Assessing the State of Digital Security in North Macedonia: a Study of Readiness, Capacity and Threats

Simon Atanasovski, Marinela Mihajlovska, Elissa Mollakuqe , Aleksandra Popovska-Mitrovikj and Vesna Dimitrova
Faculty of Computer Science and Eng.
Ss. Cyril and Methodius University
Skopje, Republic of North Macedonia

simon.atanasovski@students.finki.ukim.mk
marinela.mihajlovska@students.finki.ukim.mk
elissamollakuqe@gmail.com
aleksandra.popovska.mitrovikj@finki.ukim.mk
vesna.dimitrova@finki.ukim.mk

***Abstract*— Our exposure to information technology makes digital security a critical issue. The rapid increase in cyber attacks at the world level does not escape RNM either. The latest developments with the cyber attacks on state institutions, the general observation about the lack of education of non IT people in the area of digital security, and the risk from harmful consequences for state resources, but us as citizens too, was a motive to write this scientific paper. This research paper focuses on assessing the readiness and capability of North Macedonian citizens for digital security. The research examines a number of variables, including the frequency of security breaches experienced by businesses, employee awareness and training programs, the ability to recognize and stop attacks, the value of digital forensics and the amount of money spent on digital security measures. Additionally, the study examines North Macedonia's ability to address the latest digital security threats, including anonymous bomb threats, and the potential for easier detection of perpetrators. The results of this research can provide detailed information on how the digital security situation in North Macedonia is currently shaping future practices and policies aimed at improving that situation. The overall objective of this study is to support ongoing efforts to strengthen digital security and protect against online threats.**

Keywords— digital security, cyber-attacks, risk assessments, incident response, digital forensics, and perpetrators detection

I. INTRODUCTION

The technological age has made digital security a crucial issue, particularly as more and more of our activities and services are conducted online. The current state of technology has given people, companies, and governments access to a number of advantages and opportunities [1][2]. But many cyber threats and security lapses come along with these advantages. To stop potential attacks on the services they provide, numerous institutions, groups, and businesses must take the appropriate precautions or even develop high-quality defenses against these threats [3]. This study paper aims to present the current state of cyber security in businesses in the (RNM) Republic of North Macedonia, including the number of security breaches committed, attack training and awareness programs provided to employees of institutions and companies, the ability of institutions and companies to detect and prevent attacks, the importance of digital forensics in their overall security strategy, and the amount spent on digital security measures.

In addition, this research will explore the RNM's capacity to deal with the latest digital security threats, including anonymous bomb threats, and the potential for easier detection of perpetrators. The findings of this research will provide valuable insights into the current state of digital security in the RNM and can be used to inform future policies and practices to improve digital security.

The rest of the paper is organized in the following way. In Section II we present the related works on digital security in companies that have been conducted globally, with varying degrees of focus on specific regions or industries. We briefly outline the legal framework for computer crime in North Macedonia in Section III. Next, in the fourth section, we explain our research methodology. Analysis of the survey and some recommendations are given in Section V. At the end we derived some conclusions, and we note some ideas for further work.

II. RELATED WORK

Related works on digital security in companies have been conducted globally, with varying degrees of focus on specific regions or industries. A study conducted by IBM Security and the Ponemon Institute in 2020 found that the average cost of a data breach was $3.86 million, highlighting the importance of digital security measures for companies [4]. In a similar study, Accenture found that the average cost of cybercrime for companies increased by 13% in 2020, with the healthcare industry being hit the hardest [5].

Studies have also been conducted on the effectiveness of training and awareness-raising programs for employees in improving digital security in companies [6][7]. A study by the Cybersecurity and Infrastructure Security Agency (CISA)

found that regular training reduced the likelihood of employees falling for phishing scams by 67% [8]. However, a study by the cybersecurity firm, KnowBe4, found that only 53% of organizations conduct training for their employees on a quarterly basis [9].

