |
| RONSI [Proposed] | 43 |

**Table 10** Complexity

| Methods | Complexity (Mb) |
|---|---|
| SAEM [27] | 71 |
| ROSI [34] | 62 |
| VTAIM [51] | 81 |
| RONSI [Proposed] | 52 |

transaction features. Session time and transaction support are based on complexity analysis in online banking services. Figure 6 shows the complexity of the proposed system. SAEM has attained 71%, ROSI has acquired 62%, VTAIM has reached 81%, and the proposed system has attained 52% complexity. It demonstrates that the proposed approach has more practical, shown in Table 10.

An optimal amount through mathematical modeling demonstrated the relationship between vulnerability and the ideal degree of information security investment. The optimal amount spent on information security will always be at most 37% of the anticipated harm brought on by the security incident. Besides, investing in the files with the most significant risks is very costly, as shown in Fig. 7.

## 5 Discussion

Without using quantitative estimations and models, the chance of an assault is only estimated based on documented data or personal experience, which results in an erroneous assessment. The platform includes exact asset classifications, threat models, and methods to study the impact. The proposed system employs Eqs. 1 and 2 to calculate and emphasize assets. Additionally, it collects ISO 27001 techniques for asset lists. These are reasonable first steps to determine which assets risk significant losses. Identification of the assets on which the manifestation of a threat could inflict considerable damage depends on asset classification and priority. The suggested method calculates the statistical likelihood of a danger materializing using the potent Bayesian theorem (Eq. 3). The CVSS attack dataset, vulnerability scan, internal and external penetration test reports, and threat modeling results are used as input to calculate the likelihood of threat scenarios in an organization. The proposed RONSI framework employs a practical, forward-looking Bayesian methodology to reduce the likelihood of danger. As shown in Tables 4 and 5, traditional methods frequently need to offer a way to estimate exposure and pertinent dangers. Traditional ROSI frameworks rely on conjecture, historical data, employee knowledge, and estimation. Traditional ROSI frameworks rely on conjecture, historical data, employee knowledge, and estimation.

In contrast to existing approaches, the proposed approach includes a mathematical formula to compute single losses. Equations 7 and 8, based on validities and attacks in the provided framework, determine the likelihood of the annual loss and the overall investment cost in network systems. This makes it more manageable to investigate how network security investments affect the overall infrastructure, which needs to be addressed by more traditional approaches.

An analyst or investigator conducts structured interviews with I.T. and security managers for the initial data as part of SAEM's quantitative risk and benefit evaluation [27]. A variation of the well-known accounting statistic used to compare

