The Impact of Robust Cybersecurity Practices on Consumer Confidence, and Economic Outcomes in SME Investments

Madalina Carcea

This manuscript was compiled on October 18, 2024

Abstract

This study examines the impact of robust cybersecurity policies on consumer confidence, and economic performance among Small, and Medium Enterprises (SMEs). Employing a mixed-methods approach—comprising case studies, surveys, and interviews—this research explores the extent to, which investments in cybersecurity influence customer trust, and contribute to the financial success of SMEs. The quantitative analysis reveals a significant positive correlation between strong cybersecurity practices, and heightened consumer loyalty, with measurable economic gains resulting from enhanced customer retention, and trust. Complementary qualitative findings highlight the critical role of transparency in data protection, reinforcing that clear communication of cybersecurity efforts fosters consumer trust. The study underscores cybersecurity as a strategic asset for SMEs, enhancing their competitive advantage, and fostering sustained growth in an increasingly digital marketplace. These findings suggest that SMEs prioritising cybersecurity can realise considerable benefits, thereby positioning themselves more effectively within the digital economy.

Keywords: *Cybersecurity, Consumer Confidence, SME Investments, Economic Impact, Digital Trust, Cyber Resilience*

1. Introduction

Technology is evolving rapidly, making effective cybersecurity practices essential, especially for small and medium-sized enterprises (SMEs). As these businesses navigate various complex digital issues, they face the dual challenge of securing sensitive data while building consumer trust. The research investigates the complex interactions amongst strong cybersecurity policies, user trust, and SME cybersecurity investments, as well as, their overall economic negative consequences.

On the one hand, the digital transition has opened doors for high growth, and operational efficiency enabling SMEs to create and reach markets otherwise impossible.

On the other hand, this transition has also put these businesses in the line of cyber-attacks such as data breaches or phishing that could disrupt their business operations, and damage their image ("Cost of a Data Breach Report 2020", 2020). With cyber threats becoming more frequent, and complex, the imperative to build effective security architectures is far greater than in the past.

The study holds significance given the increasing influence of cybersecurity within the business landscape, particularly regarding its potential effects on consumer behaviour and the economic performance of small and medium-sized enterprises (SMEs) (Sharma & Lijuan, 2020). Achieving this objective will provide SMEs with valuable insights, specifically clarifying the relationship between investment in cybersecurity measures and the financial benefits from such expenditures. Additionally, this understanding will aid in safeguarding their digital assets and fostering strong consumer confidence over time.

This paper is built upon identifying existing limitations and gaps. The primary research question is: ***How do robust cybersecurity practices impact consumer confidence and the economic benefits of SME investments?*** To effectively address this question, the following research objectives will be outlined:

1. Analyse Cybersecurity Challenges SMEs Face: Determining the most critical cybersecurity risks for SMEs, while including vulnerabilities that make them frequent targets for cyberattacks.
2. Cybersecurity Practices on Consumer Confidence: Investigate how visible, and robust cybersecurity measures affect consumer trust, particularly in e-commerce, and digital transactions.
3. Economic Impact of Cybersecurity Investments for SMEs: Measure the relationship between cybersecurity spending, and its substantial monetary benefits, such as revenue growth, customer loyalty, and competitive positioning.
4. Develop Practical Cybersecurity Strategies for SMEs: Formulate actionable recommendations that enable SMEs to improve data security, comply with regulations, and foster consumer confidence effectively.
5. Identify Gaps, and Areas for Future Research in SME Cybersecurity: Highlight limitations within existing cybersecurity practices, and suggest areas for further study to optimise cybersecurity approaches across various SME sectors.

Indeed, since the SMEs in this case study are evolving to meet the challenges of modern times, it should be applied that effective security is more than just technology, it is pragmatic. It is crucial in the sustenance of consumer confidence, and for any SME that is growth-oriented (Gartner, 2020).

2. Literature Review

2.1. Introduction

Cyber threats are rapidly growing in the global digital world, and SMEs are becoming more susceptible to being affected.

Mostly, these organizations lack the resources, and robust security measures of larger corporations to protect their assets and sustain consumer trust.

