CYBERSECURITY POSTURE RESEARCH IN SMALL ORGANIZATIONS

Neven Trajchevski[1], Goce Stevanoski[1]

[1]*University "Goce Delchev" – Shtip, Militarry academy "General Mihailo Apostolski" – Skopje, associate member*

Abstract: This study presents the results of empirical research of cybersecurity posture of small organizations in North Macedonia. The results are present as quantitative determined value within a defined taxonomy based on the theoretical foundation of prospect theory and status quo bias. The analyzed quantity is a relation between two key parameters of the cybersecurity posture of an organization, the cybersecurity readiness and the decision makers' perceived risk of cyber-attack. The study also consists of a comparative analysis between these results and gain results during other studies in EU and USA.

Keywords: North Macedonia, Cybersecurity, Posture, Risk, NIST.

INTRODUCTION

Cybersecurity is becoming challenging and even existentially important for small enterprises and organizations as never before, as they are shifting towards higher dependence on information technology. The information technology is also the main propulsion which provides their development. Therefore it is challenging to be dependent on information technology which can be vulnerable and can become costly if it is not properly protected. According to (DCMS, 2020) in UK almost half of the businesses (46%) reported having cybersecurity breaches or attacks within a 12 month period. The small enterprises are considered the backbone of the EU's economy and they also account for more than half of Europe's GDP. Taking this in consideration it is very important to estimate their cybersecurity posture and further to implement measures for improvement.

There is no general accepted definition what is a "small organization". For example according to EU definition (EC, 2021) the SME (small and medium-sized enterprises) are if the staff headcount is less than 50 and the enterprise turnover is less than €10m. However this research is not limited to business enterprises but includes also public/government administration, non-government organizations, utility providers, etc. Therefore the term "small organization" in this study is regarding any organization which is provider of services, regardless of the sector, and it has IT infrastructure consist of minimum web site and local network with less than 50 user stations in the sector that is focus of the research or in the whole organization.

This study has goal to estimate the cybersecurity posture of small organizations in North Macedonia and to make a comparative analysis with results which are gained in EU and USA. Need of such study is recommended in the conclusions of the very comprehensive study given by (Eilts, 2020). Therefore, we adopted that reliable comparative analysis can be done with the results given in (ENISA, 2021) and (Eilts, 2020). In order to make a quantitative and qualitative assessment appropriate for comparison with these studies, this research utilize the instrument which have been developed within one of them (Eilts, 2020).

METHODOLOGY

This study consist of 7 phases/steps in order to give answer to two research questions: what is the cybersecurity posture of small organizations in North Macedonia and if there is a significant difference in comparison with EU and USA. Overview of this research process is presented on figure 1. In the phase 1 we have defined the opened researched questions based on relevant references and we decided that our approach should be in line with the contemporary findings in this field in EU and USA. Thus, we adopted that we will use already developed taxonomy for evaluating cybersecurity posture and already developed instrument within the (Eilts, 2020) in order to be able to make relevant comparison with EU and USA, phase 2 and phase 3. Further in phase 3 we have executed a quantitative study, following by data analysis of the gained data from 20 small organizations in North Macedonia. On the end we have made a quantitative and qualitative comparison with the other studies in EU and USA in phase 6 and the last phase was to derive certain conclusions about the further strategic direction of managing the cybersecurity posture in North Macedonia, as well as certain direction for further research. Following is description of the most important elements of the implemented taxonomy and research instrument.

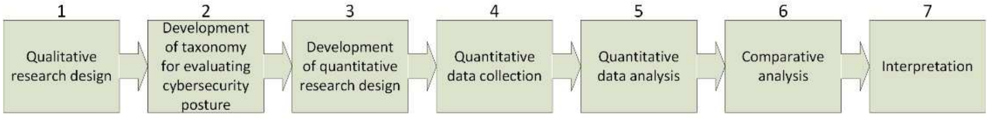

1
Qualitative research design
2
Development of taxonomy for evaluating cybersecurity posture
3
Development of quantitative research design
4
Quantitative data collection
5
Quantitative data analysis
6
Comparative analysis
7
Interpretation

Figure 1. Research study phases

This research utilize developed new construct and research instrument, a taxonomy for assessment of cybersecurity posture **Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)**. The new construct is a relation of **two key parameters** of the cybersecurity posture of an organization, the **cybersecurity readiness** and the **decision makers' perceived risk of cyber-attack**.

Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)

The base of the newly defined CyPRisT is on social theories of risk management. This is supported by published findings in papers like (Gupta & Hammond, 2005), which presents that businesses were affected by the decision makers' indifference towards cybersecurity threats while they were focused on the doing the primary business activities. Such theories are the *Prospect theory* and *Status quo bias*. The Prospect theory of Kahneman & Tversky offered new insight into why nonoptimal decisions are made when they are framed in different ways. (Bazerman, 1984) analyses the framing effect of the Prospect theory and he gives his findings that decision makers' tend to be risk averse in positively framed situations, while being risk seeking in negatively framed situations. In addition (Tversky & Kahneman, 1991) presented that the retention of the status quo is an option in many decision problems referring to the status quo bias effect and that there is relation between the status quo bias and the loss aversion. According to (Tversky & Kahneman, 1991) the value function given on figure 2 illustrates the prospect theory in the decision-making process where the reference point is intersect between the subjective value of the perceived gain or loss. Furthermore, (Tversky & Kahneman, 1992) introduces their new Cumulative prospect theory, which applies to uncertain as well as to risky prospects with any number of outcomes, and it allows different weighting functions for gains and for losses.

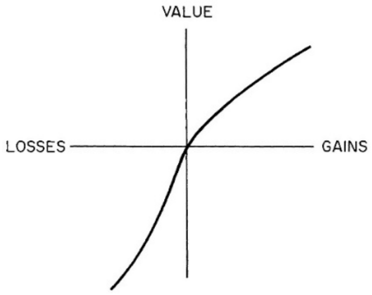


Figure 2. An illustration of a Value Function (Tversky & Kahneman, 1991)

The review of Prospect theory and Status quo bias literature provides the theoretical foundations for the relationship between *risk management activities* and *decision makers' perceptions* of threat. Applying these theoretical lens in the filed of information systems security defines the taxonomy quadrants of the CyPRisT. Measuring the cybersecurity preparedness, as well as the decision makers' perceived risk of cyber-attack and further classifying them in the CyPRisT gives a representation of the cybersecurity posture. There are four quadrants in the CyPRisT as shown in figure 3. The first quadrant *indifference* (Q1) is explained by the decision maker's unwillingness to abandon the status quo and they are at risk of loss due to a cyber-attack. The second quadrant *susceptible* (Q2), refers to risk-seeking behaviors where exists decision maker's awareness of cyber threats and possible loss, but there is not actions toward mitigation of cyber threats.

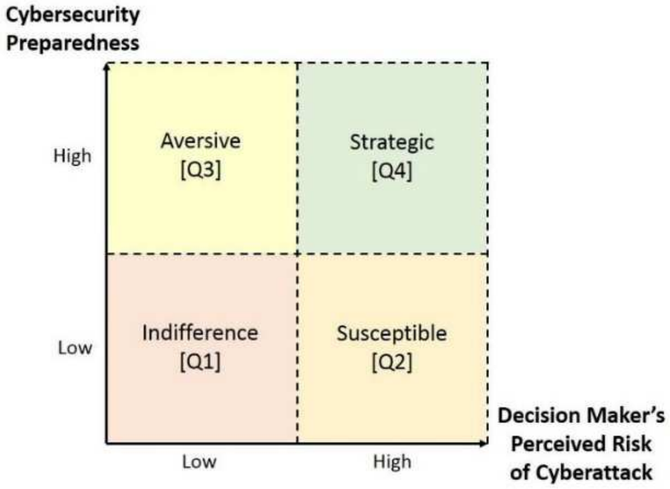


Figure 3. Cybersecurity Preparedness-Risk Taxonomy - CyPRisT (Eilts, 2020)

The third quadrant *aversive* (Q3), refers to the loss aversion effect based on the choice to become risk-averse based on the perceived point of reference for cyber risk and potential loss. In this case the decision maker is less focused on managing of cyber risk due to low perceived risk. The fourth quadrant *strategic* (Q4) is posture where there is balanced ratio between the understanding cyber risk and the actions for mitigating the threats.

Cybersecurity Preparedness

The cybersecurity preparedness refers to risk management that includes both cybersecurity readiness and resilience. Assessment of this quantity is based on the application of NIST Cybersecurity Framework activities (NIST 2018). Within the framework these activities are grouped in five functions: Identify, Protect, Detect, Respond and Recover. The activities are transformed in questions in an iterative process of the Delphi method engaging certain number of subject mater experts and also validated and weighted (Eilts, 2020). This process resulted in 70 (Yes=1/No=0) questions within the five NIST function. During this process each question is also accompanied by calculated mean level of importance (weights) given by the subject matter experts by using a 7-point Likert scale. The final result is the quantity CPS (Cybersecurity Preparedness Scores) which can have value between 0 and 5. The CPS is normalized sum (between the 5 groups of question according the 5 NIST functions) of the products between the answers of the question (0 or 1) and the certain question weight.