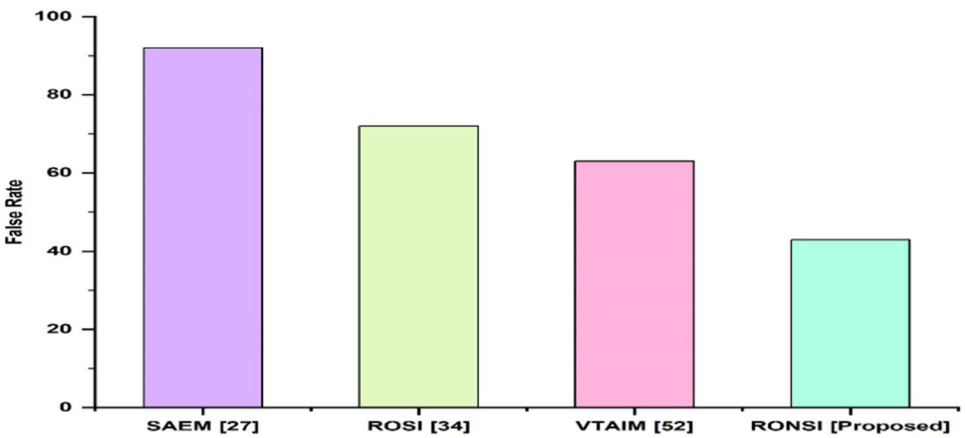


**Fig. 5** False rate

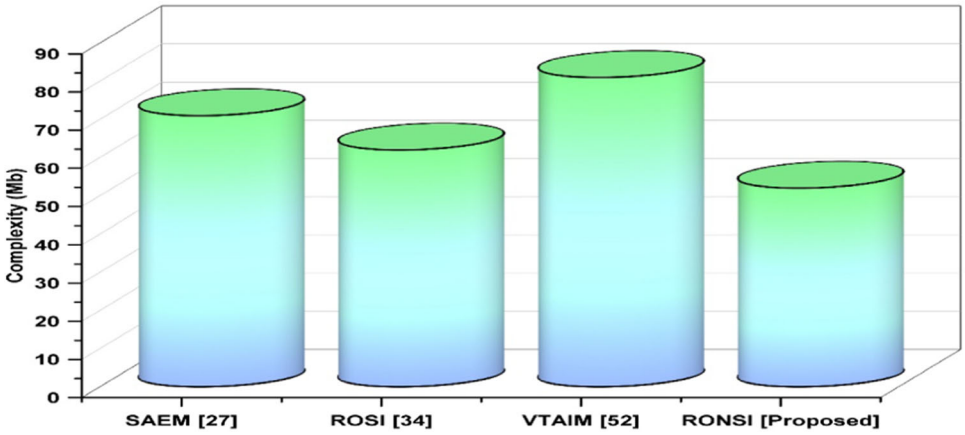


**Fig. 6** Complexity

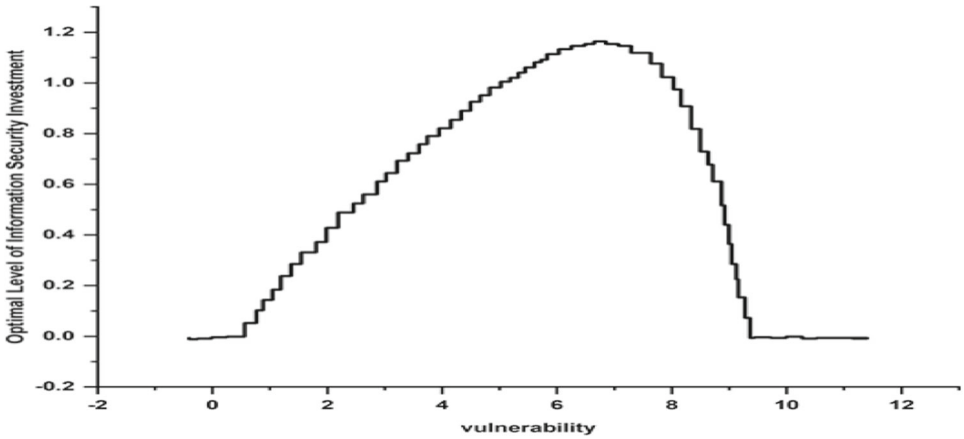


**Fig. 7** The optimal value of security investments as a function of vulnerability

ROI (Return on Investment) investments, the return on security investment (ROSI) calculation method, was developed. ROSI measures the value an organization receives for each dollar spent [34]. The volatile Transaction Authentication Insurance Method (VTAIM) employing banking services aims to increase security services in the online banking platform for available customers by lowering the false rate and failures based on the transaction server [51]. Table 7 emphasizes the comparison between the proposed method and the existing approach. A comparative study in terms of accuracy, false rate, and complexity is presented in Tables 8, 9 and 10, respectively.

### 5.1 Threats to validity

The primary concern of categorizing cyber security threats by data sets and selecting patterns is evaluated. The first significant step combines attack statistics, vulnerability scan results, and penetration test reports. The possibility of new attacks could change, affecting priority setting and effect evaluations.

### 5.2 Limitation of the study

The study is considered using a specific attack dataset, a vulnerability and penetration testing report, and the proposed RONSI methodology. The study does not assess other losses, including reputational damage and potential legal action due to data loss. Further analysis of diverse network attack datasets is needed to support investment choices.

## 6 Conclusion and future work

The proposed network-based investment framework (RONSI) is presented for adequate network security controls and related systems to justify the investment. The paper extends current frameworks and compares and analyses the various ROSI models. There are several ROSI-related approaches presented. The complexity of attacks, however, makes it challenging to predict how investment affects multiple aspects of an organization. Similar to how the current understanding of attack occurrences is rampant with uncertainty, considerably required to overcome.

