information

Article

Mapping Cybersecurity in SMEs: The Role of Ownership and Firm Characteristics in the Silesian Region of Poland

Leoš Šafár [1], Marek Pekarčik [1], Patryk Morawiec [2], Paulina Rutecka [2] and Monika Wieczorek-Kosmala [3,*]

[1] Faculty of Economics, Technical University of Košice, 040 01 Košice, Slovakia; leos.safar@tuke.sk (L.Š.); marek.pekarcik@tuke.sk (M.P.)
[2] Faculty of Informatics and Communication, University of Economics in Katowice, 40-287 Katowice, Poland; patryk.morawiec@uekat.pl (P.M.); paulina.rutecka@uekat.pl (P.R.)
[3] Faculty of Spatial Economy and Regions in Transition, University of Economics in Katowice, 40-287 Katowice, Poland
* Correspondence: monika.wieczorek-kosmala@uekat.pl

Abstract

As we move toward a more digitalized and interconnected world, new cybersecurity challenges emerge. While most related research has focused on large companies, this 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 cybersecurity perception. We surveyed 200 SMEs at random 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.

Keywords: cybersecurity; SMEs; family-owned business; intellectual capital; survey

Academic Editor: Sokratis Katsikas

Received: 24 May 2025
Revised: 3 July 2025
Accepted: 5 July 2025
Published: 8 July 2025

Citation: Šafár, L.; Pekarčik, M.; Morawiec, P.; Rutecka, P.; Wieczorek-Kosmala, M. Mapping Cybersecurity in SMEs: The Role of Ownership and Firm Characteristics in the Silesian Region of Poland. *Information* **2025**, *16*, 590. https://doi.org/10.3390/info16070590

1. Introduction

Companies, especially those that decide to engage in modern technology and enter the Industry 4.0 phase, must realize how important cybersecurity is for their smooth functioning. Although many citizens of the European Union declare that they have knowledge in the field of cybersecurity [1], the scale of attacks is large, and many of them are caused by human error or oversight. It should be remembered that when the internet was created in the 1960s, no one assumed that it would be popular and accessible. Therefore, the security of this network was not considered. Soon after, the rapid development of the internet in the following decades made it impossible to fix the gaps in network foundations [2]. Further development of technology was based on cores that have serious flaws that can be used by people who want to harm the company. Thus, each new technology potentially has vulnerabilities that constitute vulnerabilities in component systems.

The numbers that illustrate the scale of the cybersecurity problem can help us imagine the potential implications for businesses. In 2008, the global costs of cyberattacks were USD 0.86 trillion and USD 11.5 trillion in 2023. The cost of cyberattacks could reach more than

USD 23 trillion in 2027 [3]. Most attacks remain undetected, or they are discovered many days after the incident, when the costs accrue because of the consequences. According to the report of the World Economic Forum entitled "The Global Risks Report 2020", only 0.05% of incidents are detected in the United States [4]. There is a popular belief that the problem of cybersecurity concerns only large companies; however, this is not true. Approximately 43% of cyberattacks target small and medium-sized enterprises (SMEs) [5]. This may be because SMEs, due to their small operating budget, are often not prepared for self-defense. They are easy targets for attacks aiming to find, steal, and disturb important information, organizational capital, and intellectual property or exploit vulnerabilities in new technology.

The omnipresent threat of cyberattacks casts a long shadow on businesses of all sizes, forcing them to constantly adapt and strengthen their cybersecurity posture. Compared with larger corporations, small and medium-sized enterprises (SMEs) are often perceived as particularly vulnerable due to their potentially limited resources, lower cybersecurity awareness, and less robust security infrastructure [6,7].

The traditional emphasis in cybersecurity research has been on technical solutions and advancements, focusing on firewalls, intrusion detection systems, and vulnerability assessments [6]. A substantial body of research has been dedicated to exploring various technical aspects of cybersecurity, such as intrusion detection systems, encryption protocols, and blockchain-based security solutions [8–10]. While these are undoubtedly crucial for mitigating cyber threats, neglecting the human element—the awareness, perceptions, and behaviors of SME owners and employees—can leave significant vulnerabilities. To complement the technical dimensions described above, we now turn to the human and organizational (non-technical) factors that influence cybersecurity in SMEs. Several studies emphasize the critical role of user education in mitigating cyber risks [11,12]. Eliminating basic mistakes, incorporating best practices, and constant education can increase the security of computer systems that are responsible for storing key business data and controlling production and other processes in enterprises. This can lead to an improvement in the functioning of enterprises, understood as financial savings for the company related to the incident itself, elimination of risk among employees, e.g., health damage due to malfunction of a machine or robots whose control has been taken over by a hacker, elimination of the risk of stopping production, the risk of production containing defect components, and much more. Especially in the context of Industry 4.0, the security of systems in enterprises becomes the security of everything [2].

There is a crucial gap in our understanding of the nontechnical factors influencing cybersecurity practices within SMEs. This study aims to contribute to bridging this gap by investigating the interplay between ownership structure, cybersecurity awareness, and financial performance in SMEs. Ownership structure, encompassing factors such as family ownership versus venture-backed structures, has been largely overlooked in cybersecurity research despite its potential influence on decision-making processes and resource allocation within organizations [13]. Understanding how ownership structures shape SMEs' perceptions of cybersecurity threats and their willingness to invest in mitigation strategies is critical for developing targeted interventions and promoting a more holistic approach to cybersecurity within this vital sector of the global economy.

Our research investigates the Silesian region of Poland, focusing on how ownership structure relates to cybersecurity awareness and perceived risk levels among SMEs. By exploring these relationships, we hope to gain a more nuanced understanding of the complex factors shaping cybersecurity within the SME landscape. The findings can inform targeted strategies for promoting cybersecurity awareness, implementing cost-effective security measures, and ultimately improving cyber resilience among SMEs. By addressing

the gap in research on the nontechnical aspects of cybersecurity in SMEs, this study contributes to a more comprehensive approach to safeguarding these vital economic actors from cyber threats and ensuring their continued growth and success. By incorporating these less-explored aspects, this study aims to provide a more holistic understanding of cybersecurity within the SME landscape.

The structure of this paper is as follows: Section 2 provides the theoretical framework and develops the research hypotheses based on relevant literature. Section 3 presents the research methodology, including the sample, measures, and analytical approach. Section 4 outlines the results of the statistical analyses. In Section 5, we discuss the key findings in light of the existing literature and highlight practical implications. Finally, the concluding section addresses the study's limitations and outlines directions for future research.

