CYBER THREATS MODELING: AN EMPIRICAL STUDY

Serghei Ohrimenco[1],
Dinara Orlova[2],
Valeriu Cernei[3]

Abstract: The immediacy of this study is determined by the need to fight back against the modern cyber threats that arise in the process of building a digital economy. The issues of countering various cyber threats in the activities of small and medium enterprises, firms stand to be a serious problem. Its relevance is constantly increasing. This is due to a number of objective reasons, the main of which are the following.

Firstly, the globalization of economic processes, which leads to a situation where the technical, software and information component of the Information System (IS) is the same in relation to all countries developed in terms of information.

Secondly, a significant change in the landscape of the IS threats themselves. It should be noted that the changes affected both quantitative and qualitative characteristics.

Malware, Network Scanning, Man in the Middle, Phishing, DNS Spoofing, Trojan Horses. These are just a few examples of cyber threats carried out against small and mid-sized businesses and government information systems every day.

The current condition of the information security system of governmental and commercial structures does not provide efficient resolving of up-to-date cybersecurity problems and creation of confident interaction between the critical infrastructure objects.

It should be assumed that there is a need to update the theoretical and methodological base and practical developments that can protect the rights and legitimate interests of the individual, business and the state from modern security threats and increase the level of security of our economy.

[1] Doctor of Economic Sciences, Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova, Chisinau, Moldova, e-mail: osa@ase.md, ORCID: 0000-0002-6734-4321

[2] Doctor of Economic Sciences, Professor, Department of Economics, Financial University under the Government of the Russian Federation, Moscow, Russia, e-mail: drorlova@fa.ru, ORCID: 0000-0002-2901-070X

[3] PhD student, Laboratory of Information Security, Academy of Economic Studies of Moldova, Chisinau, Moldova, e-mail: valeriu.cernei@bsd.md, ORCID: 0000-0003-3300-334X

The article logically combines the study of the modern landscape of cybersecurity threats, the construction of an empirical model of security threats (with the allocation of a monetization block), the demonstration of the results of processing statistical data characterizing the distribution of the frequency of occurrence of specific threats.

The paper aims to build an empirical model of cyber threats based on a study of huge number of relevant literature sources and statistical data.

Key words: empirical model, cyber threats, shadow digital economy.

JEL: E26, C8, O17, M15.

DOI: https://doi.org/10.58861/tae.bm.2023.3.06

Literature review

The authors conducted a study of special literature on the research topic within the time interval from 2019 to 2022, highlighting the following sections: Classification of cyber security threats, Special purpose cyber security threats, Security Development Lifecycle (SDL) threat modeling methodology.

1. Classification of cyber security threats

Erdal Ozkaya, Rafiqul Islam (Ozkaya & Islam, 2019) introduced a detailed description of the security threats associated with the operation of the Dark Net. In particular, such threats as Ransomware, Malware, Worms, Horses, Botnets and Zombies, DDoS Attack, Scareware, Social Network Attacks, Key Hitches are being explained. The dark net provides an almost ideal platform for cybercriminals to carry out their activities: Computer Fraud, Business Email Compromise, Data Breach, Email Account Compromise. A specific chapter is devoted to study Cybercriminal Activities in Dark Net, distinguishing Cybercrime and its categories, Cybercriminal activities through the Dark net, Data exfiltration, Monetization of cybercrime, Malware-as-a-service and money laundering.

Thomas A. Johnson, in the book “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare” (Jonson, 2015), suggests a short description of critical infrastructure, allots optimization models of Cyber Attacks influence on Critical Infrastructures. The questions of Cybersecurity Insurance (Cyber Resilience Program Policies, Cyber Liability, First-Party, and Third-Party Insurance) are studied. Cyber insurance is considered dependent on the following types of cyber liability:

- Unauthorized access to data;
- Disclosure of confidential data;

- Loss of data or digital assets;
- Introduction of malware, viruses, and worms;
- Ransomware or cyber extortion;
- Denial-of-service attacks;
- Advanced persistent threat attacks;
- Identity theft;
- Invasion of privacy lawsuits;
- Defamation from an employee's email;
- Failure of notification of breach.

The book "Cybersecurity Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics" by Yuri Diogenes and Erdal Ozkaya (Diogenes, 2018) labels and analyses the most complete list of cyber attacks and threats: Extortion attacks, Data manipulation attacks, IoT device attacks, Backdoors, Mobile device attacks, Hacking everyday devices, Hacking the cloud, Phishing, Exploiting a vulnerability, Zero-day, Fuzzing, Source code analysis, Types of zero-day exploits, Buffer overflows, Structured exception handler overwrites, Performing the steps to compromise a system, etc.