In the RNM limited research has been conducted on the state of digital security in companies. In terms of the RNM specifically, limited research has been conducted on the state of digital security in companies. However, in 2019, the government of RNM implemented a new cybersecurity strategy aimed at improving the country's overall digital security [10]. This strategy includes measures such as improving cybersecurity education and awareness, establishing a national cybersecurity center, and improving collaboration between the public and private sectors. Part of the research from the journal "Politic in Central Europe" was done on "What hybrid threats are North Macedonia exposed to?" [11].

III. Legal provisions

In this section, we briefly analyze the legal provisions in the RNM that regulate "cyber protection" or so-called "computer crime".

In general, the central framework in the RNM focused on crime is wide and controls: the Criminal Code, Criminal Procedure Law, Law on Electronic Communication, Law on Monitoring Communication, Law on Electronic Commerce, Law on Electronic Management and Electronic Services, Monetary Procedure Law, Law on Data in Electronic Form and Electronic Signature and Declaration for a safer internet [12].

A special review of more specific provisions regulated by the Criminal Code:

A general remark is that there are a large number of actions that are common in our Criminal Code, where punishments ranging from fines to prison sentences are provided, from a minimum of 3 months to ten years. Bearing in mind the previously presented broad legal framework in which there are segments where the so-called "computer crime" is regulated, here we highlight only the most characteristic acts that are covered by the Criminal Code of the RNM: Abuse of personal data (Article 149), Prevention of access to a public information system (Article 149-a), Damage and unauthorized entry into a computer system (Article 251) and Creating and spreading computer viruses Article (251-a) [13].

IV. Methodology

The assessment of the respondents' knowledge was carried out through a well-constructed survey with which we wanted to cover as many citizen categories as possible. The survey allowed us to measure the level of information, knowledge of digital security as well as cyber security.

The survey was sectioned into 4 categories and from one category divided into 3 subcategories, the stakeholders are as follows: high school students, students from different spheres, employees in IT companies and others (employees in public institutions, employees in private institutions and unemployed).

It should be noted that this research is based on our own survey and there is no third-party involvement. For the purposes of preventing, to the extent possible, the risk of not understanding or misunderstanding the questions, the survey was tested before it was released online.

V. Survey analysis and recommendations

The survey was conducted in a range from 22.03.2023 till 30.03.2023 with 315 respondents, covering high schools (54), higher education (202), others (49) and IT companies (10). The survey was split into several parts and they are as follows. The first category is by grouping common questions from high school students (Students from the 4th year of high school, which assumes that they are generally 18 years old), students from different universities and others. While the second category is only IT companies because we realized that they need a separate and different analysis. The third and last one is about current events related to digital security, which are currently extremely relevant in the RNM. In this paper, we will present and analyze in detail the answers to some of the questions in the survey, but our recommendations and conclusions are derived from all questions.

A. Analysis of the common questions for high school students, students from different universities and others

Here, we analyze the answers given to the survey's common questions for students and others. In Fig. 1 we present the percentages for the answers to the first question about familiarity with the term cyber security.

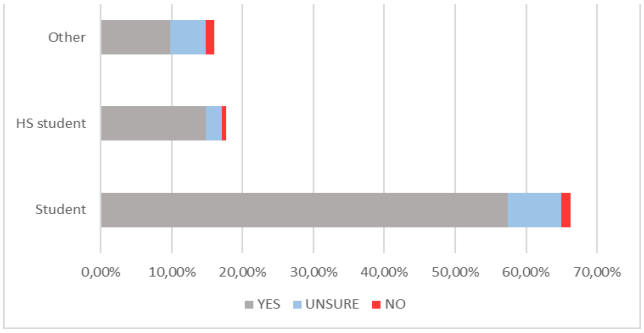

Fig. 1. Results for question: Do you know what the term cyber security means?

As we can see (Fig.1) most of the respondents (82%) are familiar, which indicates an awareness of the need for cyber security.