2. Theoretical Framework and Hypothesis Development

2.1. Theoretical Framework

The achievement of the full potential of new technologies is an opportunity to improve many people's quality of life or career due to almost unlimited value creation opportunities [14]. In businesses oriented toward production, potential solutions for their problems might come with the development of digital technologies [15]. This is a great opportunity to introduce changes, especially in post-coal regions. However, the automation and digital connectivity introduced in Industry 4.0 also involve risks, e.g., cyberattacks, which can affect process stability and IT security [16]. Potential losses may also be the result of access to data from third-party providers [17] and human errors, including primarily employees with access to the systems.

In the context of Industry 4.0, cybersecurity is analyzed mainly in the case of basic security functions, namely loss of confidentiality and integrity and availability of data associated with networked manufacturing machines [18–20]. The top threats related to Industry 4.0 include social engineering and phishing [21]. According to the Industry 4.0 paradigm, many firms have started connecting their plants and factories across the supply chain to the internet to improve their effectiveness and efficiency. However, this process is associated with cyber threats against networked systems and applications from organizations. According to Ramim and Hueca [22], the world's dependence on information systems is increasing, and cybersecurity incidents are constantly growing. The risks related to cybersecurity and safety are recommended to be a priority for managers in Industry 4.0 environments [23]. According to Boletsis et al. [24], the cybersecurity strategies for SMEs include (1) mapping existing cybersecurity practices, (2) identifying potential threats to the business, and (3) suggesting solutions to mitigate those potential threats. Companies worldwide are facing problems related to cybersecurity and vulnerability to security threats. Additionally, the level of detection of cybersecurity issues according to reports and the literature is extremely low [4]. However, according to reports, companies are increasing their spending on cybersecurity annually [25]; thus, awareness of the importance of cybersecurity in organizations is growing.

Digitalization and processes related to implementing Industry 4.0 features come with processes possessing rather severe challenges from an employee's perspective. Only successful adaptation to new work-related responsibilities and activities should result in overall security of the data, money, know-how, and personal information. Within large corporations, we can easily find whole departments devoted to such threat seeking and effectively countering them. SMEs, on the other hand, do not possess the financial resources of manpower dedicated only to such protection. In addition, almost half of SME employees use personally owned (private) devices to execute business-related activities [26]. Therefore, we consider assessing general knowledge of cybersecurity-related issues among companies,

especially SMEs, as crucial in a highly dynamic environment of transition to a digital environment in the ongoing fourth industrial revolution. While the Industry 4.0 framework provides a useful lens for identifying emerging cybersecurity risks, it is important to recognize that not all companies are equally equipped to respond to these challenges. In particular, SMEs in post-industrial regions—like those in our study—often lack advanced technical infrastructure and specialized cybersecurity personnel. These firms typically operate with limited digital maturity, making them especially vulnerable to human-centered threats such as phishing or social engineering. Therefore, in the following sections, we shift focus from the general cybersecurity landscape in Industry 4.0 to the specific realities of non-technical SMEs, highlighting how ownership structures, organizational culture, and human capital influence cybersecurity awareness and practices. According to the European Commission [26], 76% of the SMEs surveyed currently use an online bank account; the majority also have a website for their business (71%), followed by 55% who use internet-connected "smart" devices. Almost four in ten (39%) use online payment (or ordering) systems of (for) business partners (30% have their own online payment or ordering customer services). Similarly, 38% of the surveyed SMEs reported using cloud computing or cloud storage, with 35% having web-based applications (payroll processing, e-signatures, etc.). All the abovementioned tools and features represent, first, a way to improve a company's processes to make them more effective or less costly. On the other hand, they also present a potential target for security breaches at the digital/virtual level. Only a minority of the SMEs (3%) surveyed replied that there was no usage of online tools listed in the survey. This study further supports our concern, stating that, should we aggregate all types of cybercrimes, 28% of SMEs in the EU have faced at least some type of cybercrime during the last 12 months. Divided among the countries, Portugal (48%), Greece (41%), Slovakia (39%) and Czechia (38%) had the worst results. On average, in European Union countries, as many as 28% of enterprises declare that they have been victims of an attack. Poland obtained a result identical to the average of European Union countries, which makes the case of this country adequate for analysis.

However, important aspects of cyber protection include not only technical and technological security but also the quality of human capital [27]. Human error, or incompetence of employees, is a major threat in terms of cyber protection. Therefore, we conducted our research to analyze the current state of human capital and cyber protection, in particular, in connection with the already identified top vulnerabilities for Industry 4.0: social engineering and phishing [21].

We are witnessing an ever-growing gap in cybersecurity skill sets; therefore, it is essential to have a shared understanding of the current skills, to what those skills represent in the form of human capital both from an individual's and a company's perspective. Understanding the development of human capital to meet current and future needs in the field of cybersecurity is necessary for the continual online safety of individuals, governments, and SMEs. If employees lack risk awareness in IT, they pose a considerable potential threat.

According to Ponsard & Grandclaudon [28], raising awareness of SME employees is inevitable (e.g., employees had to answer a cybersecurity quiz composed of a set of questions dealing with managing passwords, performing backups, and electronic signatures to urge participants to engage in the cybersecurity improvement process). Nobles [29] argued that SMEs must turn their attention to the cybersecurity skills and literacy of their workforce because cybersecurity incidents impact not only individuals or governments [30] but also corporations and small businesses. The latter (SMEs) are very important because they are one of the most vital parts of a nation's economy. Moreover, SMEs are facing major cybersecurity challenges, mainly because of their low security budget, lack of cyber skills and possibility of cyberattacks, which can seriously impact their competitiveness. Due to these factors, SMEs

are often easier targets for cyberattacks, and severe damage could occur should the attack be successful. Even though some individuals understand the possibility of threats, there are still severe security shortcomings that make their information systems vulnerable.

Based on the current knowledge, related research has focused primarily on the technological (software and hardware) area of cyber protection and risk assessment of cyberattack and defense strategies [31], understanding the security threats in cyber-physical systems [32], and determining the determinants of information and digital technology implementation for smart manufacturing [33]. In addition, most of the related research concerns mainly large and well-established companies.

