11th International Conference of
Management and Industrial Engineering
2023, Bucharest

ISSN 2344-0937
ISSN-L 2344-0937
Volume 11
Website: https://icmie-faima-upb.ro

IDENTIFICATION OF CRITICAL FACTORS FOR IMPROVINF THE SECURITY OF TELECOMMUNICATION SYSTEMS

Alina-Elena ANCU[1], Andreea BARBU[2]
[1]Vodafone Romania
[1]ORCID: 0009-0009-0025-5226
[1]Email: ancualina@gmail.com

[2]National University for Science and Technology Politehnica Bucharest
[2]ORCID: 0000-0003-3119-8753
[2]Email: barbu.andreeab@yahoo.com

Abstract: The objective of this study is to identify the vulnerabilities that can affect the security of telecommunication systems and to determine the critical factors for improving the security of telecommunication systems. The authors conducted a focus group as qualitative method used for this research with twelve specialists who have a technical position and a vast experience in the telecommunication industry to highlight the critical factors for improving the security of the telecommunication systems. Based on the given answers by the specialists, there were identified thirty-one factors that can be spitted in three categories: technological factors, human factors, and legal factors. For the research limitation, the factors were strictly identified based on the given answers by the selected participants to the focus group. As the practical implication, the authors highlighted first the factors that were defined as vulnerabilities for the security of telecommunication system and determined the critical factors that must be monitored on a regular basis by every company to maintain a safe telecommunication system. As the value of this paper, the authors selected twelve important specialists who have a vast experience in this area and using their answers, it was designed a model of the critical factors that will help every company to improve their security capabilities.

Keywords: *telecommunication system, security, critical factors, risks, vulnerabilities*

INTRODUCTION

The telecommunications business is a key infrastructure that is required for modern society to function and is considered a target for cyber-attacks due to the big amount of processed, controlled and stored sensitive data. A successful telecommunication network attack may potentially reveal the personal information of millions of users and important investment in security is the only way of protecting the company's confidential information that could lead to the interruption of the company's business continuity.

The chosen qualitative method for this research was a focus group that had the scope to highlight 31 factors that affect the security of telecommunication system. These factors can be grouped in three categories as technological factors, human factors, and legal factors. Based on the identified critical factors, every company can design a framework to monitor all company's resources. In this way, the risk assessment of the company's processes will facilitate the mitigation and will conduct to the business continuity of the product or services. The identified critical factors present a great impact in the security of the telecommunication system and the company needs a framework which have the capability of continuous monitoring. This research can create a framework which covers three areas. The first area is from the theoretical perspective and this research has a contribution to the security of telecommunication system. The second area is from managerial perspective, this research will help the company's management to identify, evaluate and reduce the risks using controls in place of the identified critical factors. The third area is the operational part of the companies, these critical factors can help the experts to design and implement processes or activities, to purchase technology, therefore the impact of critical factors on the company's performance will be reduced using the procedure, rules, processes that were created accordingly. Based on the analysis of the published articles from the literature, the authors concluded that there are not enough resources which highlight all the critical factors that will improve the security of the telecommunication system based on a focus group performed with twelve specialists who are working in two kind of departments, with different objectives as follows: specialists who are working in the operational or business department, involved in the service delivery to the customers and specialists who are working in the support department as IT or security and have the responsibility to maintain and create a safe framework for the delivery departments in order to achieve the goal as service delivery to the customers on the agreed terms, conditions and expected quality.

This research will complete the literature with the focus on the security of telecommunication system and will present the critical factors that will help every company to increase the security, based on the experience of twelve specialists who are facing in their daily work issues that must be identified on time to prevent possible security incidents. This article will be structured as follows: introduction will present the context and the scope of identifying the critical factors for improving the security of telecommunication system, literature review will present relevant definitions of telecommunication systems and relevant researches with the obtained results for this subject, methodology will present the used method for this

research, data collection and results analysis will present the input of the focus group and the analysis of the results and the conclusion will present the main objectives of the research and the summary of the article.