Decision makers' perceived risk of cyber-attack

During the literature review in the study of Eilts, (whose instrument we have selected for the measuring and the comparative analysis of the cybersecurity posture), the risk is assessed by measuring the perceived impact and probability of threats. The 10 cyber-attack categories are defined according the classification types of cyber-attacks from (Ponemon Institute, 2018): General malware, Advanced malware/zero-day attack, Compromised/stolen devices, Cross-site scripting, Denial of services, Malicious insider, Phishing/social engineering, SQL injection, Web-based attack, Other. Further, for these 10 categories (also formulated in the form of questions), on the 7-point Likert range it is measured the perceived likelihood, as well as, the perceived impact. Then, for each of the 10 categories, the average value of the products (likelihood x impact) is represented in percent and given as DMPRCA (Decision makers' perceived risk of cyber-attack score).

RESEARCH AND RESULTS

Previously described methodology have been utilized by using online survey instrument in order to make the quantitative assessment of the cybersecurity posture of small organizations in North Macedonia. We have selected certain number of small organizations from different industries. The data collection was in the period of November 2022 and March 2023. The organizations were approached by phone, email and on site. Before the survey, the decisions' makers in these organizations were briefed that their answers and data will remain anonymous and only summarized and statistical results on national level will be published. In order to avoid unreliable results, the survey was conducted only when the research team was convinced that the decision makers' in the selected organizations were motivated to take a participation in the survey.

There is many different recommendations for the sample size for quantitative research in this and similar fields in order to have appropriate sample size justifications, ranging from 20 to 30 to 40 or more (Kothari 2004, Sauro & Lewis 2016, Lakens D. 2022). In this study the size of the sample was 20, which we consider it as enough taking in considerations the nature of the study, the complicated process of performing the survey and the resource constrains. However, we have validated this sample size by statistical approach based on precision rate and confidence level with the relation $n=(z\times\sigma/e)$^2, where n is the size of the sample size, z is the value of the standard variate equal to 1,96 for a 95% confidence level, σ is the standard deviation of the quantity CPS that was calculated to 1.08 and e is the standard error ($e=z\times\sigma/$sqrt(n)=0.46). Thus, a value of n=20 was obtained. For the quantity DMPRCA also a value of n=20 was obtained, where the σ was calculated to 0.188 and e was calculated as 0.0824.

The data collected through the previously described instrument was quantitatively analyzed and values for CPS and DMPRCA were obtained. The values were positioned on the CyPRisT with the DMPRCA on the horizontal axis and the CPS on the vertical axis, figure 4.

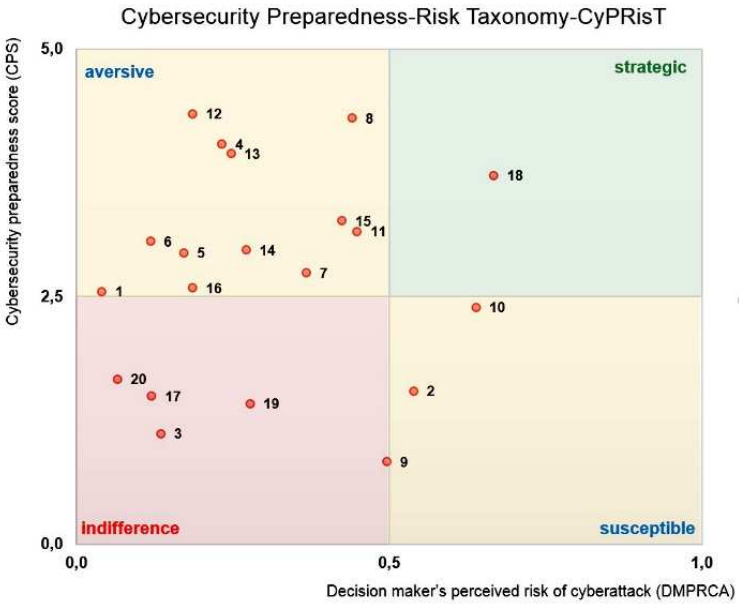


Figure 4. Position of the organizations in the CyPRisT

The summarized scores of the overall cybersecurity posture given by the quantities DMPRCA and CPS, on the sample of 20 organizations, are presented by the descriptive statistics in table 1. This is done by calculating of the central tendency measure, the mean value, which is also accompanied by the standard deviation. The mean score of DMPRCA was 0.3, which suggest low level of perceived risk of cyber attack. The mean score of CPS was 2.71 which indicate a middle range value of cybersecurity preparedness of the sample.