In this review, we analyse the economic incentives of SME's investment in cybersecurity and highlight how such intentions can influence consumer trust. Covering the cybersecurity landscape for small, and medium-sized enterprises (SMEs), how cybersecurity addresses consumer confidence, as well as, the economics of investing in cybersecurity.

2.2. SME's Landscape

Because of this, SMEs are increasingly a target for cyberattacks since they have (presumably) fewer resources, therefore their overall security stands to be weaker than compared to larger corporations like companies in the top 500 list.(Verizon, 2021): 43% of Cyber-attacks target Small Businesses It is further exacerbated by the fact that many SMEs underestimate how likely they are to be targeted.(Tawileh et al., 2021), the most common threats are phishing attacks, ransomware, and malware infections – these all represent immediate financial risk, as well as, long-term reputational damage.

According to a ("Cost of a Data Breach Report 2020", 2020) report, small businesses are bound to incur an average data breach cost of $3.86 million, which also includes costs such as legal fees compliance with regulations, and fines, loss from business impact due to damage control reputation damage etc.

The larger monetary cost underlines the unequal effects of these breaches on smaller SMEs, that tend not to have enough financial padding for something like this.

On top of that, the rapidly changing face of cyber threats requires SMEs to be on constant alert with their security measures. The Uptake of Cybersecurity As a matter of fact, up to 68% of business leaders believe that their cybersecurity risks are growing (Accenture, 2019).

This understanding reinforces the necessity for continuous investment in cyber safety to combat ever-growing advanced threats.

2.3. Cybersecurity, and Consumer Confidence

Strong cybersecurity techniques are important so as not to lose consumers' trust.Sharma and Lijuan (2020) established an agreement between e-business perceived security, and consumer trust with a positive linear correlation. Businesses that invest in data protection have more chances of retaining existing customers and acquiring new ones.

This aligns with the findings of Kim et al. (2019), who indicated that 85% of consumers would steer clear of a brand online following a security incident. This underscores the essential economic rationale for maintaining robust security systems.

Equally vital to cultivating trust is the transparency of data handling practices. Alharbi et al. (2022) carried out a meta-analysis of various studies examining the relationship between consumers and cybersecurity.

They hypothesize that enhanced brand communications can lead to greater consumer confidence in a brand's ability to address security issues.

This increases the level of confidence of consumers that their data is secure and breached. Deloitte (2021) in its report cited consumer perception towards security as a major factor influencing their behaviour.

The study reported that 81% of the users would avoid a web brand after a data breach occurred despite the users not being impacted by the breach.

2.4. Economic Impact of Cybersecurity Investments

The damage that cybersecurity breaches cause is known, however not many realize the economic value of investing in cybersecurity.

According to Gartner (2020), by 2025, the boards of directors who consider cybersecurity an integral part of the organizational strategy will create a separate cyberspace committee. This shift in focus indicates that many businesses are starting to appreciate the wider implications of cybersecurity on their general well-being.

According to a recent report (Forum, 2020), effective cybersecurity could add an average of 5% annual revenue for SMEs. This expansion has been fueled by a rise in consumer confidence along with operational efficiencies, and lower downtime related to security incidents. Cybersecurity can keep the assets, and reputation of SMEs safe in addition to operational performance (Amir et al., 2018).

The quantitative analysis performed by Amir et al. (2018), explores the relationship between cybersecurity investments and firm performance. The researchers conclude that companies focusing on cybersecurity have a long-term enhancement to their financial performance, and greater stock market returns overall. What does it tell us: The positive correlation further underscores the monetary advantage of investing in cybersecurity strength over time. According to IBM (2021), organizations with security automation fully in place were able to reduce the average total cost of a data breach by 80% across all countries. The decrease in the average charge of incidents, is a clear indicator, that the investment in cybersecurity to prevent and detect security breaches will provide financial implications on total costs when critical events occur. By automating security, enterprises can detect,

and react to threats faster than manually driven environments. In return, it helps reduce the risk that breaches go unnoticed or unaddressed.

2.5. Implications for SMEs

The literature consistently points to the critical importance of cybersecurity investments for SMEs. These investments protect against potential financial losses from breaches and play a crucial role in building, and maintaining consumer trust.

Kurpjuhn (2021) argued that SMEs should view cybersecurity as a competitive advantage rather than just a necessary expense. Robust security measures can differentiate a business in a crowded market, and attract security-conscious consumers.