Based on the definition, any form of long-distance communication that makes use of common carriers, such as radio, television, and phone, is referred to as telecommunications in general. Telecommunication technologies are used to accomplish data communications, which is defined as a subset of telecommunications. Communications technologies are interwoven in modern enterprises. Electronic communications are becoming a business necessity for reducing time and distance constraints. When clients, suppliers, vendors, and regulators are a part of a global company that operates someplace around the clock, seven days a week (”24/7”), telecommunications take on a unique function. An integrated computer and telecommunications system, which is typical in any commercial environment, is represented by the Figure 1. [1]

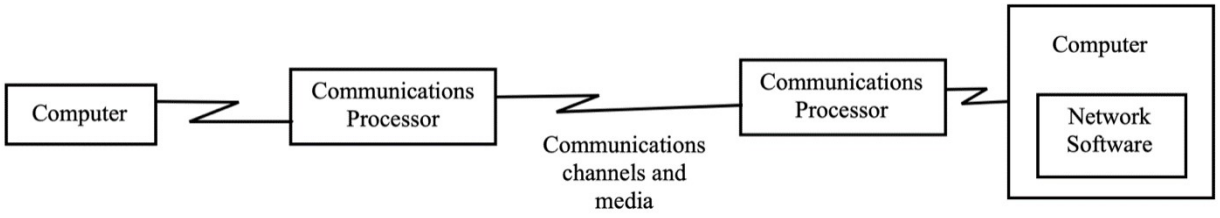

Figure 1: An integrated computer and telecommunications system
Source: adapted from Efraim Turban, Ephraim McLean, James Wetherbe, 2004, Information Technology for Management: Transforming Organizations in the Digital Economy

A telecommunication is defined as “a collection of compatible hardware and software arranged to communicate information from one location to another” and these systems will facilitate the transmission of text, data, graphics, voice, documents, or video information. A typical telecommunications system is shown in Figure 2 and according to the authors, those systems have two sides: the transmitter and the receiver. [1]

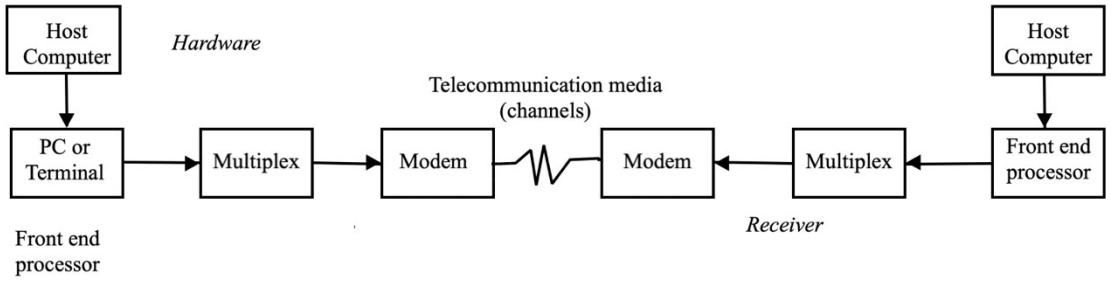

Figure 2: A telecommunications system.
Source: adapted from Efraim Turban, Ephraim McLean, James Wetherbe, 2004, Information Technology for Management: Transforming Organizations in the Digital Economy

The major components of a typical telecommunications system are the following: hardware—all types of computers and communications processors (such as a modems or small computers dedicated solely to communications); communications media—the physical media through which electronic signals are transferred; includes both wireline and wireless media; communications networks—the linkages among computers and communications devices; communications processors—devices that perform specialized data communication functions; includes front-end processors, controllers, multiplexors, and modems; communications software—software that controls the telecommunications system and the entire transmission process; data communications providers—regulated utilities or private firms that provide data communications services; communications protocols—the rules for transferring information across the system; communications applications—electronic data interchange (EDI), teleconferencing, videoconferencing, e-mail, facsimile, electronic funds transfer, and others. [1]

One of the relevant research projects analysed it was published by (Elham et al. 2022), with the title “Key Factors Influence on Decision Making to IoT Adoption in Telecommunication Companies: A Review”, where the authors determined the main factors of decision making to adopt IoT in telecommunication company. Their paper identified four critical factors as: Security; Cost; Technology developers such as telecom companies, connectivity platform developers, data network developers; Users and customers (corporate users, corporate customers, individual customers). According to the authors, these fours critical factors contribute to the success, expand markets, facilitate communication and competition in the companies, and benefit enterprises, users, and customers and at the same time, these fours factors are considered key players for the IoT adaptation. [2]