2. Special purpose cyber security threats

Special literature related to specific threats is available for experts. Brij B. Gupta and Amrita Dahiya (Gupta & Dahiya, 2021) thoroughly research the concept of DDoS. Topical issues of DDoS Attack are consistently considered. The second chapter of the book contains material describing the economic factors for cybersecurity. The authors highlight two subparagraphs 2.1.3 and 2.1.4 Vulnerability Trade and Cyber Insurance. The authors discuss the problem of public disclosure of information about vulnerabilities, arguments for and against. It is concluded that it is necessary to give preference to investing in the process of eliminating vulnerabilities and errors at the initial stage of software development. Cyber insurance processes are associated with an exponential increase in the economic costs associated with cybercrime. It is stated that cyber risk management is a practice that is used as long as the firm has assets to protect. Accordingly, this includes the identification of risks and threats, as well as the use of strategic measures and systematic approaches to ensure the security of information assets. A scheme for covering losses with the help of cyber insurance, as well as Cyber insurance cycle, has been proposed. It should be noted that this book

contains a very important chapter "Taxonomy of Economical Solutions" with a highlight of Cybersecurity Economics (Pricing Strategies, Challenges in Pricing Schemes).

The next important source is the book by Maxie Reynolds (Reynolds, 2021) with the intriguing title “The Art of Attack: Attacker Mindset for Security Professionals”. The author begins his book with the wonderful epigraph “Attackers don’t acknowledge people. They target them.” The author describes in detail the concept of Attacker Mindset (AM) and highlights two main states of attacker mindset: there's before the vulnerable information has been carved out and there's after. It's the application of the skills against the laws that makes the mindset:

• The first law of AMs states that you start with the end in mind, knowing your objective. This will allow you to use laws 2, 3, and 4 most effectively.

• Law 2 states that you gather, weaponize, and leverage information for the good of the objective. This is how you serve law 1.

• Law 3 says that you never break pretext. You must remain disguised as a threat at all times.

• Law 4 tells you that everything you do is for the benefit of the objective. The objective is the central point from which all moves an attacker makes hinge. You cannot diverge from the objective set out because of law 1.

The following threats are considered as attacker's tools: Phishing, Mass Phish, Spearphish, Whaling, Vishing, Smishing/Smshing, etc. Indicators of attack (IOA) and Indicators of Compromise-based are considered (IOC based). Indicators of Attack are actions or a series of actions that an attacker must execute in order to succeed. A spear phish is a good example in order to illustrate the idea of an IOA. An important addition is the availability of information about Nontechnical Measures (for example, Covid-19).

In general, the book allows you to plunge into the problems of evaluating the activities of violators from the standpoint of a systematic approach.

The authors of the next work (Gautam et al, 2021) devoted to the study of cyber defense mechanisms present two groups of threats, which can be conditionally called "classical" and "modern". The first group includes the following: Malware, Phishing, etc. This group also includes the modification Malware on Mobile Apps. The second group “Security Challenges in Modern Day” includes the following: Cloud Computing, Social Media, Smart Phones, GDPR, Attacks Based on ML and AI, Attacks against Cryptocurrencies and Blockchain Systems. Attention should be paid to the emergence of new areas

of interest, for example, Attacks Based on ML and AI, Cryptocurrencies and Blockchain Systems, etc.

The book by Emmanuel C. Ogu (Ogu, 2022) is devoted to practical cybersecurity considerations for healthcare professionals. Its distinctive feature is the consideration of not only the basics of cybersecurity, but also The Cybersecurity Threat Landscape for eHealth. Typically, attackers' actions include data breaches & leaks, espionage, and unavailability or failure of medical and healthcare IT systems/devices. The trail that leads towards these outcomes features:

• Threat Objectives such as reconnaissance/enumeration, digital/electronic interceptions, service disruptions, induced systems/device malfunction, erode security culture/protocols/operations, credential stuffing, and identity theft/digital impersonation;

