


Opportunity Makes the Thief. A Risk Analysis and Vulnerability Identification Approach in Information Security Management Systems as a Method of Countering Cybercrimes

Krzysztof Świtała

PhD, Department of Informatics Law, The Law and Administration Faculty, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Wóycickiego 1/3, 01-938 Warsaw, Poland; e-mail: k.switala@uksw.edu.pl

 <https://orcid.org/0000-0003-0426-5383>

Keywords:

cybersecurity,
cybercrime,
ISMS,
risk management,
vulnerability analysis

Abstract: Data processing in ICT systems is a fundamental activity in the information society. The aim of this article is to present tools specific to information security management systems, such as risk and vulnerability analysis as solutions that can contribute to reducing the incidence of cybercrimes. Limiting the occurrence of such incidents can therefore be considered as a proactive method of preventing the presence of such criminal acts. Considerations include legal instruments such as the GDPR and the NIS2 Directive, which provide for breach and incident management procedures, as well as a risk-based approach. An analysis of vulnerabilities, together with mechanisms for their reporting and the exchange of such information between authorized entities, is proposed in the new NIS2 Directive. It is an essential tool for increasing the resilience of ICT systems by securing their weakest links. Technical standards from the information security area ISO 27000 are also covered in this article. The interdisciplinary nature of the subject matter analyzed implies a discussion of such methods of increasing the effectiveness of security in ICT systems as penetration testing and hardening.

1. Introduction

The purpose of this article is to present the approach to securing data processing, taking into account the results of the risk management process. Its application is part of the implementation of legal requirements arising from the GDPR¹ and NIS2 Directive.² The issue of identifying and responding to vulnerabilities, assuming a proactive approach to ensuring the security of information systems, the mature form of which is proposed in the NIS2 Directive, will also be addressed. The application of an attitude based on ongoing risk management allows for the realization of the principle of continuous improvement in the effectiveness of security features in information systems, leading to a reduction in the number of offences committed against them.

Information is a transferable, intangible asset that reduces uncertainty.³ Recent decades have been distinguished by dynamic political, social and technological changes, influencing the reality in the era of globalization and the development of the knowledge economy. In the information society, computing is recognized as a fundamental process determining economic growth and the formation of a network society, characterized by the dispersion and interpenetration of social relationships and open access to diverse social groups, both stationary and online. These changes were made possible by the development of the Internet and social media. The shift of social and business contacts to the online environment, apart from the undoubted benefits associated with improved communication, has also brought new risks.

Due to the global nature of the internet, countering cybercrime is an important international issue. Ensuring information security and cybersecurity is particularly important for achieving the following four goals

¹ Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L119/1, 4 May 2016).

² Directive (EU) 2022/2555 of The European Parliament and of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L333/80, 27 December 2022).

³ Irena Lipowicz et al., *Prawo administracyjne. Część materialna* (Warsaw: LexisNexis, 2014), 97.

of the UN 2030 Agenda for Sustainable Development⁴: build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation (goal 9), as well as ensuring healthy lives and promote well-being for all at all ages (goal 3) – e-health solutions, ensuring inclusive and equitable quality education and promote lifelong learning opportunities for all (goal 4) – e-learning tools, and making cities and human settlements inclusive, safe, resilient and sustainable (goal 11) – smart-cities concept. Current legislative work underway at the UN includes a convention against cybercrime.⁵

In the case of Europe, the Cybercrime Convention already has a 20-year history.⁶ In the European Union legal system, Chapter 5 of the soft law Declaration on Digital Rights and Principles for the Digital Decade provides for the entitlement of users of cyberspace to a protected, safe and secure digital environment.⁷ Furthermore, Article 3(1)(k) of the Digital Decade Policy Programme 2030 sets a target for the European Union related to seeking to improve its resilience to cyberattacks.⁸ According to the content of Article 6(2) of the NIS2 Directive, maintaining the security of networks and information systems means precisely guaranteeing their resilience against any event that might compromise the availability, authenticity, integrity or confidentiality of the data processed therein. Negative situations that turn into incidents, as described here, may result from cybercriminal activities. Reducing the occurrence of such incidents can therefore be considered a proactive method of preventing the commission of criminal acts in cyberspace.