According to (V. Chellappan et al. 2016), to implement Internet of Things solutions in organizations (telecom companies), security threats to data and service privacy, as well as authentication, must be addressed. To combat cyber-attacks, telecommunications businesses must ensure the development of IoT solutions with robust security and face difficulties in finding staff with IoT security capabilities. Another author (J. H. Ziegeldorf et al. 2014) concluded that the loss of an

organization's reputation and a relevant example is exposing customer privacy is considered of the most serious consequences of flaws, resulting in costly legal action. Given the IoT reference model described in ITU-T Guideline Y.4000/Y.2060, which integrates security capabilities classified into two categories (Anaam et al 2018), this is one of the barriers to the performance of IoT projects derived from R&D efforts. General security capabilities (independent of applications, included in the application, network, and device layers, such as permissiveness, authentication, incoming monitoring, data privacy, device safety validation) and application-specific security capabilities (related to application-specific demand and mobile payment). Furthermore, the IoT development participant will almost certainly use the following documents to safeguard the security and privacy of the IoT solution's characters: (1) ITU-T Recommendation X.1205: Fundamentals of Cybersecurity (Anaam et al 2020), which provides a taxonomy of security threats to an organization. (2) ITU-T Y.4806: Security Capabilities Enhancing Internet of Things Security; identifies security issues that may impact Internet of Things security and safety capabilities. (ITU-T 2017). [2]

According to (I. Lee and K. Lee, 2016), a lack of safety and privacy may contribute to the failure of IoT adoption programs. One strategy to dealing with this issue is to focus on the staff skills of IoT professionals to deploy and get settlement based on R&D efforts. In this regard, the CIO is expected to collaborate closely with the CISO to ensure that competent personnel with IoT security experience are included in the IoT development team and that IoT devices and software solutions to install safe IoT applications are purchased.

According to (Chellappan et al, 2016) to combat cyber-attacks, telecommunications businesses must ensure the development of IoT solutions with robust security and face difficulties in finding staff with IoT security capabilities. Three types of dangers have an impact on Internet of Things solutions. Take a picture (is responsible for capturing information), tamper (refusing, destroying, and interrupting the IoT solution), and Disrupt (refusing, destroying, and disrupting the IoT solution due to data modification). Passive threats (snooping or transmission monitoring) as well as active threats (attacking the Internet of Things network) are both potential concerns (misrepresentation, man-in-the-middle, re-enactment) Denial-of-Service (DoS) attacks).

Another relevant research was published by (Syarulnaziah at al, 2023), where the study was focused in addressing the following research questions: "RQ1 - What are the perceived security and privacy risks by the telecommunication provider for big data adoption? and RQ2 - What are the specific mitigation strategies to address the security and privacy challenges?". Based on the focus group performed on 8 experts, 14 themes were structured as follows: technological, organisational, environmental challenge and mitigation strategies. The challenges mentioned were structured as follows: data management; data privacy; integrity and reactive security; big data compliance; data governance; subject matter expertise; competition intensity and market structure; regulatory orchestration; technological support and as the mitigation strategies: advanced security tools; continuous security assessment; security culture promotion; security talent development and strategic plan. [5]

Another analysed research was published by (S. Benqdara I. Alshiekhy, 2023), where the authors have the objective to assess the hypothetical risks of the implementation of an information security policy as well as to examine the vulnerabilities and effectiveness of that policy. In the context where telecommunications companies must maintain an extensive client database, if such a database is exposed to a third party, it may constitute a significant risk to both the user and the service provider and having a robust information policy in place must be one of the priorities to create a safe framework. [7] Any organization's information security is critical. Information security safeguards data resources and ensures the three pillars of data security: confidentiality, integrity, and data availability. This is due in part to the increasing number of threats to information technology infrastructure around the world. Organizational information security challenges endure because of ongoing data breaches, system outages, and malicious software. [8] An organization's information security policy offers the required platform and regulatory framework to regulate users' security-related behaviour. [9] Policies must offer guidelines of how challenges or issues should be addressed, how technologies should be used and does not include the explanation of how to operate equipment or software because this kind of information should be included in user manuals and system documentation as standards, procedures, and practices. Policy should never contradict the law since doing so can expose the business to serious responsibility. Security rules are the cheapest control to establish but the most difficult to apply correctly. [8]

EXPERIMENTAL

To find the factors that will affect the security of telecom systems and after that to highlight the critical factors that will improve the security of telecom system, for the experimental part, the used qualitative method was a focus group.
A focus group is defined as a small group of carefully chosen people who contribute to open conversations for research purposes. The hosting organization carefully selects study participants to represent the larger community they are seeking to reach. A moderator is involved in this study and his role is to assure valid outcomes and to prevent bias in conversations. [13]

