https://doi.org/10.52326/ic-ecco.2022/SEC.01

A Differentiated Beneficiary Cybersecurity Approach

Ion Bolun [1], ORCID ID: 0000-0003-1961-7310
Svetlana Cojocaru [1], ORCID ID: 0000-0002-1187-4294
[1] Technical University of Moldova; 168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova;
ion.bolun@isa.utm.md, https://utm.md/

***Abstract*. The considerable losses caused by the low level of infospace's cybersecurity and the limited financial resources available imply the need to found effective ways to improve the implementation of measures counteracting cyber-attacks. First, some aspects regarding the situation in the field are characterized, including: industries most targeted by cyber-attacks, common types of cyber-attacks, industries' readiness to counteract cyber-attacks, and causes of cybersecurity breaches. Reducing the costs with cyber-securing the beneficiaries may be achieved by typifying the solutions. For this purpose, criteria are selected and categories of beneficiaries are defined. Then the necessary actions for the differentiated cybersecurity (by categories) of beneficiaries are formulated.**

Keywords: cyber-attack; cybersecurity breache; criteria; cybercrime costs; categories of beneficiaries.

I. Introduction [1]

Information has always been, is and will be a strategic resource: "Who owns the information - controls the situation". This motivates intruders to obtain illegal access to informatics (IT) resources and to operate for their own benefit with the owners' information. In such conditions, the owners of informatics resources are forced to take measures to counteract such actions.

The development and upward use of informatics means by businesses, organizations, institutions, and the population, especially of the Internet, has facilitated obtaining new information and operating with it. According to report [1], the total global data storage in the world is projected to exceed 200 zettabytes ($200x10^{21}$) by 2025. Worldwide there will be 29.3 billion networked devices by 2023, that is 3.6 networked devices per capita [2]. At 30 June 2022 they were 5.47 billion Internet users in the World [3] and IP traffic has reached an annual run rate of 2.3 zettabytes in 2020 [4].

But with the facilitation of obtaining new information and operating with it, the problem of cybersecurity in all areas of human activity has become more acute. From both sides (intruders – owners), efforts are being made and resources are being spent (human, financial, etc.) increasingly.

According to Cybersecurity Ventures, cybercrime will cost the world in excess of $7 trillion in 2022 and $10.5 trillion in 2025 [4], that is approx. 8.5% of global GDP of $129.7 trillion [5]. Cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion (cumulatively) for the five-year period from 2021 to 2025, including $459 billion in 2025 [4]. For example, in august 2021 was announced that Microsoft will invest $20 billion to advance the security solutions over the next 5 years and Google will invest $10 billion over the next five years in cybersecurity [6].

So, both the global losses caused by the low cybersecurity of infospace and the costs of securing it are considerable. Obviously, costs reduction at a high quality of cybersecurity is possible by typifying the solutions - aspects that will be partially addressed in this article. But, first, some aspects regarding the situation in the field will be systematized.

II. Some Cybersecurity Aspects

A. *Industries Most Targeted by Cyber-Attacks*

According to [8], to types of businesses or organizations most targeted (vulnerable) by cyber-attacks refer:

- **Banks and financial institutions** (credit card information, bank account information, and personal customer or client data);
- **Healthcare institutions** (repositories for health records, clinical research data, and patient records such as social security numbers, billing information, etc.);

[1] Research is supported by the National Agency for Research and Development of the Republic of Moldova, project 20.80009.5007.26.

- **Corporations** (product concepts, intellectual property, marketing strategies, client and employee databases, contract deals, client pitches, etc.);
- **Higher education** (information on enrollment data, academic research, financial records, and personally identifiable information like names, addresses, and billing info).

Also, at state level they are distinguished critical cybersecurity infrastructures, which incapacitation would have a debilitating effect on overall security, national economic security, national public health or safety. For example, in United States they are defined 16 critical infrastructure sectors, including: Communications, Critical Manufacturing, Energy, Financial Services, Government Facilities, Transportation Systems, and others [9].

Based on 2647 separate interviews conducted by Ponemon Institute in 355 companies in eleven countries, approx. 68 percent of business leaders feel their cybersecurity risks are increasing [10]. Cyber-attacks on all businesses, but particularly small to medium sized businesses (SMBs), are becoming more frequent - more than half of all cyber-attacks [11].

