Information Security Awareness in Romanian Public Administration: An Exploratory Case Study

Doina BANCIU[1]*, Mireille RĂDOI[2], Stefan BELLOIU[3]

[1] Institute for Advanced Interdisciplinary Research "Constantin Angelescu", Academy of the Romanian Scientists,
54 Splaiul Independenței, 050094, sector 5, Bucharest, Romania
banciu.doina@gmail.com (**Corresponding author*)

[2] "Carol I" Central University Library, Bucharest, 1 Boteanu Street, Bucharest 010027, Romania
mireille.radoi@bcub.ro

[3] Intelligent Security Management SRL, Calea Mosilor 237 B, Bucharest, Romania
stefan@i-secure.ro

Abstract: This article analyzes the way public servants understand the necessity for information security in the digitalisation of public administration and sets out to describe a series of technical solutions with a view to protecting digital data. This paper focuses on a study which was carried out on the basis of a questionnaire submitted to three entities from the Romanian Public administration. The objective of this questionnaire was to identify the vulnerable points in certain areas, such as: managing accessibility in user interface design, password management, preventing cybersecurity incidents, response capacity to cybersecurity incidents, personal data protection, data backup and recovery and personal evaluation. The analysis of the results emerging from this questionnaire provides certain conceptual solutions, which can be adopted so that information security in the Romanian digital public administration can be ensured. The solutions presented in this paper are based on the analysis of international documents in this field. This article can also be a practical guide both for the Romanian decision makers and civil servants, enabling them to ensure data security and protection in the organisational structures of public administration.

Keywords: Digital public administration, Information security, Preventing cyber-security incidents, Protecting personal data, Data security solutions.

1. Introduction

The Romanian digital transformation is in accordance with the European directives in this field, but also with the global trends of the 21st century. Without going into detail, it is unanimously recognized that as we move towards an information society, unwanted "phenomena" in the field of cybersecurity may appear as well. Along with the technical approaches in this regard, it is completely self-evident that the office staff of an organization need to be advised, initiated and properly trained with regard to cybersecurity so that they can protect themselves from cyber-attacks. This matter is all the more important the objective of the European countries – as well as that of the European Commission – is to use, on a broad scale, digital technologies in every domain, including public administration. The Digital Europe clearly states: "*Cyberthreats presents a major obstacle to Europe's path to prosperity. Economic loss due to cybercrime is predicted to reach € 2.5 trillion by 2020, and 74% of the world's businesses can expect to be hacked in the coming year. Unfortunately, only 32% of European businesses have a cybersecurity strategy. Such global threat requires a coordinated global response.*" https://www.digitaleurope.org/policies/cybersecurity/ - Digital Europe.

In order to evaluate the degree of awareness of the Romanian public administration regarding the need to secure digital systems, a study was carried out based on data provided by certain entities of the Public Administration and, in this regard, a questionnaire with 26 questions was elaborated.

The questionnaire has been developed so as to meet the objectives of the above-mentioned study from October 1st, 2019 and three entities of the central public administration were chosen for this purpose: a city hall from the capital of a county, a county council and a town hall from a town with less than 30.000 inhabitants. The questionnaire was submitted to the three aforementioned entities and data collection was carried out both online and offline. The interpretation of the collected data was performed in two ways, so that the beneficiaries could gain the best possible understanding of the objectives of the study. It is necessary to underline the fact that the respondents from the city halls work in various departments and at the County Council they stated that the one who collects and transmits data is the one responsible with data handling (the total member of respondents was 42).

Two platforms have been used for data interpretation, which provided the eloquent graphical information for further analysis and

https://doi.org/10.24846/v29i1y202012

synthesis. After data processing had been carried out, it could be observed that the results were similar and gave a significant understanding of the objectives of the study.

2. Research Problem and Methodology

This study combines elements aligned with today`s international standards for cybersecurity audits, with guidelines and best practices in the field of information technology, along with different technics for data processing, based on an anonymous questionnaire.

a) ***ISO 27001.*** The standard employed with a view to elaborating the questionnaire and the related report is *ISO 27001:2017 – Information Technology, Security Technics, Management Systems for Information Security*, elaborated by the International Organization for Standardization and translated by the Romanian Standards Association.

b) ***Questionnaire.*** The questionnaire includes 26 questions regarding information security, divided as follows:

I. Information about the respondent

II. Managing the users` accessibility

III. Password management

IV. Preventing cybersecurity incidents

V. Response capacity to cybersecurity incidents

VI. Use of personal devices

VII. External storage devices

VIII. Protecting personal data

IX. Data back-up

3. Interpretation of Results

The results derived from the analysis of the questionnaire are presented below:

3.1 Information About the Respondents

It can be noticed that senior respondents are prevalent, based on hierarchy and biological age. These categories are not included in the pilot study, in relation to the total number of employees. Also, hierarchy and age-related categories are not represented at all. It is recommended to incorporate as many public institutions as possible in the second phase of the project in order to increase the number of respondents and with a view to improving the statistical significance of the study.

