STM JOURNALS

International Journal of
Information Security Engineering

ISSN: 3049-1150
Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

What Is the Meaning and Purpose of Risk Management in Cyber Security?

Dhaval Chudasama*

Abstract

Organizations and their information systems are increasingly exposed to risk and uncertainty from a variety of sources, including computer fraud, espionage, and sabotage or cyber-attacks. The purpose of this article is to outline several steps, protocols, and factors that any organization should consider in the event of a cyber-attack. Over time, some damage causes, including denial of service or intrusion attacks, have grown more frequent, aggressive, and complex. Complete security is unattainable. For this reason, companies need to implement strategies and tactics that allow them to rank risks according to their impact and likelihood, which indicates a higher risk to the company. When preparing for possible cyber-attacks, it is important to understand the logical flow of actions that can be taken during an attack, to incorporate best practices, to assess the level of risk the organization faces and proactively design a handbook to respond to these situations.

Keywords: Cyber-attack, incident response, cyber security, cyber risk analysis, risk management

INTRODUCTION

Since data is the basis for nearly all company decisions, dependable information technology (IT) is essential to business continuity and, thus, to the economy [1]. The importance of information technologies has led to the urgent need to ensure their continued and reliable operation as well as to protect the information processed and saved. The effect of security breaches on an organization's market value has been demonstrated by recent studies. A security compromise has caused companies to lose an average of 2.1% of their market value in just two days. The global economic system's interconnection facilitates the rapid spread of information security concerns like computer viruses. Although almost any organization's connection to the internet and the spread of computer viruses are just two potential information security vulnerabilities and risks to the organization, they still illustrate the changing environment that threatens the company. Threatened for decades in recent years there are reasons why businesses should make an effort to adequately manage these risks [2]. According to Sage and White [3], risk is often defined as the likelihood that a unit cost burden will occur per unit of time. In the context of information security, risk refers to the probability that a specific threat could exploit a particular vulnerability and the resulting impact of such an event on the organization [4].

***Author for Correspondence**
Dhaval Chudasama
E-mail: Dhavalchudasama16@gmail.com

Assistant Professor, Department of Cyber Security, Gandhinagar University, Gandhinagar, Gujarat, India

Received Date: December 13, 2024
Accepted Date: January 28, 2025
Published Date: February 12, 2025

Citation: Dhaval Chudasama. What Is the Meaning and Purpose of Risk Management in Cyber Security?. International Journal of Information Security Engineering. 2025; 3(1): 46–53p.

Since the security measures needed to reduce risk almost always come with a cost, organizations look for ways to reduce risk to an acceptable level at the lowest possible cost. In Special Publication 800-30, the National Institute of Standards and Technology (NIST) identified information security risk management as the process that helps IT managers balance operational and economic costs by implementing safeguards and achieve mission capability by safeguarding the data and computer systems that support their organization's missions [4]. Managing information security risks is critical

to ensuring long-term business success. Numerous methods have been proposed by experts to put into practice a sufficient information security risk management plan [1, 2].

Regardless of which data protection threat control method is considered, it continually consists of the evaluation of business-vital belongings of capacity threats, vulnerabilities, and measures which could lessen the threat to a suitable stage [5]. While in-intensity expertise of the corporation in query and the data protection area as an entire is essential to the provided approaches [6], very few studies has been performed at the formal expertise illustration of the domain names which are applicable to data protection threat control. Recent studies have proven that the shortage of data protection expertise on the control stage is one motive for insufficient or non-existent data protection threat control strategies, and that elevating the control's stage of data protection cognizance and expertise results in greater powerful strategies. Diagnosed data protection threat control as one of the pinnacle ten grand demanding situations in data generation protection and known as for sound theories and techniques to assist and enhance present data protection threat control approaches. In 2006, the European Network and Information Security Agency (ENISA) addressed those issues and rated the established order of unified databases for data protection threat control and the improvement of threat dimension techniques as excessive precedence issues. Only a quick time later, showed the shortage of a hard and fast of well-described formal fashions for helping the data protection threat control process. Out of 1007 UK organizations surveyed, only 48% formally validate data protection risks (2008 Information Security Breaches Survey. To date such businesses have primarily depended on satisfactory exercise guidelines, data protection standards, and/or area professionals to behaviour the threat evaluation and mitigation phases [3, 4].