As a channel from which they have been informed about cyber security, in Fig.2 we can see that most of them indicated the Internet, which is understandably compared to the time that each individual spends on the Internet. But on the other hand, the question "Is the Internet the right place for information on topics of crucial importance in the 21st century" should be opened.

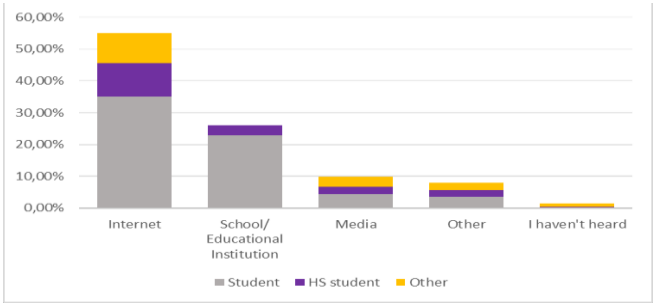

Fig. 2. Results for question: Where did you hear about the term cyber security?

Analyzing the results for the third question "Does the price of a particular security software influence whether you will use it?" (given in Fig. 3) in correlation with the above, we can conclude that in the process of protection and awareness of cyber security, the economic situation of a larger number of respondents is key. Because most of the respondents, despite being informed, do not use certain software because they stated that the price plays a role in the process of choosing the software to use.

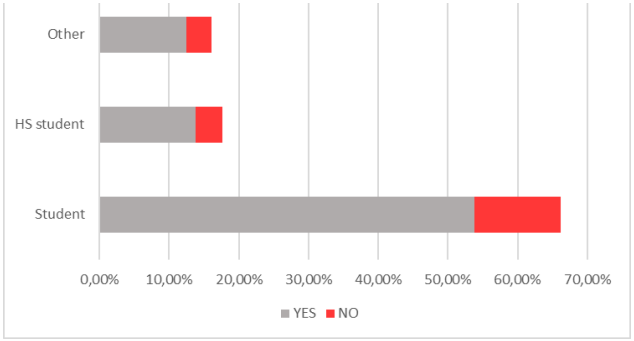

Fig. 3. Results for question: Does the price of a particular security software influence whether you will use it?

A very large part of the respondents on the question for the frequency of password changing gave an answer that is below the recommended limit is worrying (Fig. 4). Knowing that the recommended limit of passwords usually, in accordance with the results of the survey, even 63.28% change their password below the prescribed limit, 16.72% change it within the prescribed period, and 20% change it more often than the recommendations.

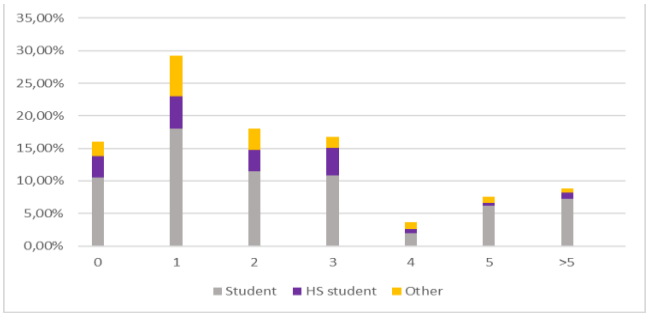

Fig. 4. Results for question: How many times a year do you change your passwords?

In Fig.5 we present answers to the "Do you have information that your educational institution has software systems for information protection?" divided by the category of the respondent (university students and high school students). From here, a general conclusion can be drawn that the educational institutions should still work on increasing the number of positive responses on this question.

