Management approaches and application areas of information security in organizations

Ivan Gaidarski
Institute of Robotics
"St. Ap. and Gospeller Matthew"
Bulgarian Academy of Sciences
Sofia, Bulgaria
ivangaidarski@ir.bas.bg

Neda Chehlarova
Institute of Robotics "St. Ap. and Gospeller Matthew"
Bulgarian Academy of Sciences
Sofia, Bulgaria
nedachehlarova@ir.bas.bg

Abstract. **In organizations, two types of communication can be distinguished, predetermining approaches to Information Security (IS): communication based on equality - "Network communication" (Networks from/in organizations) and "Hierarchical organizational communication". A primary task of IS in an organization is to protect sensitive data in both types of communication. The IS approach must be tailored and cover all options – a holistic approach. Existing IS management approaches can be divided into two large groups: Information security approaches in Network Communications and data security approaches in Hierarchical Organizational Communication. Approaches to managing IS in network communications include Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-Virus, Anti Malware, Endpoint Protection, Perimeter Security and Cyber-threat intelligence systems. IS management approaches in Hierarchical Communication include Data Classification and Data Leakage Prevention (DLP) systems. In the article are examined the areas of application of the different approaches to information security in an organization - External network, Network Perimeter, Internal network, Computer equipment, Applications and Data.**

Keywords: communications, competence, data, digital information, management, protection, security

I. INTRODUCTION

The daily development of Information and Communication Technologies (ICT) in all spheres of life requires constant support and monitoring in maintaining the security and accessibility of data and information between the parties involved in specific economic relations. At the state and international level, policies and strategies regarding the qualification of employees in the field of information security (IS) and work with ICT continue to be updated in accordance with various regulations and security standards such as EU GDPR [1], ISO 27001 [2], Sarbanes-Oxley Act [3], HIPAA [4], PCI Security Standards [5], as well as local regulations such as the Minimum Requirements for Network and Information Security Ordinance [6].

In the National Strategic Document "Digital Transformation of Bulgaria for the period 2020-2030 [7], objective IV. Unlocking the potential of data includes an emphasis" on expanding the volume of open data generated and processed by government institutions and businesses and facilitating data sharing between private entities."

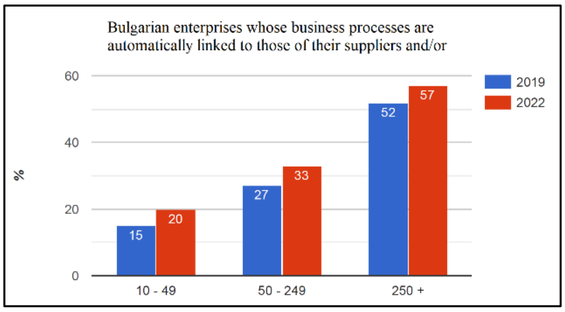

Fig. 1. Bulgarian enterprises whose business processes are automatically linked to those of their suppliers and/or consumers.

“Fig.1” shows the National Statistical Institute of Bulgaria data from the last two state observations regarding "Enterprises whose business processes are automatically connected to those of their suppliers and/or consumers" [8]. In 2023, there is a 5% decrease in organizations with the number of employees "10-49" and a 3% decrease in those with "50-249", compared to the data from 2017. Large enterprises in the country have continued their digital policy in the past year - 36%, which is almost double the value compared to small and medium-sized enterprises.

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8062

The enterprises that have a written policy for managing ICT security processes in the country [9] are presented in “Fig.2”. A 5% increase in 2022 is observed for all enterprises, regardless of their size. Here again, enterprises with more than 250 employees have the highest percentage - 57%, which is double the value compared to the small "10-49".

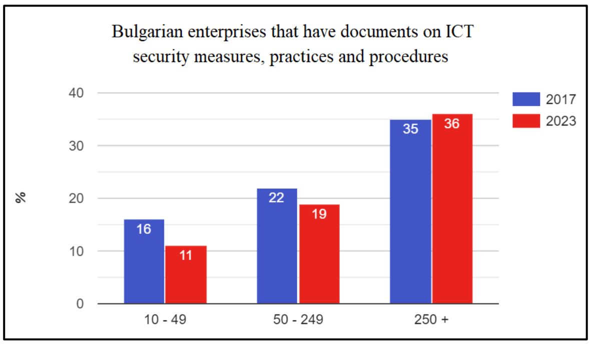

Fig. 2. Bulgarian enterprises that have documents on ICT security measures, practices and procedures.