• Methods, Strategies, or Approaches like spoofing (of emails, packets, location, addresses, protocol operations, websites, biometric & non-biometric identifiers, etc.), social engineering, advanced persistence (or, APTs), physical events and activities on site (including insider operations that could be either naive or maliciously intended), wardriving, man-in-the-middle (MITM), injection/poisoning, privilege escalation, transloading, shadowing digital activities, scavenging, hijacking, subversion/bypass of protocols and routines, and denial of service (DoS);

• Tools and Techniques that include malware (ransomware, trojans, viruses, spyware, rootkits, logic bombs, worms, and autorun scripts), data recovery software, phishing/vishing, scanners & trackers, piggybacking/tailgating, shoulder surfing, packet tracers, hidden tunnels in network protocols & services, cross-site scripting (XSS), SQL injection, signal jammers/interference generators, network sniffers & analyzers, keyloggers, smash & grab, bots, and botnets.

Timo Steffens' book “Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage” (Steffens, 2020), deals with the following issues: Phases of Attacks by APTs; attack infrastructure; geopolitical analysis; strategical aspects. Particularly interesting is the material on Methods of Intelligence Agencies (Attacker Perspective, Open-Source Intelligence, Human Intelligence, Hacking Back).

Another very interesting and useful book for scientific and practical work is the collective monograph “Cyber-Security Threats, Actors, and Dynamic Mitigation” edited by Nicholas Kolokotronis and Stavros Shiaeles (Kolokotronis, & Shiaeles, 2021). This book builds upon the fundamentals of computer and network security to provide advanced perspectives of cyber-

security. A team of authors describes a taxonomy of attackers and provides a detailed analysis of the available methodologies and frameworks to model and classify cyber-threats; threats (focusing on malware) targeting personal computers and information systems; focuses on cryptographic threats; addresses dealing with new (or possibly unknown) emerging attacks by means of problem of anomaly-based detection systems; deals with dynamic risk management; presents a classification of graphical security models and particular instances that have been proposed in the literature, discussing their pros and cons.

3. Security Development Lifecycle (SDL) threat modeling methodology

One of the important books in this section is by Lorenzo Magnani, Tommaso Bertolotti "Springer Handbook of Model-Based Science" (Magnani, & Bertolotti 2017). This book is a universal tool for professionals conducting research in security threat modeling. In particular, the authors present material that characterizes the following sections: The Ontology of Models, Models and Theories, Model and Representations, Models and Simulations, The Logic of Hypothetical Reasoning, Abduction and Models.

Research Methodology

The following research methods were applied during our study: grouping (clustering) method; balance method; medial allegation (mean-value method); index construction (index method), graphical approach and others. The MITRE ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE ATT&CK framework (MITRE ATT&CK, a guide for businesses in 2022, 2023) provides information in the following sections:

– Threat Identification, which involves identifying threat vectors and listing threat events;

– Attack Modelling, which involves mapping sequence of attack, describing tactics, techniques and procedures.

The useful threat information typically has the following characteristics:

Timely – information should be received in a timely manner as information that is outdated is useless to users; Relevant – information needs

to be relevant to the context of the users. For example, industrial control systems may have different priorities compared to financial institutions; and Actionable – information should be actionable for the correct group of users. Users must be able to react to information at the appropriate level, e.g. tactical or strategic level.

"Threat Modeling. Designing for Security" by Adam Shostack (Shostack, 2014) is yet another book used in our research that should be mentioned as some kind of Bible for Programming and IT security experts.

Analysis

Modeling is the creation of a model of an object of knowledge to study its properties and characteristics. A sufficiently large set of methods can be used to develop a threat model (Shevchenko et al., 2018), (Furterer, 2022), (Kneuper, 2018), (Modeling, 2021). Threat-modeling methods are used to create an abstraction of the system, profiles of potential attackers, including their goals and methods, a catalog of potential threats that may arise.

It should be borne in mind that the above models have, in addition to positive aspects, disadvantages.

Summarizing the overview of modern models, it is necessary to identify one important research detail. The problem is that the STRIDE method allows you to simulate not threats, but computer attacks. These terms are undoubtedly related, but still they should not be confused. Threats are a broader concept than attacks, and at the same time each threat can be implemented by many different attacks. Comprehensive measures to combat threats are of a preventive nature. Threat coverage provides protection against a large layer of attacks. Therefore, the formation of a threat model is of paramount importance. Therefore, in the future, in this work, the category "threat" will be used as the most representative and comprehensive.