According to study [10], 43% of cyber-attacks are aimed at small businesses. This situation is caused to some extent by the fact that such businesses are not always aware of the degree of related risks, respectively they do not make the necessary cybersecuring efforts; but also because they have fewer resources (human, financial, etc.) that could be directed towards ensuring adequate cybersecurity.

B. Most Common Types of Cyber-Attacks

The World Economic Forum Global Cybersecurity Outlook 2022 report [12] surveyed 120 global cyber leaders from 20 countries on their greatest concerns when it comes to cyber threats. They were identified that Ransomware attacks are number one, followed by Social-engineering attacks and Malicious insider (employees and contractors inside the organization) activity.

According to Ponemon Institute's report [13], most common types of attacks on small businesses include: Phishing - 57%, Compromised/Stolen Devices - 33%, and Credential Theft - 30%. No matter of the size of businesses, the most common types of cyber-attacks are considered:

- according to Krontech [14] - Malware, Ransomware, Phishing, DoS (Denial of Service) and DDoS (Distributed DoS), Man in the Middle (MITM), Credential Stuffing, Password Attacks, IoT-Based Attacks, Cross-Site Scripting (XSS), and SQL Injections;
- according to CrowdStrike [15] - Ransomware, Malware, DoS and DDoS, Phishing, MITM, XSS, SQL Injections, DNS Tunneling, Password Attacks, Birthday Attacks, Drive By Attacks, Cryptojacking, and IoT-Based Attacks;
- according to Fortinet [16] - DoS and DDoS Attacks, MITM, Phishing, Ransomware, Password Attacks, SQL Injections, URL Interpretation, DNS Spoofing, Session Hijacking, Brute force attacks, Web Attacks, Insider Threats, Trojan Horses, Drive-by Attacks, XSS, Eavesdropping Attacks, Birthday Attacks, and Malware;
- according to Cisco [17] - Malware, Phishing, MITM, DoS and DDoS, SQL injections, Zero-day exploit, and DNS Tunneling.
- according to Varonis [18]: Ransomware, Malware, Phishing, and DoS.

One can observe that there are many common types of cyber-attacks in these estimations, including: Malware, Ransomware, Phishing, DoS and DDoS, MITM, Credential Stuffing/Password Attacks, IoT-Based Attacks, XSS, and SQL Injections.

C. Industries' Readiness to Counteract Cyber-Attacks

Organized cybercrime entities are joining forces, and their likelihood of detection and prosecution is estimated to be as low as 0.05 percent in the U.S., according to the World Economic Forum's report [25]. Only 14% of small businesses under cyber-attacks are prepared to defend themselves [10].

As a result of a survey were found [12] that 59 percent of all respondents would find it challenging to respond to a cybersecurity incident due to the shortage of skills within their team. About 46 percent of Cisco survey [26] respondents feel they are unable to effectively protect their data today. At the same time, according to the Cisco report [27] based on a survey of almost 500 SMBs (250-499 employees), less than 1 percent of SMB do not have anyone dedicated to security; 72 percent have employees dedicated to threat hunting; 56 percent have a daily or weekly patch routine; and an impressive 86 percent have clear metrics for assessing the effectiveness of their security.

D. Causes of Most Cybersecurity Breaches

Of course, cybersecurity breaches are caused by cyber-attacks. At the same time, a considerable part of these are also caused by unsuccessful actions of the owners of informatics resources, including:

- human errors - about 95 percent [19];
- Weak passwords, Application vulnerabilities, Back doors, Social engineering, Improper permission management, User errors, Insider threats, and Physical threats [20];

- Weak and stolen credentials, Back doors, Application vulnerabilities, Social engineering, Too many permissions, Insider threats, Physical attacks, Improper configuration, User errors [21];
- Weak and stolen credentials, Application vulnerabilities, and Insider errors [22];
- Human errors, Physical Theft/Loss of Devices, Stolen/Weak credentials, and Application/OS vulnerabilities [23].

By many of these estimations, such factors that cause cyber security breaches are common as: User/Human errors, Weak and stolen credentials, Application vulnerabilities, Improper permission management; Insider threats, and Physical threats.

It should also be mentioned that according to [24] mobile devices account for more than 60 percent of digital frauds.

III. Organization of Works to Cybersecuring the Beneficiaries

There are theoretical results and relatively effective practical means of cybersecurity in the world. They constitute a strong support for the determination of cybersecurity policies and means of beneficiaries. Under conditions of an acute shortage of financial resources, characteristic for the Republic of Moldova, it is opportune to typify related solutions by categories of beneficiaries with their subsequent adaptation to implementation.

