CYBERTAX: A NEW APPROACH TO CYBERSECURITY RISK MANAGEMENT

Prof. Serghei Ohrimenco, DSc.[1]
Valeriu Cernei[2]

Abstract: *In our modern world, it may seem that we have a complete understanding of threats, means of counteraction, risk management, and potential impact. However, reality turns out to be much more complex and less evident. The theory of risk management is constantly evolving and expanding, and this also applies to a new direction - risk management in cyberspace.*

This paper presents an analysis of the concept of „Cybertax" proposed by George K. Tsantes and James F. Ransome. The emergence and evolution of this concept are driven by the necessity to enhance the management of cyber security both in governmental and commercial organizations, as well as among individual users.

It should be recognized that „Cybertax" - is a measure of the effort and resources used to prove the current state of cybersecurity to others, primarily business partners, regulators, and auditors.

Keywords: *Cybersecurity, Cybertax, Cyberthreats, Risk, Management*
JEL: P41, D74, D89, H12, K24
DOI:

1. Introduction

Digital transformation encompasses virtually all types of business activities. Promoting cybersecurity as a part of digital transformation creates opportunities and gives rise to a number of challenges. Entrepreneurs are accelerating the processes of digitization to develop their businesses, expand their customer base, engage with suppliers using information technology, speed up decision-making, and more.

At the same time, cybersecurity has become a serious global issue (Sandhu, 2021). The number of cyberattacks worldwide has increased exponentially. While digital transformation makes business processes more efficient, the increasing cyberattacks create obstacles, threats, and serious risks. Cyberattacks are driven by political or financial interests and aim to gain access to private and confidential information, by using ransomware, stealing personal data, disrupting critical infrastructure, such as energy, water, telecommunications, transportation, healthcare, and more.

[1] osa@ase.md, Academy of Economic Studies of Moldova, Laboratory of Information Security, Chisinau, Moldova

[2] valeriu.cernei@bsd.md, Academy of Economic Studies of Moldova, Laboratory of Information Security, Chisinau, Moldova

2. Cybersecurity, Cyber risk – Concept, Definition and Models

Conceptually, cybersecurity brings together many specialists and their knowledge from various fields. This is primarily related to the problems that business owners solve in the process of operating information systems in both government and commercial domains. Additional contributions are made by changes in the landscape of cyber threats, which lead to significant damage and violations of principles such as confidentiality, integrity, availability, non-repudiation, and more. Ultimately, all of the above affect the cost of information processing, leading to an increase and eroding trust among suppliers and partners.

Here are several definitions characterizing this subject area:

„Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have on the organization.“ (Leirvik, 2022)

„Cybersecurity is a set of methods and practices for protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.“

In order to counter cyber threats, the scientific and practical community has developed and consistently implemented a number of specific concepts. These include intrusion prevention strategies that contribute to increased efficiency and reduced costs in security measures, the Zero Trust strategy, among others (Business, 2022), (Sandhu, 2021), (Cindy Green-Ortiz, 2023), (Das, 2023). Currently, the following defense methods have gained widespread use: IDS (Intrusion Detection Systems), traffic analysis, sandboxing, honeypots, big data analysis.

The issue of cybercrime is impossible to overlook, given its direct impact on the structure and expenses associated with maintaining a robust security posture. In today's world, cyber threats stand out as one of the most pressing global challenges. Effective cybersecurity management hinges on in-depth research that delves into the broader landscape of cybercrime while evaluating strategic and organizational facets related to cybersecurity (Kshetri, 2021). Within this context, it's noteworthy that this publication presents a compelling outlook for global cybersecurity expenditure, with projections indicating a surge to $133.8 billion by 2024, in stark contrast to the $3.5 billion recorded in 2004. This remarkable growth signifies a staggering increase of over 30-fold from the initial figure.