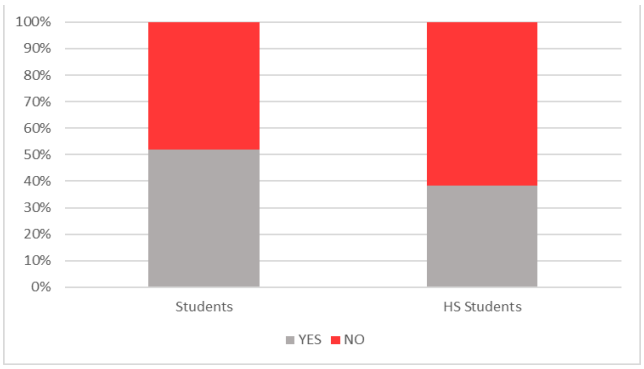

Fig. 5. Results for question: Do you have information that your educational institution has software systems for information protection?

Protection of the IT systems is an important segment and of critical importance. Therefore, we ask the students for their opinion about the protection level of the educational institutions' IT systems. As we can on Fig.6, high school students have a more negative attitude, unlike students who have divided opinions.

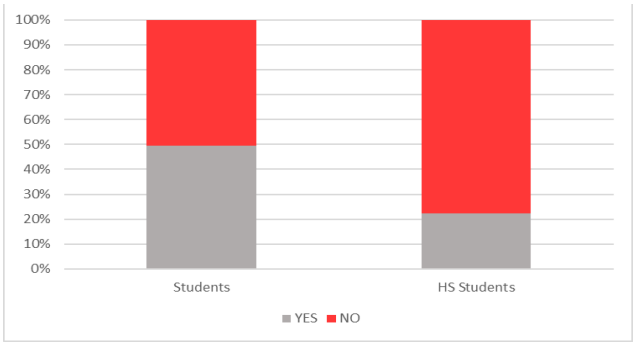

Fig.6 Results for question: Do you think that the IT system of your educational institution is insufficiently protected?

B. Analysis of the survey for IT companies

In analyzing the responses from the IT sector, a general observation is that there was a very low response to the survey, partly due to the questions asking for information about their business policy and ability to deal with a cyber-attack. However, from the available answers, it can be concluded that in general they had no cyber incidents in the last 12 months (60%) and we have only one answer that they had two incidents (10%), one answer with one incident and one that they had "very few". This brings to the conclusion that IT companies either implement more serious cyber protection or are not sufficiently targeted due to the specificity of their activity and fear of potential threats that they could be detected more easily.

From the results for the question about the frequency of security training, given in Fig. 7, we can see that 30% answered that they do not have such programs, 10% answered that they implement one in a year and 10% that they implement two pieces of training on annual level.

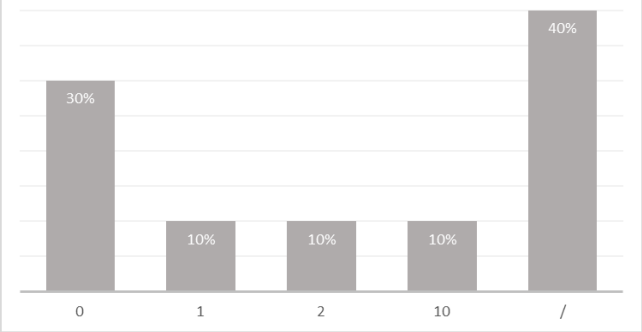

Fig. 7. Results for question: On an annual basis, how many training or awareness programs does your company conduct for employees on digital security best practices?

However, that IT companies seriously care about their digital security is indicated by the question "On an annual level, how often does your company carry out risk assessments for digital security?", where 50% answered that it is carried out five times, 40% twice, 10% once.

To the question "How long does it take your company to detect a breach of digital security" and according to the space left for a free, descriptive answer, there are the most different answers, from "very quickly" to "two hours". "one day" until the answer "one to seven days" etc.

The answers to the question "How long does it take for your company to deal with the consequences of cyber-attacks?" are similar, and those answers are within the framework of the answers to the previous question.

Regarding the question about the company's ability to recover from a digital security breach, Fig. 8, 60% of the respondents answered with the highest score of 5, 20% answered with a score of 3, and 10% answered with scores of 2 or 4.

