METHODS OF IDENTIFYING VULNERABILITIES IN THE INFORMATION SECURITY INCIDENT MANAGEMENT PROCESS

Associate Professor Claudia CÂRSTEA, PhD

"Henri Coandă" Air Force Academy, Brașov

DOI: 10.55535/RMT.2023.1.7

The application of tools and methods to improve the effectiveness of the information security management system by detecting and neutralizing cyber attacks, monitoring and blocking DDoS attacks, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), blocking TOR Exit Nodes, blocking Layer 7 Regular Expression attacks, web filtering, blocking malware attacks, ransomware, spammers and spam servers has become a sine-qua-non requirement in the management of information security incidents in order to minimize their impact on IT systems. The paper provides insight into the impact of integrating much-needed security requirements for information technology users in military systems. The collection of information was carried out on a statistical sample of 128 students from military academies in Romania, Bulgaria, Poland. The research methods are complemented by cross-sectional (questionnaire, survey, observation) and observational methods.

Keywords: information security; confidentiality; integrity; vulnerability; information systems;

ABOUT INFORMATION SECURITY MANAGEMENT

When talking about information security, the user thinks directly about the privacy aspect, ignoring the integrity and availability of the information. In such situations, it is important to implement good practices in the organization, through which all categories of users get familiar with the three dimensions of information security: authenticity, non-repudiation and reliability.

According to the *Methodology and instructions for completing major incident reporting forms/Regulation 2/2020 on security measures regarding operational risks*, *confidentiality* is the property of information not to be available to unauthorized persons, entities or processes, and *integrity* refers to ensuring accuracy and completeness of the methods by which information is processed.

Confidentiality is the property of information not to be available to unauthorized persons, entities or processes, and integrity refers to ensuring accuracy and completeness of the methods by which information is processed.

However, there are often requests regarding the accessibility upon request of an authorized entity of the information to be processed, and then it will certainly be necessary to establish in real time the timeliness of the requests and the availability of the information in relation to the specific requirements of the users.

Are there tools to assist users in making the decision? It is considered that there are such tools! But how to select those that adapt to the specifics of the activity carried out? It should be evaluated according to the following criteria:

- authenticity – as the property of an entity to be what it claims to be;
- non-repudiation – as the ability to demonstrate the occurrence of a claimed event or action or the entities that generated them;
- reliability – as the property of consistent behaviour and results.

AN ORGANIZATION'S SECURITY MANAGEMENT POLICIES AND IT SYSTEM THREATS

IT systems should be analysed and perceived taking into account all the components, namely the hardware equipment, the information base, the software base with platforms and application programs, human resources with all categories of users and, last but not least, the mathematical models for optimizing and increasing the efficiency and effectiveness of an IT system. From here to an effective management system is a single step, because there is the whole set of elements of an organization that interact to establish policies, to achieve objectives and to carry out the processes necessary to achieve objectives, to successfully meet performance indicators and performance criteria. It means that any potential cause of an unwanted incident can cause damage to a subsystem, a system or the entire organization, at which point we speak of a threat. It means that there is potential for a particular system vulnerability to be exploited, either accidentally or intentionally.

IT systems should be analysed and perceived taking into account all the components, namely the hardware equipment, the information base, the software base with platforms and application programs, human resources with all categories of users and, last but not least, the mathematical models for optimizing and increasing the efficiency and effectiveness of an IT system.

Vulnerability always refers to the weakness of an asset or control tool that can be directly or indirectly exploited by one or more threats. For example, any flaw or weakness in the design, implementation, operation or administration of a system can be exploited to violate the system's security policy. Very important at this moment is the correct estimation of the risk, i.e. of the effect of an uncertainty in achieving the objectives. The elements that must be found in coherent security policies are the following:

- the sets of interrelated activities that transform inputs into outputs, often called *processes*;
- the status of a process or activity, which means monitoring.

The group selected for the study of the impact of the implementation of information security requirements, following the investigation and the observation carried out, consists of 128 students from military academies in Europe (Romania, Bulgaria and Poland) as follows: *"Henri Coandă"* Air Force Academy in Brașov (56 students), National Military University in Veliko Tarnovo (42 students) and University of Military Studies in Warsaw (30 students).

The methods of gathering information are based on questionnaires, direct observation and interview. Being a quantitative research method, the questionnaire is very useful in this case, due to the variety and target of the questions asked.

The scope of questions includes computer network security, technology trust and risk management, storage device policy, platform configuration, user access, remote working and the importance of user information and cyber education. The students who answered the questions had three answer options for each question: *NO, YES, It is possible.*

The direct aim of the research is to understand the barriers and risks, to adopt a rigorous and responsible behaviour in the use of information on storage media, to understand the strategies to reduce the risks, the behaviour in the event of a security incident, the responsibilities regarding the planning of resources to respond to an incident. The secondary aim of this research is to make users aware of the general context of using an IT system.

The direct aim of the research is to understand the barriers and risks, to adopt a rigorous and responsible behaviour in the use of information on storage media, to understand the strategies to reduce the risks, the behaviour in the event of a security incident, the responsibilities regarding the planning of resources to respond to an incident. The secondary aim of this research is to make users aware of the general context of using an IT system.