2.2. Hypothesis Development

We generally expect our results to provide valuable insight into the current SME environment in terms of cybersecurity awareness, the perception of risks, and the relationships between the financial health of the company and the respective aspects. Based on the hypothesis clustering, we define 5 hypotheses. Research has suggested a potential link between business size and cybersecurity posture [34,35]. Compared with larger businesses, smaller businesses might have fewer resources to allocate to robust security measures [6].

Based on this, we propose the following:

H1. *Medium-sized businesses will achieve a significantly greater level of cybersecurity than will small businesses.*

The nature of the data handled by a business can significantly influence its cybersecurity risk profile [36]. For example, businesses in the financial services sector that handle sensitive financial data might prioritize cybersecurity more than a bakery with less sensitive data. We hypothesize the following:

H2. *The performance of the service sector will achieve a statistically significant increase in cybersecurity compared with that of the industry sector.*

The ownership structure of a business can potentially influence its approach to cybersecurity. Family-owned businesses might have different decision-making processes and risk tolerances than non-family businesses [13,37]. In addition to structural characteristics, behavioral economics provides a valuable lens for understanding decision-making in family firms. These businesses often exhibit distinct risk cultures influenced by emotional ties, long-term orientation, and trust-based governance, which can lead to heuristic-driven or conservative responses to perceived cyber threats. As highlighted by Brustbauer [37], family-owned SMEs may underinvest in formal risk management practices due to reliance on informal decision-making processes and aversion to external interference. This behavior aligns with findings from behavioral economics, which emphasize bounded rationality and status quo bias in organizational decision-making. Integrating this perspective allows for a richer understanding of how ownership dynamics influence cybersecurity awareness and strategic investment. We propose the following:

H3. *Non-family businesses will achieve a significantly greater level of cybersecurity than family businesses.*

By examining the relationships between business demographics (size, sector, ownership structure) and cybersecurity practices [38,39], we aim to assess their combined predictive power. We hypothesize the following:

H4. *There is a statistically significant predictive power of business demographic features on the level of cybersecurity.*

Investing in cybersecurity can have a demonstrably positive impact on a company's financial health by reducing the risk of costly data breaches and operational disruptions [40]. We propose the following:

H5. *There is a mutually significant predictive relationship between the level of response in cybersecurity and financial performance and company health.*

These additional hypotheses allow us to explore the influence of various business demographics on cybersecurity practices within SMEs.

3. Materials and Methods

This study uses survey research, as this is a suitable method for studying emerging topics in business [41], such as cybersecurity. Moreover, survey research is a suitable tool for narrowing the gap between practice and theory, whereby academics are asked by practitioners for insights at scale and economically [42]. The questions were chosen according to Erdogan et al. [43].

Our survey focused on screening three categories of cybersecurity in SMEs in the Silesian region of Poland:

1. Cybersecurity practices,
2. Cybersecurity awareness,
3. Cybersecurity perception.

The first category includes taking measures to protect their systems and sensitive data to prevent cyberattacks, identifying vulnerabilities in systems and production applications through various processes and tools, and assessing cyber risks within a cybersecurity framework. The second category includes the implementation of various activities dedicated to raising employee awareness of cybersecurity, creating job roles that are primarily dedicated to cybersecurity, and raising awareness of the possibility of using work tools for private purposes and vice versa. The second category is directly related to improving the quality of human capital. This includes preparing and training employees for the potential risks that are associated with cyberattacks. This represents a key factor in increasing the level of cybersecurity in SMEs. The third category is the cybersecurity perception of SMEs regarding the cyberattacks they have faced or could face. It also looks at the potential impact of such attacks on the functioning of the company. We also cover the typical business demographic features of SMEs.

These are the following variables that the survey tracked:

1. Number of SMEs' years on the market.
2. Size of SMEs (small companies with fewer than 50 employees or medium-sized companies with fewer than 249 employees).
3. Sector of the SME's performance (three main sectors: industry, services, and trade).
4. Form of SME ownership (family-owned and -run enterprises and non-family-owned and -run).
5. Year-on-year growth in the number of employees in SMEs.
6. Market share.
7. Sales revenue.
8. Profitability.
9. Financial liquidity.
10. Overall financial situation.

11. Operating profit margin (difference between sales revenue and operating expenses).

We used the IBM SPSS 21 tool, where we sequentially performed descriptive statistics, factor analysis and regression analysis. The results are described in the following subchapters.

3.1. Sample

The study involved 200 entrepreneurs representing small and medium-sized enterprises (SMEs), with microenterprises excluded from the Silesia region (Poland). Based on available data, there are approximately 21,320 SMEs registered in Silesia (out of a total of 533,000 companies in Silesia, 96% of which are microenterprises) [44]. For this population, a sample of 200 SMEs ensures a maximum error margin of 7% at a 95% confidence level. It is also worth noting that, even if we refer to the entire population of companies in Silesia (533,000), a sample of 200 still results in a maximum error margin of 7% at a 95% confidence level. The data were collected by a professional external agency (BioStat® Research & Development Centre, Rybnik, Poland) in the period from 1 September to 31 December 2023, which ensured standardized data collection.

The descriptive statistics of the basic indicators are presented in Table 1. The sample included 124 (62%) small enterprises (10–49 employees) and 76 (38%) medium-sized enterprises (50–249 employees). The smallest firm had 10 employees, and the largest had 249 employees. The mean number of employees was 61 (SD = 60). The firm with the shortest tenure had been in business for 3 years and that with the longest had been in business for 125 years. On average, the firms had been in business for 29 years (SD = 17). In general, 12 (6%) "Civil societies", 113 (56.5%) Ltd., and 75 (37.5%) other companies participated in the present research. Of these firms, 122 (61%) perceived themselves as family businesses and 78 (39%) did not perceive themselves as family businesses. According to the main business profile, the firms were divided into 29 Trade (14.5%), 79 Production (39.5%), and 92 Services (46%). All responses were screened for completeness prior to analysis. Cases with substantial missing data (i.e., unanswered core items in the cybersecurity or financial performance sections) were excluded from the dataset. As the survey was administered via computer-assisted telephone interviews (CATI) by a professional agency (BioStat®), the rate of incomplete responses was minimal. The final sample of 200 SMEs includes only fully completed questionnaires.

Table 1. Descriptive statistics of business demographic features. Source: ExCORE survey.

Characteristics of Companies	N (%)
Size of SME	
Small enterprise (0–49 employees)	124 (62)
Medium enterprise (0–49 employees)	76 (38)
Sector of SME's performance	
Trade business	29 (14.5)
Production	79 (39.5)
Services	92 (46)
Form of SME's ownership	
Family business	122 (61)
Non-family business	78 (39)

In the following sections, we present the procedures followed and the individual scales of cybersecurity, financial performance, and company health.