3.2 Managing the Users` Accessibility

a) It can be noticed that passwords are used extensively for each and every application utilised by the employees of public institutions. Nevertheless, in 25% of cases users have reported using the same login credentials for several applications, which represents a cybersecurity risk. This can be improved by specialized training and knowledge transfer regarding the best possible way to use passwords and applications.

b) None of the respondents reported using the “single sign-on” system (a single authentication for every application using a single server base system from Active Directory or LDAP-*Lightweight Directory Access Protocol*). This system is the most efficient one for preventing the repetition of passwords used for several applications and for preventing other misuse instances related to the login credentials.

c) 75% of the respondents do not gain access to their office through a magnetic card and this leads to the impossibility to restrict physical access only to the authorized employees. The inexistence of these access restriction systems makes the cybersecurity audit impossible in case a security incident occurs.

d) The VPN usage percentage for securing connections is 0%. The interception of communications represents a major risk for any network. The immediate transition to a secure communication network by using VPN is advised for all employees.

Making information security simple for employees is key for ensuring that the security policies are understood and applied down to the most basic activities. A single sign-on system is adequate for employees who work with many applications in their daily activities. Login credentials are no longer stored within multiple data bases, and because there is only one set of credentials, employees won’t be tempted to write it down in a separate physical or electronic document as they do when they are faced with a lot of login credentials – as they reported. Moreover, a single sign-on system will make sure that best practices are followed with regard to the regular change of passwords. In this respect, it should be mentioned that only 25% of the employees participating in the survey reported that they change the passports

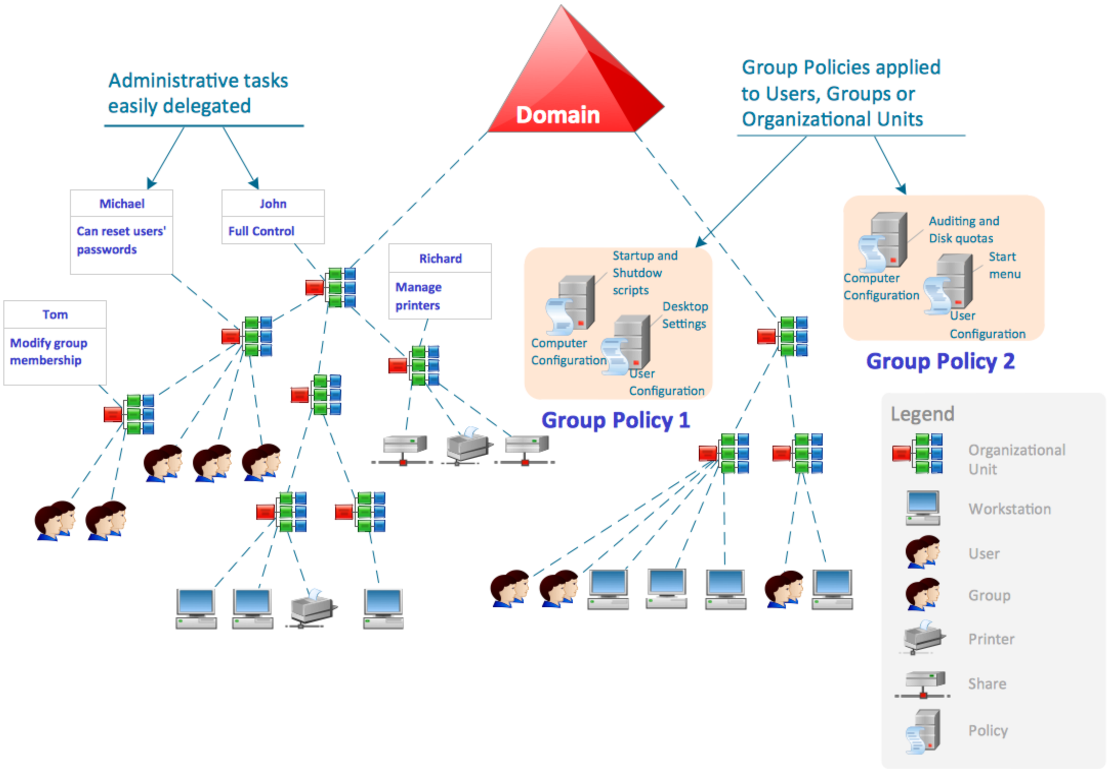

Figure 1. https://www.conceptdraw.com/solution-park/computer-active-directory

they use accordingly. Figure 1 illustrates an Active Directory deployment which is suitable for public institutions.