The research's objectives of security of telecommunication systems are the following: (1) identify the factors that affect the security of telecommunication system and (2) identify the critical factors for improving the security of telecommunication system. To achieve the research's objectives, twelve specialists were selected to be part of the focus group. The criteria for the selection of the participants were the following: working in the telecommunication company, have more than 5 years' experience in this industry, and have a technical position which needs technical expertise. The selected participants in this focus group have technical position and they are part of business departments which are responsible for the service delivery to the customers and in the support department as IT and security department. In this way, all the factors that can affect the security from both perspectives will be covered and discussed in this research. In the analysis, every participant receives a code starting from P1 and Table 1 contains the position of every expert who participated in the focus group.
Table 1: Participants of the qualitative research

Participant code	Participant position
P1	Service Delivery Manager
P2	Network Administrator
P3	Network Administrator
P4	Quality & Security Engineer
P5	IP Engineer
P6	Service Delivery Manager
P7	IT Helpdesk engineer
P8	Cyber Security Officer
P9	IT Manager
P10	Front Office Team Leader
P11	MBB Product Manager
P12	Security Engineer

In the first phase, the participants were involved in the identification of the factors that affect the security of telecommunication systems. Based on their answers, the authors concluded 31 factors. In the second phase, based on these 31 factors identified, every participant was requested to choose from his experience what are the critical factors that improve the security of telecommunication system.

RESULTS

In the data collection phase, the participants defined based on their experience the factors that affect the security of telecommunication system, and the Table 2 presents the answers of 12 participants as input. As notation Part. Code represents the code received by every participant to the focus group.

Table 2: The answers of participants for the phase I.

Part. code	Factors defined by each participant
P1	Employees' security knowledge; Proactivity and company/platform processes Monitoring, reactivity, containment and remediation tools and capabilities used by the company
P2	Access control type
P3	Correct identification of users, applications, services, etc. Security parameters: control access to applications, data, etc. only authorised users can access. Data privacy: protect data through encryption protocol, tunnelling. E.g., IPsec VPN Testing and monitoring: proactivity in terms of testing and monitoring the implementation of security systems. Management tools: long-term planning of a strategy that allows data centralisation and scalability.
P4	Poor management involvement, poor physical security, lack of internal security procedures for telecommunications systems
P5	Ransomware attacks, vulnerability of certain network equipment.
P6	Physical security; Mobile terminals in byod system; Virtualization and cloud migration; Internal awareness of security risks; Attacks on telecom customers (phishing, malware, DDoS, DNS attacks etc).
P7	According to the type of threats, there are three categories: trojans, worms; buffer overflow; DoS, DDoS.
P8	Human Resources
P9	Vulnerabilities, misconfiguration of equipment, poor identification of company assets.
P10	Quality and training of human resources operating the network. Physical and remote access control within the organization. Training and enforcement on contemporary risks and vulnerabilities. Internal personal and IT data security processes. Network-wide implementation of up-to-date security patches. Analyse and mitigate risks identified from security reports and audits.
P11	Network security is influenced by components and users in the sense that a network that is prepared to face cyber-attacks of any kind must be as up to date as possible on both the hardware and software side so that users can use it securely. We're talking about firewalls, routers, servers and their up-to-date software, equipment that is compliant with the latest communications protocols and ready to face network attack attempts. Robustness, availability, speed of access, encryption, network access mode, controlled user access, multi-step authentication, network segmentation are examples of the elements that make up network security.
P12	The increasing number and complexity of cyber-attacks on networks. Not very good coordination between EU member countries, especially in the prevention of attacks against networks; Sometimes unclear and uneven security regulations between EU countries and sometimes ambiguous legal framework in this area; Low involvement of governments; Low investment including in research on the development of security solutions for telecommunication networks

Based on the phase I, there were structured 31 factors that affect the security of telecommunication system based on the answer given by the participants and these factors are presented in the Table 3.

Table 3: Factors that affect the security of telecommunication systems.