3.2. Variables and Measures—Cybersecurity

We surveyed cybersecurity using 10 items selected from the original Erdogan et al. questionnaire [43]. The items were selected based on their relevance to our research. The survey questions are divided into three dimensions based on the implemented factor

analysis. All 10 questions were answered on a 7-point scale (1. Definitely No to 7. Definitely Yes). Due to the nonstandardized nature of the scale, we conducted reliability, validity, and internal consistency analysis of the scale to strengthen the quality of the results of our statistical and econometric analyses. The final score of a given scale reflects the degree of cybersecurity of the firm.

The reliability of our adaptation of the Cybersecurity Scale was $\alpha = 0.84$. According to the factor analysis, the Kaiser–Meyer–Olkin measure of sampling adequacy was 0.8, and the results of Bartlett's test of sphericity were significant ($p < 0.001$). Three components had eigenvalues greater than 1, which was confirmed by a scree plot. The distribution of items into our components followed the item distribution of Erdogan et al. [43]. The reliability of the individual components ranged from $\alpha = 0.56$ to $\alpha = 0.92$. The total variance explained by all three components was 65.3%. Based on the literature review and the results of the factor analysis, we divided the items into the following three dimensions, which we characterized as follows:

1. Questions related to cybersecurity practices.

We used three questions focusing on the preparation and implementation of tools and processes to prevent and detect cyberattacks.

- We have implemented processes or tools to assess risks associated with IT assets.
- We have implemented certain processes or tools to identify cyber vulnerabilities.
- We have implemented certain processes or tools to identify cyberattacks.

2. Questions related to cybersecurity awareness (quality of human capital).

We used four questions aimed at assessing the quality of human capital and its awareness, preparedness, and resilience to cyberattacks.

- We offer courses or training to employees to increase their cybersecurity awareness.
- We have positions dedicated to cybersecurity at all levels of management.
- We hold meetings or presentations internally on cybersecurity issues.
- Employees can use company devices (e.g., laptops) and applications at home.

3. Questions related to cybersecurity perception.

We use four questions aimed at assessing processes for detecting and evaluating real and potential cyberattacks.

- We believe that our company is vulnerable to cyberattacks.
- The impact of previous cyberattacks on our company has been significant.
- The loss of data in the cyberattack will cause serious disruptions to our business.

3.3. Variables and Measures—Financial Performance and Company Health

The items tracking the financial performance and health of companies were measured using 7 items selected based on their relevance to our research. All 7 items were measured on a 7-point scale (1. Definitely No to 7. Definitely Yes). Due to the nonstandardized nature of the scale, we conducted reliability, validity, and internal consistency analyses of the scale to strengthen the quality of the results of our statistical and econometric analyses. The resulting scores from a given scale describe a measure of a firm's financial performance and health.

The reliability of our adaptation of the Financial Performance and Business Health scale was $\alpha = 0.83$. In the factor analysis, the Kaiser–Meyer–Olkin measure of sampling adequacy was 0.81, and Bartlett's test of sphericity was significant ($p < 0.001$). Two components had eigenvalues greater than 1, which was confirmed by a scree plot. The reliability of the individual components ranged from $\alpha = 0.75$ to $\alpha = 0.86$. The total variance explained by the 2 components was 71.2%. Based on the literature review and the results of the factor

analysis, we divided the items into the following two dimensions, which we characterized as follows:

4. Questions related to financial performance.

We use three questions aimed at identifying SMEs' performance and growth in terms of number of employees, market share, and sales growth.

- We increased the number of employees.
- We have increased our market share.
- Our sales revenue increased.

5. Questions related to the financial health of the company.

We use four questions aimed at identifying the financial health of companies. These are questions associated with profitability, liquidity, financial position, and operating margin.

- Our company maintains profitability (profitability).
- Our company maintains financial liquidity at a good and stable level (there is no payment stress—cash shortage).
- The overall financial situation of our company is good (no risk of bankruptcy).
- We are satisfied with the operating profit margin (the difference between sales revenue and operating costs).

This study is situated within the social sciences' paradigm (management and economics), where statistical models often exhibit limited ability to explain variance due to the behavioral complexity of the phenomena under investigation. In this context, coefficient of determination R^2 values of 12–17% should be interpreted through the disciplinary lens, consistent with the findings of Ozili [45,46]. As emphasized by Ozili [45], in social sciences research, an R^2 threshold of $\geq$10% is acceptable provided the statistical significance of key predictors ($p < 0.05$). In our model, all main independent variables (ownership, managerial experience) achieved significance at $p < 0.01$, confirming their theoretical relevance.

4. Results

The results of the descriptive analysis of Erdogan et al.'s [43] self-modification of the cybersecurity scale are shown in Table 2.

Table 2. Descriptive statistics of the cybersecurity scale according to IBM SPSS. Source: ExCORE survey.

	Minimum	Maximum	Mean	Std. Deviation	Skewness	Kurtosis
Cybersecurity scale	10	67	38.60	11.05	−0.02	−0.17
Financial performance and company health	7	49	31.56	7.69	−0.36	0.39

We conclude that the average score on the scale is 38.60 out of 70, indicating a 55.14% level of cybersecurity. We observed the lowest score, with a value of 10. The highest scoring firm scored 67 on the cybersecurity scale. Given the skewness and kurtosis, we used parametric methods of statistical analysis. Based on the results of Table 2, we can conclude that the average score of the financial performance and company health scale is 31.56 out of 49, which indicates a 64.40% level of financial performance in firms on average. The firm with the lowest score was 7, the firm with the highest score was 49, and hence the maximum level of financial performance and company health was reached. Considering skewness and kurtosis, and the histogram, we used the scale used in parametric methods of statistical analysis.

We used the parametric methods of ANOVA and the independent sample test to evaluate significant differences between the selected unbiased variables. Table 3 shows the descriptive statistics of the cybersecurity scale divided by the independent variables.

Table 3. Results of the descriptive statistics of the cybersecurity scale by the firms according to IBM SPSS.