It is necessary to pay attention to one more important, according to the authors, circumstance. The threat model is always informal in nature, and, as a result, there is no strictly unambiguous methodology for compiling it. As a result, situations are possible when information security specialists are forced to draw up special regulatory and methodological documents, since existing models do not satisfy all features of the work of a particular company. The creation, and then processing of a general model for a particular case cannot always be correctly carried out for various reasons (whether it is insufficient professionalism of an employee, or a banal lack of time). Possible redundancy in the final model will not cause harm, while gaps may leave "holes" in the security system.

Discussion

Our model is based on the methods of attribution that are used throughout the InfoSec community.

Phase 1: Collect data

Phase 2: Clustering

Phase 3: State-sponsored versus criminal activity

Phase 4: Attribution to a country of origin

Phase 5: Attribution to organizations and persons

Phase 6: Assessing confidence and communicating hypotheses.

Fig. 1 presents the general overview of the suggested model.

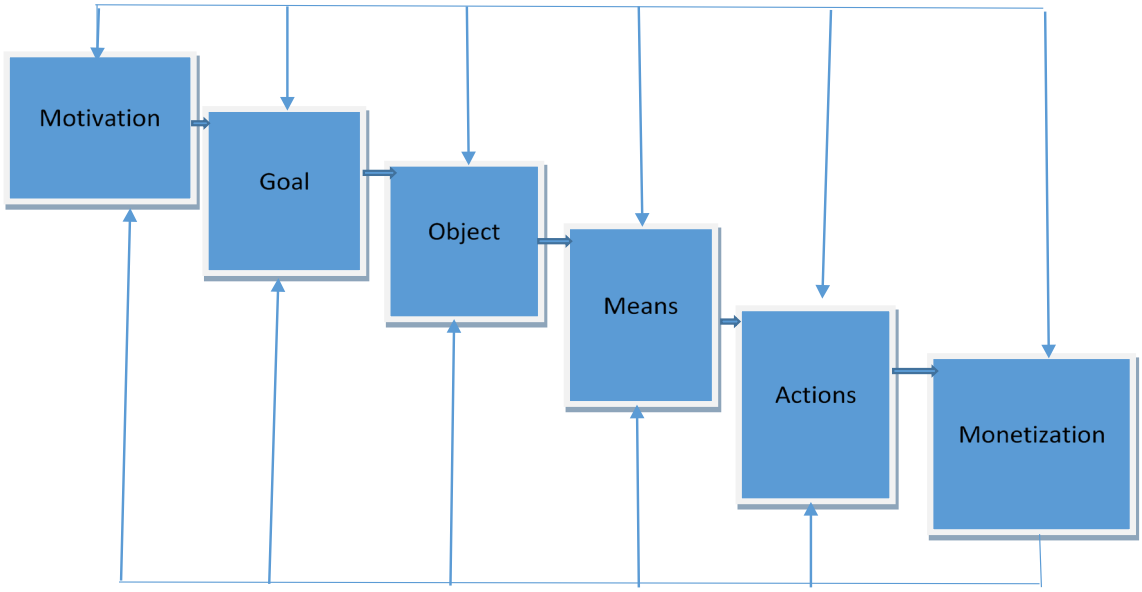


Fig.1 Empirical security threats model

Let's describes the key elements of the model.

Personality and external environment

The model is based on information about the individual and the external environment. Personal information is decisive and characterizes such aspects as equipment, technical competence, knowledge, etc. In (Fuentes, 2020), (Kropotov et al., 2020) the main categories of attackers involved in the creation of software abuses are identified: organized crime (groups involved in cybercrime and having the capabilities and skills to conduct targeted attacks on IS end users); scammers; malicious insiders; hacktivists. The external environment characterizes, first of all, the state of legislative support in general and, in the information sphere, in particular, judicial practice, etc. There are strong presumptions to believe that interest in illegal activities in

the digital economy will grow rapidly and specialists should be prepared to prevent serious consequences.

In addition, the starting point for building our model should be to accept and use the concept of the "shadow digital economy" (SDE). SDE should be understood as individual or collective illegal activities related to the design, production, distribution, support and use of information and communication technology components. In other words, these are criminal products, services and processes based on IT or using IT.

There are three types of cybercriminals that functionally correspond to three types of personal data thieves (Ohrimenco et al., 2021), (Ohrimenco & Borta, 2021):

- criminals motivated by money and performing their actions for the sake of financial reward;
- state-sponsored and terrorist organizations-sponsored attackers to damage infrastructure systems;
- simply thrill-seekers who find satisfaction in being able to intervene in the daily lives of individuals and organizations.