Quantity	N	Min	Max	Mean	Std. Dev.
DMPRCA	20	0.04	0.67	0.30	0.19
CPS	20	0.84	4.35	2.71	1.08

Table 1. Descriptive Statistics of DMPRCA and CPS in North Macedonia

Quantity	N	Min	Max	Mean	Std. Dev.
DMPRCA	216	0.02	0.85	0.28	0.16
CPS	216	0.14	4.47	2.29	1.06

Table 2. Descriptive Statistics of DMPRCA and CPS in USA, (Eilts 2020)

The data from table 1 were compared with the data from (Eilts 2020), given in table 2. The comparison between the position of the mean values in CyPRisT is presented on figure 5, where with label "MK" is marked the result obtained with the experimental research within this study in North Macedonia (table 1) and with "US" is marked the result obtained in USA (table 2).

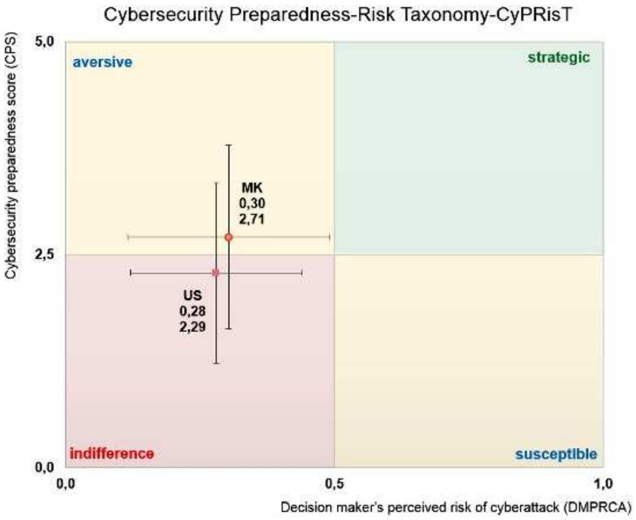


Figure 5. North Macedonia and USA CyPRisT score with standard deviations

These results were analyzed by using unequal variances t-test (Welch's t-test) for both quantities for DMPRCA and CPS, to compare the calculated means and to determine if statistically significant differences exist, taking in consideration that the researched populations are different, as well as the sample sizes and the variances. Results of the test are presented in table 3. The results indicated that statistically there were no significant differences between the means $DMPRCA_{MK}$ and $DMPRCA_{US}$, as well as, between CPS_{MK} and $CPS_{US.}$ However, we can observe increase in both the CPSs and DMPRCA in North Macedonia that moved the position toward the 'aversive' quadrant of the CyPRisT.

Also, a qualitative comparison have been done with the results presented within (ENISA, 2021), where there are presented findings of study which includes 249 SMEs from 25 European Member States. The low $DMPRCA_{MK}$ is overlapping with the conclusion in (ENISA, 2021) that many SMEs do not realize the potential resultant cybersecurity risks posed to their business. Also the middle range value of CPS_{MK} is overlapping with the conclusion in (ENISA, 2021) that SMSs appear to implement some of the basic cybersecurity measures mostly as part of their overall IT implementation or legal obligations.

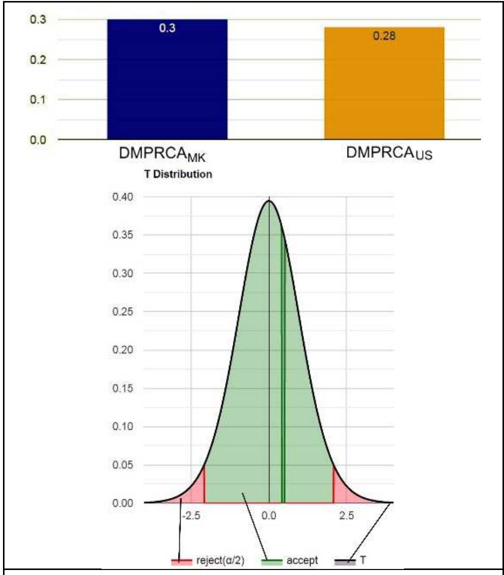
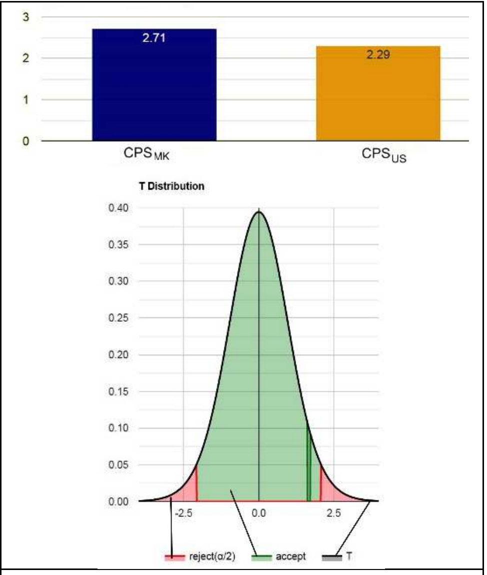
<table>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>α=0.05
df=21.5688 (two-tailed)
Since p-value &gt; α, H_0 cannot be rejected
p-value = 0.6529
T = 0.456
$\overline{\mathrm{DMPRCA}_{\mathrm{MK}}} - \overline{\mathrm{DMPRCA}_{\mathrm{USA}}}$=0.02
standard dev. of the difference, S' = 0.0439
The observed effect size d is small, 0.12</td>
<td>α=0.05
df=22.5247 (two-tailed)
Since p-value &gt; α, H_0 cannot be rejected
p-value = 0.1095
T = 1.6664
$\overline{\mathrm{CPS}_{\mathrm{MK}}} - \overline{\mathrm{CPS}_{\mathrm{USA}}}$=0.42
standard dev. of the difference, S' = 0.252
The observed effect size d is small, 0.4</td>
</tr>
</table>