The National Agency for the Security of Information Systems in the *"Code of good practices for the security of information and communication systems"* (2022, p. 4) promotes the formation and development of an organizational culture that understands the need for risk management as an inevitable element in carrying out the activity and making decisions.

THE CURRENT CONTEXT OF THE EXPONENTIAL DEVELOPMENT OF DIGITIZATION IS BECOMING A MAGNET FOR CYBER ATTACKS

Computer security companies anticipate that attacks will become more and more sophisticated, with devastating consequences for people's activities and for companies. As a result, knowing the current trend of the manifestations of computer threats allows for adopting the technical and organizational measures that are necessary for organizations to protect information. We are referring here to more vulnerabilities with greater impact on IT systems as well as to the number of reported vulnerabilities that will certainly increase, according to the monitoring of recent years. (*Infosfera*, no. 2/2021, p. 49).

Another *"magnet"* factor is the increasing use of *"open-source"* applications, which increases the risk of becoming more vulnerable to attackers. Tutorials on offensive and defensive tools are now available to all users, increasing exposure to risks.

Social engineering techniques, artificial intelligence and the development of skills in detecting physical errors are factors favouring the increase in the effectiveness of computer attacks. Of course, criminals will adapt their attack methods and find new ways to threaten systems, becoming harder and harder to identify.

More and more intelligent devices are used and the user behaviour is increasingly insecure and unprotected. Andrea Radu, in the article *"IT Security"* (2019), estimated a number of 20 billion connected smart devices. Protection, security and privacy solutions will obviously go towards compliance with standards regarding the production of devices, compliance with integrity restrictions regarding data collection and processing and, last but not least, ensuring an IT system maintenance process adapted to the information requirements of all users.

Social engineering techniques, artificial intelligence and the development of skills in detecting physical errors are factors favouring the increase in the effectiveness of computer attacks. Of course, criminals will adapt their attack methods and find new ways to threaten systems, becoming harder and harder to identify.

The focus will be on respecting privacy rights through restrictions on software producers and consistent legislation.

Encrypting information and protecting the online activity of all categories of users are fundamental requirements in the use of computer applications. The exponential development of all economic fields, the Internet of Things, big data systems, cloud technologies and the digitization of systems are obviously accompanied by an increase in the exposure to vulnerabilities, allowing malicious actors to target more and more sources of cyber exploitation. In this context, the information security strategy defined by each organization represents the plan that integrates the major information security objectives, policies and action sequences of the organization into a cohesive unitary system. It is a document drawn up by the organization and it includes an assessment of IT threats as well as a set of countermeasures for their annihilation, which are financially assured. Of course, the strategy is seen as a method to influence the internal environment of the organization through the careful selection of the means of internal control.

RESEARCH RESULTS AND TRENDS IN THE IMPLEMENTATION OF INFORMATION SECURITY TECHNIQUES AND METHODS IN MILITARY SYSTEMS

Threats from within organizations can lead to security incidents, which means an educated user is a key element in every organization cybersecurity culture. The implementation of good cyber security practices is a *"must"* in the current context of technology use. Adopting an organization's information security strategy greatly increases the quality of the information security program provided there is a close link between it and the organization's strategy. Information security strategy is not defined in itself, but is an orientation of security policies, security control and audit, and security system management. The information security objectives should be consistent with the information security policy and measurable (if possible). They should also consider the applicable information security requirements and the results of the risk assessment and treatment. Last but not least, they should be communicated and updated as necessary.

The implementation of good cyber security practices is a "must" in the current context of technology use. Adopting an organization's information security strategy greatly increases the quality of the information security program provided there is a close link between it and the organization's strategy. Information security strategy is not defined in itself, but is an orientation of security policies, security control and audit, and security system management.

The conducted research highlights the vulnerable points in the implementation of good cyber security practices. In this context, the main criteria for evaluating the vulnerabilities of IT systems are formulated and graphically represented as follows:

- *Securing workstations connected to networks is an essential condition for ensuring confidentiality (Chart no. 1);*
- *Encrypting classified data is important (Chart no. 2);*
- *Managing passwords and using complex algorithms to change them periodically (Chart no. 3);*
- *Use of accounts with limited rights (Chart no. 4);*
- *Data synchronization with mobile devices (Chart no. 5);*
- *Disable unused connections on mobile devices (Chart no. 6);*
- *Sharing of personal information (Chart no. 7);*
- *Use of verified storage media (Chart no. 8);*
- *Secure data connections (Chart no. 9);*
- *Tracking third-party access to data in wireless networks (Chart no. 10);*
- *Installating updated antivirus solutions (Chart no. 11);*
- *Installation of firewall applications (Chart no. 12);*

- *Security incident reporting (Chart no. 13);*
- *Using an application whitelist (Chart no. 14);*
- *Web content restriction (Chart no. 15);*
- *Carrying out risk and exposure to vulnerabilities assessment (Chart no. 16).*