Motivation

The following motives should be singled out as the main ones: personal; corporate; obtaining economic benefits; narcissism; blackmail; ideology, etc. It should be noted that recently the emphasis has shifted towards economic gain.

Goal

A set of indicators should be considered as a goal, including such as personal data, corporate data, global data, suppression of competitive advantages, self-assertion, invasion of social networks, etc.

Object

The objects shall include the company and its resources (information, technical, software, personnel). Additionally, a product or service can also act as an object. The minimum list of objects of influence may include the following: information (data), software and hardware for processing and storing information, software, computer media, telecommunications equipment, information security tools, etc.

Means

It should be noted that the main means of influencing company's resources are software developments and related technologies (Steffens, 2020), (Lenhard, 2021).

To evaluate the means used one needs to utilize the MITER ATT@CK threat modeling methodology. The new methodology stipulates implementation of the following stages: identification of negative impacts, identification of impact objects, assessment of threats feasibility, with additional analysis of violators and potential attack scenarios. This technique depicts the commonly available intruder's tactics, procedures and methods of intruders in the form of a matrix based on real observations.

Actions

The theft of information for further illegal activities are to be considered the main actions in the Empirical security threats model. Intruders' actions chase the designed threats (Peiris et al., 2022), (Rai, & Mandoria, 2019), (Shiaeles, & Stavros 2021), (Benson, & Calaney, 2021).

The authors set the task to evaluate the frequency of use of specific threats, based on reports from well-known companies specializing in information security. For these purposes, 13 Internet sources were selected, analyzed and processed (the list of sources is given below Table. 1).

The most ominous information security threats were evaluated and set in Table 1. Numbers in the table correspond to certain sources outlined below Table 1.

Table 1.
List of ominous threats

Threats	1	2	3	4	5	6	7	8	9	10	11	12	13
DoS and DDoS Attacks	+	+	+	+	+	+	+	+	+	+	+	+	+
MITM Attacks	+	+	+	+	+		+	+	+	+	+	+	+
Phishing Attacks	+		+		+	+	+	+	+	+	+	+	+
Whale-phishing Attacks													+
Spear-phishing Attacks				+									+
Ransomware	+					+					+		+
Password Attack				+	+		+	+	+	+	+	+	+
SQL Injection Attack		+	+	+	+		+	+	+	+	+	+	+
URL Interpretation													+
DNS Spoofing													+
Session Hijacking													+
Brute force attack													+
Web Attacks													+
Insider Threats						+			+				+

Trojan Horses													+
Drive-by Attacks				+	+			+		+	+		
XSS Attacks			+	+	+		+	+		+	+	+	+
Eavesdropping Attacks				+	+					+		+	+
Birthday Attack				+	+					+	+		+
Malware Attack	+	+	+	+	+		+	+	+	+	+	+	+
Data Leaks	+												
Social Engineering Attacks		+											
Supply Chain Attacks		+											
Zero-Day Exploit			+				+	+	+			+	
DNS Tunneling			+								+	+	
Credential Reuse			+					+					
Exploit Kits						+							
Drive-by Attack			+			+						+	+
Viruses and Worms						+							
Botnets						+							
Advanced persistent threat attacks						+							
Malvertising						+							
Rootkits							+						
Internet of Things (IoT) Attacks							+				+	+	
Cryptojacking									+		+	+	
Watering Hole Attack									+				
Malware as a Service (MaaS)											+		
Business Email Compromise (BEC)												+	
AI-Powered Attacks												+	

1. The Most Common Types of Cyber Attacks in 2021. https://10guards.com/fr/articles/the-most-common-types-of-cyber-attacks-in-2021/

2. Cyber Security Threats. https://www.imperva.com/learn/application-security/cyber-security-threats/

3. 10 Most Common Types of Cyber-Attacks and Tips to Prevent Them. https://www.exai.com/blog/types-of-cyber-attacks

4. Top 10: Most Common Types of Cyber Attacks. https://secuvy.ai/blog/top-10-most-common-types-of-cyber-attacks/
5. Top 10 Most Common Types of Cyber Attacks. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
6. Top 10 types of information security threats for IT teams. https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams
7. Elizabeth Fichtner (2022). Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks. https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks
8. Top 10 Most Common Types of Cyber Attacks. https://www.testbytes.net/blog/types-of-cyber-attacks/
9. 10 Types of Cyber Attacks You Should Be Aware in 2021. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
10. Top 10 Most Common Types of Cyber Attacks https://itchronicles.com/information-security/top-10-most-common-types-of-cyber-attacks/
11. The 14 Most Common Cyber Attacks https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/
12. The 15 Most Common Types of Cyber Attacks. https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/
13. Types of Cyber Attacks. Top 20 Most Common Types of Cyber Attacks. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

The results of data processing using standard statistics tools are illustrated as follows (Table 2, Fig.2).

