PRACTITIONERS’ BROAD VIEW

PROSEC TEST FOR THRIVE PROTECTIVE SECURITY RULES AGAINST THREATS, RISKS AND VULNERABILITIES

Florin BUȘTIUC[*]

Abstract:

Protecting assets critical to organization's functionality is everyone responsibility – information leakage, unauthorized access, destruction can cost an organization dearly in lost productivity, decreased morale and public confidence. Security should be integrated into the organisation's practices and plans (as physical security, information security, personnel security etc.). There are two sides to security risks – threats and vulnerabilities. This article is about the human factor in the equation vulnerabilities-threats. The PROSEC test is a set of questions (and requirements) designed to determine an individual to become aware of security rules. By introducing the PROSEC test in security education program, you reduce the chances that your personnel will become a victim of today's data security threats. Because it's about self-education.

Keywords *security rules, security responsibilities, information security, security education.*

Introduction

In order to understand the importance of security, it is necessary to know which factors influence the functionality of organization – strategic policy, objectives, laws and regulations, organizational culture, financial, economic climate, and the categories of assets because it will allow you to achieve your security goals – primary assets (information and processes) and secondary assets (information systems and communications networks, software and operating systems, service, maintenance, personnel, locations, services and utilities, subcontractors, suppliers, customers). The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the

[*] PhD "Mihai Viteazul" National Intelligence Academy, email: florinnn11@yahoo.com

individual understands them. There are two sides to security risks – threats and vulnerabilities. This article is about the human factor in the equation vulnerabilities-threats.

The Protective security[1] is an organized system of policies, procedures and standards whose objective is to preserve the integrity of an organization's assets against adverse acts/influences, in areas such as physical security, personnel security, document security, IT and communications security (*The Protective Security Policy Framework*). The aim of this paper is to address the protective security critical for any organization. The assets that are necessary for the efficient and competitive functioning of an organization are classified (BS ISO/IEC 27005:2008, p. 30) into primary assets (processes and information) and support assets (the elements that ensure the functionality of the primary values).

Regarding the processes, we have:

a) processes whose degradation generates consequences on the functionality/existence of the organization;
b) processes that, if modified/disclosed, affect the achievement of the organization's objectives;
c) processes that are necessary for the organization, regarding to compliance with legal and contractual provisions.

As for information, protective security rules ensure its confidentiality, integrity and availability. Confidentiality refers to the ability to protect data against people who do not have the authorization (Andress and Leary, 2017, p. 4) to know them, access to information being granted to those who, in order to fulfil their job duties, have to work with a certain type of information. Integrity refers to the property of data and processes not to be modified or destroyed without authorization, intentionally or accidentally (*Glosar de termeni pentru domeniul securității cibernetice*), and availability indicates that information can be accessed by an authorized person at any time when needed (*Cybersecurity-glossary*).

[1] Some aspects have been taken from the author's doctoral thesis, *Pregătirea contrainformativă a persoanelor cu acces la informații clasificate/nepublice*, defended in 2021, at the "Mihai Viteazul" National Intelligence Academy.

The supporting assets are represented by:

a) IT and communication systems, networks (with internal / external use; fixed and mobile equipment);
b) software and operating systems (the programs that ensure the performance of certain operations);
c) service, maintenance and administration of the programs (with methods of selecting the companies that provide such services and contractual clauses regarding confidentiality);
d) peripherals (equipment connected to computer systems);
e) electronic media (for data storage);
f) personnel (human resources);
g) internal areas/locations (spaces within which activities are carried out);
h) services and utilities;
i) subcontractors/suppliers/ partners/ customers (BS ISO/IEC 27005:2008, pp. 31-34).

In this context, physical security refers to three categories of values, namely personnel, equipment and data (Andress, 2011, p. 97), delimiting areas/spaces, access control, photo-video surveillance, anti-burglary and anti-fire systems etc.

The physical security rules are embodied in:

a) monitoring and control of persons entering the premises of the organization (current employees, former employees, service staff, courier staff etc.);
b) verification of the identity of the persons and the purpose of the visit;
c) storage (and inventory) of keys, access cards, uniforms, badges, etc. (Speed, 2011, p. 218).

Document security refers to:

a) the modalities to identify the people who accessed them;
b) access based on the need-to-know principle;
c) authorizing specific people to make the copies (and the procedure of approving the copying);

d) records of the number of copies and the persons to whom they were distributed;
e) modality of transport;
f) the procedures for destroying documents;
g) marking modality;
h) prohibition of multiplication or transmission to a third party, without the consent of the issuer (Mendell, 2007, pp. 75-76).

IT and communications security refer to equipment, access rules, software implementation etc., referring to the reporting of the following cases:

a) trying to obtain information about computer systems – configuration, access rules, installed software, technical equipment used, problems / malfunctions etc.;
b) the attempt / to obtain unauthorized access to the computer system or to the data from the system;
c) unauthorized hardware/software changes;
d) receiving suspicious emails, which have attached unsolicited files and/or requests for personal or organization information (BS ISO/IEC 27002:2005, p. 37).