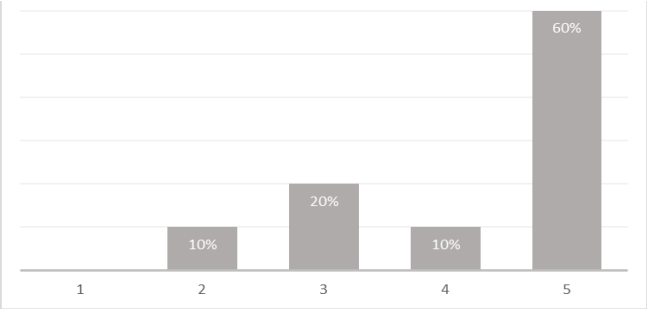

Fig. 8. Results for question: How confident are you in your company's ability to recover from a digital security breach?

The next question was “How important do you consider digital forensics to be in your company's overall digital security strategy?” and from the results given in Fig. 9 we can see that 50% answered with the highest grade 5, 40% graded it with a grade 4 and 10% with a grade 3.

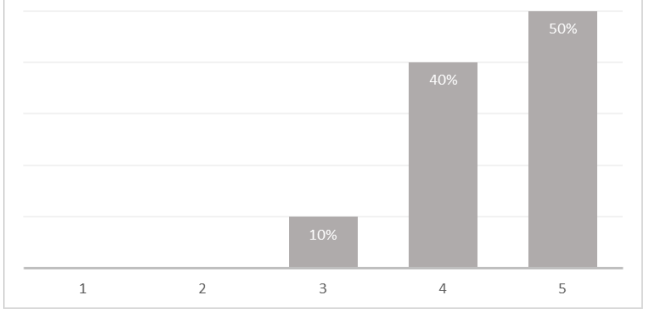

Fig. 9. Results for question: How important do you consider digital forensics to be in your company's overall digital security strategy?

To the last question “Have you hired additional, specialized firms, i.e., outsourcing companies for the digital protection of your company” even 90% answered that they do not have such additional engagement and only 10% that they have hired such a specialized company.

C. Current events related to digital security in North Macedonia.

In the last year in the RNM, the events of the so-called "anonymous reports of planted bombs" have been current. With that, we decided to ask all respondents 3 questions related to this topic and we obtained the following results.

Namely, even 89.4% of the respondents answered that RNM does not successfully deal with digital threats, which is a worrying percentage of public opinion. At the same time, the next question Do you think that the RNM has the capacity to deal with the last so-called "anonymous reports of planted bombs"? also gives seriously unfavorable results that the state does not have the capacity to deal with these threats (78.8%). Simultaneously, even 78.3% think that it is possible to detect the latest digital bomb threats more easily.

Analyzing the results from the above questions and other questions in our survey we come to the following recommendations for the improvement of cyber security in North Macedonia.

- Drafting a National plan for a more comprehensive education of a larger number of categories of citizens about the meaning and methods of digital security in the RNM, which would include the following. Increased education for the cyber security of young people both in primary and secondary education, examination of the possibility of developing certain projects, supported by the state for the methods of education and its wider availability (for example, mandatory topics on “digital protection” in the subjects of informatics, organizing additional lectures by experts, people who deal with this issue and etc.), special lectures (possibility of cooperation with the Ministry of Interior Affairs in the area of prevention) and an indication of legal consequences of a large number of legally prohibited activities, etc.
- Making certain computer programs intended for information protection more accessible and financially acceptable (with subsidizing and support from the state institutions for certain categories of citizens, etc.).
- Organizing a wider media campaign about danger in cyberspace, informing about the latest and current threats, ways of adequate protection and indication of the legal consequences of the intentional abuse of digital security and the legal consequences thereof.