	Form	N	Minimum	Maximum	Mean	Std. Deviation
Size of SME	Small	124	10	67	36.12	10.62
	Medium	76	10	63	**42.62**	10.60
Form of SME's ownership (family business)	No	78	10	67	**41.51**	11.27
	Yes	122	10	63	36.72	10.53
Sector of SME's performance	Trade	29	14	62	39.76	10.85
	Industry	79	10	61	38.81	10.56
	Services	92	10	67	38.03	11.60

We tested for differences in cybersecurity scores across enterprise sizes and family business levels using the independent samples test. Levene's test for equality of variances did not allow us to reject the null hypothesis in either case, so we assumed equal variances. The results of the independent samples test suggest that firms that identified themselves as family businesses had lower cybersecurity level scores. Based on this, we can conclude that firms that were not identified as family firms performed better in terms of cybersecurity. The results suggest that larger firms (medium-sized enterprises) also perform better in terms of cybersecurity. Based on this, we can conclude that the greater the size of a firm is, the better its cybersecurity performance.

There was a significant difference in the mean cybersecurity scale score between small and medium-sized enterprises ($t_{198} = -4.201$, $p < 0.001$). From Table 3, we can see that medium-sized businesses, on average, scored better on the cybersecurity scale. Thus, we can conclude that the larger the firm is, the better the cybersecurity level is. We confirm that medium-sized businesses will achieve a significantly greater level of cybersecurity than will small businesses (hypothesis H1). Additionally, there was a significant difference in the mean cybersecurity scale score between family businesses and non-family businesses ($t_{198} = 3.050$, $p = 0.003$). Table 3 shows that non-family businesses, on average, score better on the cybersecurity scale.

Differences in cybersecurity scores in the main business profile were verified using one-way ANOVA. Again, the results of Levene's test for equality of variances assume equal variances. Thus, the ANOVA results suggest that there are no statistically significant results. However, there are indeed minimal differences in the sector in which they operate at the level of cybersecurity. Based on this, we can conclude that the sector of operation of SMEs does not affect the level of cybersecurity. It should be noted here that in the case of a more detailed breakdown by the NACE, we could identify companies operating in digital and technology-intensive sectors or those working with sensitive data from clients, production, etc.

There was no significant difference in the mean cybersecurity scale score between the main business profiles (t2.197 = 0.293, $p = 0.747$). It is true that there is a difference in scores, but it is statistically insignificant; therefore, we reject hypothesis H2.

To predict the cybersecurity level achieved by a company through firm characteristics (size of enterprises, form of ownership, and main business profile) and economic factors (financial profitability and health), we chose hierarchical linear regression. To test the ability of cybersecurity level to predict firm economic growth, we used simple linear regression. There are no outliers in the research sample after processing the research set. The variables used in the regression analysis were at least interval variables. When nominal variables are used, the variables are dichotomized. The necessary file size was sufficient to implement the models. Based on multicollinearity testing using the VIF and tolerance for individual models, we can confirm that our regression models also meet this condition. Normality, linearity, and homoscedasticity of the residuals were accepted after the regression analysis was performed by examining the histograms, Q-Q plots, and scatter

plots. Error independence and autocorrelation were tested using the Durbin–Watson test, where the values ranged from 1.5–2.5.

Table 4 summarizes the results of the hierarchical regression analysis for cybersecurity level. The first model including firm characteristics as predictors was statistically significant ($F(2.197) = 13.87$, $p < 0.000$). The index of determination ($R^2 = 0.12$) indicated that the first model explained 12% of the variability in cybersecurity level. A statistically significant comparison revealed that the size of the enterprise (B = 6.36; β = 0.28; $p = 0.000$) and the form of ownership (B = −4.61; β = −0.20; $p = 0.003$) were statistically significant predictors in the first model.

Table 4. Results of hierarchical linear regression analysis of the cybersecurity scale by IBM SPSS.

Predictor	Model 1 (R^2 = 0.12 ***)				Model 2 (ΔR^2 = 0.05 **)			
	B (CI)	**SE (B)**	**β**	***p***	**B (CI)**	**SE (B)**	**β**	***p***
Size of SME's	6.36 (3.38;9.35)	1.52	0.28	**0.000**	6.21 (3.29;9.13)	1.48	0.27	**0.000**
Form of SME's ownership	−4.61 (−7.58;−1.64)	1.51	−0.20	**0.003**	−4.59 (−7.49;−1.68)	1.47	−0.20	**0.002**
Financial performance and health					0.30 (0.12;0.48)	0.09	0.21	**0.002**
F	13.87 ***				13.11 ***			

Note: B = nonstandardized regression coefficient, CI = 95% confidence interval, SE = standard deviation, b = standardized regression coefficient, *p* = *p* value. ** = $p < 0.01$; *** = $p < 0.001$.

The second model examined the effect of adding economic growth characteristics as a predictor of cybersecurity level. The coefficient of determination increased by 5% ($\Delta R^2 = 0.05$), which was a significant change ($F(1.196) = 10.30$, $p < 0.002$). The index of determination for the second model ($R^2 = 0.17$) indicated that it explained 17% of the variability in cybersecurity level. The results indicated that all the selected predictors used in the second hierarchical regression model were statistically significant: size of enterprises (B = 6.21; β = 0.27; $p = 0.000$), form of ownership (B = −4.59; β = −0.20; $p = 0.002$), and financial performance and company health (B = 0.30; β = 0.21; $p = 0.002$). We confirmed the first hypothesis that the bigger the company is, the better the level of cybersecurity. We also confirm that non-family businesses gain a greater level of cybersecurity than family businesses (hypothesis H3). Based on the results presented in Tables 4 and 5, we also confirm a mutually positive relationship between the level of cybersecurity and financial performance and company health (hypothesis H4).

Table 5. Results of simple linear regression analysis of financial performance and company health level by IBM SPSS.

Predictor	Model 1 (R^2 = 0.05 **)			
	B (CI)	**SE (B)**	**B**	***p***
Cybersecurity level	0.15 (0.06;0.25)	0.05	0.22	**0.002**
F	10.02 **			

Note: B = nonstandardized regression coefficient, CI = 95% confidence interval, SE = standard deviation, b = standardized regression coefficient, *p* = *p* value. ** = $p < 0.01$.

Table 5 shows the results of simple regression analysis for financial performance and company health. The model including cybersecurity level as a predictor was statistically significant ($F(1.198) = 10.02$, $p = 0.002$). The index of determination ($R^2 = 0.05$) indicated that the model explained 5% of the variability in firms' financial performance and company health. A statistically significant comparison revealed that cybersecurity level (B = 0.15;

$\beta = 0.22$; $p = 0.002$) was a statistically significant predictor. Therefore, we confirm that the greater the cybersecurity level is, the greater the financial performance and overall health of the company (hypothesis H5).