Company (2022) emphasized the need for a holistic approach to cybersecurity that goes beyond technical solutions. The authors recommend integrating cybersecurity into all business operations and fostering a culture of security awareness among employees.

This comprehensive strategy guarantees that every individual within the organization recognizes the critical significance of cybersecurity and possesses the necessary means and knowledge to enhance the company's security.

Furthermore, SMEs can benefit from collaborating with industry partners and participating in information-sharing initiatives. By staying informed about the latest threats, and best practices, SMEs can continuously improve their security measures, and stay ahead of potential attackers.

This proactive approach enhances security while also signifies a strong commitment to safeguarding customer data, which in turn fosters consumer trust.

2.6. Conclusion

The literature indicates that there is a nuanced relationship between cybersecurity investments, consumer confidence, and economic benefits for SMEs.

Effective cybersecurity measures help to keep potential threats at bay, while also delivering consumer confidence and bottom-line benefits. Research continually shows that investment in cybersecurity is much more than a defensive measure: it has repeatedly been proven as one of the smartest business moves you can make for growth and success.

The existing literature reveals significant gaps, particularly regarding the long-term economic implications of cybersecurity investments and the identification of industry-specific best practices. Future research should focus on longitudinal studies to assess the sustained returns on cybersecurity initiatives over time. Additionally, exploring the trade-offs associated with optimizing security investments across various sectors could provide valuable insights into effective strategies for safeguarding assets in a rapidly evolving digital landscape.

Researchers can help SMEs better invest in cyber security to achieve the desired economic benefits by filling these gaps as shown in table (Table 1).

Table 1. Summary of Studies on Cybersecurity, and SMEs

Study	Year	Findings	Implications
Verizon	2021	43% of cyber attacks target SMEs, highlighting their vulnerability.	SMEs must prioritize cybersecurity to protect assets and maintain trust.
Ponemon Institute	2020	Average cost of data breach: $3.86 million, indicating significant financial risks.	The financial burden highlights the need for robust cybersecurity investments.
Accenture	2019	68% of business leaders feel cybersecurity risks are increasing.	Growing awareness suggests a shift towards proactive cybersecurity measures.

3. Methodology

3.1. Data collection methods

The research adopts a mixed-matched approach by combining qualitative, and quantitative research methods to identify the impact of robust cybersecurity practices on consumer confidence, and the economic benefits of SMEs. The data collection methods include structured surveys and semi-structured interviews.

3.1.1. Quantitative

Surveys A structured survey was administered to a fixed number of SMEs to gather quantitative data on their cybersecurity practices, perceived risks, and the economic impacts of their cybersecurity investments. The survey included questions on the following topics:

1. Types of cybersecurity measures implemented
2. Frequency, and types of cyber threats encountered
3. Costs associated with cybersecurity investments
4. Perceived benefits of cybersecurity measures, including impacts on sales, customer trust, and investor interest

3.1.2. Qualitative

Interviews In addition to the survey, qualitative data was collected through semi-structured interviews with ten consumers aged 20 to 30. These interviews aimed to explore consumer perceptions of cybersecurity, and its effects on trust, and purchasing behaviour. The interview questions focused on:

1. Awareness of cybersecurity issues
2. Experiences with data breaches, and their impact on trust
3. Expectations of businesses regarding data protection
4. Factors influencing trust in online transactions

3.2. Sampling procedures

Survey Sampling SMEs from various industries were included in the study. We employed a stratified random sampling technique for selecting respondents, which allowed us to represent different segments and sizes of SMEs. This approach enhances the applicability of the results to the broader SME population, enabling more generalized conclusions and insights across the sector, and ensuring a diverse and representative sample.

Interview Sampling Several participants were interviewed for the qualitative study and chosen as representatives of a research sample comprising consumers aged 20 to 30 who had prior interactions with SMEs on their online platforms. This age group is particularly suitable, as it includes individuals who are more likely to engage in online transactions and are more conscious of cybersecurity issues. This thoughtful sampling method ensures that the selected participants have relevant insights regarding their experiences and perceptions, which they are more inclined to express.