Information security management is not a state, but a continuous iterative process that should be constantly improved by identifying new

⁴ UN General Assembly, A/RES/70/1, Transforming our world: the 2030 Agenda for Sustainable Development.

⁵ UN General Assembly, A/79/460, Countering the use of information and communications technologies for criminal purposes.

⁶ Council of Europe Convention on Cybercrime (CETS No. 185), Journal of Laws 2015, item 728.

⁷ European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01 (OJ C23, 23 January 2023), 1–7.

⁸ Decision (EU) 2022/2481 of The European Parliament and of The Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L323/4, 19 December 2022).

vulnerabilities to information assets and the threats that may affect them. It is therefore necessary to monitor data processing processes to identify deviations from assumed parameters that form the basis for a review, the outcome of which can provide concrete justification for decisions to make changes. Information security measures should not be *ad hoc* activities, but organized in a planned and structured process.

2. Information Security Management Systems and Their Cyber Resilience

Within the scope of general systems theory, this concept is defined as a set of elements that are in a reciprocal relationship.⁹ As a result of analyzing cybersecurity regulations, data protection and technical standards in the field of information security, the following features of information security management systems in a specific organization can be identified:

- It encompasses the policies, procedures, guidelines and associated resources and activities, collectively managed, undertaken to protect information.
- It represents a structured approach to establishing, implementing, operating, monitoring, maintaining and improving information security for the achievement of its business objectives.
- Technical and organizational measures for safeguarding information assets are implemented as part of the process of dealing with risks, carried out after analyzing and assessing them.

According to ISO 27001 technical standard, achieving a satisfactory level of information security implies maintaining information attributes such as confidentiality, integrity and availability. In addition, other properties such as authenticity, accountability, non-repudiation and reliability may be taken into account.¹⁰ Ensuring the security of personal data presupposes the preservation of confidentiality and integrity (Article 5(1)(f)), as well as availability (Article 25(2) GDPR) by controllers. In turn, the NIS2 Directive implies the preservation of the availability,

⁹ Ludwig von Bertalanffy, *General System Theory: Essays on Its Foundation and Development* (New York: George Braziller, 1968), 55.

¹⁰ ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, Geneva 2022.

authenticity, integrity or confidentiality of information processed by important and essential entities.

The implementation of the obligations imposed on personal data controllers and essential services operators by ensuring an adequate level of security of the resources they use requires the implementation of technical and organizational safeguards that are appropriate to the state of identified vulnerabilities and threats (Articles 24 and 32 of the GDPR, as well as Article 21(1) of NIS2). These should form a complementary, effective and coherent set of elements at the core of the security management system for processed information assets.

3. Risk-Based Approach

Risk is a concept that appears in various contexts in both the legal and management sciences. For example, strict liability occurs in civil law (Articles 430, 433–436, 474 of the Civil Code¹¹), as a theory of legal responsibility for consequences of inherently dangerous activities, even in the absence of fault on the part of the defendant. In technical standards, on the other hand, risk management in organizations refers to ISO 31000.¹² In the areas of information security and cybersecurity, the following levels of understanding of the concept of risk are indicated:

- It is considered as the impact of uncertainty on objectives, causing a positive or negative deviation from expectations.
- It is a potential situation in which a specific threat will exploit the vulnerability of an asset or group of assets, thereby causing harm to the organization.
- It is measured as a combination of the probability of an event and its consequences.¹³

The analyzed legal regulations concerning the protection of personal data contain a number of references to the risk-based approach. It refers both to the risks related to potential infringement of the rights and freedoms of data subjects (Article 24(1) GDPR) and those related to the specificity of

¹¹ Act on the Civil Code of 23 April 1964, Journal of Laws 2024, item 1061.