5. Discussion and Conclusions

This study represents one of the few bridging the ownership structure and the overall cybersecurity level of the respective company. We analyze a questionnaire consisting of 200 responses from SMEs in a historically coal-dependent and coal-transformation region in Poland. An important contribution is in the first step to standardizing the questions associated with the cybersecurity survey, as the original source [43] has not yet been implemented. We contribute to the literature by concluding the following:

i. Three factors (predictors) influence the level of cybersecurity of the surveyed companies. These variables are *the size of the SME, the form of the SME's ownership, and the level of financial performance and company health*.
ii. The size of the SME is a statistically significant predictor of the level of cybersecurity, so we can conclude that the larger the enterprise is, the better its cybersecurity protection.
iii. The level of cybersecurity is also influenced by the form of SME ownership. This means that family businesses have a worse level of cybersecurity than those that did not identify as family businesses in the survey. This may be because non-family firms may fill positions based not on family ties but on expertise. It may also be that non-family firms are more open to know-how.

As anticipated, our results confirm that SMEs with stronger financial performance are more likely to invest in cybersecurity, and that larger enterprises—due to their scale and internal communication structures—are better positioned to promote cybersecurity awareness among employees. These findings are consistent with existing literature emphasizing the role of organizational resources and capacity in shaping cybersecurity outcomes [47]. However, beyond these expected correlations, our study also reveals unique behavioral and structural factors specific to non-technical, family-owned firms. In particular, reliance on intra-family trust and informal communication channels appears to substitute for formal security measures, a trend that may undermine resilience in digital contexts. These soft factors—including employee education and cultural perceptions of risk—emerge as critical dimensions of cybersecurity readiness in resource-constrained SMEs.

Furthermore, we conclude that cybersecurity perception and overall cybersecurity level are significantly affected by ownership structure, where the question of managerial level arises [47].

Our results suggest that investing in and establishing processes to improve cybersecurity can positively impact not only the protection of businesses from cyberattacks but also their financial stability and performance; moreover, we find that other studies have been more specifically oriented toward building training and programs to increase cybersecurity awareness [48,49]. This conclusion is primarily grounded in the analysis of the "cybersecurity practices" subsection of our scale adapted from Erdogan et al. [43], which specifically examined the implementation of tools and processes aimed at preventing and detecting cyberattacks. These practices were assessed using a dedicated set of three survey items (see Section 3.3), and their aggregated scores contributed to the overall cybersecurity index used in our regression models (Tables 3 and 4). The statistically significant relationships identified between cybersecurity level and financial health ($p = 0.002$) support the claim that active investment in cybersecurity processes enhances not only resilience but also financial outcomes. Thus, the findings directly relate to the "cybersecurity practices" category of our instrument, confirming its relevance in interpreting organizational performance

outcomes. By avoiding cyberattacks, data loss, and disclosure, SMEs build better trust with customers and partners, leading to improved market share, profitability growth, and potential economies of scale, resulting in higher operating margins.

Based on our results, we make several proposals for improving cybersecurity in family businesses. Our analyses showed that family firms scored significantly lower in cybersecurity than non-family firms (mean = 36.72 vs. 41.51; $t_{198} = 3.050$, $p = 0.003$) and that higher cybersecurity levels were positively associated with better financial performance and company health (B = 0.15, $p = 0.002$). Family firms should strengthen employee training and awareness, as lower cybersecurity scores in our study were linked to insufficient cybersecurity awareness. Formalizing cybersecurity policies and governance structures can reduce reliance on informal decision-making and improve cybersecurity outcomes. Aligning cybersecurity with financial objectives is crucial, given the positive relationship we observed between cybersecurity levels and financial performance. Finally, engaging external experts may help family SMEs implement essential cybersecurity practices where internal capacities are limited [39,50–52].

Therefore, it is crucial for SMEs to incorporate cybersecurity improvement into their strategic planning and risk management. This focus ultimately enhances their competitiveness (increasing market share), financial performance (profitability, headcount), and overall business health (liquidity, profitability, operating margin).

Limitations and Further Research

Our study is limited to the Silesian region of Poland, and the generalizability of the findings to other regions or countries may require further investigation. While our study is limited to SMEs in the Silesian region of Poland, this focus was intentional to capture the cybersecurity dynamics of a post-industrial economy undergoing digital transformation. Silesia's economic legacy—dominated historically by mining and heavy industry—provides a valuable lens to study non-technical SMEs transitioning into Industry 4.0 environments. To support the external relevance of our findings, we have identified similar studies conducted in other post-industrial regions (e.g., the Ruhr region in Germany or Northern England), where comparable challenges in SME cybersecurity readiness and awareness have been observed, e.g., [24,47]. These parallels suggest that our findings may be cautiously generalized to other regions with similar structural characteristics, although broader national or cross-border comparisons are encouraged in future research. Additionally, a more detailed breakdown of the "service" sector could reveal variations in cybersecurity practices within different service industries. We recognize that many SMEs operate with less formalized structures and limited technical resources compared to larger organizations. Each SME may adopt its own unique management framework and resource allocation model, as legal directives often do not constitute mandatory statutory requirements for them. Our research findings must be generalized cautiously, with the caveat that individual organizational approaches to cybersecurity matters may vary significantly.

Future research could explore the specific cybersecurity challenges faced by different industry sectors and how ownership structures influence cybersecurity decision-making processes within SMEs. It would also be valuable to examine the role of government regulations and industry best practices in shaping cybersecurity awareness and practices within the SME landscape. The second limitation is the level of the survey, as it would be interesting to observe the structure of SMEs at a more detailed level. Furthermore, the current categorization of SMEs into broad sectors—industry, trade, and services—may obscure relevant intra-sector differences, particularly regarding cybersecurity readiness. Future studies should consider using the NACE Rev. 2 classification, which allows for more detailed differentiation between technology-intensive and low-tech firms, potentially

revealing sector-specific cybersecurity patterns. In our research, we work with overall cybersecurity, although in the empirical part, we quantitatively defined three dimensions. A further limitation of this study is the exclusive reliance on cross-sectional quantitative data. Although the use of structured surveys allowed for statistical generalization across SMEs, the absence of qualitative insights limits the depth of understanding regarding individual decision-making processes, especially in relation to cybersecurity perception and cultural attitudes. Moreover, the inability to conduct longitudinal tracking restricts our capacity to infer causal relationships over time. These constraints stem from the nature of our data collection, which was carried out anonymously by an external agency (BioStat®), preventing follow-up contact with the participants. Future research could address this limitation by incorporating mixed-method designs, including in-depth interviews, case studies, or panel studies, to capture dynamic changes in cybersecurity practices and perceptions over time. However, in this paper, we used the overall questionnaire items.