The relationships between the critical components and methods for determining the RONSI are demonstrated. Different approaches are provided for calculating the likelihood and consequences of a network attack. The proposed framework is validated using CVSS datasets and compared with existing studies. The results demonstrate that, after implementing the security strategy plan and using the suggested analytical model to compute RONSI, which has been significantly decreased, the annual loss has been reduced by 75%. The evaluation's discoveries exhibit that the proposed method effectively considers uncertainty. Automating a thorough exploratory analysis of the suggested RONSI approach in various organizational scenarios is paramount.

**Supplementary Information** The online version contains supplementary material available at https://doi.org/10.1007/s11235-023-01039-9.

**Funding** The authors didn't receive any funding from any sources.

## Declarations

**Conflict of interest** Authors do not have any conflict of interest with anybody.



## References

1. Herrera, L. C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. *International Journal of Critical Infrastructure Protection, 25*, 50–61.
2. The Top 10 Data Breaches of 2021, Security Magazine, https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
3. Itgoverence, UK, Data breaches and cyber attacks in 2021: 5.1 billion breaches records, https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2021-5-1-billion-breached-records
4. Itgoverence, UK, Cyber Attacks and Data Breaches in Review: February 2022, https://www.itgovernance.eu/blog/en/cyber-attacks-and-data-breaches-in-review-february-2022
5. Special Report: Cyberwelfare In the C-Suite, 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
6. Das, L., Munikoti, S., Natarajan, B., & Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges and opportunities. *Renewable and Sustainable Energy Reviews, 130*, 109918.
7. Paul, J. A., & Wang, X. J. (2019). Socially optimal I.T. investment for cybersecurity. *Decision Support Systems, 122*, 113069.
8. Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics–balancing operational security spending. *Information Technology & People, 32*, 1318.
9. Li, Y., & Xu, L. (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research, 59*(4), 1216–1238.
10. Cybersecurity statistics 2021, https://nordlayer.com/blog/cybersecurity-statistics-2021-review/
11. ZDNet, Most companies take over six months to detect data breaches, May 2015, https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/
12. Feldmann, M., & Morgan, G. (2022). Business elites and populism: Understanding business responses. *New Political Economy, 27*(2), 347–359.
13. Zhou, C., Hu, B., Shi, Y., Tian, Y. C., Li, X., & Zhao, Y. (2020). A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE, 109*(4), 517–541.
14. Li, X., & Xue, Q. (2021). An economic analysis of information security investment decision making for substitutable enterprises. *Managerial and Decision Economics, 42*(5), 1306–1316.
15. Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. *Risk analysis, 19*(4), 689–701.
16. Smets, P. (1993). Belief functions: The disjunctive rule of combination and the generalized Bayesian theorem. *International Journal of approximate reasoning, 9*(1), 1–35.
17. Locher, C. (2005). Methodologies for evaluating information security Investments-What Basel II can change in the financial industry.
18. The NIST, "Return on Investment Initiative Draft Green Paper intitiative" https://www.nist.gov/system/files/documents/2018/12/06/roi_initiative_draft_green_paper_nist_sp_1234.pdf
19. ENISA, "Investing for Security ROI "https://www.enisa.europa.eu/news/enisa-news/investing-in-security-for-roi
20. Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010, June). Using Bayesian networks for cyber security analysis. In 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN) (pp. 211–220). IEEE.
21. Bistarelli, S., Fioravanti, F., Peretti, P., & Santini, F. (2012). Evaluation of complex security scenarios using defense trees and economic indexes. *Journal of Experimental & Theoretical Artificial Intelligence, 24*(2), 161–192.
22. Roy, A., Kim, D. S., & Trivedi, K. S. (2012, June). Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees. In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012) (pp. 1–12). IEEE.
23. Ji, X., Yu, H., Fan, G., & Fu, W. (2016, May). Attack-defense trees based cyber security analysis for CPSs. In 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) (pp. 693–698). IEEE.
24. Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat modeling using attack trees. *Journal of Computing Sciences in Colleges, 23*(4), 124–131.
25. Enoch, S. Y., Hong, J. B., Ge, M., Alzaid, H., & Kim, D. S. (2018, January). Automated security investment analysis of dynamic networks. In Proceedings of the Australasian Computer Science Week Multiconference (pp. 1–10).
26. Enoch, S. Y., Ge, M., Hong, J. B., & Kim, D. S. (2021, May). Model-based Cybersecurity Analysis: Past Work and Future Directions. In 2021 Annual Reliability and Maintainability Symposium (RAMS) (pp. 1–7). IEEE.
27. Butler, S. A. (2002, May). Security attribute evaluation method: a cost-benefit approach. In Proceedings of the 24th international conference on Software engineering (pp. 232–240).