¹² ISO 31000 – Risk management – Guidelines, Geneva 2018.

¹³ ISO/IEC 27005 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks, Geneva 2022, 2.

the processing of these resources themselves (Article 32(2) GDPR). The organizational arrangements analyzed here are also closely related to the concept of privacy by design, which is reflected in Article 25(1) GDPR.

In the case of the NIS2 Directive, the concept of cybersecurity risk management refers to the obligations of important and essential entities to select appropriate data security safeguards (Article 21 NIS2), as well as EU coordinated efforts to improve the security of critical supply chains (Article 22 NIS2).

The technical standard ISO 27005 provides guidance on how to establish an organization's risk management process. It is iterative in nature and includes the following phases: establishing the context for the analysis, risk assessment (including its identification, analysis and evaluation), selecting methods to deal with it (risk treatment) and accepting the residual risk remaining after the procedure. In addition, ongoing monitoring of the risks and reporting of the results of the actions is carried out throughout the iteration. The described process can be used both when implementing risk management mechanisms under the GDPR¹⁴ and the NIS2 Directive.¹⁵

Risk management, on the one hand, allows the identification of potential events that could become incidents and the implementation of safeguards to prevent their occurrence. On the other hand, it is a method of seeking the most optimal choice of safeguards for the specific conditions and circumstances of data processing. In either case, risk mitigation will contribute to reducing the likelihood of cybercrimes in an organization using this approach.

4. Vulnerability Analysis as a Proactive Approach to Ensuring the Security of Information Systems

Complementary to the risk-based approach is the process of analyzing and exchanging information about the vulnerability of resources held, in

¹⁴ Andrzej Kaczmarek et al., *Jak rozumieć podejście oparte na ryzyku według RODO?* (Warsaw: UODO, 2018), 10, accessed September 30, 2024, <https://uodo.gov.pl/pl/file/706>.

¹⁵ Jan Kolouch et al., "Cybersecurity: Notorious, but Often Misused and Confused Terms," *Masaryk University Journal of Law and Technology* 17, no. 2 (2023): 284–5.

particular software and hardware for data processing. This is an example of activities classified in criminology as cybercrime prevention.¹⁶

In ISO 27000 standard, vulnerability is defined as weakness of an asset or safeguard that can be exploited by one or more threats.¹⁷ In an analogous way, this concept is understood in Article 6(15) of the NIS2 Directive. Countermeasure activities are the cornerstone of prevention not even prior to the incident itself, but before the emergence of the threat that could potentially cause it. It is intended to lead to the elimination of causes rather than merely blocking the possibility of the effect itself. Vulnerability handling precedes and later complements the classic risk-based continuous improvement methods for information security management systems. These processes should be primarily oriented towards identifying and neutralizing established vulnerabilities of protected assets.

One of the most significant challenges for the analyzed method of cybersecurity prevention is the detection, analysis and protection of zero-day system vulnerabilities, previously unknown to its owners and developers, which have already been disclosed but is not yet patched. These vulnerabilities pose a significant threat to ICT systems because they are not mitigated by specific security features assigned to them. An attacker can therefore more easily bypass them in order to directly exploit a specific vulnerability.

Recital 44 of the NIS2 Directive indicates that a CSIRT should be able to monitor their resources connected to the Wide Area Network (in particular the Internet) at the request of important or essential entities, in order to better understand and react more quickly to critical vulnerabilities. Recital 58 et seq. points to the role of identifying and addressing vulnerabilities, as well as sharing information about them among authorized information actors, in enhancing the maturity and effectiveness of the EU cybersecurity delivery system. The wording of Article 7(2)(c) states that each Member State shall adopt a national cybersecurity strategy with policies on vulnerability management, including the promotion and facilitation of coordinated disclosure of vulnerabilities and, in accordance with

¹⁶ Wojciech Filipkowski, "Przestępczość z użyciem komputerów i ich sieci," in *Kryminologia. Stan i perspektywy rozwoju*, eds. Emil Pływaczewski et al. (Warsaw: Wolters Kluwer, 2019), 526–8.