Despite the positive national trends, in 2022 Bulgaria is still in one of the last places in the European Union according to the same indicators. With average European values of over 35%, just over 20% of the surveyed organizations in our country have a similar approach to their information security policy [10].

In this article, the main approaches to information security (IS) in modern organizations are examined, depending on its structure and communication inside and outside it [11].

II. Materials and Methods

In the first part of the study the types of communication in modern organizations are examined. Regardless of the specifics of its activity, every contemporary organization has a clearly defined structure with established relationships between employees. With the development of organizations, the need arises for effective coordination of the main activities, and accordingly for evolution in their organizational structure. It is gradually changing from a flat to a vertical hierarchical structure, with different levels of management, roles and responsibilities for employees. Organizational roles are a set of clearly defined rights and responsibilities described in the job description of the respective position. They reflect the needs of the organization, not the personal qualities of the employees occupying a given position. Thus, the relevant position does not depend on specific individuals and allows flexibility when changing employees. As organizations evolve as social structures, communication among its employees changes from simply sending and receiving messages to processing and interpreting messages inside and outside the organization, as well as the information contained in them. The contemporary organization operates as a large-scale integrated system in which individual day-to-day operations are interdependent. Hence the need for standardized communication procedures and their formalization.

Natural day-to-day communication between employees can be defined as informal communication. It does not follow a given form, pattern or certain formalized rules. Informal communication is vital to an organization because it is how everyday tasks are carried out. It is characterized by the fact that it does not obey a strict hierarchy, in contrast to formal communication, which follows the hierarchical structure of the organization. Formal communication follows strictly formalized rules, with set templates that are characteristic of a given type of organization. It is characterized by the observance of certain priorities and subordination, such as messages descending from management down the structure. From the point of view of the communication implementation approaches, two types can be distinguished: *Network communication*, ensuring equality between its participants and *Hierarchical organizational communication* based on the hierarchical structure of the organization [12].

Next part of the study examines the approaches for information security management and areas of information security application in the organizations.

Based on the main types of communication, two main types of IS management approaches can be defined - IS approaches in *Hierarchical organizational communication* and IS approaches in *Network communications* “Fig. 3”.

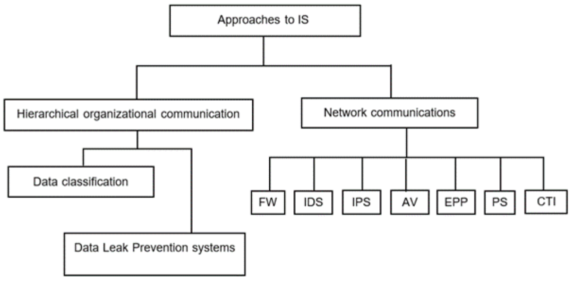

Fig. 3. Approaches to IS based on the type of communication.

IS management approaches in *Network communications* include various hardware and software solutions such as: Cyber-Threat Intelligence (CTI), Antivirus and AntiMalware (AV), Endpoint Protection (EPP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Firewalls (FW), Perimeter Security (PS).

Cyber-Threat Intelligence collects raw data on emerging or existing threats, analyses them and provides real-time information on currently evolving cyber-threats targeting the organization. They provide a comprehensive picture of the threats to the organization outside its protected perimeter [13], [14].

Antivirus and AntiMalware solutions protect an organization's applications and files by scanning them for viruses, Trojans, and other malicious code in real-time, and eliminating them when detected [13] - [15].

End Point Protection solutions protect the so-called endpoints - any device that can process data - workstations, servers, mobile and IoT. Protection includes both threats and data leakage, corruption or falsification [13], [14].

Intrusion Detection Systems solutions monitor and analyse the organization's internal network traffic, identifying potential malicious applications or attempts to penetrate the protected network [13], [14].

Intrusion Prevention Systems work together with IDS systems, eliminating detected threats [13] - [15].

FireWalls are tasked with preventing unauthorized access by monitoring incoming and outgoing network traffic and filtering it according to set criteria [13].

Perimeter Security provides the protection of data and resources in the perimeter of the corporate IT network [16], [17].

Hierarchical Communication IS management approaches include Data Classification (DC) and Data Leak Prevention (DLP) solutions.

Data Classification solutions allow organizations to accurately identify protected data by marking it according to the organization's adopted classification system. Visual markers (labels) and metadata are used, which unambiguously identify the protected information. DC systems also ensure accurate identification of the creators of the corresponding document or message, for example emails, ensuring personal responsibility for their content. Tagging reduces the risk of sensitive data leaking into the organization by enabling accurate identification from other IS approaches, such as Data Leak Prevention systems [17], [18].