Local government institutions communicate mainly with other government institutions, and with citizens and companies. To the largest extent, office communication lies in document transfers. At this point the main focus is on the outbound traffic that takes place throughout the internet infrastructure, which is a highly insecure environment. Because of the way Romanian bureaucracy works, the types of documents transferred, and the destinations are the same. Therefore, data transfers can be secured much more easily. The model proposed is a Gateway-to-Gateway IPsec VPN. This Architecture protects communication between networks by setting up specific servers / gateways in those networks in order to establish an encrypted communication channel between them. This ensures data confidentiality and integrity through cryptographic checksums and encryption (see Figure 2).

As the data communication is only protected between the two VPN gateways, it follows that the networks in the institutions implementing such a system should be secured.

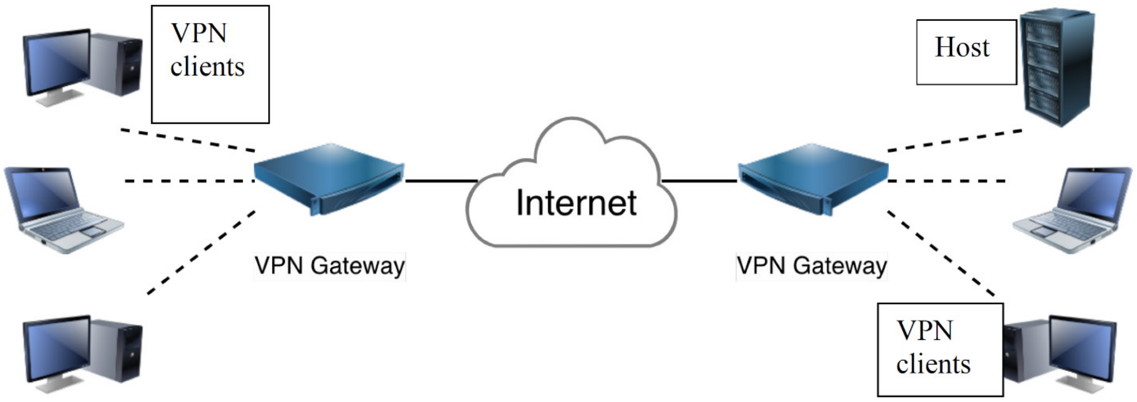

Figure 2. Gateway-to-Gateway VPN - Draft NIST Special Publication 800-77, Revision 1, Guide to IPsec VPN

The authors of this paper have no knowledge of penetration testing and vulnerability scans being performed at the target institutions and as such, establishing the security level of the respective networks is outside the scope of this paper.

3.3 Password Management

a) Only 25% of the respondents regularly change passwords in accordance with the standards and best practices in the cybersecurity domain. Keeping the same password for a long period of time, in conjunction with the fact that the respective passwords are weak (few characters, generic formulations found in hacker's dictionaries), and that they are often transmitted to work colleagues can lead to a high risk level as cybersecurity is concerned.

b) The number of characters a password contains is very important for its security. The average number of characters reported by respondents is 8,25 which is low and it is advisable that the passwords contain at least 16 characters, and use the full ASCII character set, which would turn them into strong passwords.

c) 25% of the respondents keep their passwords on paper. This represents a security risk. It is advised that in case that the single sign-on system does not exist one use a password manager for improving security.

3.4 Preventing Cybersecurity Incidents

a) In the surveyed institutions, preventing cybersecurity incidents lies in the installation of antivirus and anti-malware programs on the computer terminals of the employees. This solution is substandard if one takes into account that the employees of these institutions work with confidential information and sensitive data. The number of training sessions provided to each employee is below the recommended standards and best practices in the cybersecurity domain. To a significant extent, the cybersecurity-related attack vectors are targeted towards people and not the information systems so as to speculate on the lack of attention and also on lack of awareness and training.

b) Many answers show that the employees have not been trained through courses and workshops in order to understand the nature of cyber threats, to know how to identify them and how to prevent them. All employees should participate in a series of periodical courses that would increase their awareness towards cyber threats and improve the related prevention methods.

c) 50% of the IT specialized departments of the surveyed institutions regularly send instructions and notifications regarding the prevention methods related to cyber-attacks. These notifications are among the simplest ways for keeping the employees with regard to the cybersecurity risks related to their activities, especially as the phishing attack vectors (electronic deception) are concerned. The other 50% of the surveyed institutions have a merely passive role in the cybersecurity policy – they send notifications and instructions to their own employees only after a security incident occurred.

