

Research on Data Security Measures in Romania

Mirona Ana Maria POPESCU

*National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania
mirona.popescu15@gmail.com*

Andreea BARBU

*National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania
barbu.andreeab@yahoo.com*

Petronela Cristina SIMION

*National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
cristinas_upb@yahoo.com*

Georgiana MOICEANU

*National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania
moiceanugeorgiana@gmail.com*

Abstract. Information from the online environment is constantly increasing, as well as its value. In this context, for companies data security becomes a central pillar to protect sensitive information and to ensure its integrity, confidentiality and availability (CIA Triangle). The security measures adopted by the companies also increase the degree of trust of their partners and customers. But data security is not just about implementing the right technologies and policies; equally important is the awareness and proper training of personnel who interact with this data or the applications that contain it.

Human resource in companies plays an important role in protecting sensitive information by understanding the negative consequences of not securing and manipulating in a risky manner the confidential data used in their daily activities. To prepare the human resource and educate the employees in order to raise their awareness towards which is considered sensitive data, what measures and tools must be applied when handling it, trainings by specialized personnel can be implemented. In this manner, the risks of cyber security attacks, data leak, are minimized and the business environment is strengthened. In this research it is presented a review of specialized literature that treat the subject of data security to highlight the current stage of development and have a general landscape from a scientific point of view. Having this as a base, the authors have developed a questionnaire that was distributed to romanian companies to find out the business perspective towards this subject. Therefore, by analysing the two perspectives, this study has the goal to present the dynamics of data security, the challenges brought by it and the good practices that can be adopted.

Keywords: data security, digitalization, security measures, personnel training, information security

Introduction

In the digital age, information security has become a top concern for organizations around the world. Regardless of their size or industry, all organizations are exposed to various cyber threats that aim to compromise the integrity, confidentiality and availability of their data. Since the pandemic of COVID-19, more and more government organizations and businesses improved their

processes and tried to digitalize them. As a consequence of moving data in the digital environment, its volume has increased exponentially and the need of measures and procedures to protect business information and systems has become crucial.

The relevant statistics are used in the context of the European Cyber Security Strategy, which provides the overall strategic framework for EU initiatives on cyber security and cybercrime (figure 1).

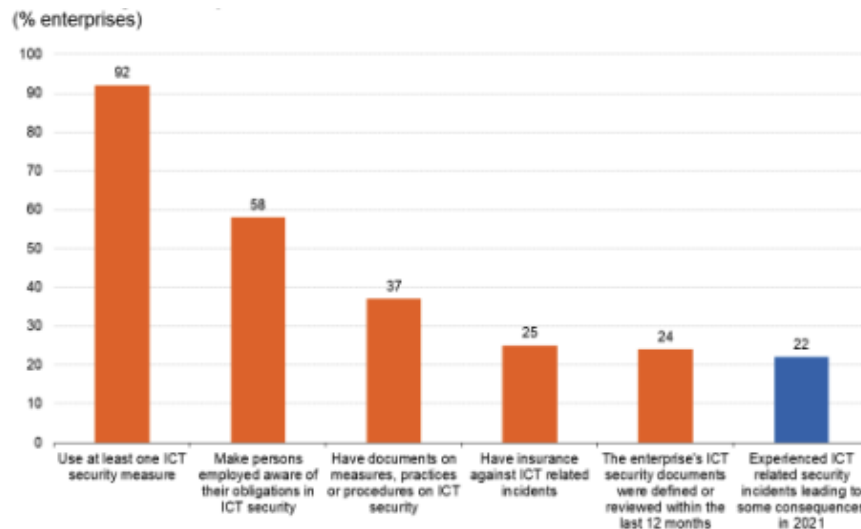


Figure 1. ICT security in enterprises, EU, 2022

Source: Eurostat, 2022.

Data security has become a central concern in the digital age as organizations face increasingly sophisticated cyber threats and increasingly stringent regulations on the protection of sensitive information. In this research it is presented the analysis of recent specialized literature that focuses on security of data and information, along with new measures to protect sensitive data. This was the starting point for a quantitative research that aims to determine the general knowledge of Romanian companies towards cyber security and their degree of preoccupation, investment in this area. The results of the paper want to bring up front a complete view on data security from a business perspective, gathering and filtering information from both scientific and businesses environments. Also, by having an overview to the current landscape, companies can understand and implement security measures to protect their data from potential threats that may come both from the internal and external environment.