Factor code	Factor
F1	Security knowledge of employees
F2	Proactivity and company/platform processes
F3	Monitoring, reactivity, containment and remediation tools and capabilities used by the company
F4	Access control type
F5	Correct identification of users, applications, services
F6	Security parameters: control access to applications, data, etc. only authorised users can access.
F7	Data privacy: protecting data through encryption protocol, tunnelling. Ex: IPsec VPN
F8	Testing and monitoring: proactivity in terms of testing and monitoring the implementation of security systems.
F9	Management tools: the long-term planning of a strategy that allows the centralisation of data and the possibility of expansion.
F10	Weak management involvement
F11	Ransomware attacks
F12	Vulnerability of certain network equipment's.
F13	Physical security
F14	Mobile terminals in byod system
F15	Virtualisation and cloud migration
F16	Internal awareness of security risks, attacks on telecom customers (phishing, malware, DDoS, DNS attacks)
F17	The three categories, depending on the type of threat: trojans, worms; buffer overflow; DoS, DDoS
F18	Poor identification of company's resources
F19	Quality and training of human resources who are operating the network.
F20	Control physical and remote access within the organisation.
F21	Training and application on contemporary risks and vulnerabilities
F22	Internal personal and IT data security processes
F23	Deployment of security patches, keeping them up to date, network wide.
F24	Analysing and mitigating risks identified from security reports and audits.
F25	Hardware and software updates
F26	Network robustness and availability
F27	Increasing number and complexity of cyber-attacks on networks
F28	Poor coordination between EU member countries on work to prevent network attacks
F29	Weak regulations and ambiguous legal framework in this area
F30	Research on the development of telecommunications network security solutions
F31	Low involvement at government level

After the moderator listed the factors that were identified in the first step, every participant selected the critical factors that can improve the security of telecommunication system and the centralization of the critical factors were performed by the highest number of mentions by each participant. There was calculated the percentage for each factor of how many times it was mentioned as critical factors and the results are presented in the Table 4.

Table 4: Critical factors that improve the security of telecommunication system.

Factor code	Factor	Number of mentions	Percentage
F1	Security knowledge of employees	2	16,60%
F2	Proactivity and company/platform's processes	2	16,60%
F3	Monitoring, reactivity, containment and remediation tools and capabilities used by the company	2	16,60%
F4	Access control type	1	8,33%
F5	Correct identification of users, applications, services	2	16,60%
F6	Security parameters: control access to applications, data, etc. only authorised users can access.	3	25%
F7	Data privacy: protecting data through encryption protocol, tunnelling. Ex: IPsec VPN	3	25%
F8	Testing and monitoring: proactivity in terms of testing and monitoring the implementation of security systems.	2	16,60%
F10	Weak management involvement	3	25%
F15	Virtualisation and cloud migration	1	8,33%

Factor code	Factor	Number of mentions	Percentage
F18	Weak identification of company's resources	1	8,33%
F19	Quality and training of human resources who are operating the network.	1	8,33%
F20	Control physical and remote access within the organisation.	1	8,33%
F22	Internal personal and IT data security processes	1	8,33%
F23	Deployment of security patches, keeping them up to date, network wide.	1	8,33%
F24	Analysing and mitigating risks identified from security reports and audits.	1	8,33%
F25	Hardware and software updates	1	8,33%
F29	Weak regulations and ambiguous legal framework in this area	1	8,33%

DISCUSSION

Based on the results obtained from the responses of the twelve specialists who participated in the focus group, 25% of them chose the following three factors: security parameters as controlling access to applications, data, etc. only authorised users can access, data confidentiality: protecting data through encryption protocol, tunnelling. E.g., IPsec VPN and low management involvement. These have been identified as critical factors as they have the greatest impact through network access control, restricting access to unauthorised persons, correct identification of unauthorised persons and a continuous evaluation of the access received must be carried out to prevent incidents that may affect the company financially and in terms of image. As telecommunications systems must process a large amount of sensitive, confidential data, the company must implement methods to prevent any unauthorised access and data leakage, which can compromise the company's business and image. Another important factor chosen by respondents is the low management involvement which is essential in investment for areas that need improvement, investment in equipment or tools that can increase the security of systems. Management plays a key role and provides clear direction through their day-to-day activities, through the active involvement that employees see on issues involving the security of services or systems. At the same time, management can create processes, checks if these ones are implemented by employees and test the applicability. One of the most well-known information security standards, ISO 27001, which audits the company's information security management capabilities, also provides for these two areas, the work of management, which must be focused on prevention and constant improvement of security, but also the processes created by the company for controlling access given to employees and the methods by which it is restricted and can prevent incidents with a disastrous effect on the company. ISO 27701 is the standard that covers this area of personal data, the measures that the company applies in the event of incidents, as well as their prevention.