3.3. Data analysis techniques

Quantitative Data Analysis The survey data will be examined using statistical methods to identify patterns and correlations. Descriptive statistics will give an overview of the cybersecurity landscape among SMEs, including the types, and frequency of cyber threats, the costs, and benefits associated with cybersecurity investments. Inferential statistics, such as regression analysis, will evaluate the hypotheses regarding the connections between cybersecurity procedures, and economic outcomes. This study seeks to quantify the effect of cybersecurity measures on sales, consumer trust, and investor interest as shown in the.

Data Cleaning , and Preparation Data preparation involves a detailed process with multiple steps to enhance the quality and integrity of the analysis.

1. ***Handling Missing Data***: The missing values were identified methodically, and taken care of. Imputed missing data for categorical variables using mode, and numerical ones with the median to keep more information even after doing so.
2. ***Remove Duplicates***: The process of data cleaning included a thorough check for duplicates to ensure that no entry appeared more than once in the dataset. This step is crucial for maintaining the integrity and accuracy of the data analysis.
3. ***Outlier Detection***: The outliers were detected using the IQR method, and then considered these outliers as independent classes of data points. This step ensured that anomalous data points did not majorly affect the accuracy of our study.
4. ***Data Transformation***: Certain variables were transformed or modified as needed to sustain the analysis. There was a common data fair that date formats would be the same, and categorical variables were understood or encoded correctly for doing statistical analysis.

Exploratory Data Analysis (EDA) EDA: This was conducted to summarize, and visualize the data, gaining insights into the cybersecurity practices of SMEs. Key steps included:

1. ***Descriptive Statistics***: Descriptive statistics including frequencies, means, medians, and standard deviations were used to summarize the data.
2. ***Types of Visualizations***: Different visualizations, i.e., histograms, bar charts, pie charts, and

scatter plots were displayed to recognize patterns or trends in the data.

3. ***Correlation Assessment***: Correlation matrices were prepared to demonstrate the relationship between different variables, and it was observed that there are certain relationships amongst cybersecurity practices on its output variable indicating significant correlation.

Qualitative Data Analysis The qualitative data acquired through the interviews has been thematically analysed to present common trends and insights on the client's perception of cybersecurity. Thematic analysis is the identification of different themes, and patterns in the coded data. This method offers a comprehensive understanding of customer perceptions and experiences regarding data breaches, by showcasing their expectations from organizations concerning data security. The findings of the thematic analysis will be presented together with the quantitative data to have a better perspective of the impact of cyber security on customer trust, and behaviour patterns.

4. Results

4.1. Quantitative

The data for this quantitative research was collected through a structured survey conducted with about 200 SMEs. The survey aimed to collect detailed information on SME cybersecurity behaviours, risk perceptions, and economic consequences associated with their investments in these areas. The data were cleaned, and processed to avoid any inaccuracies in the findings, followed by exploratory analysis, as shown in figure 1.

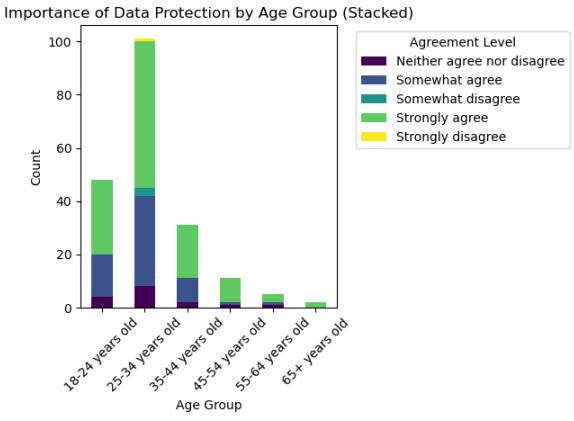

Figure 1. *Q: It is important to me that measures are taken to protect my data.*

Key Findings Slightly more SMEs had basic cybersecurity measures, like firewalls, and antivirus software. However, advanced measures such as multi-factor authentication, and encryption are less commonly used, suggesting a gap in adopting sophisticated security technologies.

Phishing remains the most prevalent cyber threat, followed by malware, and ransomware.SMEs in finance, and healthcare face higher-than-average incidences, as shown in the figure 2.