¹⁷ ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, Geneva 2018, 11.

Article 12, the creation of a European vulnerability database on the basis of this information.

Vulnerability management and the coordinated sharing of information on vulnerabilities among authorized actors should contribute to a more effective and flexible response to new cybersecurity threats. This proactive approach in the context of cybercrime issues can be seen as a preventive measure.

5. Technical Approaches to Reducing Vulnerabilities in Information Systems – Penetration Testing and Hardening

Penetration testing involves conducting a controlled attack on an ICT system to detect vulnerabilities that could lead to a real-world incident. The procedure is divided into three basic phases:

- Information gathering – involves obtaining data about the ICT system under test.
- Vulnerability analysis – allows to check the configuration of the tested system in order to find security gaps.
- Vulnerability exploit – exploitation of previously identified weaknesses of a system by means of algorithms adapted to their specifics, in order to gain unauthorized access to an ICT system.¹⁸

Penetration testing is a method of empirically verifying the security status of ICT systems. It is a simulation of an attack scenario on such solutions, which in everyday circumstances can be exploited by a threat and cause real damage to an organization.¹⁹ Following the penetration test, a post exploitation analysis is carried out, where the aim is to assess to what extent the identified vulnerabilities are relevant to maintaining the security of resources in the information system. Once everything has been done, a report is produced as a knowledge base and source of experience.

Hardening involves the implementation of safeguards aimed not only at risk reduction, but also at blocking vulnerabilities.²⁰ The measures

¹⁸ Aileen Bacudio et al., “An Overview of Penetration Testing,” *International Journal of Network Security and Its Applications* 6, no. 3 (2011): 22.

¹⁹ David Kennedy et al., *Metasploit. The Penetration Tester’s Guide* (San Francisco: No Starch Press, 2025), 1–2.

²⁰ Aaron Echeverria et al., “Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation,” *Applied Science* 11, no. 7 (2021): 2.

carried out are intended to group security features into complementary layers, which constitute a hierarchically ordered arrangement of elements (vertical coherence). There should be no security gaps between ICT system components that can be exploited by threats (horizontal coherence). Improving security configurations can be a consequence of failing to achieve satisfactory security metrics after a penetration test. The hardening process involves disabling unused computer network ports (TCP/UDP) and removing unused services in order to reduce the impact of a potential ICT attack on the infrastructure in use.

As a rule, a person who performs penetration tests in consultation with an ICT system administrator (data controller) is not committing a crime because they are acting under the administrator's authority. Moreover, in 2017, the justification of acting to detect security flaws in ICT systems was introduced into the Polish legal system (Article 269c of the Penal Code²¹). *De lege ferenda*, it should be pointed out that the indicated premise limiting liability could also cover situations where, as part of Intrusion Prevention Systems and related solutions, proactive actions are taken by the system administrator to repel an ICT attack and may interfere with the attacker's ICT system.²² It is legitimate to ask the question whether the justification of self-defense can be applied in such a situation. Can such action be regarded as repelling a straightforward attack on a good protected by law? Interpreting the ideas on the subject expressed in the literature, taking action that interferes with the functioning of the information and communication system in which protected information resources are processed can be regarded as a direct interference, by its inevitability, with an asset protected by law.²³ Undoubtedly, the Polish legal regulation in the context of the problem discussed here should be as coherent, clear and precise as possible.

The purpose of penetration testing and hardening is to increase the resistance of an ICT system to threats by reducing new identified vulnerabilities. From the point of view of cybercriminals, carrying out such activities

²¹ Act on the Penal Code of 6 June 1997, Journal of Laws 2024, item 17.