28. Pontes, E., Guelfi, A. E., Silva, A. A., &Kofuji, S. T. (2011). A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI). Risk Management in Environment, Production and Economy, 149–170.
29. Aguiar Rodriquez, A. (2017). Understanding the dynamics of information security investments. A simulation-based approach.
30. Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a healthcare information exchange: An economic analysis. *Decision Support Systems, 61*, 1–11.
31. Wu, Y., Feng, G., Wang, N., & Liang, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications, 42*(15–16), 6132–6146.
32. Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology, 38*(1), 45–56.
33. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision support systems, 86*, 13–23.
34. Yaqoob, T., Arshad, A., Abbas, H., Amjad, M. F., & Shafqat, N. (2019). Framework for calculating return on security investment (ROSI) for security-oriented organizations. *Future Generation Computer Systems, 95*, 754–763.
35. Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Murat, K. (2022). Cybersecurity deep: Approaches, attacks dataset, and comparative study. *Applied Artificial Intelligence, 36*, 1–24.
36. Halpern, J. I., Leininger, K. E., Toth, R. D., & Shaw, O. A. (2018). U.S. Patent No. 10,129,215. Washington, DC: U.S. Patent and Trademark Office.
37. Harrell, C. R., Patton, M., Chen, H., &Samtani, S. (2018, November). Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 148–153). IEEE.
38. Proença, D., & Borbinha, J. (2018). Information security management systems-A maturity model based on ISO/IEC 27001. In Witold Abramowicz & Adrian Paschke (Eds.), *Business information systems: 21st international conference, BIS 2018, Berlin, Germany proceedings* (pp. 102–114). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-93931-5_8
39. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering, 45*(4), 3171–3189.
40. Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security, 109*, 102382.
41. Smith, M. D., & Pate-Cornell, M. E. (2018). Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment. *IEEE Transactions on Engineering Management, 65*(3), 434–447.
42. Pinzon, C., De Paz, J. F., Bajo, J., Herrero, A., &Corchado, E. (2010, August). AIIDA-SQL: an adaptive intelligent intrusion detector agent for detecting SQL injection attacks. In 2010 10th International Conference on Hybrid Intelligent Systems (pp. 73–78). IEEE.
43. Pajila, P. J., Julie, E. G., & Robinson, Y. H. (2022). FBDR-fuzzy based DDoS attack detection and recovery mechanism for wireless sensor networks. *Wireless Personal Communications, 122*(4), 3053–3083.
44. Skoufis, A., Chatzithanasis, G., Dede, G., Filiopoulou, E., Kamalakis, T., & Michalakelis, C. (2022). Technoeconomic assessment of an FTTH network investment in the Greek telecommunications market. *Telecommunication Systems, 822*, 1–17.
45. Mamane, A., Fattah, M., El Ghazi, M., & El Bekkali, M. (2022). 5G enhanced mobile broadband multi-criteria scheduler for dense urban scenario. *Telecommunication Systems, 80*(1), 33–43.
46. Eswaran, S., & Honnavalli, P. (2022). Private 5G networks: a survey on enabling technologies, deployment models, use cases and research directions. *Telecommunication Systems, 82*, 1–24.
47. Vajanapoom, K., Tipper, D., & Akavipat, S. (2013). Risk based resilient network design. *Telecommunication Systems, 52*(2), 799–811.
48. Kliks, A., Musznicki, B., Kowalik, K., & Kryszkiewicz, P. (2018). Perspectives for resource sharing in 5G networks. *Telecommunication Systems, 68*(4), 605–619.
49. Gardikis, G., Koumaras, H., Sakkas, C., & Koumaras, V. (2017). Towards SDN/NFV-enabled satellite networks. *Telecommunication Systems, 66*(4), 615–628.
50. Zghaibeh, M., & Harmantzis, F. C. (2008). A lottery-based pricing scheme for peer-to-peer networks. *Telecommunication Systems, 37*(4), 217–230.
51. Almatari, O., Wang, X., Zhang, W. and Khan, M.K., 2023. VTAIM: volatile transaction authentication insurance method for cyber security risk insurance of banking services.