For this purpose, it is necessary, first of all, to define the criteria and categorize (with the respective characterization) the beneficiaries of cybersecurity actions and measures. As beneficiaries, it is appropriate to examine the enterprises/organizations/institutions [28], hereafter "***organizations***", but also the ***population***. In case of population, the use of informatics means by persons outside the organizations is considered. At the same time, the organizations and, also, individuals can differ considerably from the point of view of cybersecurity needs. Therefore, in order to define the categories of beneficiaries in question, it is necessary to establish additional criteria.

The Center for Internet Security in [29] proposes the implementation of cybersecurity controls, depending on the scale of organizations (the ***number of employees***):

- small (up to 10 employees)
- medium;
- large.

In [28], when estimating the degree of cybersecurity readiness, they were distinguished five categories of organizations by the number of employees:

- up to 10 inclusive;
- 11-50;
- 51-100;
- 101-500;
- over 500.

At the same time, according to [8] because of the nature of their business, some industries are more targeted by cyber-attacks than others. Therefore, it is opportune to differentiate the beneficiaries also by the ***degree of cybersecurity*** actions and measures needed. For the beginning, it will used the latter of the nominated above classifications of organizations by the number of employees. Of course, as a result of additional research, it may be modified. Also, they will be distinguished the following four types of degree of cybersecurity (see Table 1):

- high;
- enhanced;
- medium;
- ordinary.

TABLE 1. CATEGORIES OF ORGANIZATIONS-BENEFICIARIES (17)

Degree of cybersecurity	Number of employees				
	< 11	11÷50	51÷100	101÷500	> 500
High cybersecurity	-	-	+	+	+
Enhanced cybersecurity	-	+	+	+	+
Medium cybersecurity	+	+	+	+	+
Ordinary cybersecurity	+	+	+	+	+

With refer to the population, it is also appropriate to use as criteria the ***person's age*** and for adults – the ***social status***: employed or unemployed. Employees, even outside of the work place, sometimes operate with work information using informatics means; this imposes higher requirements of cybersecurity to the respective activities compared to the ones to those of unemployed persons. Thus, for the population it is proposed to use the following five categories:

1. Children (up to and including 11 years old).
2. Teenagers (12÷17 years old).
3. Adults (18+ years old) employed - enhanced cybersecurity.
4. Adults (18+ years old) employed - medium cybersecurity.
5. Adults (18+ years old) - ordinary cybersecurity.

Knowing the categories of beneficiaries, they are also necessary to:

a) identify and systemize the dangers, vulnerabilities and needs regarding the cybersecurity of beneficiaries (by categories);
b) define the priorities and stage the measures and actions for cybersecuring the beneficiaries, taking into account the approach [30];
c) systemize the cybersecurity means to be used, taking into account the priorities (b);
d) set up the models of cybersecuring the beneficiaries (by categories);

e) define the set of criteria characterizing the degree of cybersecurity provided by models (d);
f) explore and characterize the system of models (d);
g) implement step by step the models (d) in practice, taking into account the results obtained according to items (e) and (f).

IV. Conclusions

The systematization of major aspects of infospace cybersecurity in the world allows the formation of a clearer vision regarding the state of affairs in the field. Losses caused by cyber-attacks and the costs of counter-acting them are considerable. In order to reduce costs and implement as successfully as possible, it is opportune the differentiated cybersecuring (by categories) of enterprises/organizations/institutions and the population, using the typification of respective solutions with rigorous adaptations to their implementation in practice. Based on certain criteria, the categories of beneficiaries are defined. Also, the necessary actions and measures for the differentiated cybersecurity (by categories) of beneficiaries are broadly formulated.

References

[1] *The 2020 Data Attack Surface Report*. Arcserve, 2020. https://goto.storagecraft.com/rs/431-WBH-895/images/The%2020 20%20Data%20Attack%20Surface%20Report%20_%20Arcserve.pdf (accessed 14.08.2022).

[2] *Cisco Annual Internet Report (2018–2023*). https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf (accessed 10.08.2022).

[3] *Internet World Stats*. https://www.internetworldstats.com/stats.htm (accessed 10.08.2022).

[4] S. Morgan. *Boardroom Cybersecurity 2022 Report*. Cybersecurity Ventures, 2022.