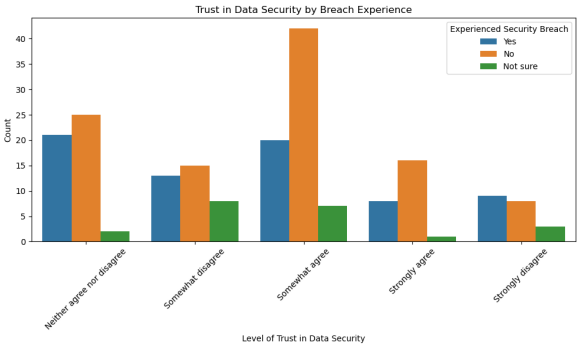

Figure 2. *Q: I trust most companies will protect, and secure my data against breaches or attacks. I have been the victim of a security breach myself.*

SMEs spend an average of $10,000 a year in cybersecurity protections — but it did vary drastically from one business to another. Interestingly, SMEs that spend more on security had fewer data breaches and undertook fewer financial implications associated with ROI on cybersecurity. The data reveals a positive correlation between higher sales growth and increased interest from potential investors with greater investments in cybersecurity. These findings illustrate that cybersecurity investments help mitigate risks, foster business development and enhance market reputation.

4.2. Statistical Analysis, and Effect Sizes

We conducted statistical analyses to explore the relationship between awareness of data sharing and the importance placed on data protection measures. Additionally, we examined the differences in attitudes between consumers who have ceased doing business with companies due to privacy concerns and those who have not.

4.2.1. Correlation Analysis

The correlation between awareness of data sharing, and the importance of data protection measures was $r = 0.41$, 95% CI [0.29, 0.52], $p < .001$. This represents a moderate positive relationship, indicating that individuals aware of the data they share also tend to place higher importance on data protection measures.

A post-hoc power analysis revealed that with our sample size of 198, and $\alpha = 0.05$, we achieved a power of 0.9999856 to detect this correlation. This indicates that our study had more than adequate power to de-

tect the observed effect, minimizing the risk of Type II errors.

4.2.2. Group Comparison

We also examined the difference in attitudes towards data protection between consumers who have and those who have not stopped doing business with companies due to privacy concerns. The effect size for this difference was Cohen's d = 0.25, 95% CI [-0.06, 0.57]. This represents a small effect size, suggesting a modest difference in the importance placed on data protection between these two groups. However, the confidence interval includes zero, suggesting, the difference is not statistically significant at the $\alpha = 0.05$ level.

4.2.3. Implications

These findings highlight the tie between consumer awareness and perspectives toward data protection. Educating consumers about data-sharing practices may increase concern for data protection.

However, the minimal difference between those who have stopped doing business due to privacy concerns, and those who have not suggests that factors like convenience often overpower privacy issues in decision-making.

SMEs should implement strong data protection measures, and effectively communicate them to customers. While raising awareness may enhance the perceived importance of data protection, it may not necessarily change consumer behaviour without additional stimuli or reassurances.

4.3. Qualitative

The findings from qualitative interviews with consumers between the ages of 20, and 30 regarding their perspectives, experiences, and expectations about cybersecurity procedures in SMEs provide a sophisticated overview of consumer views towards cybersecurity, trust, and communication.

The interview participants had varying levels of awareness regarding SMEs' cybersecurity practices. The ones with professional expertise in technology or cybersecurity showcased awareness of specific procedures like two-factor authentication, and safe payment methods.

Conversely, many admitted to inadequate involvement with these activities, frequently clicking the "accept" on cookie rules without understanding the consequences.

Respondents preferred organizations that clearly described data handling methods, considering well-designed, modern websites, indicating reliability. They felt more confident dealing with businesses that maintained a professional online presence.

Several participants said they avoided connecting with companies because they were concerned about data security as shown in figure 3.

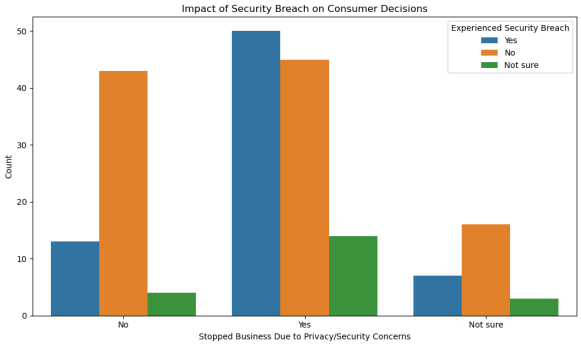

Figure 3. *Q: Have you ever stopped doing business with a company due to privacy/security concerns?*

The reputation of SMEs, the initial appearance of their website, and the business's history have significantly influenced customer decisions. Additionally, word-of-mouth and social media played a crucial role in shaping consumer opinions, emphasizing the extent of maintaining a positive reputation.