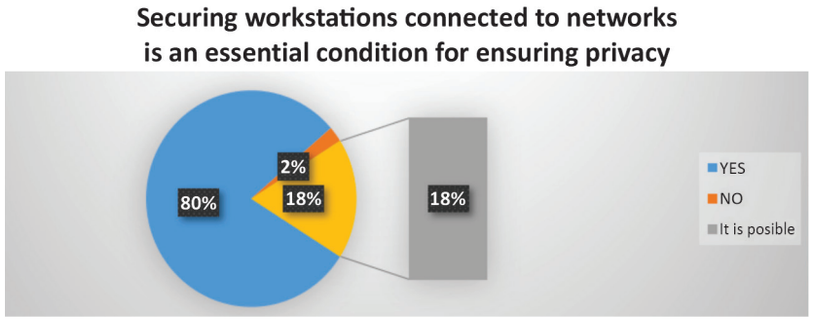

Chart no. 1

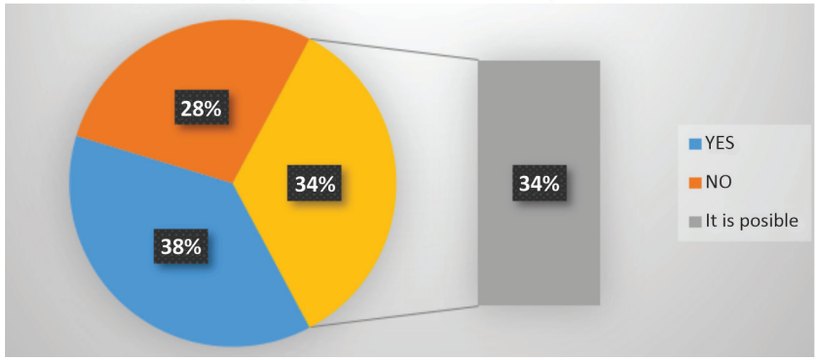

Chart no. 2

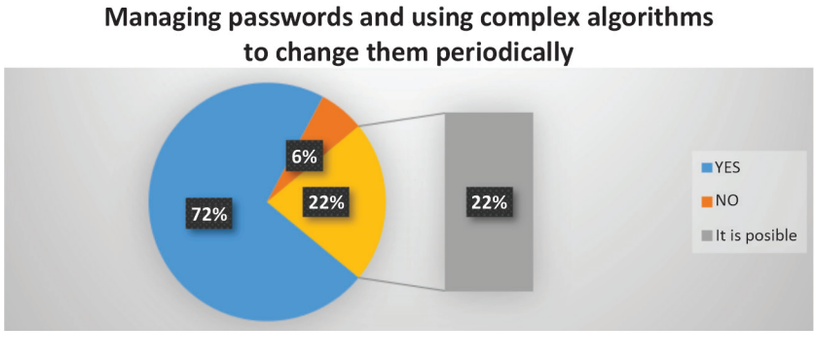

Chart no. 3

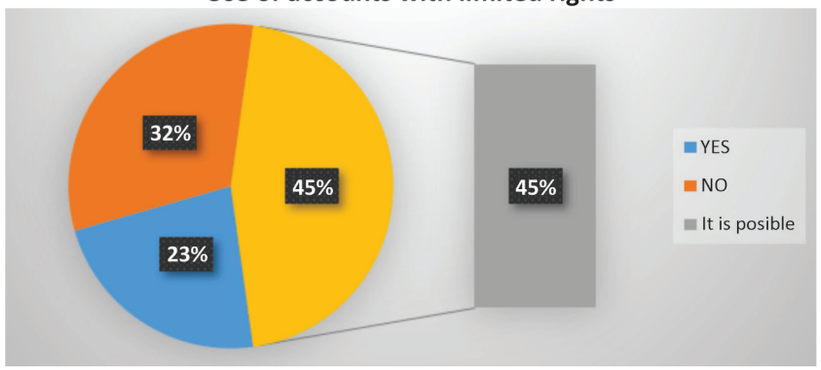

Chart no. 4

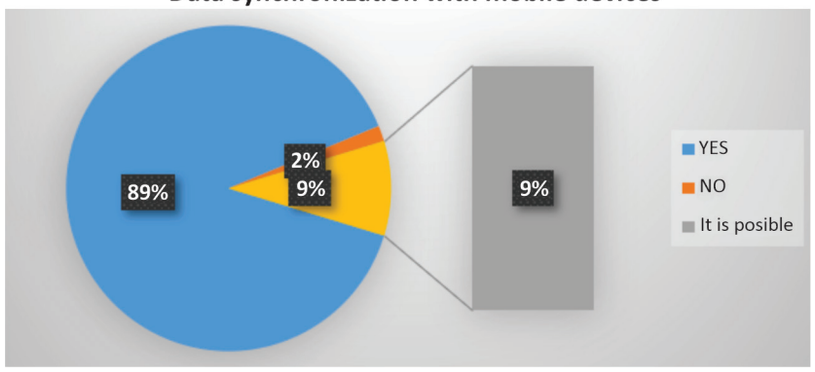

Chart no. 5

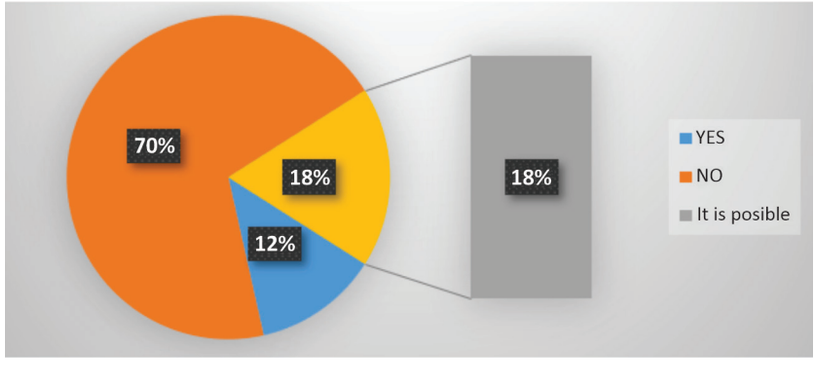

Chart no. 6

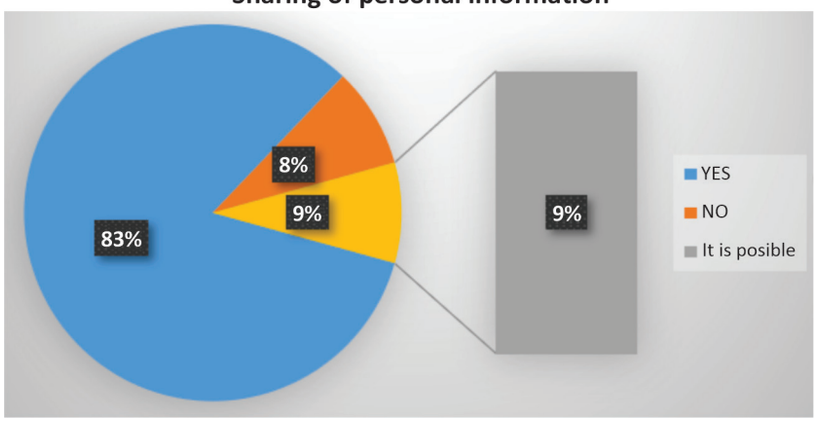

Chart no. 7

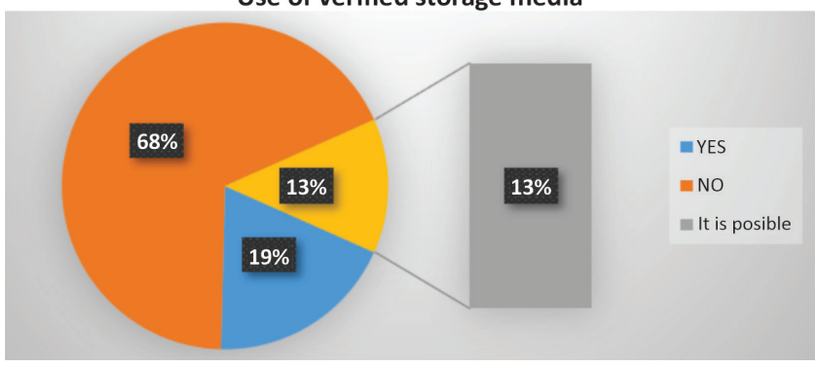

Chart no. 8

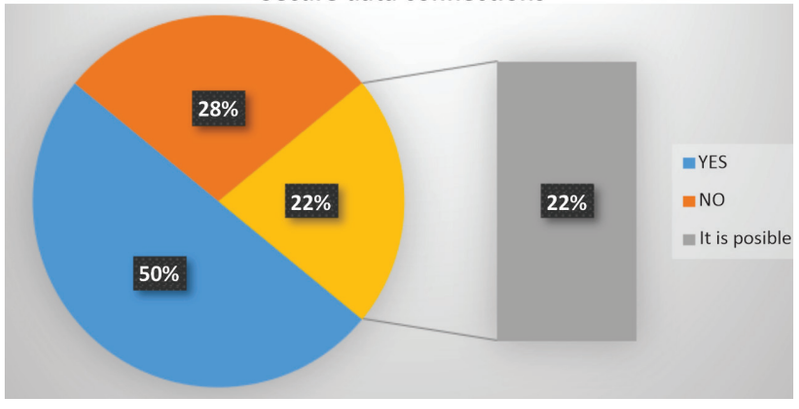

Chart no. 9

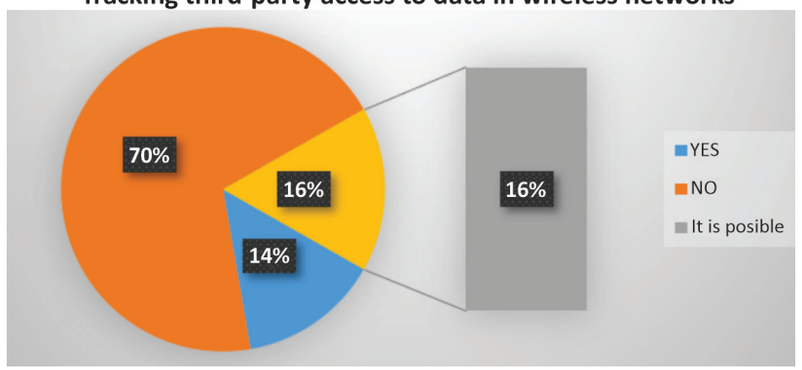

Chart no. 10