The implementation of a preventive approach with regard to cybersecurity risks among the employees of the surveyed institutions starts by focusing on the related standards, guidelines and best practices. These need to be implemented and adapted to the specific needs of the respective institution and to its infrastructure.

3.5 Response Capacity to Cybersecurity Incidents

a) 50% of the respondents failed to act properly when dealing with a cybersecurity incident. These incidents are tackled by specialized departments, such the IT or Cybersecurity Department and any delay in reporting them leads to damages and data theft. It is advisable that the employees of an institution be trained about how to act properly in this kind of situations.

b) 75% of the respondents did not receive instructions and did not get acquainted with the procedures related to the way they should react when a security incident occurs. This leads to major risks for the surveyed institutions, such as an interruption or delay related to the provided services, data leakage, as well as the impossibility to audit the respective incidents. An immediate elaboration of instructions and data security procedures is advised in order to improve the response capacity of the employees of the respective institutions.

Employees need to be aware of the existing threats and of how to identify them, and how to respond to them in order to protect the assets of an institution,

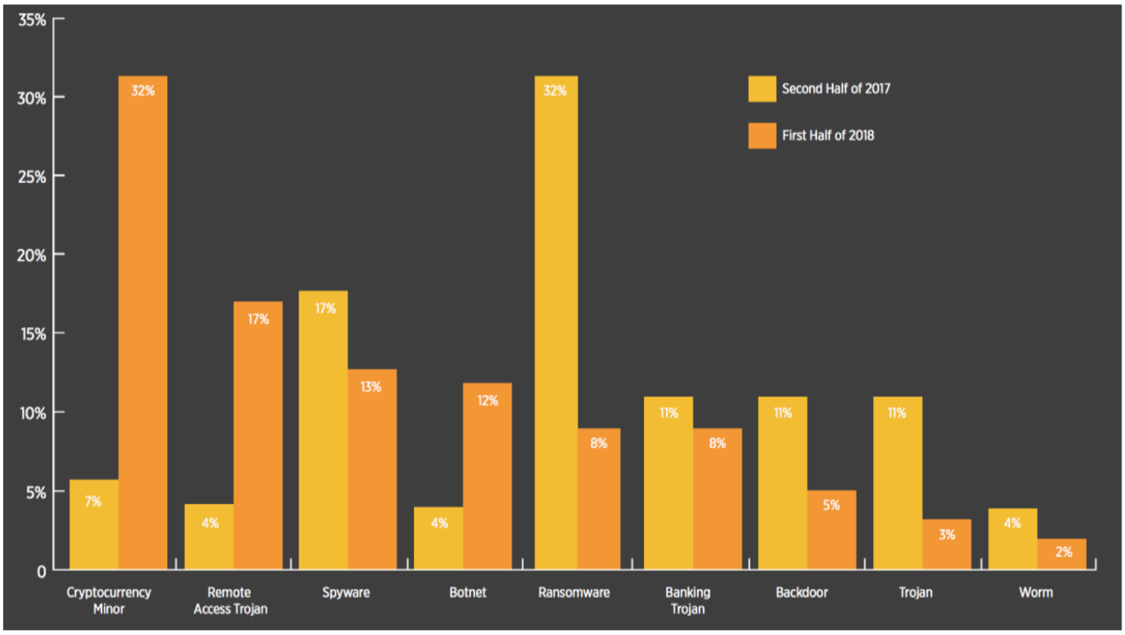

Figure 3. WP2018 O.1.2.1 - ENISA Threat Landscape 2018

its sensitive data and the personal data related to its employees. According to the European Union Agency for Cybersecurity, the main threats for European citizens are shown in Figure 3:

The employees of the IT or Cybersecurity departments within the surveyed institutions must take the necessary measures in order to raise the awareness among the rest of the employees on the above-mentioned topics otherwise suspicious activities and security incidents may go unnoticed and/or unreported, which would lead to a widespread cybersecurity risk.

Data security procedures should be designed in order to reduce cybersecurity risks and incident response times and increase the cyber resilience of the systems of the surveyed institutions, along the guidelines related to the risk management framework (see Figure 4).

3.6 Use of Personal Devices

a) In 50% of cases respondents have reported that they use at least one personal device for work. This leads to security risks for the institution, because it cannot control personal devices or know what kind of confidential information or personal data is stored on it, therefore it cannot improve its security level, because this aspect is out of its jurisdiction. It is advisable that employees of an institution use only work with devices provided by the respective institution and not with personal ones.