In the field of personnel security, the following are established:

a) selection, vetting and employment rules;
b) elements of incompatibility in relation to access to sensitive/classified information;
c) security training and education programs, etc. (Reid, 2005, p. 249).

Threats are represented by external factors that affect the operation and existence of the organization:

a) physical causes – fire, flood, explosions, earthquake, climatic phenomena;
b) suppliers of equipment and programs – spyware, data transmission devices;
c) the human factor – terrorist attacks, espionage etc.

Vulnerabilities represent the lack of standards or poor application of procedures in the following areas:

a) physical security: lack or poor application of access procedures, inadequate equipment for photo-video surveillance, lack of protection of doors, windows and cards;
b) security of documents: the absence of a policy for the multiplication, destruction and transport of documents, keeping them in inappropriate premises;
c) IT and communications security: poor maintenance, erroneous installation of programs, lack of audit in terms of access, allocation and access rights, not protecting/not changing passwords periodically, lack of monitoring the use of programs, unprotected communication equipment;
d) staff security: inadequate recruitment and selection procedures, the existence of personal vulnerabilities (financial problems etc.), insufficient training and preparation, incorrect use of computer and communication equipment and programs, the absence of external staff verification (BS ISO/IEC 27005:2008, p. 43).

Risk is the intersection of threats and vulnerabilities and is reflected in:

a) unauthorized access to premises, to information and processes;
b) compromising some information and processes;
c) loss of programs, equipment;
d) impairment of functionality;
e) damage to image and credibility (BS ISO/IEC 27005:2008, p. 44).

In order to protect assets (locations, information, personnel), it is necessary that individuals to be aware of the threats, since they are the first target of adverse intelligence activities. Circumscribed to the awareness by each employee that the lack of knowledge and involvement has real consequences on data compromise, operation and survival of the organization (Friedman et. al. 1997, p. 233) the most common security rules that apply, in general, to all categories of non-public data (classified information, personal data, contracts, research, negotiations – for the rules about classified/secret information etc.) have been synthesized in the form of PROSEC test.

*

In this context, we appreciate that it is relevant for a person to have the possibility to address through a questionnaire/test this issue appropriately. There are 30 sentences-statements regarding security rules and we have to determine which is true or false.

1. Computer programs with classified data can be installed on one's own initiative, if they are purchased personally and have a license.
□True □False

2. Non-public documents are not left unattended, when leaving the office, and must be apply "the clean-desk policy" to avoid viewing by unauthorized persons.
□True □False

3. It must not be accessed the links received by e-mails that request the updating of personal information. Legitimate entities do not request to provide or verify sensitive information through an insecure medium such as email.
□True □False

4. If it is an emergency, classified information can be transmitted by telephone, fax, e-mail or by means of other non-accredited means of communication.
□True □False

5. The contents of non-public documents are not discussed in the presence of unknown persons or persons who would not be authorized to know their contents.
□True □False

6. At the end of the work schedule, it must be done a check to establish that non-public documents have not been mixed with personal ones, so as not to leave with them.
□True □False

7. For passwords must be used a combination of letters (uppercase and lowercase), symbols and numbers, and must be changed at regular intervals.
□True □False

8. It must be not used or connected your own equipment/ accessories within the organization without the consent of the IT department.
□True □False

9. In the case of problems regarding the use of the institution's computer / network, these must be reported to the IT department.
□True □False

10. If a telephone conversation involving classified information is absolutely necessary, only specially designed telephones should be used.
□True □False

11. If the mobile phone, tablet, work laptop is lost and found, it is recommended to be checked by a specialist of the institution, because programs can be installed to transmit the data from these devices.
□True □False

12. If it is a necessity and emergency to access personal mail to send or download a document, the computer on which classified information is being processed can be connected to the Internet.
□True □False

13. Unannounced visitors are never accepted in the work office, respectively: a) it is sent a messagae that no staff is available to

accompany and an appointment is made, or b) the meeting is held in a room used for relations with the public.

□True □False

14. At various events (conferences, workshops etc.) only the aspects for which approval has been received are presented.

□True □False

15. Classified documents can be duplicated at public photocopying centres outside the organization, if at least two employees are carrying the documents and are present in that location.

□True □False

16. The persons who have accessed non-public materials have the obligation to maintain the confidentiality of their content including after leaving the position, for the periods and under the conditions provided by law.

□True □False

17. The first rule on the Internet is to remain as anonymous as possible, so it is not recommended to publish personal information – full name, address, telephone number, CNP/ID number, passwords, names of family members, credit card numbers.

□True □False

18. If there are emergencies to finish something job related, classified materials can be taken and studied at home.

□True □False

19. Personal data and pictures posted in the virtual environment may be used against you, so it is recommended to be as discreet as possible regarding your profile on online social networks, such as Facebook, Twitter etc.

□True □False

20. Classified documents are received / handed over by signature, verifying their integrity (registration number, number of files, level of secrecy).

□True □False

21. Classified materials are not transported personally between the offices of different institutions / between offices of the same institution.

□True □False

22. Only classified documents for which approval has been received are sent / taken at a meeting, respectively the meeting takes place in authorized locations.