However, these approaches have several problems:

- *Dependency on a subject matter expert:* Best practice guidelines provide an excellent understanding of potential threats, weaknesses, and controls, but without an information security expert, an organization may not always understand the many complex relationships between all relevant information security concepts. As a result, the organization's goal is threatened by an uneven approach to information security.
- *Infrastructure Mapping:* To identify specific infrastructure components that are threatened by specific threats, an organization must manually map the knowledge derived from best practice recommendations to the actual architecture [5].
- *Abstract implementation proposals:* Information security standards often contain only very abstract implementation proposals to reduce risk.
- *Determining the probability of a subjective hazard:* This process relies more on subjective impressions than on objective evaluations.
- *The incalculable efficacy of IT security solutions:* Businesses frequently look for ways to cut costs, but they are frequently ignorant of the extent of their IT security expenditures and, more crucially, their effectiveness.

Decision makers in management, like CPOs or CIOs, face the challenge of choosing the most suitable IT security investments from a wide array of options. Current methods provide inadequate or unintuitive decision support, lacking interactivity, which makes it difficult for them to assess the right balance between risk and costs when selecting IT security solutions [5, 6].

WHAT IS CYBER RISK MANAGEMENT?

Introduction units for assessment and risk management and management, but the main purpose of this document is a frame for assessing and managing risk in the context of cyber. Digital technology becomes more and more disseminated and based on almost every aspect of our everyday life. It is expected that with increasing internet items, connected devices will reach the level of over 50 billion. Human tasks such as driving and making decisions are being replaced by automated technology, and massive system infrastructure was indiscriminately wiped out during the 2017 Wanna Cry

Ransomware outbreak. As a result, cyber security is a basic particular case that everyone who lives and works in the digital industry should be aware of. A uniform methodology for evaluating cyber security risks is intended to be formalized and provided by a number of international standards. Let us start with high-level definitions of some of the most crucial roles in terms of risk before looking at some of them in this part. The United Kingdom is ranked first in the Global Cybersecurity Index (GCI) 2018, a science-based assessment of global cyber security situation and participation on a country-by-country basis.

A total score is generated by combining the evaluation's five pillars:

1. Legal,
2. Technical,
3. Organizational,
4. Capacity building, and
5. Collaboration.

As a leader in CGI, the UK's National Cyber Security enter (NCSC) has advice on risk management. It is crucial to note that the NCSC clearly emphasizes that risk assessment and management should not follow a one-size-fits-all model, and conducting a branded risk assessment and management could be more detrimental than not performing one at all. Because they are not adequately prepared, this gives people at risk a false sense of security that could make them more vulnerable. Cyber security is an ever-changing field, and while achieving complete security may not be possible, we can certainly improve our preparedness. The Potomac Institute of Political Studies offers a framework for assessing cyber readiness, along with country profiles for various nations [7, 8].

WHAT MAKES RISK MANAGEMENT AND ASSESSMENT CRUCIAL?

The risk assessment consists of three main components: (i) identification and, where applicable, (ii) hazard estimation, exposure and/or vulnerability assessment, and (iii) risk estimate risk, combining probability and severity. Determination is concerned with establishing subsequent events and outcomes, while estimation is concerned with the relative strength of outcomes. Exposure deals with aspects of a system that are open to threat actors (e.g., people, devices, databases), Vulnerability refers to characteristics of elements that can be targeted (e.g., vulnerability, hardware failure, software exploit). Risk estimates can be quantitative (e.g., probabilistic) or qualitative (e.g., scenario-based) and capture the expected impact of the outcome. The fundamental idea behind risk assessment is the use of analytical and systematic procedures to measure potential outcomes and impacts, as well as to gather data, perceptions, and evidence regarding issues and the possibility of both desired and unwanted events. We cannot comprehend our vulnerability to dangers or create a strategy to mitigate them without any of the aforementioned information. The evaluation of concerns is a frequently disregarded step in the risk assessment process. This concept is grounded in research on public risk perception, but it also plays a crucial role in cyber risk assessment, which will be explored further in this document. Beyond the persuasive elements, the scientific aspects of risk assessment encompass a range of factors, including stakeholders' views on hazards, the potential consequences of risks, concerns about impacts, personal or organizational control over managing risks, and trust in those handling the risks. Analyzing data gathered during a risk (and concern) assessment is an essential part of the risk management process. For any perceived danger, judgements based on this information result in three different outcomes [9].