- Performing appropriate analysis, organizing work groups, international cooperation and exchange of experiences with the aim of identifying the latest types of cyber threats and giving appropriate recommendations for avoiding them or remedying their consequences.
- Additional investment for professional upgrading, of course supplementing with appropriate financial resources in the human resource who deal with this problem and are employed in the state organs of the RNM with aim of adequate and maximum possible protection of state institutions and their computer systems, adequate protection of personal data of citizens and official record of these state institutions.

VI. Conclusion and Future Work

From the analysis in our research as a general conclusion, it can be stated that the citizens (of course without the IT companies and their employees) although they are most familiar with the term "cyber security" do not pay too much attention to the real dangers that are possible, since they do not take additional appropriate protection measures outside than the standard ones as a result of objective and subjective reasons. Namely, the deteriorating economic situation does not allow them to purchase more serious and newer protection programs, and in combination with insufficient education and standard carelessness (for example, insufficient changing of passwords which does not require much education or financial means) affects the previously stated conclusion.

At the same time, there is a lack of familiarity with the legal provisions intended for some of those who have recently caused unrest in the RNM. According to the latest data, some of the discovered perpetrators of those anonymous reports through the computer system are minors. This leads to the opinion that a more comprehensive plan by the state and of course its full implementation in this part would mean a serious improvement of the situation in this sphere and a serious reduction of the risks that "cyberspace" brings in addition to the great benefits.

Here, the proposed measures for serious improvement of the situation in state institutions should be taken into account, with the aim of preventing possible computer threats or quick and decisive detection of the perpetrators.

The space of "cyber security", especially in the situation of its actuality, offers a wide field for our further research, especially in an appropriate contribution in the area of drafting a suitable strategy and offering proposals for adequate protection of state institutions.

References

[1] Anderson, R. (2008). Security engineering: A guide to building dependable distributed systems. John Wiley & Sons.

[2] Data and Goliath: *The hidden battles to collect your data and control your world*. WW Norton & Company.

[3] Clarke, R. A., & Knake, R. K. (2010). *Cyberwar: The next threat to national security and what to do about* it. HarperCollins.

[4] Ponemon Institute. (2020). Cost of a Data Breach Report 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

[5] Accenture. (2020). Ninth Annual Cost of Cybercrime Study. https://www.accenture.com/_acnmedia/PDF-112/Accenture-2020-Cost-of-Cybercrime-Study-Final.pdf

[6] Charles J. Brooks and Christopher Grow. "*Cybersecurity Essentials*"

[7] Information Resources Management Association."Cybersecurity and Cybercrime: Concepts, Methodologies, Tools, and Applications"

[8] Cybersecurity and Infrastructure Security Agency (CISA). (2020). 2020 Cybersecurity Awareness Month Resource Kit. https://www.cisa.gov/sites/default/files/publications/CISA-2020-Cybersecurity-Awareness-Month-Resource-Kit_508.pdf

[9] KnowBe4. (2021). 2021 Phishing by Industry Benchmarking Report. https://www.knowbe4.com/hubfs/2021%20Phishing%20by%20Industry%20Benchmarking%20Report.pdf

[10] Government of North Macedonia. (2019). National Cyber Security Strategy of North Macedonia 2019-2023. https://www.cio.gov.mk/Uploads/Documents/Cyber%20security%20strategy%20of%20North%20Macedonia%202019-2023.pdf

[11] Robert Mikac, Marina Mitrevska, Mirza SmajiĆ, "*Hybrid threats and counter-hybrid solutions: A comparative case study analysis of Croatia, North Macedonia, and Bosnia and Herzegovina",* Politics in Central Europe, 2015.

[12] Blagojce Krstevski and Mimoza Bogdanoska Jovanovska, "*Analysis of standard operating procedures and modeling of solutions for modernization of the pre-investigation computer crime procedure,"* master's thesis, Faculty of information and communication technologies – Bitola, 2022.

[13] Parliament of Republic of North Macedonia, "Criminal Code of the Republic of North Macedonia ", jorm.gov.mk, 2015