University of Economics in Katowice

NAWA POLISH NATIONAL AGENCY FOR ACADEMIC EXCHANGE

International Centre of Research Excellence in Transition of Coal Regions (ExCORE)

ExCORE

FINAL RESEARCH REPORT

TITLE OF THE PROJECT

Cybersecurity of SMEs in Coal-Dependent Regions: Evidence Based Survey

TEAM

Marek Pekarčík[1], Leoš Šafár2*, Patryk Morawiec[3], Paulina Rutecka[3]

1. *Technical University of Košice, Faculty of Economics, Department of Economy, Slovakia*
2. *Technical University of Košice, Faculty of Economics, Department of Banking and Investment, Slovakia*
3. *University of Economics in Katowice, Faculty of Informatics and Communication, Department of Informatics, Poland*

Project supervised by:
Leaders: prof. Monika Wieczorek-Kosmala & prof. Jozef Glova
Mentors: prof. Cristina Florio, prof. Francesca Rossignoli

UNIVERSITÀ di VERONA

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

TECHNICKÁ UNIVERZITA V KOŠICIACH

VSB TECHNICAL UNIVERSITY OF OSTRAVA

Development of project proposal

The project was developed during Hackathon in Ostrava. During this event, a team was built that had the opportunity to get to know each other and their research interests. The first outline of the study was also outlined and a draft of an extended abstract of the scientific article was prepared, under the supervision of the team leaders.

The motivation to undertake this scientific topic was the research interests of team members: IT management on the one hand, and economists related to Industry 4.0 on the other. We realized that the full potential of new technologies offers opportunities to improve the quality of life and careers through value creation. For production-oriented businesses, digital technologies can solve problems and drive change, especially in post-coal regions. However, Industry 4.0's automation and digital connectivity pose risks such as cyberattacks, affecting process stability and IT security. Losses can also arise from third-party data access and human errors. Companies engaging in modern technology and Industry 4.0 must prioritize cybersecurity for smooth operations. Despite many EU citizens claiming cybersecurity knowledge, the high number of attacks often results from human error. Cyberattacks threaten businesses of all sizes, necessitating constant adaptation and strengthening of cybersecurity measures. Small and medium-sized enterprises (SMEs) are particularly vulnerable due to limited resources, lower cybersecurity awareness, and weaker security infrastructure compared to larger corporations.

The presentation during Hackaton - appendix no 1

Further presentations of the project:

(1) University of Southampton study visit - appendix 2

During the study visit at the University of Southampton, the initial outline of the comprehensive research plan was presented, alongside the proposed research methodology. Additionally, a draft of the research tool was introduced. These elements collectively provided a foundational framework for the forthcoming research project, ensuring clarity and direction for its subsequent stages. The proposal was reviewed and commented upon by professors from the University of Southampton, resulting in several revisions and improvements to the research project.

(2) University of Bari / 10th European Risk Conference Conference - appendix 3

The improved research proposal, along with the prepared research tool, was presented at the 10th European Risk Conference held at the University of Bari in Italy. It was introduced to a broader audience and reviewed by professors from the University of Bari and the University of Verona. Their comments and feedback resulted in several revisions and improvements to the research project, ultimately leading to the formulation of the final hypotheses and the adoption of the research methodology.

(3) University of Verona - appendix 4

During the meeting at the University of Verona, preliminary results achieved using the selected research methodology and the outcomes of the conducted analyses were presented. Mentors from the University of Bari and the University of Verona, along with leaders from VSB Czech Republic, TUKE Slovakia, and UE Katowice, provided significant suggestions that influenced the final structure of the article. These included the addition of selected elements and the removal of less relevant sections, particularly in the area of motivation. They also recommended additional methods of data analysis to obtain broader results.

(4) Final conference in Katowice - appendix 5

During the final conference at the University of Economics in Katowice, the final research results were presented in a Flash presentation. Valuable suggestions were gathered from mentors and leaders, including those from the University of Bari, University of Southampton, VSB Czech Republic, TUKE Slovakia, and UE Katowice. Based on this feedback, cosmetic modifications were made to the final version of the article, which was subsequently submitted for review to a renowned international journal.

Outcomes of the project work:

Study aims to fill a gap in the literature by exploring cybersecurity issues in small and medium-sized enterprises (SMEs), particularly in relation to nontechnical, soft-skill, and intellectual capital aspects. This study examines the interplay between cybersecurity awareness and perception and ownership structure in SMEs in the Silesian region of Poland. Unlike the majority of cybersecurity literature, our focus is on how ownership structure influences risk perception. We surveyed 200 random SMEs through the BioStat® Research & Development Centre within the respective region and utilized hierarchical and simple linear regression analyses to assess the relationships between these factors and financial performance. Our results indicate that larger enterprises and those without a family-owned structure exhibit significantly greater levels of cybersecurity. Additionally, we found a positive correlation between cybersecurity and a firm's financial performance and overall health. These findings underscore the importance of cybersecurity awareness and practices for the growth and stability of SMEs.

The **ultimate outcome** of our project is a paper Unveiling the Impact of Ownership Structure on SMEs' Cybersecurity Perceptions.

The paper was submitted to the journal: Information Technology and Management, Springer Nature. This journal explores the impact of IT technologies on information system design, functionality, operations, and management. Journal Impact Factor: 2.3 (2023). The paper is in the revision process.

The documents that confirm the submission - appendix 6

Other results of project collaboration

An additional effect of the team's work on this project is:

- submitting an application for a joint project led by Leoš Šafár, from Technical University of Košice and Paulina Rutecka, from University of Economics in Katowice, related to cybersecurity issues to Slovak National Agency;
- submitting an application under the Erasmus+ Strategic Partnerships program regarding cybersecurity for seniors (SILWERS) - partnership covering, among others, University of Economics in Katowice (project leaders and participants) and VSB Czech Republic (project leaders and participants)