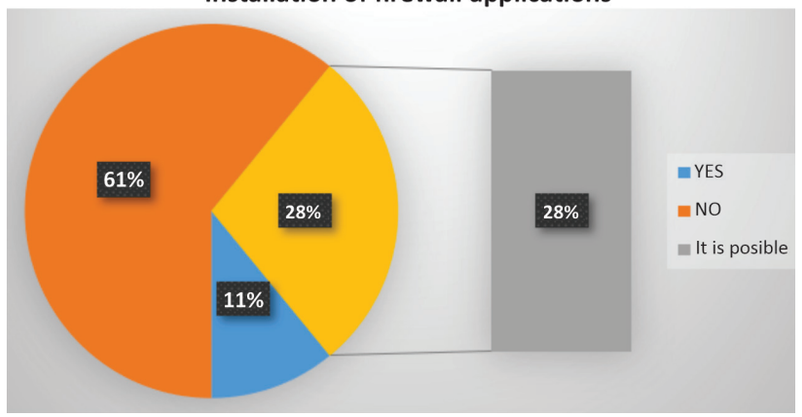

Chart no. 11

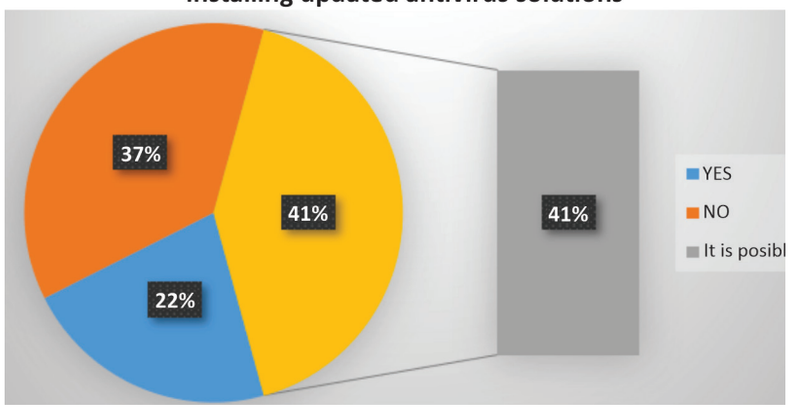

Chart no. 12

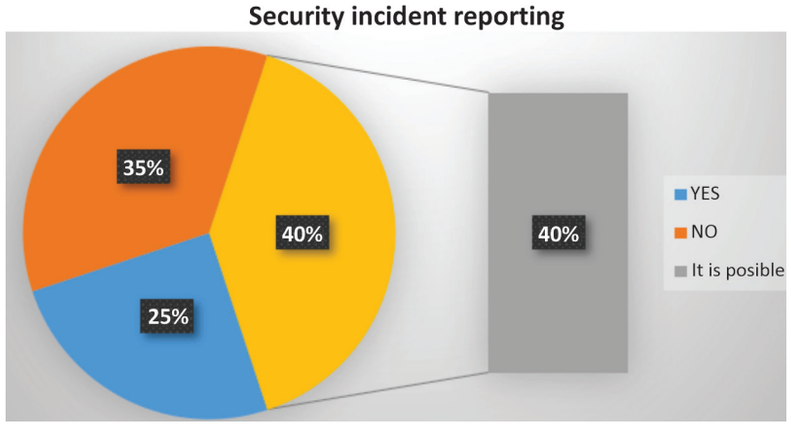

Chart no. 13

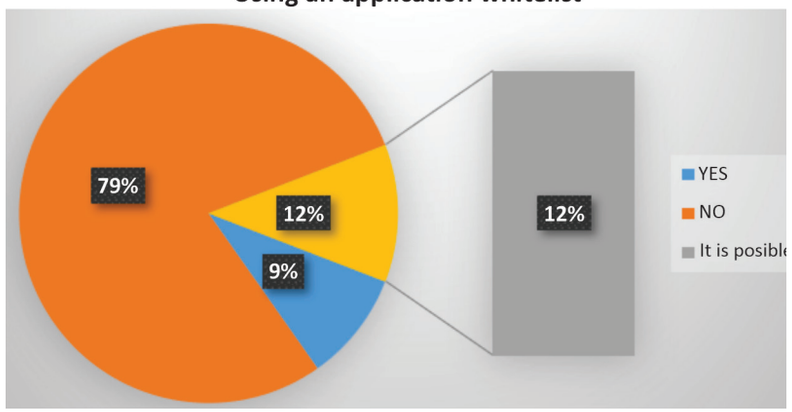

Chart no. 14

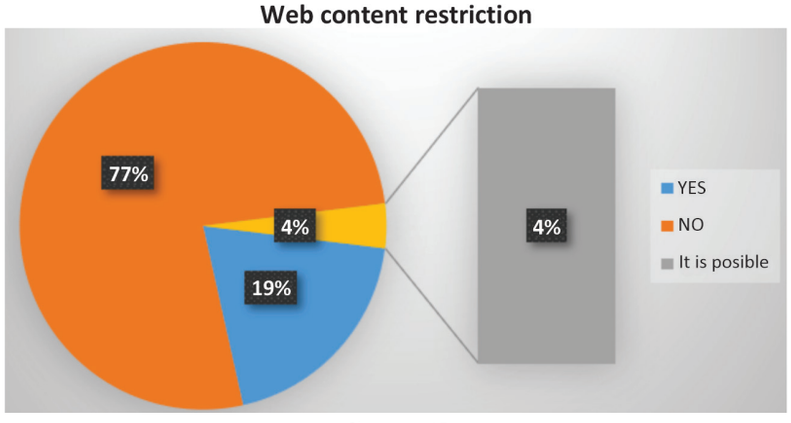

Chart no. 15

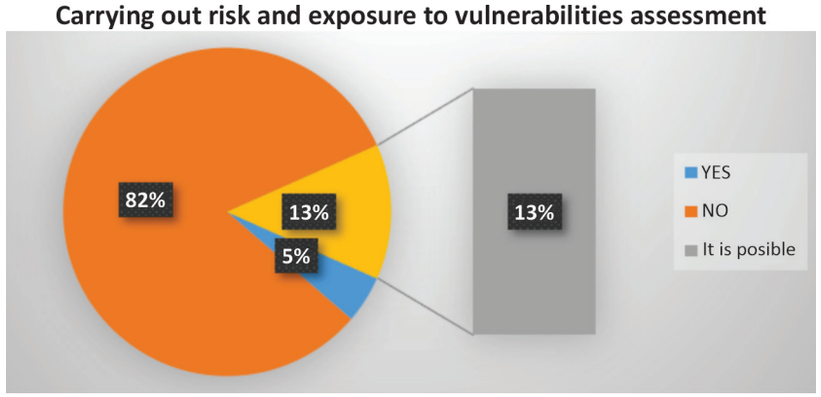

Chart no. 16

The result summarizing the information security risk assessment criteria *(Chart no. 17)* clearly and coherently highlights the vulnerable points in security. Retrieving this information allows the establishment of clear strategies to identify and minimize the vulnerabilities of the implemented IT systems. Lack of discipline in the use and synchronization of mobile devices and wireless networks increases information security risks by 70%. End users intentionally expose themselves to risks by not following general security rules and principles, without thinking about the subsequent consequences of their imprudent actions.

BLACK SWAN SECURITY INCIDENT ALERT

Nassim Nicholas Taleb states that *"Black Swan"* type incidents are rare as events; they cannot be predicted, but they are unpleasant events that have a major impact and can only be explained after they occur and produce effects. For example, *"Black Swan"* type incidents can be considered the following: the explosion of the Internet network, the First World War, the dissolution of the Soviet Union, the event on 11 September, the nuclear disaster at Fukushima Daiichi. (Mambet, 2012).

The COVID-19 pandemic has accelerated the development of the virtual environment and *"world"*, even its acceptance in different systems where it was supposed to be impossible to use. Is COVID-19