Literature review

Properly applied security strategies lead to the protection of an organization's assets against potential internal or external cyber attacks. The most common are represented by human errors. An important component of data security is represented by adopting the proper technology and instruments to identify the company sensitive data easier and protect it. Favorably, these solutions would be able to automate reporting, streamline audits and adhere to regulatory standards, while applying safeguards such as encryption, data masking and redaction of sensitive information. Among the main aspects when it comes to data security at the organization level, the following

elements appear: Identity and access management, data encryption, cyber security, network security, application security and mobile security.

IAM (Identity and Access Management) allows the usage of resource needed by entities without the need of an interface. It is embodied in procedures and systems that let IT managers to give each entity a unique digital identity, verify them upon login, provide them access to certain resources, and keep an eye on and manage these identities over the course of their lives., (Grassi, 2020).

Encryption helps protect the data that is sent, received and stored. This can include text messages stored on smartphones, running logs saved on smartwatches and banking information sent from an online account. Encryption involves rearranging readable text so that only the holder of the decryption key or secret code can decipher it. This promotes the protection of the security of sensitive data, (Becker, 2020), (Fabbrini, 2020).

General cybersecurity and information security have become among the most important ways to protect organizational assets. IT professionals such as risk managers, information security specialists, network administrators and others must have the skills to implement strict measures in the organization to ensure maximum protection of networks, servers, applications and data. Security management certification training is available for those who wish to deepen the field, including risk management and specialize in it at expert level, (Hulshof, 2021).

Network security is the protection of network infrastructure against unauthorized access, misuse or theft. All devices and softwares used by a company, along with users can be protected by creating a secured infrastructure. It is composed of hardware and software technologies and ideally involves layers that include applications, antivirus, access management, servers, firewalls, physical access and policies, (Do, 2020), (Enoch, 2020).

Application-level security procedures to stop data or code theft or diversion within the application are referred to as application-level security measures. It encompasses technology and techniques as methods, software and hardware to protect applications through the entire process of development. One kind of hardware application security is a router that blocks anyone from seeing a computer's IP address online. Software usually includes application-level security features as well, such an application firewall that tightly limits what can and cannot be done. Procedures might include things like an application security regimen with regular testing and other standards, (Al-Kahla, 2021).

Protecting laptops, tablets, and smartphones against risks related to wireless computing is known as mobile security, or more precisely mobile device security. In mobile computing, its significance has grown. The security of corporate and personal data currently kept on cellphones is a major source of worry. Employees that adhere to the "bring your own device" (BYOD) policy utilize their own devices to access work-related systems and perhaps private information over an organization's network, (Marabathuni, 2021), (Palanisamy, 2020).

Methodology

A challenge within organizations is currently represented by securing the handling of private data, both internally and externally by transferring it using different channels and means. A primary research was carried out to determine different aspects towards data security in the romanian business environment.

By understanding the companies concerns and their level of knowledge and importance given to this topic, it can be created a framework to improve the security of sensitive data.

The secondary objectives were represented by identifying the knowledge of the main Security measures for data protection, determining the concern of organizations to invest in data security and the training of the personnel who handle this type of data, applications.

The target group was formed by people who work within the management teams or departments of the organizations, as they are more likely to know details about the adopted measures and investments. The questionnaire was sent to them individually, digitally (email, social media platforms), in the form of a link that directed them to the first page of the questionnaire. Due to the limited amount of responses achieved this research is an exploratory one, that can only present trends and be used as guidance for more comprehensive researches.

The quantitative research was carried out to determine investment trends in security both from the point of view of private data and of the personnel who handle this type of data, obtaining a number of 33 valid responses. The instrument used consisted of questionnaire-based survey and included analysis methods represented by questions with single, multiple answers, semantic differential scale and Likert scale. An online survey was built through the Office suite from Google (<https://docs.google.com/forms/>).