Data Leak Prevention solutions provide detection and subsequent prevention of attempts to leak sensitive data outside the organization's protected network [15,16]. Sensitive data can include both corporate information (patents, know-how, trade secrets, bank accounts and credit card numbers) and personal data such as social security number, residential addresses, medical data and others, subject to protection by various standards and regulations [13], [15].

IS approaches, in addition to having a certain functionality in relation to the object of protection (data, applications), are also characterized by a certain area of application, defining their place in the ICT infrastructure of the organization. As an example, the multilayer protection model of “Fig.4” can be used. Each layer is subject to unique threats and different IS approaches are used to protect against them.

The External network layer includes networks external to the organization, for example the Internet. A characteristic feature of external networks is that they are unprotected. For their protection, IS approaches such as Vulnerability Analysis, Audit, Virtual Private Networks, Logging, Demilitarized Zone, Penetration Tests and SIEM are used.

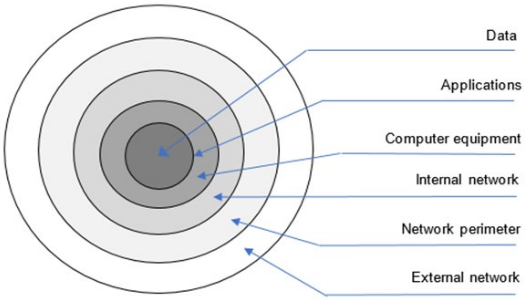

Fig. 4. Multilayer model for protection.

Network perimeter is the border area between the unprotected external network and the protected internal network. In this area of application, approaches to IS such as AntiVirus and AntiMalware, Static and Dynamic Packet Filtering, Proxy Server, Firewalls, Vulnerability Analysis and Penetration Tests find application.

Internal network is the protected internal network of the organization. It is usually well protected as the organization conducts its day-to-day operations within it. The IS approaches used in the internal network include solutions such as AV, IDS, IPS solutions, access control, encryption solutions, etc.

Computer equipment – a unifying term for the ICT infrastructure of the organization - servers, workstations, mobile devices and peripheral devices connected in a network. IS approaches include Endpoint protection, Firewalls, Authentication, Logging, Password hashing, Audit and DLP solutions.

Applications – the software applications installed on the computer equipment and used in the day-to-day activities of the organization. These include Data Classification, Data validation, Content filtering, Audit tools.

Data – includes the data collected, generated, used, analysed and processed in the organization. This includes data owned by the organization but used by third parties such as suppliers and partners. IS approaches include Access control, Data backup, Encryption solutions, Data classification and DLP solutions.

III. Results and discussion

The use of innovative approaches for IS management in organizations in the Republic of Bulgaria allows effective protection of their information resources and, in particular, the protection of their sensitive information from leakage or replacement. For example, the widespread introduction of Data Classification Systems, Document Management Systems (DMS) and Content Management Systems (CMS) [19].

Another suitable example is the results of the implementation of a solution for Data Leak Prevention of the manufacturer Acronis DeviceLock [20] in 18 Bulgarian organizations from different sectors, including the national security sector. As a result of the monitoring of the data flows in the endpoints - workstations and laptops, the following general conclusions were drawn “Fig.5” - reduction of incidents of leakage of sensitive data, limitation of channels of data leakage, increase of visibility of sensitive data in the organization by scanning Data-in-rest data and improving compliance with internal and external security policies and regulations [21].

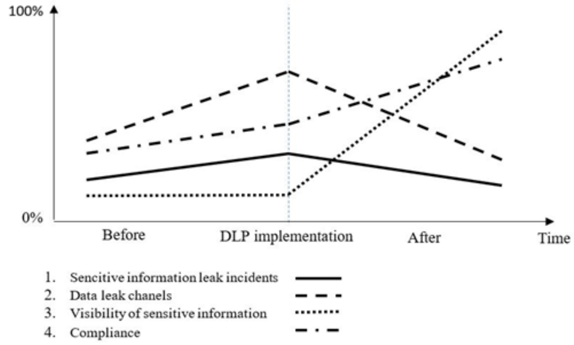

Fig. 5. Generalized results from DLP system validation.

According to data from Statista, the estimated market share of DLP revenue for 2025 will grow 3 times to 3.5 billion compared to the reported values in 2019 [22].