Table 2.
Threat Average Frequency Distribution

	Interval	*Frequency*	*Integral %*	*Interval*	*Frequency*	*Integral%*
1	0.076923	20	50.00%	0.076923	20	50.00%
2	0.230769	6	65.00%	0.384615	7	67.50%
3	0.384615	7	82.50%	0.230769	6	82.50%
4	0.538462	0	82.50%	0.846154	3	90.00%
5	0.692308	2	87.50%	0.692308	2	95.00%
6	0.846154	2	92.50%	0.846154	2	100.00%
7	0.846154	3	100.00%	0.538462	0	100.00%
		40				

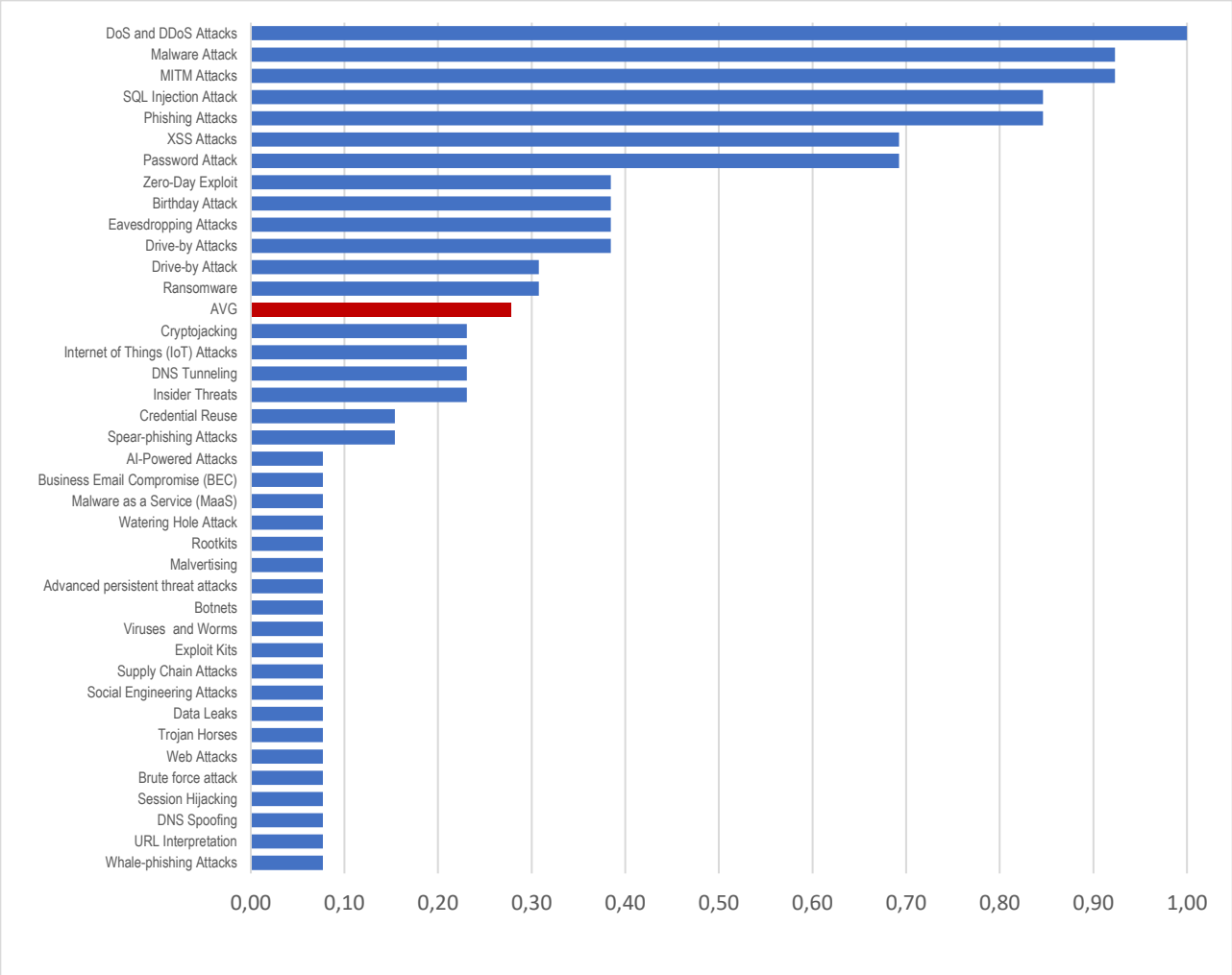


Figure 2. Threats frequency occurring distribution

The obtained statistical and graphical results indicate two interrelated groups of cybersecurity threats. The first group includes threats with a high frequency of occurrence (for example, DDoS, SQL Injection, etc.). This group includes "classic" and well-known threats that are currently widely used by violators.

The second group contains a list of threats that are significantly inferior in frequency of use (from 0.30 to 1.00 for the first part, from 0.10 to 0.25 for the second part). But in the second group there are threats that can be called "conditionally promising", which are characterized by a low frequency of occurrence, but their use is gaining momentum. These are, first of all, Business Email Compromise (BEC), Internet of Things (IoT) Attacks, Software Supply Chain Attacks, Malware as a Services (MaaS) and others. This indicates the need for constant attention to new threats, the formation of an up-to-date matrix of values and recalculation of the frequency of

occurrence. We consider it necessary to note the possibility of constructing a dynamic empirical model based on new statistical data.

Monetization

This is the final block of the presented empirical model. It is not sufficiently developed despite the significant number of publications (Pavlakis, 2022), (Clay, 2022). For this block, it is necessary to study scenarios for transformation of threats into finances, including money laundering (De Sanctis, 2013).

For example, the development of scenarios for designing software abuse (ransomware) and software tools for capturing and forming a botnet based on a certain company, as well as the possible cost of renting a part of the botnet for customers. At the same time, this block should contain extended data on the costs of obtaining benefits (profits).

Data processing according to the proposed model is performed in the following sequence:

1. Within each block, the corresponding evaluation indicators are selected.
2. For each indicator, determine the rating scale (for example, from 0 to 4, from 0 to 9 or from 0 to 99).