In order to implement this recommendation, an immediate elaboration of the current procedures and instructions is necessary, with a view to restricting the use of personal devices at work. Also, these devices need to be connected to a network which is different from the one to which the devices at the workplace are connected in order to minimize cross-contamination.

b) The answers to subsequent questions show us that institutions have succeeded in segregating the employees` home environment from their work environment as far as the use of personal applications is concerned. None of the respondents use personal applications for dialogue or for sending work-related documents.

3.7 External Storage Devices

a) 100% of the employees who use external storage devices do not secure these devices, do not restrict access to them through passwords and do not encrypt those devices so that unauthorized people cannot read them. This is a major security risk for the surveyed institutions, because memory sticks, hard disks and DVDs can store a huge volume of data, and they can circulate freely and unaudited inside and outside of the institution therefore is impossible to guarantee the integrity of the data stored on these devices. Also, due to the fact that anyone can copy anything on these unsecured storage devices they represent an important attack vector for malware and viruses.

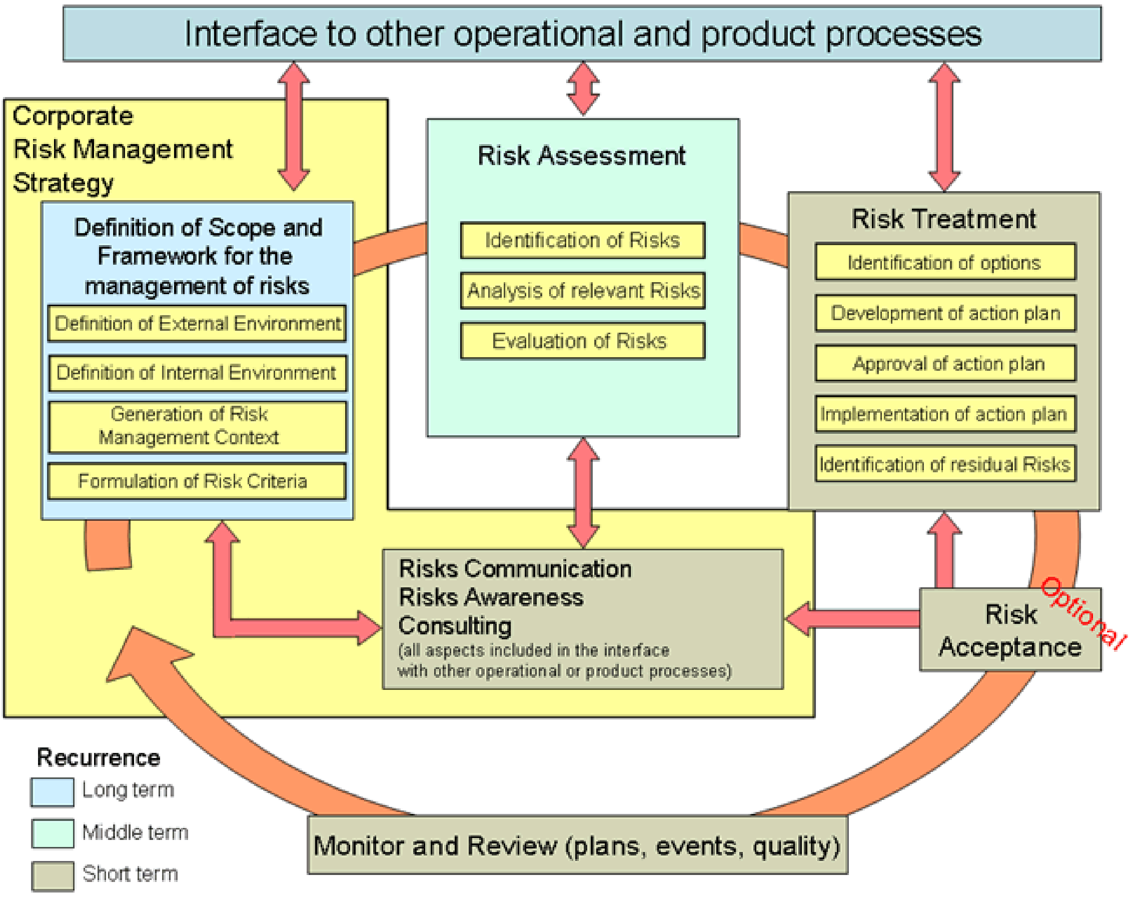
Interface to other operational and product processes
Corporate
Risk Management
Strategy
Definition of Scope and
Framework for the
management of risks
Definition of External Environment
Definition of Internal Environment
Generation of Risk
Management Context
Formulation of Risk Criteria
Risk Assessment
Identification of Risks
Analysis of relevant Risks
Evaluation of Risks
Risk Treatment
Identification of options
Development of action plan
Approval of action plan
Implementation of action plan
Identification of residual Risks
Risks Communication
Risks Awareness
Consulting
(all aspects included in the interface
with other operational or product processes)
Risk
Acceptance
Optional
Recurrence
Long term
Middle term
Short term
Monitor and Review (plans, events, quality)