Some of the main directions in scientific and practical activities in this field are asset management, Business continuity management (BCM), Cybersecurity management, ICT readiness for business continuity (IRBC) or IT service continuity management (ITSCM), (Cybersecurity) Incident management, Information risk management (IRM), Information security management (ISM), Stakeholder and issue management, etc. (Kaschner, 2021).

It's also important to mention the Cyber Kill Chain model (CKC), which is a process-based model used by cybersecurity analysts to analyze APT (Advanced

Persistent Threat) attacks systematically. The CKC is a structured attack model in which the attacker progresses through the attack stages according to a plan. It helps analysts break down complex attacks into smaller, more manageable steps and enables defenders to develop countermeasures for each stage (Ankang Ju, 2020), (Kim, 2018),

3. CyberTax

The Genesis of CyberTax can be traced back to the works and proposals of George K. Tsantes and James F. Ransome. Their forward-thinking approach aimed at addressing the growing challenges of cybersecurity management in an increasingly digital world.

They recognized a critical gap in how cybersecurity was funded and managed. Traditionally, organizations and individuals invested substantial resources in cybersecurity to protect their digital assets. These investments encompassed a wide range of activities, including prevention, monitoring, remediation, and ongoing enhancements. However, there was no standardized or structured approach to incentivize these investments, and the true cost of cybersecurity often went unnoticed.

„Cybertax“ includes all the resources needed to ensure and validate cybersecurity governance. This includes prevention, monitoring, remediation, enhancements, and validation. It includes due diligence to select technology products and services that will improve cybersecurity. This includes the time and effort required to design, implement, and monitor secure business processes. It also includes the resources required to monitor the security of third-party vendors of products and services. The authors believe that the development of a new field will lead to the inevitable introduction of a „Cybertax.“ This requires interdisciplinary research into the nature of cybersecurity, a comprehensive analysis of factors affecting security processes, and the elimination of causes and conditions that negatively affect cybersecurity (George K.Tsantes, 2023).

It's worth mentioning another, earlier work by Luc Soete and Bas ter Weel, dedicated to Cybertax (Luc Soete, 1998). The forecast is made that in 30 years (the work was published in 1998), consumer activity on the Internet could account for more than 30% of total consumer activity, leading to a dilution of the national tax base. The main conclusion of this article is the introduction of a per-bit tax as a last resort. It is suggested that the idea of a tax on information, in terms of diluting the tax base in a rapidly changing society, deserves attention.

Let's consider the modern concept of Cybertax. It is based on The Seven C's Intro:

- Complexity—All aspects of complexity, including business, location, vendors, technology, and regulatory. Take, for example, laptop PCs. Limited complexity is a single laptop standard where extreme complexity is allowing any PC that can run the required business software. Obviously, it’s easier to design a cybersecurity program around a single PC standard than one designed to protect

nearly all PCs. The same is true of other business decisions that increase or limit business and technical complexity.

- Capability—The reasonable throughput that the cyber-security team can process. Capability is the measure of the organization's ability to address cybersecurity issues and responsibilities proactively and reactively. This is measured against internal policy goals as well as relative to peers. Capability factors include the following: Technology footprint, Ability of the cybersecurity team to effectively use the technology, Skills and industry knowledge of the cybersecurity team, Cybersecurity interaction with organization leadership.
- Competency—How effective the organization is in finding, fixing, and remediating cybersecurity events. This measures the effective execution of cybersecurity across the organization. Good cybersecurity can be measured, for example, in the following ways: Are we finding new issues and not repeating others? Are we finding issues sooner? Are we spending more time providing cybersecurity rather than proving it to others?
- Comparison—How does our organization compare to peers in cybersecurity. Although each organization must determine their own cybersecurity goals and capabilities, Cybertax Management it's often helpful to understand how one's organization compares to similar organizations. Comparison data delivers valuable reference information.
- Conceptualization—Modeling how business and technology decisions will impact the cybertax. Organizations can analyze and understand how changes in one area will impact the overall cybersecurity posture score. This method provides factors that can be adjusted to determine the impact of potential changes or improvements.
- Cost—All costs related to cybersecurity, including outside assessments and regulatory review and input. Organizations can understand the approximate cost of investments that could reduce complexity, improve capabilities, and increase data frequency to drive improved competency.
- Continuous—For the Seven C's to be effective, measures must be used frequently to spot negative trends early. Unlike annual assessments that are conducted at a specific point in time, this method relies on information that is frequently updated from daily to near real-time (NRT), so that it can more accurately communicate trends and velocity of change in key factors of cybersecurity risk. Frequent information updates also reduce the human bias found in traditional cybersecurity assessments.