1. The risk system's intolerable aspects should be either discarded or replaced. If that is not feasible, the vulnerabilities must be minimized and exposure limited.
2. Tolerable - Risk should be minimized by reasonable and appropriate methods to the lowest achievable (ALARP) or lowest allowable (ALARA). Accepting, avoiding, minimizing, sharing, or transferring the risk are some of the possible possibilities.
3. Risk reduction is not necessary and can be carried out without any intervention. More effort is needed to ensure against the risk or further reduce it [6–8].

In addition to this decision-making framework, Renn identifies four types of risks that require different risk mitigation plans.

These include the following:

- *Routine Risks* – They follow a decision-making process quite normal for management. Relevant statistics and data are provided, desired results and acceptability limits are identified, and risk mitigation measures implemented and implemented.
- *Complex hazards* – For less evident concerns, a more comprehensive body of information may be required, and a comparison method, like a cost-benefit analysis, may be essential. Examples of scientific disagreements include the effects of medication treatments and climate change.
- When dealing with uncertain risks, factors like reversibility, persistence, and ubiquity are important to consider. Preventive approaches need to be taken with an ongoing and managed approach to developing systems by which negative side effects can be prevented and eliminated. Resilience to uncertain outcomes is essential here.
- *Ambiguous risks* – When broader stakeholders such as operators or civil society interpret risk differently (e.g., different perspectives exist). Differences, lack of consensus on management controls), risk management must address the causes of different perspectives. Renn illustrates the case of genetically modified foods, where concerns about welfare clash with more sustainable alternatives. In this case, risk management should enable participatory decision-making, with explicit measures to reduce ambiguity to a manageable and assessable number of options and more reviews [9, 10].

Therefore, the management options include a resilience-based approach (risk management using ALARA/ALARP principles and risk control), a risk-based approach (risk-benefit analysis or comparative options), or a speech-based approach (including risk communication and conflict resolution of ambiguities). The reaction to side effects is likely to be disorganized, ineffective, and is also likely to accelerate the spread of side effects if risk acceptability is not adequately considered and a suitable risk reduction plan is not in place. Since our firm is not very proficient in this area, despite having an operational definition of risk that focuses on its impact on people, it is essential to manage risk effectively using structured assessment methods. To assess this risk. Ranked as the highest risk to the layman, but a much lower risk to experts in the field who understand the evidence related to the security limits and controls of these systems. Experts prefer to classify risks based on documented or anticipated negative results, including deaths, but laypeople are more influenced by their gut feelings (a nuclear catastrophe may affect my entire family). As a result, there is a mismatch between how people perceive risks and the actual risks. People tend to overestimate the dangers of rare events like nuclear accidents and terrorist attacks, while underestimating more common threats, such as street crime and household accidents, which cause far more fatalities. Therefore, accurately assessing risks and evaluating concerns are essential components of effective risk management. We naturally feel safer in our surroundings and more vulnerable outside of them, according to Schneider's book *Beyond Fear*. For example, we feel safe walking on a street near our home, but at the limit when we arrive in a new city. We rarely look at numbers as a society when making these judgements; instead, we base them on how exposed we believe we are to risks, how much control we believe we have over them, and their potential consequences. We can realistically estimate our level of certainty that unfavorable events will occur and their influence on our most valued possessions by using risk assessment to better understand both the quantitative and qualitative components of the world [6–8]. This holds true for every one of us individually as well as for groups of people that share the same objectives, such as protecting the environment, operating a business, or educating children. We need to grasp our goals, understand what might lead to their failure, and put in place processes to align realistic measures to reduce the inane damage to our goals. When done right, risk assessment and management enable responsible decision-makers to keep the system running to achieve desired goals. Additionally, it can guarantee that the system is not intentionally or inadvertently manipulated to yield unwanted outcomes and that procedures are in place to lessen the impact in the event that such outcomes do occur.