3. Expert assessments determine the number of points scored characterizing the level of danger of a particular threat.

Conclusion

It should be noted that the presented material does not cover all the problems of building an empirical model in the era of digital society transformation. It seems necessary to continue these studies towards creation of assessment indicators set, expanding the list of threats, and construction of a suitable scientific platform. Interest in the problems of work related to information security is objectively increasing and requires a search for answers to unresolved up-to-date issues. In this regard, the authors propose to carry out the following tasks.

1. Expand the composition and structure of existing threats, highlighting the main areas (for example, ransomware, threats to mobile systems, etc.).
2. Supplement the nomenclature of performance indicators, link it with existing methods, databases, tactics and MITER techniques.
3. Enlarge threats estimating scales.

4. Develop a testing ground for working out the tasks of assessing existing threats, as well as prepare a logical apparatus for assessing the attractiveness of threats to develop means and methods of counteraction in the context of the use of artificial intelligence and machine learning.

References

Benson, V., & Calaney, J.M. (2021). *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier Inc. ISBN: 978-0-12-816203-3

Clay, J. (2022). Hacking the Crypto-Monetized Web. Available online: https://www.trendmicro.com/en_za/research/22/f/hacking-the-crypto-monetized-web.html

De Sanctis, F. (2013). *Money Laundering Through Art: A Criminal Justice Perspective*. Springer. ISBN 978-3-319-00173-9 DOI 10.1007/978-3-319-00173-9

Diogenes, Yu., & Ozkaya, E. (2018). *Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing Ltd. ISBN 978-1-78847-529-7

Furterer, S. (2022). *Systems Engineering: Holistic Life Cycle Architecture, Modeling and Design with Real-World Applications. Taylor & Francis Group*, LLC. ISBN: 978-1-003-08125-8 DOI: 10.1201/9781003081258

GUIDE TO CYBER THREAT MODELLING. FEBRUARY 2021. Available online: https://www.csa.gov.sg/media/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling---feb-2021.pdf

Gupta, B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges, and Countermeasures*. Taylor & Francis Group, LLC. ISBN: 9781003107354

Johnson, T. (2015). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* CRC Press Taylor & Francis Group. ISBN 978-1-4822-3923-2