There are many cybersecurity frameworks and assessments that are derived from the ISO 27001 standard.

4. Conclusion

In conclusion, CyberTax emerges as a crucial area of focus amid the digital transformation era. The increasing complexity of cybersecurity challenges, coupled with escalating cyber threats, impose development of comprehensive

strategies and allocation of resources. Organizations must continuously assess their cybersecurity posture, strive for competency in identifying and remediating security events, and compare themselves with peers to drive improvements. Moreover, the continuous monitoring of cybersecurity factors, along with their frequent updates, is essential to detect negative trends early and facilitate data-driven decision-making.

As organizations navigate the ever-evolving cybersecurity landscape, frameworks like ISO 27001 provide valuable guidance and support in their journey to enhance cybersecurity. The concept of CyberTax encapsulates the commitment to cybersecurity governance, emphasizing its role as a cornerstone of digital transformation and a safeguard against emerging threats in the interconnected digital age.

References:

Sandhu, Kamaljeet (2021). Handbook of Research on Advancing Cybersecurity for Digital Transformation. IGI Global. ISBN 9781799869764

Ryan Leirvik (2022). Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program. APress Media. ISBN 978-1-4842-7821-5 https://doi.org/10.1007/978-1-4842-7821-5

George Finney (2022). Project Zero Trust: A Story about a Strategy for Aligning Security and the Business. John Wiley & Sons. ISBN: 978-1-119-88486-6

Sandhu, Kamaljeet (2021). Handbook of Research on Advancing Cybersecurity for Digital Transformation. IGI Global. ISBN 9781799869764

Cindy Green-Ortiz, Brandon Fowler, David Houck, Hank Hensel, Patrick Lloyd, Andrew McDonald, Jason Frazier (2023). Zero Trust Architecture (Networking Technology: Security). Cisco Press. ISBN 978-0-13-789973-9

Ravindra Das (2023). The Zero Trust Framework: Threat Hunting & Quantum Mechanics. CRC Press. ISBN 978-1-032-49278-0

Cindy Green-Ortiz; Brandon Fowler; Jason Frazier; David Houck; Hank Hensel; Patrick Lloyd; Andrew McDonald (2023). Zero Trust Architecture. Cisco Press. ISBN 978-0-13-789973-9

Nir Kshetri (2021). Cybersecurity Management: An Organizational and Strategic Approach. University of Toronto Press. ISBN: 1487504969, 9781487504960

Holger Kaschner (2021). Cyber Crisis Management: The Practical Handbook on Crisis Management and Crisis Communication. Springer Nature. ISBN 978-3-658-35489-3 https://doi.org/10.1007/978-3-658-35489-3

Ankang Ju, Yuanbo Guo, Tao Li (2020). MCKC: A Modified Cyber Kill Chain Model for Cognitive Apts Analysis Within Enterprise Multimedia Network. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-020-09444-x

Kim, H., Kwon, H., & Kim, K. K. (2018). Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications. doi:10.1007/s11042-018-5897-5

George K.Tsantes, James F. Ransome (2023). Cybertax: Managing the Risks and Results. CRC Press. ISBN 089-1-032-42225-1

Luc Soete, Bas ter Weel (1998). Cybertax. Futures, Vol. 30, No. 9, pp. 853–871, 1998. Elsevier Science Ltd. https://doi.org/10.1016/S0016-3287(98)00089-5