To ensure that responsible stakeholders understand the risks, how they are managed, who is accountable for their management, and what defines risk exposure, it is essential to communicate this information clearly, understandably, and in a way that is easy to interpret for different audiences. The impact of management failure threats is disregarded and the system remains vulnerable if the risks—whether technical, social, economic, or otherwise—are not communicated to decision-makers in a clear and concise manner. Effective risk management is crucial for this reason. If the objectives of risk management, along with the responsibilities and liabilities individuals face for potential risks, are not clearly communicated to those at the operational level, they may fail to adhere to the risk management plan, leaving the system vulnerable. Overall, the suggested system may be widely rejected if the wider concerns of stakeholders—such as civil society—are not taken into consideration or if there is mistrust of the risk management strategy [6–8]. In addition to clearly communicating risks to stakeholders, it is equally important to emphasize that cannot always be eliminated. Discussion between decision makers and others involved in the running of a system is necessary since there is likely to be a (acceptable) existential risk to the things we value.to determine if the risk should be shared, avoided, managed, transferred, or not. Since they probably have distinct values that they are attempting to uphold, these groups of people may hold differing opinions about how to manage risk. Saving money will be crucial for certain people. For others, the primary objective is fame. For people working on the system, this can be the speed of the process or the ease of performing daily tasks. Communicating these values and ensuring that decisions are taken to appropriately manage risk in order to decrease it to a predetermined set of values are the goals of risk assessment and management. This relates to the idea of ALARP (reasonably achievable low level) in the larger context of health and safety concerns. This task may require significant effort, with calculations made to balance risk acceptance and safety-oriented risk reduction. It is crucial to emphasize that identifying concerns is a key part of the risk assessment process, ensuring that the risk assessment policy—an approach that is consistent—relies on the individuals responsible for and affected by the risks. These individuals must act accordingly to implement the management plan on a daily basis. Additionally, it is important to acknowledge that the effects of individual events can extend beyond immediate harm and ripple through broader supply chains. An event's aftermath ripples across the firm or system where it happened, then into subsystems, much like a fallen stone in a pond. As well as interconnected businesses and parts. Demonstrating adherence to different policies is one of the primary motivators for risk assessment and management [4–8].

This is frequently based on the requirement to have conformance approval confirmed by international standards organizations in order to secure commercial contracts, to fulfil legal or regulatory requirements, or to raise a company's market worth by enhancing public perception if certified. This can often lead to a “tick” risk assessment where the result is less focused on risk management and more on ticking a box. This puts the company at risk and creates a false sense of security. This brings us back to working definition of risk. All these examples cover managing the risk of non-compliance with different political positions but may not consider the broader emphasis on influencing the values of wider organizational, social or economic stakeholders. For risk management to be an effective and worthwhile exercise in boosting readiness and resilience to negative impacts, its context and scope must correspond to this larger end view. These elements make it abundantly evident that risk assessment and management are processes rather than final goods. This is something that when properly done can greatly increase the stability of your system. It can cause confusion, damage one's reputation, and negatively affect system functionality if done incorrectly or not at all. It is a process that sometimes seems irrelevant before it is needed but is critical to business continuity during a crisis. Throughout the risk assessment process, we must be aware that perceptions of risk vary widely depending on many factors, some of which will not be enough to reduce them. For instance, proving that the yearly risk of residing close to a nuclear power station is equal to the risk of driving an extra 5 km does not always lower the sense of risk because common perception varies depending on the situation. The role inherently involves clarifying and applying both qualitative and quantitative methods of risk assessment. The evidence goes no further that subjective human judgment will always be required to determine suitability and management plans [4–8].

CURRENT PROJECT RISK MANAGEMENT PRACTICES

Any set of tasks and activities with a definite objective that must be completed in accordance with predetermined guidelines, start and end dates, and financial constraints is referred to as a project. The majority of project management publications and pertinent professional groups now cover risk management since project managers are required to deal with larger degrees of uncertainty more frequently.

Here, "a measure of the likelihood and consequence of not achieving a specific project objective" is the definition of project risk. Risk effectiveness as the lowest amount of risk for a specific level of projected performance because risk in projects cannot be completely avoided. By detecting and prioritizing possible risk occurrences, creating a reaction strategy, and actively reducing risk, risk management dynamically [1–4].