Figure 4. European Union Agency for Cybersecurity, Risk Management Framework: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework

The immediate elaboration of certain procedures and restrictions regarding external storage devices is advised along with the implementation of an encryption program.

b) For securing these external storage devices, we recommend using tools for “full disk encryption”, as such access to the data is allowed only after successful authentication. The confidential data peculiar to an institution is only allowed after one`s successful authentication. Employees should use strong login credentials for these portable storage media, just like on the laptops or desktops they use at their workplace (see Figure 5).

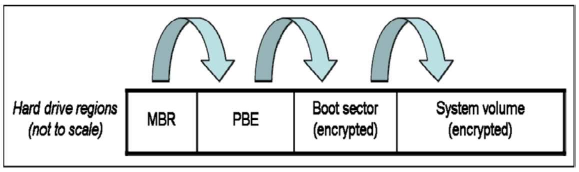

Figure 5. Boot Sequence for Full Disk Encryption Software - NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

3.8 Personal Data Protection

a) 50% of the respondents reported that they do not process personal data, although this seems unlikely due to its widespread and frequent use. This answer in conjunction with the inefficient measures reported in other question lead to the conclusion that the employees of the surveyed institutions are neither aware, nor trained to properly protect personal data according to the applicable legislation. It is advised to initiate and provide courses on the GDPR legislation in order to increase awareness and enhance practical knowledge in this field at an institutional level.

b) In this particular case, due to the fact that conformity with the legislation regarding the protection of personal data is mandatory, beside the common risks may arise by processing any kind of confidential data in an inadequate way, financial risks may also occur based on the probability of certain costly penalties that

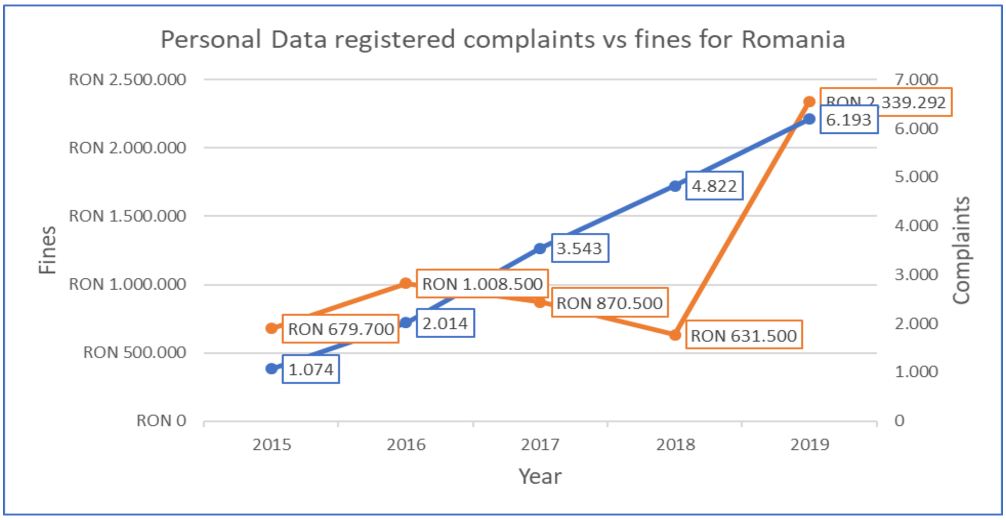

Figure 6. The registered complaints vs fines for Romania with regard to personal data protection - Annual Reports 2015-2019 of *The National Supervisory Authority for Personal Data Processing* - https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro

could be applied to the surveyed institutions by the Surveying Authorities. The lack of training in this domain can make the employees of an institution break the rights of fellow citizens without knowing it (including the rights of their colleagues) and overlook the recommendations of GDPR legislation. Hence, the stress on training the staff in this regard and on elaborating a clear set of related procedures becomes even heavier.

c) The data from The National Supervisory Authority for Personal Data Processing shows a very clear upward trend when it comes to the number of complaints received from Data Subjects.