Author Contributions: Conceptualization, L.Š. and P.M.; methodology, M.P.; software, M.P.; validation, P.R.; formal analysis, L.Š.; investigation, P.M. and P.R.; resources, P.M.; data curation, L.Š.; writing—original draft preparation, M.P. and L.Š.; writing—review and editing, P.M. and P.R.; visualization, P.R.; supervision, M.W.-K.; project administration, P.R. and L.Š.; funding acquisition, M.W.-K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Narodowa Agencja Wymiany Akademickiej (NAWA), grant number BPI/PST/2021/1/00007. This work was also supported by the Slovak Research and Development Agency under the Contract no. VV-MVP-24-0272.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

IT	Information Technology
EU	European Union
SME	Small and Medium Enterprise
ExCORE	Excellence in Transition of Coal Regions
ANOVA	Analysis of Variance
NACE	Nomenclature statistique des Activités économiques dans la Communauté Européenne —Statistical Classification of Economic Activities in the European Community
NAWA	Narodowa Agencja Wymiany Akademickiej—Polish National Agency for Academic Exchange

References

1. Directorate-General for Communication European Commission. *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security (Cybercrime)—Data Europa EU*; Directorate-General for Communication European Commission: Brussels, Belgium, 2020.
2. Schneier, B. *Kliknij Tutaj, aby Zabić Wszystkich. Bezpieczeństwo i Przetrwanie w Hiperpołączonym Świecie*; Wydawnictwo Helion: Gliwice, Poland, 2019; ISBN 978-83-283-5199-8.
3. World Economic Forum. 2023 Was a Big Year for Cybercrime—Here's How We Prepare for the Future. Available online: https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/ (accessed on 13 May 2024).
4. Granados Franco, E. *The Global Risks Report 2020. Insight Report*, 15th ed.; World Economic Forum: Geneva, Switzerland, 2020.
5. Accenture. *State of Cybersecurity Resilience 2021. How Aligning Security and the Business Creates Cyber Resilience*; Accenture: Dublin, Ireland, 2021.

6. Gupta, J.; Barzotto, M.; Khorasgani, A. Does Size Matter in Predicting SMEs Failure? *Int. J. Fin. Econ.* **2018**, *23*, 571–605. [CrossRef]
7. Ponemon Institute. *The 2023 Global Study on Closing the IT Security Gap: Addressing Cybersecurity Gaps from Edge to Cloud*; Ponemon Institute: North Traverse City, MI, USA, 2023.
8. Hu, Q.; Asghar, M.R.; Brownlee, N. Evaluating Network Intrusion Detection Systems for High-Speed Networks. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; IEEE: Melbourne, Australia, 2017; pp. 1–6.
9. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press series on discrete mathematics and its applications; CRC Press: Boca Raton, FL, USA, 1997; ISBN 978-0-8493-8523-0.
10. Casino, F.; Dasaklis, T.K.; Patsakis, C. A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
11. Rahman, N.A.A.; Sairi, I.H.; Zizi, N.A.M.; Khalid, F. The Importance of Cybersecurity Education in School. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 378–382. [CrossRef]
12. Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X. Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *Int. J. Inf. Manag.* **2019**, *45*, 13–24. [CrossRef]
13. Chen, J.; Henry, E.; Jiang, X. Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *J. Bus. Ethics* **2023**, *187*, 199–224. [CrossRef]
14. Thames, L.; Schaefer, D. Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges. In *Cybersecurity for Industry 4.0*; Thames, L., Schaefer, D., Eds.; Springer Series in Advanced Manufacturing; Springer International Publishing: Cham, Switzerland, 2017; pp. 1–33, ISBN 978-3-319-50659-3.
15. Raamets, T.; Karjust, K.; Hermaste, A.; Mahmood, K. Planning and Acquisition of Real-Time Production Data Through the Virtual Factory in Chemical Industry. In Proceedings of the ASME 2021 International Mechanical Engineering Congress and Exposition. Volume 2B: Advanced Man-ufacturing; American Society of Mechanical Engineers, Virtual, Online, 1 November 2021; p. V02BT02A017.
16. Kutzler, T.; Wolter, A.; Kenner, A.; Dassow, S. Boosting Cyber-Physical System Security. *IFAC-Pap.* **2021**, *54*, 976–981. [CrossRef]
17. Morozova, O.; Nicheporuk, A.; Tetskyi, A.; Tkachov, V. Methods and Technologies for Ensuring Cybersecurity of Industrial and Web-Oriented Systems and Networks. *Radioelectron. Comput. Syst.* **2021**, *4*, 145–156. [CrossRef]
18. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the Context of Industry 4.0: A Structured Classification of Critical Assets and Business Impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
19. Stallings, W.; Brown, L. *Bezpieczeństwo Systemów Informatycznych: Zasady i Praktyka*, 4th ed.; Wydawnictwo Helion: Gliwice, Poland, 2019; Volume 1, ISBN 978-83-283-4299-6.
20. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/82875.html (accessed on 22 November 2022).
21. Shaabany, G.; Anderl, R. Designing an Effective Course to Improve Cybersecurity Awareness for Engineering Faculties. In *Advances in Human Factors in Cybersecurity*; Ahram, T.Z., Nicholson, D., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2019; Volume 782, pp. 203–211, ISBN 978-3-319-94781-5.
22. Ramim, M.M.; Hueca, A. Cybersecurity Capacity Building of Human Capital: Nations Supporting Nations. *J. Appl. Knowl. Manag. (OJAKM)* **2021**, *9*, 65–85. [CrossRef]
23. Pandey, S.; Singh, R.K.; Gunasekaran, A. Supply Chain Risks in Industry 4.0 Environment: Review and Analysis Framework. *Prod. Plan. Control* **2023**, *34*, 1275–1302. [CrossRef]
24. Boletsis, C.; Halvorsrud, R.; Pickering, J.B.; Phillips, S.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-Technical Cybersecurity Risk Assessment. In Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, Online, 8–10 February 2021; SCITEPRESS—Science and Technology Publications: Setúbal, Portugal, 2021; Volume 3, pp. 266–274.
25. Asen, A.; Bohmayr, W.; Deutscher, S.; González, M.; Mkrtchian, D. *Are You Spending Enough on Cybersecurity?* Boston Consulting Group: Boston, MA, USA, 2019; pp. 1–7.
26. European Commission. *EUROBAROMETER No. 2280/FL496 SMEs and Cybercrime Report*; European Commission Publications Office: Luxembourg, 2022.
27. Alshboul, Y.; Streff, K. Beyond Cybersecurity Awareness: Antecedents and Satisfaction. In Proceedings of the 2017 International Conference on Software and e-Business, Hong Kong, China, 28–30 December 2017; pp. 85–91.
28. Ponsard, C.; Grandclaudon, J. Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs. In *Information Systems Security and Privacy*; Mori, P., Furnell, S., Camp, O., Eds.; Communications in Computer and Information Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 1221, pp. 335–357. ISBN 978-3-030-49442-1.
29. Nobles, C. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA—J. Bus. Public Adm.* **2022**, *13*, 49–72. [CrossRef]