The majority of organizations have a written project risk management policy and related analytical tools since risk management is so advanced in project management. Tools for risk identification (such as checklists, brainstorming, effect diagrams, and cause-and-effect diagrams), risk analysis (such as grids), expert judgement, and risk response (such as predictability matrix, risk response planning table, and project risk response planning) are all included in these analyses. Tools for risk assessment (such as portfolio management, decision tree analysis, and multi-criteria decision-making tools). There are various software packages for project risk management, such as PERT Master Project Risk, PERT Master Risk Expert, @Risk, Risk+, and the Crystal Ball simulation tool, as well as P Predict. The processes of risk planning, identification, analysis, and action formulation are the main topics of these tools.

They can be summarized as follows:

1. Limited variety of tools used. While there is a wide variety of risk planning tools available, in practice most project managers use risk event ranking as their primary or only tool.
2. For example, the 2008–2009 global financial crisis was largely driven by the popular belief that securitization of loans reduces the overall risk of a failed financial system.
3. *Poor Use Quality:* Many project managers are poorly versed in some of the most important risk planning processes, such as identifying risks and developing effective strategies. High complexity of existing tools: As projects increase in size and complexity, the effort required for effective risk planning increases exponentially, making it difficult to use current tools.
4. *Low Reliability of Project Managers:* Typically, functional managers have the necessary information and authority for most risk planning processes. This can limit the ability of project managers to effectively manage risk management processes.
5. *Low performance:* Risk management is relatively low during the tests specified by "critical success factors". Moreover, research supporting the positive impact of risk management on project success is subject to limitations (examples of members from "special risk groups" who may not represent the wider management community) [2–5].

Although these procedures are occasionally described using different nomenclature, all risk management methods follow the same fundamental steps as shown in Figure 1. A straightforward and efficient risk management procedure is produced by combining these five steps of the process.

Step 1: Risks that could impact your project or its outcomes are recognized, acknowledged, and described by you and your team. Design hazards can be identified using a variety of methods. At this stage, you start to prepare the project risk register.

Step 2: Analyze the risk. Following risk identification, you ascertain each risk's likelihood and potential outcomes. You will understand the nature of risk and its potential to influence the goals and objectives of the project. Additionally, this data is added to the Project Risk Register.

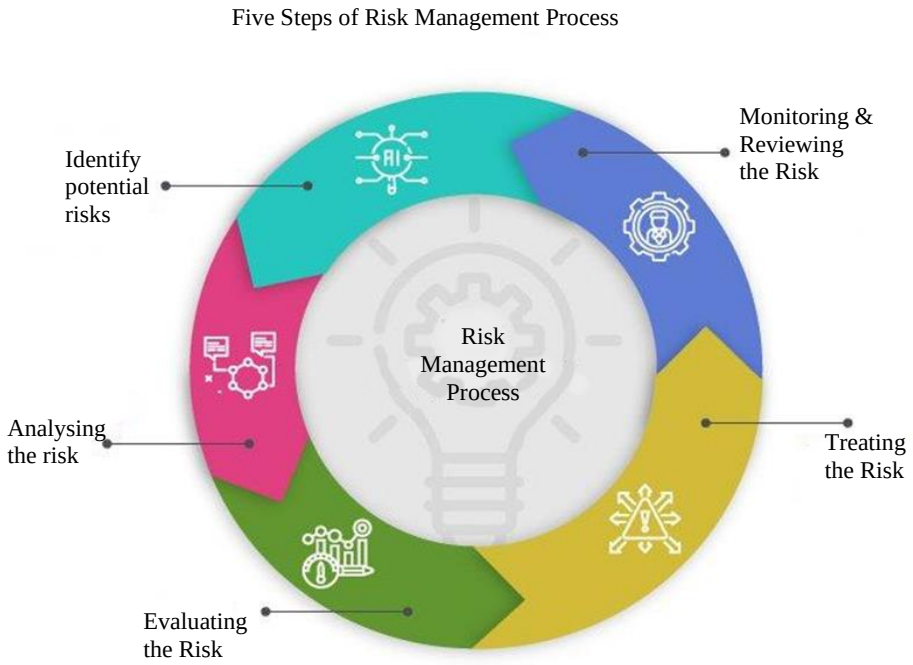

Figure 1. Risk management process [4].

Step 3: You measure or classify the risk by determining the amount of risk, which is a combination of probability and consequence. You decide whether the risk is acceptable or serious enough to justify treatment. These risk assessments are also added to the project risk register.