[5] *World Economic Outlook: War Sets Back the Global Recovery*. International Monetary Fund, April 2022.

[6] C. Mihalcik, R. Nieva. *Google, Amazon, Microsoft unveil massive cybersecurity initiatives after White House meeting*. CNET, Aug. 25, 2021, https://www.cnet.com/news/privacy/apple-google-amazon-ceos-head-to-white-house-for-cybersecurity-meeting/ (accessed 28.08.2022).

[7] *These are the biggest global risks*. World Economic Forum, Jan. 19, 2019. https://www.weforum.org/agenda/2019/01/biggest-global-risks-facing-our-world/ (accessed 23.07.2022).

[8] *2022 Must-Know Cyber Attack Statistics and Trends*. MBROKER, August 16, 2022. https://www.embroker.com/blog/cyber-attack-statistics/ (accessed 26.08.2022).

[9] *Critical infrastructure sectors*. USA Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/critical-infrastructure-sectors (accessed 28.08.2022).

[10] K. Bissell, R. LaSalle, P. DalCin. *Ninth Annual Cost of Cybercrime Study*. Ponemon Institute, March 6, 2019. – pp. 42.

[11] R. Johnson. “60 Percent of Small Companies Close Within 6 Months of Being Hacked”. *Cybercrime Magazin*, Jan. 2, 2019.

[12] A. Pipikaite et al. *Global Cybersecurity Outlook 2022*. World Economic Forum, January 2022. - 35 p.

[13] *Cybersecurity in the Remote Work Er*a. Ponemon Institute, October 2020. - 63 p.

[14] *The Most Common Types of Cyber Attacks in 2021*. Krontech, Jan 04, 2022. https://krontech.com/the-most-common-types-of-cyber-attacks-in-2021 (accessed 16.08.2022).

[15] *The 14 most common cyber attacks*. Krowdstrike, Sept. 2021. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/ (accessed 16.08.2022).

[16] *Types of Cyber Attacks*. Fortinet. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (acc. 12.08.2022).

[17] *What Are the Most Common Cyberattacks*? Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (accessed 19.07.2022).

[18] Sobers, R. *89 Must-Know Data Breach Statistics*. Varonis, May 20, 2022, https://www.varonis.com/blog/data-breach-statistics (accessed 10.08.2022).

[19] *After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk*. World Economic Forum, Dec. 17, 2020. https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education (accessed 10.08.2022).

[20] *8 Most Common Causes of a Data Breach*. EasyDMARC, July 14, 2022. https://securityboulevard.com/2022/07/8-most-common-causes-of-a-data-breach/ (accessed 14.08.2022).

[21] *8 Most Common Causes of Data Breach*. Sutcliffe & Co, 2022. https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/ (accessed 14.08.2022).

[22] L. Irwin. *The 5 most common causes of data breaches*, 28th April 2022. https://www.itgovernance.eu/blog/en/the-most-common-causes-of-data-breaches-and-how-you-can-spot-them (accessed 12.08.2022).

[23] *7 Major Causes of a Data Breach*. Incognito Forensic Foundation, https://ifflab.org/7-major-causes-of-a-data-breach/ (accessed 12.08.2022).

[24] *Top Security Threats of Smartphones*. Reader’s Digest, July 27, 2022. https://www.rd.com/article/mobile-security-threats/ (accessed 14.08.2022).

[25] *The Global Risks Report 2020, 15th Edition*. World Economic Forum, 2020. – 94 p. https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (accessed 24.08.2022).

[26] *Building Consumer Confidence Through Transparency and Control*. San Jose: Cisco Systems, Inc., 2021. – 19 p.

[27] *Big Security in a Small Business World*. San Jose: Cisco Systems, Inc., May 4, 2020.

[28] I. Bolun, D. Ciorbă, A. Zgureanu, R. Bulai, R. Călin, C. Bodoga. “Informatics security assessment in the Republic of Moldova”. *Journal of Engineering Science*, vol. XXVII, no.4, 2020, pp. 103-119.

[29] *CIS Controls v. 7.1 Measures and Metrics*. Center for Internet Security, 2019. https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/ (accessed 24.02.2020).

[30] I. Bolun. ”Prioritizing cybersecurity measures”. In: *Proceedings of The 11th International Conference on Electronics, Communications and Computing ECCO-2021*, October 21-22, 2021. Chisinau: UTM, 2021, pp. 194-199.