The following critical factors were mentioned by 16.6% of experts and cover the following areas: employee security knowledge; company/platform proactivity and processes; monitoring, reactivity, containment and remediation tools and capabilities used by the company; correct identification of users, applications, services; monitoring the implementation of security systems. These factors related to the security knowledge of employees, who in turn must carry out their work considering and respecting all the rules imposed by the company, which materializes in the prevention of high-impact incidents. Any company must implement processes that must prevent and provide guidance to its employees to carry out their work under the conditions imposed and required by the customer. Employee's proactivity can lead to risk reduction, improvement, or activities' automation. The monitoring, reactivity, containment, and remediation capabilities of the company are considered important because they must be updated according to the used technologies, their capabilities must be state-of-the-art to be used to their full capacity to detect and mitigate risks identified in those processes. To have a clear overview of a company's processes, it is essential to correctly identify users, applications, services for management and monitoring that allows timely troubleshooting and remediation. Monitoring the implementation of security systems was also considered an important factor because a company needs to continuously review the implementation of these systems which are designed to protect both physical resources and its intellectual property.

The following critical factors were identified in a percentage of 8.33% and concern: type of access control, which refers to the four access control models, access management to confidential information is done in a unique way: discretionary access control (DAC), role-based access control (RBAC), mandatory access control (MAC), attribute-based access control (ABAC). [14] Another factor is related to the weak identification of resources in the company. These resources as equipment that is necessary to carry out the business, every company needs to have a clear record of all resources as they hold confidential information that needs to be protected. Physical and remote access control within the organisation refers to the protection of all equipment and premise of unauthorised access or persons. Internal personal and IT data security processes are necessary to protect the stored sensitive data. Implementing security patches and keeping them up to date throughout the network are among the tasks of an IT department, which is responsible for protecting company equipment by implementing these methods. Analysing and mitigating the risks identified by security reports and audits is also a necessary activity for any company that needs to consider all risks that could disrupt the core business. Security audits test a company's capabilities to respond to risks that could occur in every process. Hardware and software upgrades are also necessary because from the point must be reported to technological advancement. The quality and training of the human resources operating the network is one of the factors mentioned because the skills of employees need to be regularly assessed, companies need to invest in his staff's trainings, because in this way, the employees can deliver the expected quality imposed by the company itself and by their customers. The network incidents' risks can also be prevented by

constantly preparing employees to deal with all the tasks and challenges they face in their daily work. Weak regulations and an ambiguous legal framework in this area is a legal factor mentioned by one expert, who considered that the government must analyse and standardize the appropriate legal framework in the telecommunication industry.

CONCLUSIONS

This study has provided an overview of the factors that affect the security of telecommunication system and were highlighted the critical factors that improve the security of telecommunication systems through the method used as a focus group with 12 specialists who are working in the telecommunication industry. The participants were selected based on three important criteria and have experience from both side as operations departments and support departments. In this way, there were identified all factors that can affect the security of telecommunication system from service delivery perspective and from support activities that facilitate a better understanding of the company's security framework.
In the first phase, there were identified 31 factors that can affect the security of telecommunication system and in the second phase, there were identified 18 critical factors that can improve the security of telecommunication system which covers three categories of factors: technological factors, human factors, and legal factors.

Some of these factors need to be monitored more closely by the company because they can be a major source of risk for telecommunication systems. One of the technological factors chosen in the focus group was access control, which is critical in the world of telecommunications, since it ensures the confidentiality and privacy of data in transit and at rest. Its effective implementation is critical in safeguarding network infrastructure, services, and sensitive data, preventing the introduction of vulnerabilities that could have serious consequences for resource integrity. Another critical factor is data privacy, also known as information privacy, is a branch of data protection concerned with the proper handling of sensitive data but also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements while also protecting the data's confidentiality and immutability. Proactive monitoring in the context of monitoring products typically involves spotting possible faults within IT infrastructure and applications before users notice and complain, and then taking action to prevent the issue from being user noticeable and business damaging. Proactive monitoring entails a company always looking for signals that an issue is going to occur.