Step 4: At this stage, you assess your highest risks and plan to treat or modify those risks to achieve an acceptable level of risk. How can you reduce the chances of negative risks while increasing potential opportunities? At this point, you develop proactive plans, backup plans, and risk mitigation techniques. Additionally, you update the project risk register with the risk management strategies for the greatest or most significant risk.

Step 5: Monitor and review the risk. At this point, you take the project risk record and use it for risk monitoring, tracking, and analysis.

Risk is related to uncertainty. If you keep this uncertainty in the box, you will effectively reduce the risk to your project. This implies that you can proceed with greater assurance in order to accomplish the project's objectives. You can minimize unpleasant surprises and roadblocks and seize valuable opportunities by recognizing and controlling a thorough list of project risks. Risk management also helps in addressing new challenges. These issues have been foreseen, and strategies to deal with them have already been created and approved. You avoid impulsive reactions and go into "firefighting" mode to fix any problems you might expect. This keeps project teams and stakeholders happier and less stressed. The result is to minimize the impact of design risks and capture opportunities as they arise [10–16].

CONCLUSION

Companies see security as one of the most important issues on their agenda as the increasing number of security breaches poses a serious threat to the sound implementation of corporate strategies and can negatively impact business value. Information security risk management ensures that all possible threats and vulnerabilities as well as valuable assets are considered. Existing approaches, such as best practice guidelines, information security standards or subject matter experts, and information security risk management approaches that are widely accepted in the community have disadvantages.

REFERENCES

1. Gerber M, Von Solms R. Management of risk in the information age. Computers Security. 2005; 24 (1): 16–30.
2. Bagchi K, Udo G. An analysis of the growth of computer and internet security breaches. Commun Assoc Inform Syst. 2003; 12 (1): 46.
3. Sage AP, White EB. Methodologies for risk and hazard assessment: a survey and status report. IEEE Trans Syst Man Cybernet. 1980; 10 (8): 425–446.
4. Stoneburner G, Goguen A, Feringa A. Risk management guide for information technology systems. NIST Special Publication. 2002; 800 (30): 800-30. Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf
5. Baskerville R. Information systems security design methods: implications for information systems development. ACM Comput Surveys. 1993; 25 (4): 375–414.
6. Avolio BJ, Bass BM, Jung DI. Re-examining the components of transformational and transactional leadership using the multifactor leadership. J Occup Organ Psychol. 1999; 72 (4): 441–462.
7. Kure HI, Islam S, Razzaque MA. An integrated cyber security risk management approach for a cyber-physical system. Appl Sci. 2018; 8 (6): 898.
8. Taveras P. Cyber risk management, procedures and considerations to address the threats of a cyber attack. In: Proceedings of the ForenSecure: Cybersecurity and Forensics Conference, Chicago, IL, USA, April 12, 2019.
9. Fenz S, Ekelhart A, Neubauer T. Information security risk management: in which security solutions is it worth investing? Commun Assoc Inform Syst. 2011; 28 (1): 22.
10. Burnap P, Anthi E, Reineckea P, Williams L, Cao F, Aldmoura R, Jones K. Mapping automated cyber attack intelligence to context-based impact on system-level goals. J Cybersecurity Privacy. 2024; 4 (2): 340–356.
11. Zwikael O, Ahn M. The effectiveness of risk management: an analysis of project risk planning across industries and countries. Risk Anal. 2011; 31 (1): 25–37.
12. Kamal Y, Ahmad S. Strategic approaches to e-business transformation: navigating digital disruption in the Indian business landscape. In: Taherdoost H, Drazenovic G, Madanchian M, Khan IU, Arshi O, editors. Business Transformation in the Era of Digital Disruption. Hershey, PA, USA: IGI Global; 2025. pp. 89–126.
13. Neware R, Shrawankar U, Mangulkar P, Khune S. Review on multi-factor authentication (MFA) sources and operation challenges. Int J Smart Security Technol. 2020; 7 (2): 62–76.
14. Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: a survey. Cryptography. 2018; 2 (1): 1.
15. Chudasama D. Why choose cyber security as a career. Curr Trends Inform Technol. 2021; 11 (1): 14–19.
16. Shah A, Chudasama D. Investigating various approaches and ways to detect cybercrime. J Netw Security. 2021; 9 (2): 12–20.