The number of opened investigations is also on an upward trend just like the percentage of complaints. The plotted values below show an increase of 270% in the number of fines imposed by the Supervisory Authority in 2019 as compared to 2018. Both trends, that is the increase in the number of complaints and fines, are expected to continue as more and more citizens become aware of their rights regarding the protection of personal data and defend them against any negligence or abuse from the part of public and private institutions (see Figure 6).

As such it is plausible that the institutions that took part in the afore-mentioned survey may be subject to more audits and fines as the expectations of citizens rise.

Another key piece of evidence that makes the need for GDPR training of employees even more stringent is the fact that for 2018 (the only available year for this type of data), the number of personal data breaches notified to the Supervisory Authority is higher for the public sector – 168 as compared to the private sector – 144.

This is understandable when taking into consideration the chronic underinvestment in IT and cybersecurity infrastructure in the context of Romanian public institutions and the heavy bureaucracy generated by the hundreds of copies of the same personal data which are circulated throughout the local and central government institutions.

3.9 Data Back-up

a) 75% of the employees of the surveyed institutions are not familiar with the back-up systems meant for the data they are working with. Although technical knowledge is not important for employees outside the IT department, it is important for them to know what data should be backed-up, whom they should contact for restoring the data they work with in case they lose it, how long that process might take, etc. This information is important as it can help those employees plan their workflow, and minimalize delays and data loss. In this regard, internal meetings with the IT department are highly recommended.

b) It is also recommended that one investigate the level of functionality and implementation

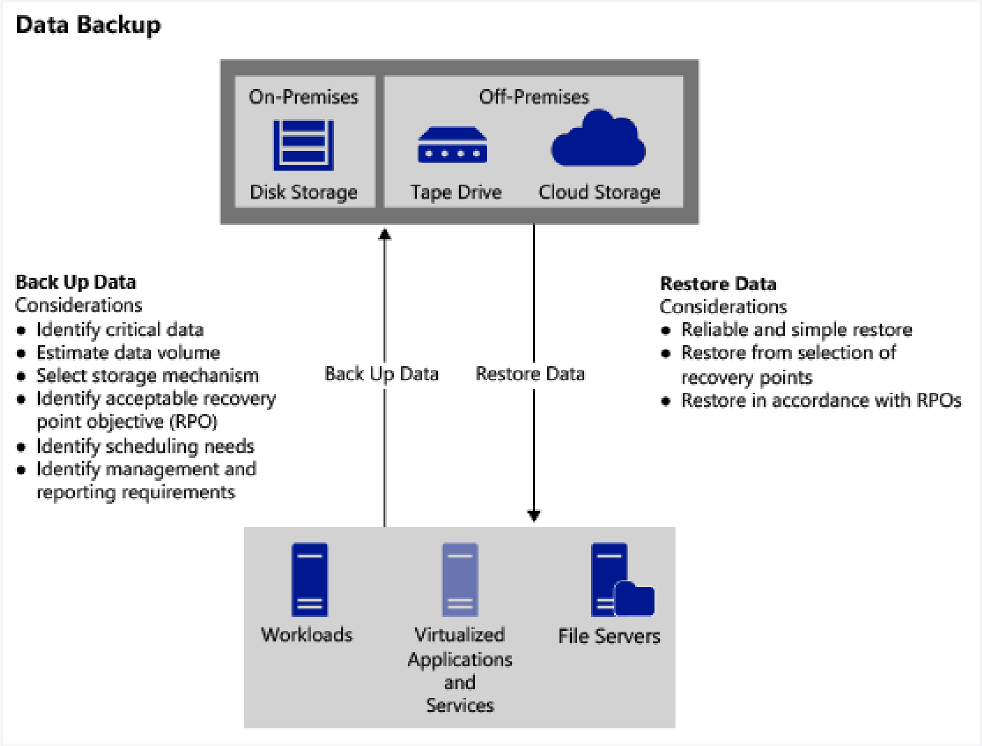
Data Backup
On-Premises
Disk Storage
Off-Premises
Tape Drive
Cloud Storage
Back Up Data
Considerations
• Identify critical data
• Estimate data volume
• Select storage mechanism
• Identify acceptable recovery point objective (RPO)
• Identify scheduling needs
• Identify management and reporting requirements
Back Up Data
Restore Data
Restore Data
Considerations
• Reliable and simple restore
• Restore from selection of recovery points
• Restore in accordance with RPOs
Workloads
Virtualized Applications and Services
File Servers