²² Nilotpal Chakraborty, "Intrusion Detection System and Intrusion Prevention System: a Comparative Study," *International Journal of Computing and Business Research* 4, no. 2 (2013): 4.

²³ Konrad Burdziak, "Bezpośredniość zamachu, czyli kilka słów na temat obrony koniecznej w polskim prawie karnym," *Przegląd Sądowy*, no. 1 (2018): 58.

makes it more difficult to implement their previously proven *modus operandi* for attacks in cyberspace.

6. Methods for Rapid Response to Cyber Security Incidents According to NIS2 Directive

Cybersecurity incident means an event compromising the availability, authenticity, integrity or confidentiality of processed data. In other words, it is a case of risk realization in a protected information system. On the basis of the 2016/1148 NIS Directive, incident response was primarily the responsibility of essential service operators and digital service providers, who, in the case of more serious incidents, were assisted by the relevant CSIRT. Under the terms of cross-border cooperation, this was done through single points of contact and CSIRT networks. However, the solutions presented here proved to be insufficiently effective. The NIS2 Directive therefore introduced a new European cyber crisis liaison organization network (EU-CyCLONe) to provide a rapid response group for large-scale incidents. It complements the already existing institutional framework for the provision of cybersecurity in the EU. It should be emphasized that the new regulation in the context of the competences of the CSIRT network also draws attention to the importance of regional and sectoral Security Operations Centres (Article 15(3)(n) NIS2), which will become an intermediate level in the organizational structure of national cybersecurity systems – between the important or essential entities and the national CSIRTs.

In current ENISA reports on the Internet threat landscape and security challenges for 2030 in the EU²⁴ indicated that one of the most visible and increasingly prevalent phenomena of this type is becoming that of Advanced Hybrid Threats/Advanced Persistent Threats, often referred to as State-nexus threat groups, whose activities are complex with a variety of attack methods (social engineering, phishing, malware, hacking, DoS), meticulously planned, and typically have multiple steps involved.²⁵

²⁴ “Identifying Emerging Cyber Security Threats and Challenges for 2030,” ENISA, Athens 2023, 17–8, accessed September 30, 2024, <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf>.

²⁵ Ping Chen, Lieven Desmet, and Christophe Huygens, “A Study on Advanced Persistent Threats,” in *Communications and Multimedia Security. Lecture Notes in Computer Science*, vol. 8735, eds. Bart De Decker and André Zúquete (Berlin: Springer, 2014), 63–72.

It is worth mentioning that Article 35 of the NIS2 Directive provides for *ex officio* notification to the supervisory authority (in Poland it is the President of the Personal Data Protection Office) of incidents which simultaneously have the characteristics of a personal data protection breach. Cooperation between institutions and exchange of information related to such incidents should make it possible to reduce duplicate, redundant formal activities and shorten the reaction time to changing circumstances of the case.

The procedures described in this part of the article are an extension of existing methods of cooperation between the actors of the EU cybersecurity system and are intended to better adapt them to the dynamics and complexity of incidents in this ICT area. This is closely related to the topic of preventing and counteracting the effects of cybercrime due to the fact that the occurrence of such incidents, excluding the spontaneous impact of natural factors, usually involves the realization of the elements of criminal acts by the attackers.

7. Conclusion

The specific nature of cybercrime, characterized by high dynamism and volatility, means that methods of preventing its occurrence and also countering its consequences require methods of reacting rapidly to the circumstances observed, involving parallel action and devoid of unjustified formalism.²⁶ It is also important to ensure a reliable and consistent chain of custody for incident evidence that creates a unified cause-and-effect sequence. Any delays in the information gathering and decision-making process may cause further damage and prevent full clarification of the facts.