All respondents emphasized the need for SMEs to provide clear information about how they handle, and secure personal data. They valued transparency, and clear explanations of data protection procedures, implying that organizations should invest in easy-to-follow privacy policies.

Participants recalled instances where effective communication—such as the implementation of two-factor authentication—enhanced their overall trust. On the other hand, inadequate communication regarding data breaches diminished their confidence in the business.

Around 25% of interviewees, reported experiencing a data breach or cyber-related issue with a small or medium-sized enterprise (SME). The way these organizations respond to data breaches significantly affects consumer trust. Quick solutions and open communication are essential for maintaining that trust. Respondents recognized that data breaches could happen, which led them to be more cautious when sharing personal information, as illustrated in figure 4.

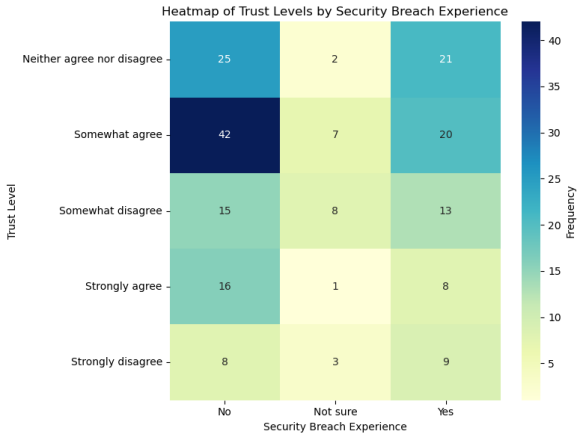

Figure 4. *Q: I trust most companies will protect, and secure my data against breaches or attacks. I have been the victim of a security breach myself.*

Respondents articulated various expectations for SMEs to boost their confidence in data security, by recommending a substantial investment in cybersecurity projects. Security first over cost reductions, thus increasing the overall profit. While some respondents showed a cautious enthusiasm about using AI to improve cybersecurity, they pointed out its potential benefits and reliability problems.

Key Insights from the conducted interviews

- ***Andrea's Interview***: Shared multiple experiences with data breaches that made her cautious about sharing her information; she highlighted the necessity for effective breach management.
- ***Anonymous Interview***: Expressed a preference for businesses using on-premises servers over cloud computing, believing it enhances security by being less accessible to external entities.
- ***Luca's Interview***: Stressed the need for businesses to be transparent about their data handling practices to build trust.
- ***Alexandra's Interview***: Emphasized the importance of two-factor authentication for online accounts and payments as it adds an extra layer of security.

5. Discussion

The findings presented in this research paper underscore the substantial influence of robust cybersecurity practices on consumer confidence, and the economic outcomes of SMEs. This part endeavours to synthesize the principal findings, juxtapose them with existing literature, elucidate practical implications, acknowledge limitations, and propose avenues for future research.

The quantitative analysis indicates that SMEs implementing advanced cybersecurity measures—such as multi-factor authentication, and data encryption—experience a marked decrease in data breaches, and financial repercussions. This observation substantiates the hypothesis that stringent cybersecurity practices can enhance consumer trust and, improve economic performance. Also, the assumption holds on qualitative interviews, as consumers are more prone to trust and interact with SMEs which have concrete cyber security policies.

5.1. Comparison of Existing Literature

While comparing previous findings with mine I observed that they were in line. In this regard,Sharma and Lijuan (2020)found that trust levels increased with the rise of customers' feeling of security associated with a particular e-business context. In the same manner (Kim et al., 2019) have also reported that a considerable market share is reported to avoid brands that were branded as having security vulnerabilities. This study advances the discourse by providing empirical evidence pertinent to the SME sector, thereby emphasizing the economic advantages associated with investments in cybersecurity.