The distribution of the questionnaire was carried out throughout 2023, using an electronic written message. It only targeted people who hold management positions in companies in organizations that have various fields of activity. The conditions under which the transmission and completion were carried out were identical for all respondents, by attaching a link in the content of the message, which redirected them to the main page of the questionnaire, in order to be able to view the content and answer the questions by selecting the predefined options.

Results and discussions

With the development of technology, protecting data from unwanted access—which might lead to its misuse—becomes increasingly crucial as more data is kept in vast networks. All organizations have data sets with private information about their operations in them. Assuring the safety of computers, networks, and related data is known as computer system security.

Figure 2 presents a summary of the degree of awareness and implementation of the main data protection measures in commercial companies. The fact that the percentages are close between the three variants suggests that there is a general tendency within these organizations to implement or be in the process of implementing these data protection measures.

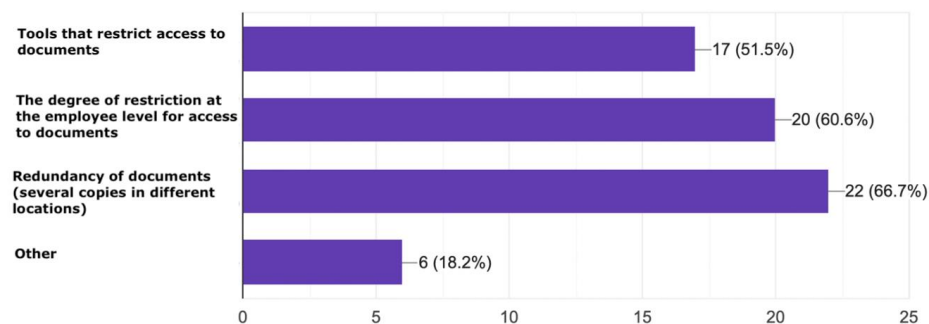


Figure 2. Main security measures to protect data

Source: Authors' own research results.

To protect sensitive data and reduce the potential cyber attacks, companies tend to invest a part of their budget in security measures. In figure 3, it is noted that 18 respondents expressed their intention to maintain their costs associated with cyber security, while 9 respondents want to increase them. Eventhough this costs may seem high, a possible breach may bring much more financial loss for the company. The financial loss ca mean more budget invested to repair the damage created, clients and partners that may leave, causing in the end also a bad reputation. Therefore, each companies tries to mantain or increase the budget designated for data security to lock their digital assets and provide an environment that is trustable.

Organization field	Reduction of costs	Maintain costs	Increase costs	Total
Information and telecommunications	0	8	6	14
Manufactorying industry	2	0	0	2
Wholesale and retail trade	0	2	1	3
Scientific and technical professional activities	0	1	0	1
Industry of Services	1	3	1	5
Transport and storage	1	1	0	2
Construction	1	1	0	2
Real estate	1	1	0	2
Health and social care	0	0	1	1
Financial Sector	0	1	0	1
Total	6	18	9	33

Figure 3. Main security measures to protect data

Source: Authors' own research results.

An aspect highlighted by the study is the prevalence of private documents, both in digital and physical format, among participants from various industries. However, figure 4 reveals that only 9 of them prefer documents in digital format. However, it is worth noting that there is a trend towards digitalization, even if there is still a significant part of respondents who keep documents in physical format. A change is always done in time, and transferring all data and processes in the digital environment will allow faster access to it, an improved organization system, tools to manipulate it easier, along with access to it from diffent locations. Having this collaboration between entities, departments and people will be more efficient. Thus, although physical documents still hold a significant part of participants' preferences, little by little, digitalization is becoming an increasingly important reality in the business environment as well.

Organization field	Traditional format	Digital format	Both	Other	Total
Information and telecommunications	0	2	11	1	14
Manufactorying industry	0	2	0	0	2
Wholesale and retail trade	0	2	1	0	3
Scientific and technical professional activities	0	0	1	0	1
Industry of Services	1	2	2	0	5
Transport and storage	0	1	1	0	2
Construction	1	0	1	0	2

Organization field	Traditional format	Digital format	Both	Other	Total
Real estate	0	0	2	0	2
Health and social care	0	0	1	0	1
Financial Sector	0	0	1	0	1
Total	2	9	21	1	33

Figure 4. Procedure to store data

Source: Authors' own research results.