**Kousik Barik** is pursuing a Ph.D. at the Dept. of Computer Science of the University of Alcalá (UAH). He earned a degree in Electronics and Telecommunication Engineering from Nagpur University, India. He earned a Master's Degree and a Post-Graduate Diploma in Information Technology Management from India. He has more than 17 years of industry experience in information security, cybersecurity, and artificial intelligence. His research interests include but are not limited to: Information Security, Networking, Cybersecurity, Information Systems.

**Sanjay Misra** a Sr. member of IEEE and ACM Distinguished Lecturer, is a Senior Scientist at the Institute of Energy Technology(IFE), Halden, Norway. Before joining IFE, he was associated with the Computer Science and Communication department of Østfold University College, Halden, Norway. He holds a Ph.D. in Information & Knowledge Engg (Software Engg) from the University of Alcala, Spain & M.Tech. (Software Engg) from MLN National Institute of Tech, India. His expertise is in the area of Applied Informatics (Cyber Security, Health Informatics, Software Engineering Applications, and Intelligent systems using AI and computational techniques) and has been published (- around 150 JCR/SCIE) in top journals like

Computers and Security, Information Processing and Management, Engineering Applications of Artificial Intelligence, Expert Systems, and Applications, etc. He has been amongst the top 2% of scientists in the world (published by Stanford University) for the last three consecutive years, ranked no 2 in the whole of Africa in computer science (as per Elsevier: Scival analysis during 2017-2022) and also got several awards for outstanding publications (2014 IET Software Premium Award (UK)), TUBITAK-Turkish Higher Education, and Atilim University). He is Editor in Chief of Int J of Human Capital & Inf Technology Professionals (IGI), IT Personnel and Project Management (IGI), and editor in various SCIE journals (Nature: Scientific Report ((Impact Factor: 4.996), Elsevier: Alex. Engineering ((Impact Factor: 6.626, Q1 7/92)), edited several special issues and 80 books from Springer (65 LNCSs, 4 LNEEs, 3 LNNSs, 3 CCISs), 10 IEEE proceedings and several books. He delivered more than 100 keynotes and invited talks and public lectures at reputed conferences and institutes (he traveled to more than 60 countries).

**Luis Fernandez-Sanz** is a full professor at the Dept. of Computer Science of the University of Alcalá (UAH). He earned a degree in Computing in 1989 at the Polytechnic University of Madrid (UPM) and his Ph.D. in Computing with a special award at University of the Basque Country in 1997. With more than 30 years of research and teaching experience (at UPM, Universidad Europea de Madrid and UAH), he has also been engaged in managing the main Spanish Computing Professionals Association (ATI: www.ati.es) as vice president and is chairman of ATI Software Quality group. He has held the position of vice-president of CEPIS (Council of European Professional Informatics Societies: www.cepis.org) from 2011 to 2013 and from 2016 to 2022 when he was elected President. His general research interests are software quality and engineering, accessibility, e-learning, and ICT professionalism and education.

**Murat Koyuncu** is Professor at Dept. of Information system engineering at Atilim University. He earned his bachelor's from Turkish Military Academy and master and master's and Ph.D. from Middle East Technical University, Ankara Turkey. His research interests includes but not limited to: Security and Privacy, Networking, Multimedia, Intelligent Systems, Information Systems, Database Management Systems. He published several papers in IEE Transactions and top journals in the field.