IV. Conclusion

The increase in the complexity of communications and the current processes of digitization at the state and international level lead to new and stricter requirements for the protection of the information resources of modern organizations. These requirements also define changes in the environment in which the information systems of a given organization operate. In the design of modern information security systems (ISS), it is mandatory to provide flexible mechanisms for easy addition and updating of new requirements to the ISS and their rapid implementation, without the main activity of the organization being affected. The complex protection of the organization's sensitive information requires the effective combination of traditional IS approaches within network and hierarchical organizational communication, as well as the addition of innovative IS approaches.

Acknowledgement

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

References

[1] General Data Protection Regulation. [Online]. Available: https://www.gdpreu.org/ , [Accessed February 24, 2024].

[2] ISO 27001 Official Page. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html, [Accessed February 24, 2024].

[3] Sarbanes-Oxley Act. [Online]. Available: https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002 [Accessed February 24, 2024].

[4] B. Herold, R. Beaver, "The Practical Guide to HIPAA Privacy and Security Compliance," 2nd Edition, CRC Press, 2014.

[5] PCI Security Standards. [Online]. Available: https://www.pcisecuritystandards.org/ [Accessed February 24, 2024].

[6] Ordinance on the minimum requirements for network and information security. [Online]. Available: https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf [Accessed February 24, 2024]. (in bulgarian).

[7] National strategic document "Digital transformation of Bulgaria for the period 2020-2030", adopted by Decision No. 493 of the Council of Ministers of 21.07.2020. [Online]. Available:https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1318 [Accessed February 24, 2024], (in bulgarian).

[8] NSI. "Enterprises whose business processes are automatically linked to those of their suppliers and/or consumers". [Online]. Available:https://infostat.nsi.bg/infostat/pages/reports/query.jsf?x_2=719 [Accessed February 24, 2024].

[9] NSI. Enterprises that have documented ICT security measures, practices and procedures. [Online]. Available: https://infostat.nsi.bg/infostat/pages/reports/query.jsf?x_2=1365 [Accessed February 24, 2024].

[10] Eurostat. ICT security in enterprises. Enterprises with documents on measures, practices or procedures on ICT security, 2022. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises&oldid=583136#Documents_on_measures.2C_practices_or_procedures_on_ICT_security [Accessed February 24, 2024].

[11] I. Gaidarski, Method and models for development of information secuity systems in organization, PhD thesis, Department of "Communication systems and services" at Institute of information and communication technologies, Bulgarian Academy of sciences. IICT-BAS, 2022.

[12] B. Wahlstrom, "Perspectives of Human Communication," Wm.C.Brown Publishers,1992.

[13] M. Rhodes-Ousley, "Information Security the Complete Reference," 2nd Edition, The McGraw-Hill, 2013.

[14] Y. Diogenes, E. Ozkaya, "Cybersecurity - Attack and Defence Strategies," Packt Publishing Ltd., 2018.

[15] C. Pfleeger, S. Pfleeger, J. Margulies, "Security in Computing," 4th Edition, Prentice Hall, 2015.

[16] M. Ciampa, "Security+ Guide to Network Security Fundamentals," 4th Edition, Course Technology, Cengage Learning, 2015.

[17] G. Santana, D. Cruz, "Modelling a network security systems using multi-agents systems engineering, Systems, Man and Cybernetics," IEEE International Conference, Vol. 5, November 2003, DOI: 10.1109/ICSMC.2003.1245655.

[18] Guidelines for Data Classification, Carnegie Mellon University. [Online]. Available: https://www.cmu.edu/iso/governance/guidelines/data-classification.html , [Accessed February 24, 2024].

[19] A. Madzharov, "Technical implementation of a reporting system and its workflows," Proceedings of International Scientific Conference "Defense Technologies" (DefTech 2019), "Vasil Levski" National Military University – Artillery, Air Defence and CIF Faculty, 2019, pp. 316-322.

[20] DeviceLock Web Page. [Online]. Available: https://www.acronis.com/en-us/products/devicelock/ [Accessed February 24, 2024].

[21] I. Gaydarski, Z. Minchev, "Conceptual Modeling of Information Security System and Its Validation Through DLP Systems," Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, pp. 36-40, DOI:10.13140/RG.2.2.32836.53123.

[22] Statista. Data loss prevention (DLP) market revenue forecast worldwide from 2019 to 2025. [Online]. Available: https://www.statista.com/statistics/986319/worldwide-dlp-market-revenue-forecast/ [Accessed February 24, 2024].