Kneuper, R. (2018). *Software Processes and Life Cycle Models. An Introduction to Modelling, Using and Managing Agile, Plan-Driven and Hybrid Processes*. Springer Nature Switzerland AG. ISBN 978-3-319-98845-0 doi.org/10.1007/978-3-319-98845-0

Kolokotronis, N., & Shiaeles, S. (ed.) (2021). *Cyber-Security Threats, Actors, and Dynamic Mitigation.* CRC Press. ISBN 978-1-003-00614-5

Kumar, G., Saini, D., & Cuong, N. (2021). *Cyber Defense Mechanisms: Security, Privacy, and Challenges*. Taylor & Francis Group, LLC. ISBN: 978-0-367-81643-8

Lenhard, T. (2021). *Data Security: Technical and Organizational Protection Measures against Data Loss and Computer Crime*. Springer. ISBN 978-3-658-35494-7 https://doi.org/10.1007/978-3-658-35494-7

Magnani, L., & Bertolotti, T. (Eds.) (2017). *Springer Handbook of Model-Based Science. Springer International Publishing AG*. ISBN: 978-3-319-30526-4 DOI 10.1007/978-3-319-30526-4

MITRE ATT&CK, a guide for businesses in 2022. Available online: https://www.computerweekly.com/ehandbook/MITRE-ATTCK-a-guide-for-businesses-in-2022

Ogu, E. (2022). *Cybersecurity for eHealth. A Simplified Guide to Practical Cybersecurity for Non-Technical Healthcare Stakeholders & Practitioners*. Taylor & Francis Group, LLC. ISBN: 978-1-003-25441-6 DOI: 10.1201/9781003254416

Ohrimenco, S., Borta, G., & Cernei, V., "Estimation of the Key Segments of the Cyber Crime Economics," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology* (PIC S&T), 2021, pp. 103-107, doi: 10.1109/PICST54195.2021.9772165.

Ohrimenco, S. & Borta, G., 2021. The nature of shadow digital economics. *MEST Journal*, 15 January, 9(1), pp. 146-156. DOI 10.12709/mest.09.09.01.17

Ozkaya, E., & Islam, R. (2019). *Inside the Dark Web*. CRC Press Taylor & Francis Group. IBSN 978-0-367-23622-9

Pavlakis, D. (2022). Cybersecurity in Manufacturing: Top 5 Strategies To Monetize Industrial Security. Available online: https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/monetize-iot-security-in-industrial-manufacturing/

Peiris, C., Pillai, B., & Kudrati, A. (2022). *Threat Hunting in the Cloud*. John Wiley & Sons, Inc. ISBN: 978-1- 119-80410-9

Rai, M., & Mandoria, H. (2019). A study on Cyber Crimes, Cyber Criminals and Major Security Breaches. *International Research Journal of Engineering and Technology (IRJET)*. Volume: 06 Issue: 07 | July 2019. P. 233-240. ISSN: 2395-0056

Reynolds, M. (2021). *The Art of Attack: Attacker Mindset for Security Professionals*. John Wiley & Sons, Inc. ISBN: 978-1-119-80547-2

Shevchenko, N. Threat Modeling: 12 Available Methods. Available online: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

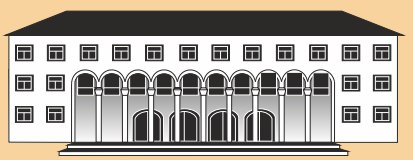
Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T., & Woody, C. Threat modeling: a summary of available methods. Available online: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Shostack A. (2014). Threat Modeling. Designing for Security. Available online: https://shostack.org/books/threat-modeling-book

Steffens, T. (2020). *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Springer-Verlag GmbH. ISBN 978-3-662-61313-9 https://doi.org/10.1007/978-3-662-61313-9

ISSN 0861 - 6604
ISSN 2534 - 8396

BUSINESS management



PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

3/2023

BUSINESS management 3/2023

The printing of the issue 3-2023 is funded with a grand from the Scientific Research Fund, Contract KP-06-NP4/75 /16.12.2022 by the competition "Bulgarian Scientific Periodicals - 2023".

Submitted for publishinq on 21.09.2023, published on 28.09.2023,
format 70x100/16, total print 80

BUSINESS management

D. A. Tsenov Academy of Economics, Svishtov

Year XXXIII * Book 3, 2023

CONTENTS