Based on this research, the first objective was achieved because using the qualitative method there were identified 31 factors that affect the security of telecommunication system. The second objective of this research was achieved based on the identification of 18 critical factors that can improve the security of telecommunication system. Based on the analysis of the relevant published articles where the authors explored this theme, some of these factors were identified in the other literature research, which means that the results will confirm the results obtained by the other researchers. Data privacy was considered one of the top challenges met in the telecommunication industry, due to the big amount of the sensitive data processed, stored, and controlled. Some of the critical factors for improving the security of telecommunication system were identified as mitigation strategies for big data adaptation as: advanced security tools which are considered very important because every company must do investment in the tools used by their employees and the capability of the tools must be up to date. Another strategy was the continuous security assessment which was also mentioned in the focus group and it's another factor that can improve the security. Security culture promotion and security talent development were also mentioned by participants because human resources are one of the important investments for every company. Besides the equipment's and tools that must be up to date, the employees need trainings for their career growth, because only in this way, the employees can demonstrate their capabilities and the trust in the company will grow.

As qualitative research, one of the limitations is considered the number of the participants who are working in the same company, 31 factors were identified strictly based on their responses which are subjective, and those ones cannot be generalized. As the future research, it will be considered relevant to extend the qualitative method on more participants that are working in more than 2 companies from the telecommunication industry.

REFERENCES

[1]. Turban, E.; McLean, E.; Wetherbe J.: Information Technology for Management: Transforming Organizations in the Digital Economy, Publisher Wiley, ISBN-13 978-0471229674, (2004)
[2]. Elham, A. et al: Key Factors Influence on Decision Making to IoT Adoption in Telecommunication Companies: A Review, *International Journal of Engineering & Technology, Website: www.sciencepubco.com/index.php/IJET*, (2022)
[3]. Chellappan, V.; Sivalingam K.M: Security and privacy in the Internet of Things. In Internet of Things (pp. 183-200). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-805395- 9.00010-1, (2016)
[4]. Ziegeldorf, J. H; Morchon, O. G; Wehrle, K: Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728-2742. https://doi.org/10.1002/sec.795, (2014)
[5]. Syarulnaziah, A. et al: Security and Privacy Challenges of Big Data Adoption: A Qualitative Study in Telecommunication Industry, ***International Journal of Interactive Mobile Technologies (iJIM)*** – eISSN: 1865-7923., (2023)
[6]. Benqdara, S; Alshiekhy, I.: Information Security Policy Implementation Assessment in Libyan Telecommunications Companies, *International Journal of Computer Applications (0975 – 8887)* Volume 185 – No. 2*, April 2023*
[7]. Safa, N.; Ghani, N.; Ismail, M.: An artificial neural network classification approach for improving the accuracy of customer identification in e-commerce; Malays J Computer Sci, vol 27(3), 171–85, (2014)
[8]. Al-Mayahi, I.; Mansoor S.P.: Information Security Culture Assessment: Case Study, *Third International Conference on Information Science and Technology*, Yangzhou, Jiangsu, China, 23-25, (2013)
[9]. Klein, R. H.; Luciano, E. M.: What Influences Information Security Behavior? A Study with Brazilian Users. *JISTEM-Journal of Information Systems and Technology Management*, vol13 (3), 479-496, (2016)

[10]. Anaam, E.; Abu Bakar, K.; Mohd Satar, N: A Model of Electronic Customer Relationship Management System Adoption In Telecommunication Companies, *Amazonia Investiga*, Vol. 9, No. 35, 61-73, https://doi.org/10.34069/AI/2020.35.11.5 , (2020)
[11] Anaam, E.; Abu Bakar, K.; Mohd Satar, N : A theoretical review of conceptual model for E-CRM success in telecommunication companies. https://doi.org/10.14419/ijet.v7i4.17674, (2018)
[12]. Anaam, E et al: Critical success factors for electronic customer relationship management success adoption: Telecommunication companies case study, *International Journal of Advanced and Applied Sciences*, http://science-gate.com/IJAAS/Articles/2021/2021-8- 10/1021833ijaas202110013, (2018)
[13]. Question Pro Communities, *Available from* https://www.questionpro.com/blog/focus-group/ *Accessed:* 2023-05-10
[14]. Microsoft Security, *Available from* https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control#:~:text=Access%20control%20selectively%20regulates%20who,access%20control%3A%20physical%20and%20logical. *Accessed:* 2023-05-10

Corresponding author:
Alina-Elena ANCU, Title: PhD Candidate
Full address: Splaiul Independenței 313, București 060042
Email: ancualina@gmail.com