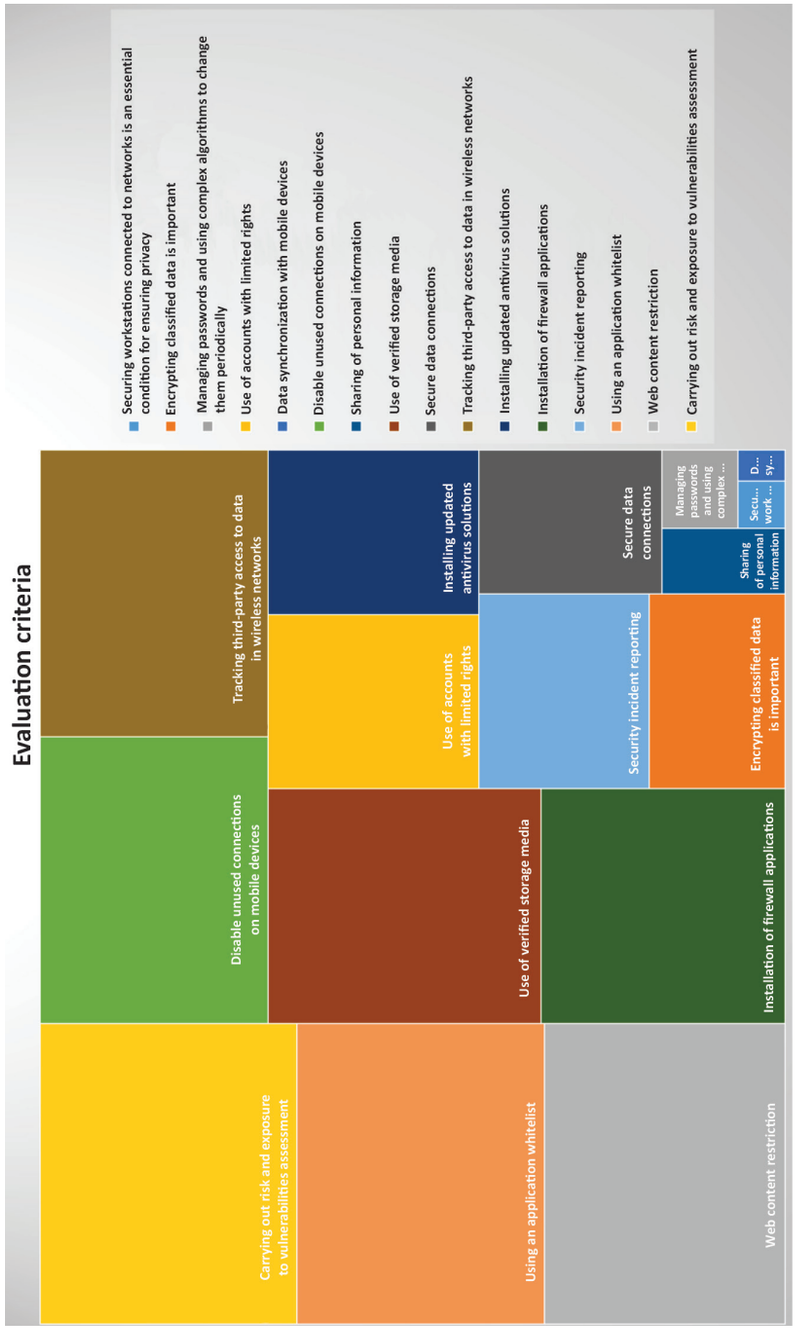

Chart no. 17

a *"Black Swan"* incident? The answer is NO, because it appears to be an imbalance between the operational and medical security components. (*Infosfera*, p. 67). We wonder if there will be *"Black Swan"* incidents? Definitely yes! It is just a matter of time. However, the COVID-19 pandemic has accelerated the development of the virtual world and created a visible imbalance between the use of technology and the security component, which obviously leads to predictive security incidents, of the *"White Swan"* type. A security model that can be successfully used is the encryption algorithm, which is a mathematical model implemented for information security. Cryptographic products can be used to protect data in communication systems or in specific applications. The evaluation algorithm is easy to understand by users and easy to implement, relative to the hardware and software resources available to the unit.

The evaluation of cryptographic modules can be done using the FIPS 140-2 standard equivalent to ISO19790; 4 security levels; functional security requirements and specific security requirements such as: specifications for the cryptographic module, ports and interfaces dedicated to the cryptographic module, specific roles, functions and authentications, physical security, consistent operating environment, consistent management of encryption keys, self-tests, securing the project, mitigating other attacks – which means effective risk management.

Common criteria are found in equivalent standards ISO15408 as follows:

- Trusted Computer System Evaluation Criteria, 1983, NSA;
- Canadian Trusted Computer Product Evaluation Criteria, 1993, Communications Security Establishment to provide common evaluation criteria for IT products;
- Information Technology Security Evaluation Criteria, May 1990 in France, Germany, Holland and Great Britain;
- Common Criteria, 31 members.

The question remains whether we will replace them with the *"Cyber Security Act"*?

The COVID-19 pandemic has accelerated the development of the virtual world and created a visible imbalance between the use of technology and the security component, which obviously leads to predictive security incidents, of the "White Swan" type. A security model that can be successfully used is the encryption algorithm, which is a mathematical model implemented for information security. Cryptographic products can be used to protect data in communication systems or in specific applications.

CONCLUSIONS

The results of the statistical research clearly and obviously reflect the vulnerable points and the way users approach security concepts, embodied in actions. In conclusion, the information security requirements must be formulated clearly, correctly and coherently by each individual organization, periodically explained to end users, emphasizing the following aspects:

- Application development – architectural design, functional specifications, design, implementation representation, security policy modelling.
- Guidance on the rules of safe use of applications.
- Knowledge of the life cycle of an IT system: life cycle definition, configuration management scope and capabilities, security during development, security of delivery, remediation flow, tools and techniques.
- Updating knowledge regarding tools used in information security: functional testing (plans, procedures and records), test coverage analysis, test depth analysis, independent testing.
- Vulnerability assessment and analysis.

The information security requirements must be formulated clearly, correctly and coherently by each individual organization, periodically explained to end users, emphasizing the following aspects: application development; knowledge of the life cycle of an IT system; updating knowledge regarding tools used in information security; vulnerability assessment and analysis.