The legal regulations analyzed in the article (GDPR and NIS2 Directive) and the accompanying technical standards in the area of information security (ISO 27000) will not, of course, replace criminal law protection instruments. However, through synergy, previously mentioned non-criminal law solutions can positively influence the effectiveness of the latter. Risk mitigation through the implementation of safeguards or the elimination of the vulnerabilities of protected resources themselves will reduce potential opportunities to commit cybercrimes, in particular those related

²⁶ Jerzy Kosiński, *Paradygmaty cyberprzestępczości* (Warsaw: Difin, 2015), 213.

to unlawful acquisition of information (cracking/hacking activity – Article 267 of the Penal Code), violation of data integrity in ICT systems (using malware, ransomware – Articles 268-269 of the Penal Code) or disruption of the operation of such systems (DoS/DDoS attacks – Article 269a of the Penal Code).

References

- Bacudio, Aileen, Xiaohong Yuan, Bill Chu, and Monique Jones. “An Overview of Penetration Testing.” *International Journal of Network Security and Its Applications* 6, no. 3 (2011): 19–38.
- von Bertalanffy, Ludwig. *General System Theory: Essays on Its Foundation and Development*. New York: George Braziller, 1968.
- Burdziak, Konrad. “Bezpośredniość zamachu, czyli kilka słów na temat obrony koniecznej w polskim prawie karnym.” *Przegląd Sądowy*, no. 1 (2018): 55–61.
- Chakraborty, Nilotpal. “Intrusion Detection System and Intrusion Prevention System: a Comparative Study.” *International Journal of Computing and Business Research* 4, no. 2 (2013): 1–8.
- Chen, Ping, Lieven Desmet, and Christophe Huygens. “A Study on Advanced Persistent Threats.” In *Communications and Multimedia Security. Lecture Notes in Computer Science*, vol. 8735, edited by Bart De Decker and André Zúquete, 63–72. Berlin: Springer, 2014.
- Echeverria, Aaron, Cristhian Cevallos, Ivan Ortiz-Garcés, and Roberto Andrade. “Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation.” *Applied Science* 11, no. 7 (2021): 3260.
- ENISA. “Identifying Emerging Cyber Security Threats and Challenges for 2030.” Athens, 2023. Accessed September 30, 2024. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf>.
- Filipkowski, Wojciech. “Przestępczość z użyciem komputerów i ich sieci.” In *Kryminologia. Stan i perspektywy rozwoju*, edited by Emil Pływaczewski, Sławomir Redo, Ewa M. Guzik-Makaruk, Katarzyna Laskowska, Wojciech Filipkowski, Ewa Glińska, Emilia Jurgielewicz-Delegacz, and Magdalena Perkowska, 511–34. Warsaw: Wolters Kluwer, 2019.
- ISO 31000 – Risk management – Guidelines. Geneva 2018.
- ISO/IEC 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva 2018.
- ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva 2022.

- ISO/IEC 27005 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva 2022.
- Kaczmarek, Andrzej, Monika Młotkiewicz, Agnieszka Łapińska, Agata Miłocha, and Michał Mazur. *Jak rozumieć podejście oparte na ryzyku według RODO?*. Warsaw: UODO, 2018. Accessed September 30, 2024. <https://uodo.gov.pl/pl/file/706>.
- Kennedy, David, Jim O’Gorman, Devon Kearns, Mati Aharoni, and Daniel Graham. *Metasploit. The Penetration Tester’s Guide*. San Francisco: No Starch Press, 2025.
- Kolouch, Jan, Daniel Tovarňák, Tomáš Plesník, Michal Javorník. “Cybersecurity: Notorious, but Often Misused and Confused Terms.” *Masaryk University Journal of Law and Technology* 17, no. 2 (2023): 281–305.
- Kosiński, Jerzy. *Paradygmaty cyberprzestępczości*. Warsaw: Difin, 2015.
- Lipowicz, Irena, Zygmunt Niewiadomski, Kazimierz Strzyczkowski, and Grażyna Szpor. *Prawo administracyjne. Część materialna*. Warsaw: LexisNexis, 2014.