Figure 7. Data Backup Considerations, source - https://i-technet.sec.s-msft.com/dynimg/IC744507.jpeg

of the back-up solutions in the afore-mentioned institutions. These services are essential for the proper functioning of any entity that processes a huge volume of data.

c) The lack of knowledge data backup systems has an important negative impact on business continuity, as without training and knowledge transfer, employees are unable to execute even some basic troubleshooting and recoveries and they cannot reduce downtimes.

d) The state of the IT backup infrastructure in the institutions that participated in this survey should be evaluated on the basis of international standards, best practices and guidelines related to information security and business continuity, mainly ISO 27001:2013 and ISO 22301:2019 – in order to to get a clear picture with regard to the critical aspects that should be improved. In this respect, Figure 7 illustrates the main points to be considered when deploying or improving a backup solution.

4. Conclusion

Taking into consideration the answers, it can be noticed that a consistent part of the employees of the surveyed institutions display a reduced trust with regard to their colleagues` level of training in cybersecurity. Namely, 50% of them think the respective level is unsatisfactory. This evaluation is in accordance with the auditors` conclusions expressed in the related observations and recommendations.

Increasing the confidence of those employees in their own training, and in their colleagues` training can be achieved by specialized training programs related to cybersecurity issues, personal data protection and the institution`s proper use of devices and applications. Also, it is recommended that the management and consultants of the Romanian public administration should focus on practice and not on theory so that the employees can eventually master the right skills, improve their vigilance and develop the reflexes needed in order to efficiently fight against the risks and threats they will encounter.

From this study one can infer that employees from the Romanian public administration know the shortcomings of the cybersecurity domain at the workplace. The public servants find the current state of affairs unsatisfactory with regard to the level of cybersecurity and that is why they show their willingness to learn to adapt to cyber security challenges so that potential risks in their workplace can be minimized.

REFERENCES

Carrasco-Saez, J. L., Careaga Butter, M. & Badilla-Quintana, M. G. (2017). The New Pyramid of Needs for the Digital Citizen: A Transition Towards Smart Human Cities, *Sustainability*, *9*(12), 2258.

Dumitrache, M. (2015). Servicii publice electronice oferite instituţiilor publice prin proiectul ICIPRO (Infrastructură de tip Cloud pentru Instituţiile Publice din România), *Revista Româna de Informatica şi Automatica, 25*(4), 27-32.

European Union Agency for Cybersecurity (2010). *Information Security Tips for Employees*. Available at: <https://www.enisa.europa.eu/publications/archive/informationsecuritytips-employees>.

European Union Agency for Cybersecurity (2018). *ENISA Threat Landscape Report - WP2018 O.1.2.1*. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.

European Union Agency for Cybersecurity. *Risk Management Framework*. Available at: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework>.

Heath, Marie K. (2018). What Kind of (Digital) Citizen?, *International Journal of Information and Learning Technology*, *35*(5), 342-356.

Institutul de Cercetări Avansate Interdisciplinare ”Constantin Angelescu” (2019). *Servicii de consultanță și analiză asupra gradului de percepție al administrației publice privind necesitatea securizării sistemelor digitale, 2019 – raport de cercetare.*

International Organization for Standardization (2013). *ISO 27001:2013*. Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>; <https://www.conceptdraw.com/solution-park/computer-active-directory>.

International Organization for Standardization. (2019). *ISO 22301:2019*. Available at: <https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en>.

Kaigo, M. (2017). The Necessity of Digital Citizenship and Participation, *Information*, *8*(1), 28.

Kim, M. & Choi, D. (2018). Development of Youth Digital Citizenship Scale and Implication for Educational Setting, *Journal of Educational Technology & Society*, *21*(1), 155-171.

Kosorukov, Artem A. (2017). Digital Government Model: Theory and Practice of Modern Public Administration, *Journal of Legal, Ethical and Regulatory*, *20*(3), 1-10.

National Institute for Standards and Technology, U.S. Department of Commerce – NIST SP 800-111. (2007). *Guide to Storage Encryption Technologies for End User Devices - 3.1.1 Full Disk Encryption*, 31-32. Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>.

National Institute for Standards and Technology, U.S. Department of Commerce (2019). *Draft NIST Special Publication 800-77, Revision 1, Guide to IPsec VPN.* Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1-draft.pdf>.

Romanian Personal Data Protection Supervisory Authority (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal). Annual Reports 2015-2018. Available at: <https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro>.

Sandu, I.-E., Smada, D.-M. & Dumitrache, M. (2019). An affordable Web-based Grant Management Software Designed to Support Romanian Scholarly Publications, *Studies in Informatics and Control, 28*(1), 95-104. DOI: 10.24846/v28i1y201910