□True □False

23. If the special/designated space is occupied, aspects of classified materials can be discussed in public places, but without strangers nearby.

□True □False

24. Classified documents are multiplied and destroyed based on approval / minutes. The individuals must participate at the destruction process of documents, they do not sign the minutes just because someone says that the documents were destroyed.

□True □False

25. The level of secrecy on the documents is not removed / modified on its personal initiative.

□True □False

26. Personal storage devices are not used for copying / transferring classified materials.

□True □False

27. Access passwords are not disclosed to unauthorized persons.

□True □False

28. Visiting the organization involves submitting a list of persons, whose identity is verified. A change to the list or substitution of a visitor is not accepted, if there is not enough time to verify his identity and general biography, and the visitors will be accompanied to the organization's premises (and if necessary they will have a distinctive pass).

□True □False

29. In order to create a classified material that requires a complex analysis, it is allowed to consult any specialists in that specific field.

□True □False

30. It must not be opened attachments related to e-mails from unknown senders.

□True □False

ANSWERS

The scores are calculated upon the relevance for the security rules and the sum is 30 points (where false is not in the following table, the score is 0).

1- F-0,5p	**7- T-0,5p**	**13- T-1,5p**	**19- T-1p**	**25- T-1p**
2- T-0,5p	**8- T-0,5p**	**14- T-1p**	**20- T-1p**	**26- T-1p**
3- T-0,5p	**9- T-0,5p**	**15- T-1p**	**21- T-1p**	**27- T-0,5p**
4- F-0,5p	**10- T-0,5p**	**16- T-1p**	**22- T-1p**	**28- T-1,5p**
5- T-0,5p	**11- T-1,5p**	**17- T-1,5p**	**23- F-0,5p**	**29- F-1p**
6- T-1,5p	**12- F-1p**	**18- F-0,5p**	**24- T-1,5p**	**30- T-1p**

How to interpret scores (the sum of the matching answers points-**p**):

1-10p – You are aware that in your professional activity is important to protect information, but you tend to ignore the security rules, perhaps because you think they are excessive or that you are smart enough and you will manage any problems based on your personal skills in order not to compromise information. So, you are selective, relying on your personal evaluation of the severity of the situations if the rules must be applied. The recommendation is that, as soon as possible, you must (re)study the security procedures of the organization and participate in presentations / trainings in the field of information security. It is also useful to study some material that explains in detail why information protection is vital to an organization and which are the rules that must be applied, regardless of personal abilities or evaluation.

11-20p – You perceive security rules as bureaucratic, but you have the professional experience and/or mind-set to recognize the importance of rules. It seems that you are generally familiar with security rules and the principle that failure to apply them in all situations, regardless of personal opinions, can result in compromising of data. However, you approach some situations superficially, relying on your personal intuition that there is no need to apply rules, because the possibility of information compromise is at minimum. The recommendation is to participate in presentations / trainings where new topics in the field of information security and case studies are addressed.

21-30p – For you, responsibility and compliance with commitments are essential benchmarks for a professional activity. You are a person who realizes that the protection of information is very important for the functionality, survival and development of an organization, and the application of security rules is a necessity. You are defined by a professional principle and/or a realistic thinking that each situation must be evaluated from the perspective of protection of organization assets – information, people etc., and consequences. Even if you will face new situations, these mind-sets will allow you to identify optimal solutions to protect organization assets. It is recommended to be involved in presentation and training activities in the field of information security.

Conclusions

Consequently, in the professional activity that involves working with non-public data, there are security rules that protect this data, as well as the personnel who manage it, against risks, vulnerabilities and threats. Protecting information is a strategic factor for the functionality, survival and development of an organization. The application of security rules is a responsibility of all employees, and the PROSEC test represents a self-assessment of their knowledge, but also a quick (re)familiarization, with positive effects in carrying out the professional activity in accordance with the security procedures provided for in laws and internal regulations.

References:

1. Andress, Jason. (2011*). The basics of information security: understanding the fundamentals of InfoSec in theory and practice*, Elsevier.

2. Andress, Jason, Leary, Mark. (2017). *Building a Practical Information Security Program*, Elsevier.

3. BS ISO/IEC 27002:2005. *Information technology - Security techniques - Code of practice for information security management*.

4. BS ISO/IEC 27005:2008. *Information technology – Security techniques – Information security risk management*.

5. Cybersecurity-glossary, accessible at https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#A

6. Friedman, George, Friedman, Meredith, Chapman, Colin, Baker, John S. (1997). *The Intelligence Edge. How to Profit in the Information Age*, Crown Publishers, New York.

7. *Glosar de termeni pentru domeniul securității cibernetice*, accessible at https://www.sri.ro/cyberint

8. Mendell, Ronald L. (2007). *Document security. Protecting Physical and Electronic Content*, Charles C. Thomas Publisher.

9. Reid. Robert N. (2005). *Facility manager's guide to security: protecting your assets*, The Fairmont Press.

10. Speed, Tyler Justin. (2011). *Asset Protection through Security Awareness*, CRC Press-Taylor & Francis Group.

11. *The Protective Security Policy Framework*, accessible at https://www.protectivesecurity.gov.au/