30. Levy, Y.; Gafni, R. Introducing the Concept of Cybersecurity Footprint. *Inf. Comput. Secur.* **2021**, *29*, 724–736. [CrossRef]
31. Süzen, A.A. A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. *Int. J. Comput. Netw. Inf. Secur.* **2020**, *12*, 1–12. [CrossRef]
32. Walker-Roberts, S.; Hammoudeh, M.; Aldabbas, O.; Aydin, M.; Dehghantanha, A. Threats on the Horizon: Understanding Security Threats in the Era of Cyber-Physical Systems. *J. Supercomput.* **2020**, *76*, 2643–2664. [CrossRef]
33. Ghobakhloo, M. Determinants of Information and Digital Technology Implementation for Smart Manufacturing. *Int. J. Prod. Res.* **2020**, *58*, 2384–2405. [CrossRef]
34. Bada, M.; Furnell, S.; Nurse, J.R.C.; Dymydiuk, J. Supporting Small and Medium-Sized Enterprises in Using Privacy Enhancing Technologies. In *HCI for Cybersecurity, Privacy and Trust*; Moallem, A., Ed.; Lecture Notes in Computer Science; Springer Nature Switzerland: Cham, Switzerland, 2023; Volume 14045, pp. 274–289. ISBN 978-3-031-35821-0.
35. Bhattacharya, D. Evolution of Cybersecurity Issues in Small Businesses. In Proceedings of the 4th Annual ACM Conference on Research in Information Technology, Chicago, IL, USA, 29 September 2015; p. 11.
36. PwC CEE Findings from the 2023 Global Digital Trust Insights. Available online: https://www.pwc.com/c1/en/2023-cee-digital-trust-insights.html (accessed on 13 May 2024).
37. Brustbauer, J. Enterprise Risk Management in SMEs: Towards a Structural Model. *Int. Small Bus. J.* **2016**, *34*, 70–85. [CrossRef]
38. Culot, G.; Fattori, F.; Podrecca, M.; Sartor, M. Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Eng. Manag. Rev.* **2019**, *47*, 79–86. [CrossRef]
39. Chaudhary, S. Driving Behaviour Change with Cybersecurity Awareness. *Comput. Secur.* **2024**, *142*, 103858. [CrossRef]
40. Ferraioli, J. Megatrends: Opportunities on the Front Lines of Cybersecurity. Available online: https://www.morganstanley.com/articles/investing-in-cybersecurity-long-term-guide (accessed on 13 May 2024).
41. Ehret, M.; Kashyap, V.; Wirtz, J. Business Models: Impact on Business Markets and Opportunities for Marketing Research. *Ind. Mark. Manag.* **2013**, *42*, 649–655. [CrossRef]
42. Kent Baker, H.; Mukherjee, T.K. Survey Research in Finance: Views from Journal Editors. *Int. J. Manag. Financ.* **2007**, *3*, 11–25. [CrossRef]
43. Erdogan, G.; Halvorsrud, R.; Boletsis, C.; Tverdal, S.; Pickering, J. Cybersecurity Awareness and Capacities of SMEs. In Proceedings of the 9th International Conference on Information Systems Security and Privacy, Lisbon, Portugal, 22–24 February 2023; SCITEPRESS—Science and Technology Publications: Lisbon, Portugal, 2023; pp. 296–304.
44. *Raport o Stanie Województwa za rok 2023—Biuletyn Informacji Publicznej Samorządu Województwa Śląskiego*; Urząd Marszałkowski Województwa Śląskiego: Katowice, Poland, 2024.
45. Ozili, P.K. The Acceptable R-Square in Empirical Modelling for Social Science Research. Available online: https://mpra.ub.uni-muenchen.de/115769/1/MPRA_paper_115769 (accessed on 13 May 2024).
46. Ozili, P.K. The Acceptable R-Square in Empirical Modelling for Social Science Research. *SSRN J.* **2023**. [CrossRef]
47. Alahmari, A.; Duncan, B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; IEEE: Dublin, Ireland, 2020; pp. 1–5.
48. Yamin, M.M.; Katt, B.; Gkioulos, V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Comput. Secur.* **2020**, *88*, 101636. [CrossRef]
49. Bada, M.; Nurse, J.R.C. Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs). *Inf. Comput. Secur.* **2019**, *27*, 393–410. [CrossRef]
50. Sabilion, R. Delivering Effective Cybersecurity Awareness Training to Support the Organizational Information Security Function. In *Research Anthology on Privatizing and Securing Data*; IGI Global: Hershey, PA, USA, 2021. [CrossRef]
51. Melaku, H.M. A Dynamic and Adaptive Cybersecurity Governance Framework. *J. Cybersecur. Priv.* **2023**, *3*, 327–350. [CrossRef]
52. Calvo-Manzano, J.A.; Feliu, T.S.; Herranz, Á.; Mariño, J.; Fredlund, L.-Å.; Colomo-Palacios, R.; Moreno, A.M. Towards an Integrated Cybersecurity Framework for Small and Medium Enterprises. In *Systems, Software and Services Process Improvement: 31st European Conference, EuroSPI 2024, Munich, Germany, 4–6 September 2024*; Communications in Computer and Information Science; Springer: Cham, Switzerland, 2024. [CrossRef]