Constant investment in the training of a company's employees is a key priority, and this trend is maintained throughout the organization, with special attention paid to the field of information and communications. Figure 5 underlines the fact that professionals in this field want to allocate an increased budget for training employees, given the rapid pace of technology development that they come into contact with daily to carry out software projects. Given that technology is in a continuous evolution, the learning process in this field is a permanent one and requires a constant effort to update and develop skills. Training organization resources in different fields needed by the company such as security and technology, will increase their performance and will have a positive impact on the company in terms of projects, goals and reputation. It will also contribute to maintain the organization in the business environment which is highly competitive.

Organization field	Reduction of costs	Maintain costs	Increase costs	Total
Information and telecommunications	1	9	4	14
Manufacturing industry	1	1	0	2
Wholesale and retail trade	1	1	1	3
Scientific and technical professional activities	0	0	1	1
Industry of Services	1	3	1	5
Transport and storage	0	2	0	2
Construction	0	1	1	2
Real estate	1	1	0	2
Health and social care	0	1	0	1
Financial Sector	0	0	1	1
Total	5	19	9	33

Figure 5. Investment in personnel training

Source: Authors' own research results.

Conclusion

The results of this research present the increased concern of companies on cyber security attacks and the importance of protecting private data. Data security is a challenging concern in the business environment and research on this topic is continuously improving. To maintain the integrity, confidentiality and disponibility of data, investments on adopting and having up to date measures to protect it are taken by romanian companies. This assures their knowledge towards information security and the negative impact a breach may bring to the business.

Also, the observation that most participants keep private documents in physical format, but that there is a clear trend towards digitization, illustrates the gradual adaptation of the business environment to new technologies and the advantages brought by digital documents.

The adoption of latest technologies and softwares by companies to keep up with the competitive environment and make processes and activities more efficient, human resource may also be trained to handle this new framework.

Human resource is a key component in protecting each business. Therefore, constant trainings for employees to keep them informed towards information security is a measure that must be taken into consideration. Apart from given them access rights only to the information needed on their position, developing a culture of protecting sensitive data and presenting personal measures that can be taken by each of them, and the potential harm of allowing a cyber attack to fulfill.

The digital environment brings both opportunities and significant challenges for organizations. Being aware, documented and proactive as a company to information security and measures to protect confidential data will help in this changing digital environment. Also, it will allow companies to perform their activities and achieve their long-term goals by ensuring a trustworth and sustainable business approach.

References

- Al-Kahla, W., Shatnawi, A.S. and Taqieddin, E., 2021, May. A Taxonomy of Web Security Vulnerabilities. In 2021 12th International Conference on Information and Communication Systems (ICICS) (pp. 424-429). IEEE.
- Becker, R., Thorogood, A., Ordish, J. and Beauvais, M.J., 2020. COVID-19 research: navigating the European general data protection regulation. *Journal of Medical Internet Research*, 22(8), p.e19799.
- Do, E.H. and Gadepally, V.N., 2020, May. Classifying anomalies for network security. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2907-2911). IEEE.
- Enoch, S.Y., Hong, J.B., Ge, M. and Kim, D.S., 2020. Composite metrics for network security analysis. *arXiv preprint arXiv:2007.03486*.
- Eurostat, 2022, ICT security in enterprises, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises&oldid=583136, accessed on 1 February 2024
- Fabbrini, F. and Celeste, E., 2020. The right to be forgotten in the digital age: the challenges of data protection beyond borders. *German law journal*, 21(S1), pp.55-65.
- Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkowitz, N.B., Danker, J.M., Choong, Y.Y. and Greene, K., 2020. Digital identity guidelines: Authentication and lifecycle management [includes updates as of 03-02-2020].
- Hulshof, M. and Daneva, M., 2021, July. Benefits and Challenges in Information Security Certification—A Systematic Literature Review. In *International Symposium on Business Modeling and Software Design* (pp. 154-169). Springer, Cham.
- Marabathuni, V. M., & Gopejenko, V. (2021). Mobile Security: Analysis and Challenges of information. In *The 19th International Scientific Conference Riga*.
- Palanisamy, R., Norman, A.A. and Mat Kiah, M.L., 2020. BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, pp.1-12.