Table 3. Two sample t-test (Welch) results, using T distribution

CONCLUSIONS

This study addresses a research questions which a relevant and significant in the field of security of IS. It presents a new findings which includes quantitative measurement of the current cyber security posture in North Macedonia, as well as, quantitative and qualitative comparison of these results with similar ones gained in studies in EU and USA.

This study showed than less than a quarter of small organizations in North Macedonia are potentially indifferent toward cybersecurity, which compared with USA is better, where more than half of the SMEs were positioned in this group. Also the results showed that, just a few of the organizations were estimated as having risk-seeking cybersecurity postures, which is overlapping with the findings in the studies in USA and EU. Most of the organizations in North Macedonia were positioned as loss aversive. Loss aversion appears to be the principle driver for decision biases. This suggest that existing regulations, especially in the banking and IT sector are giving results but the decision makers are not enough focused on managing the cyber threats. The findings also barely noted existing of posture where there is strategic balance between understanding cyber risk and implementing the security actions to deal with cyber threats, which is the same finding as in the studies in EU and USA.

One very practical implication which arise from this study is that there is necessity of further development of programs that can help small organizations to improve their cybersecurity posture. Most important would be developing the awareness of decision makers to mitigate the cybersecurity risks in parallel with the existing focus on their primary activities. This will contribute that small organizations became more risk aversive.

Recommendations for future research

During the implementation of this study within its limitations, we experienced a feeling that we just scratched the surface of the topic, so herein we can give some of the many questions which we find them as important for future research:

- Enlarging the number of the sample – number of researched organizations;
- Further statistical analysis in terms of organizations' demographic data of industry, number of employees (size), years in operation, annual revenue, IT budget;
- Analysis of CPS and DMPRCA when compared by industry, number of employees, and IT budget;
- Analysis of DMPRCA in terms of perceived likelihood of the cyber-attack by attack vectors;
- Analysis of CPS in terms of perceived impact of the cyber-attack by attack vectors.

REFERENCES:

Bazerman, M. H. (1984). The relevance of Kahneman and Tversky's concept of framing to organizational behavior. Journal of Management, 10(3), 333-343.

DCMS (2020). UK Department for Digital, Culture, Media and Sport: Cyber Security Breaches Survey 2020: Statistical Release.

EC (2021). European Commission: User guide to the SME Definition.

Eilts, D. (2020). An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses, Doctoral dissertation, College of Computing and Engineering, Nova Southeastern University.

ENISA (2021). European Union Agency for Cybersecurity: Cybersecurity for SMEs, Challenges and Recommendations.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13(4), 297-310.

Kothari C. R. (2004) Research Methodology, Methods & Techniques, New Age International Publishers.

Lakens D. (2022). Sample Size Justification. Collabra: Psychology 8(1):33267.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference dependent model. The Quarterly Journal of Economics, 106(4), 1039-1061.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty, 5*(4), 297-323.

NIST (2018) National Institute of Standards and Technology: Cybersecurity framework, Retrieved from https://www.nist.gov/cyberframework

Ponemon Institute (2018). State of cybersecurity in small & medium-sized businesses (SMB). Retrieved from
https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Sauro j., Lewis J. (2016). Quantifying the User Experience: Practical Statistics for User Research. Elsevier.