Words are insufficient when we analyse *chart no. 18*, generated on the basis of the centralizing results from the questionnaire applied to the target group. The image is relevant and at the same time

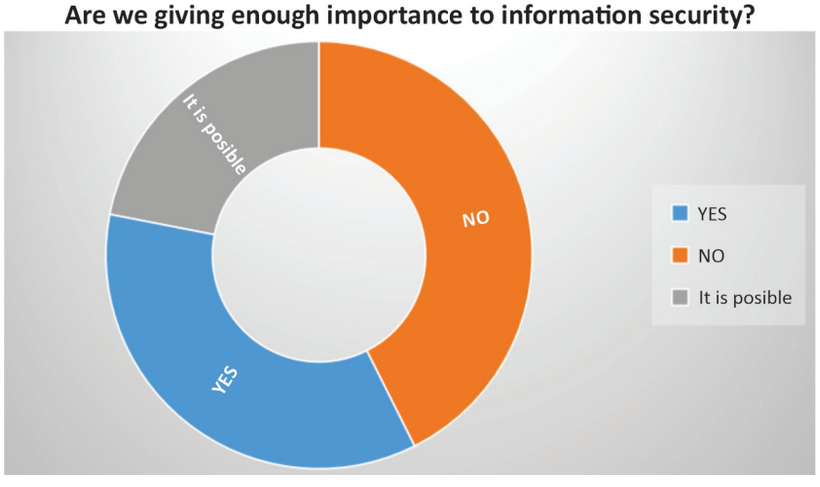

Chart no. 18

worrying. It is obvious that cyber security education is strictly necessary and must be implemented. End users do not pay enough attention to information security, often going by the principle *"it cannot happen to me"* or *"the organization I work in protects me".* The research will be developed by analysing other criteria, applying the questionnaire to specific user categories and age categories, targeting measures to minimize the vulnerabilities of military IT systems. The fragmentation of the target group will also allow more precise identification of information security risks.

BIBLIOGRAPHICAL REFERENCES:

1. Mambet, C. (2012). *Abordarea transdisciplinară a gestiunii* și *managementului riscurilor* și *al proceselor decizionale.* Doctoral Thesis, https://ciret-transdisciplinarity.org/biblio/biblio_pdf, retrieved on 22 October 2022.
2. Radu, A. (2019) *"Securitate informatică"*. In online review asig.ro, https://www.1asig.ro/Securitate-informatica-Atacurile-vor-deveni-din-ce-in-ce-mai-sofisticate-in-2020-articol-3,102-62487.htm, retrieved on 17 October 2022.
3. *"Codul de bune practici pentru securitatea sistemelor informatice și de comunicații"* (2022). București.
4. European Union Agency for Cyber security (ENISA). Publications from the Threat Landscape 2020 Series, https://www.enisa.europa.eu/publications, retrieved on 22 October 2022.
5. European Union Agency for Law Enforcement Cooperation (EUROPOL). Publications and documents on cybercrime, https://www.europol.europa.eu/publications-documents, retrieved on 12 October 2022.
6. European Union Agency for Law Enforcement Training (CEPOL). E-Journals on cybercrime, https://www.cepol.europa.eu/science-research/journals/e-journals, retrieved on 22 October 2022.
7. *Infosfera* (2021). Year XIII, no. 2.
8. International Journal of Information Security and Cybercrime (IJISC), https://www.ijisc.com retrieved on 22 October 2022.

9. *Metodologia și instrucțiunile de completare a formularelor de raportare a incidentelor majore/Regulament 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate* (2020). In *Monitorul Oficial*, Part I, no. 115 on 14 February 2020, https://lege5.ro/Gratuit/gm3dcmzxhayq/regulamentul-nr-2-2020-privind-masurile-de-securitate-referitoare-la-riscurile-operationale-si-de-securitate-si-cerintele-de-raportare-aferente-serviciilor-de-plata?pid=310681889#p-310681889, retrieved on 22 October 2022.
10. National Association for Information Systems Security (ANSSI). Guide for securing computers and networks, https://cert.ro/vezi/document/ghid-bune-practici-pentru-securizarea-calculatoarelor-personale, retrieved on 22 October 2022.
11. National Cyberint Center within the Romanian Intelligence Service. Best practices guide for cybersecurity, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf., retrieved on 22 October 2022.
12. Romanian Association for Information Security Assurance (RAISA). Considerations on challenges and future directions in cybersecurity, https://www.raisa.org/documents/CybersecurityRO2019.pdf., retrieved on 12 October 2022.
13. Romanian National Computer Security Incident Response Team (CERT-RO). Cybersecurity guides, https://cert.ro/doc/ghid, retrieved on 7 October 2022.
14. Checkmarx, https://www.checkmarx.com/, retrieved on 22 October 2022.
15. FIPS 140-2, https://csrc.nist.gov/publications/detail/fips/140/3/final, retrieved on 22 October 2022.
16. HCL (IBM) Appscan, https://www.hcltechsw.com/products/appscan retrieved on 7 October 2022.
17. ISO 15408, https://www.iso.org/standard/50341.html, retrieved on 7 October 2022.
18. ISO 19790, https://www.iso.org/standard/52906.html, retrieved on 7 October 2022.
19. MBSA, Microsoft Baseline Security Analyzer, https://www.microsoft.com/en-us/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/, retrieved on 7 October 2022.

20. NIAP, https://www.niap-ccevs.org/, retrieved on 7 October 2022.
21. Vulnerability scanners NESSUS, https://www.tenable.com/products/nessus, retrieved on 7 October 2022.
22. https://www.commoncriteriaportal.org/, retrieved on 12 October 2022.