5.2. Implications for SMEs

The practical implications of this study for SMEs are: Investments in effective cybersecurity are essential for business growth. It is not just a defensive measure, but also a legal requirement that fosters consumer trust, leading to increased sales and investment interest.

5.3. Limitations

The study acknowledges several limitations. Despite the diversity of the sample, it is possible that not all SMEs, especially those located in different regions or areas, are adequately represented. Additionally, the reliance on self-reported data from surveys and interviews may introduce bias. Future research should consider utilising a broader sample or conducting a longitudinal study to assess the long-term impact of cybersecurity investments.

Different industries may face distinct chances and threats, and future research efforts can examine the industry-specific effects of cybersecurity investment. Longitudinal studies would be useful in further clarifying the long-term net economic gain arising from HAVOC-stronger cybersecurity measures.

6. Conclusion

Ultimately, this study highlights the importance of investing in cybersecurity to achieve better business outcomes and boost consumer trust in SMEs. The findings indicate that SMEs safeguard their digital assets by adopting advanced cybersecurity solutions.

Both quantitative, and qualitative data collectively show that robust cybersecurity practices lead to fewer data breaches while enhancing consumer trust, and providing economic improvements in performance

for SMEs. These findings underscore the importance of cybersecurity as a strategic investment. For SMEs, the implications are clear, investing in cybersecurity is essential for building consumer trust and achieving economic success. SMEs should adopt comprehensive cybersecurity measures, prioritize transparency in data handling, and communicate their efforts effectively to consumers. In today's digital marketplace, cybersecurity is more than just a protective measure; it is a key driver of business success. SMEs that show concern regarding cyberspace security engage in securing their operations and preparing themselves for future growth scenarios. With volatile cyber threats, consistent infusion into security-providing technologies will remain critical for winning customers' trust and generating sustainable economic results.

7. Solutions

7.0.1. Policy Recommendations

The escalating threats in the digital landscape mandate SMEs to adopt robust policies, and changes in their operational strategies. To this end, it could be argued that effective policies should ensure sufficient access to resources, support, and frameworks that would enable them to develop strong cybersecurity capabilities. The following recommendations highlight specific areas that need government intervention, and regulation to promote cybersecurity in SMEs:

7.0.2. Mandatory Minimum Cybersecurity Standards

Setting a set of standards for cybersecurity for SMEs would be a step in the right direction as it would set a threshold every business should meet. These would form parts of more stringent data protection laws like the "General Data Protection Regulation (GDPR)" (2018), and target sections including timely installation of software patches, timely data backups, and creation of passwords. It would also help policymakers, ensuring that even the tiniest companies do not overlook security concerns at the outset.

Many SMEs cannot handle major data breaches or cyberattacks. Governments could establish centralized incident response teams or help desks specifically for SMEs, offering guidance, and technical assistance during a breach. This support could be extended through partnerships with cybersecurity firms offering discounted or emergency services to SMEs in critical situations.

7.0.3. Ethical considerations

The ethical standards for small and medium-sized enterprises (SMEs) are crucial, especially when the outcome is protecting customer information and maintaining trust. SMEs must handle customer data with high security and diligence to prevent potential vulnerabilities that organized criminals could exploit. Failure to meet these responsibilities can lead to severe consequences, including damage to their reputation and a significant loss of public trust.

7.0.4. Customer Data Consent

SMEs must obtain explicit consent from consumers to collect and use their data ethically. Providing clear privacy policies is essential to enabling consumers to make informed choices.

7.0.5. Attention to Security Threats

SMEs cannot afford to be passive regarding cybersecurity threats; they must actively address these risks with robust, up-to-date security measures, and routine assessments. Neglecting to manage these risks is unacceptable when it comes to the welfare of customers.

7.0.6. Responsibility for Breaches

SMEs should recognize the potential for data breaches as a real threat. When such incidents happen, timely communication with customers and sincere efforts to resolve the situation are essential.

8. Bibliography

References

Amir, E., et al. (2018). The financial impact of cybersecurity investments. *Journal of Financial Economics*, *29*(2), 123–145.

General data protection regulation (gdpr) [Accessed: 2024-09-17]. (2018). European Union. https://gdpr.eu/

Accenture. (2019). *Ninth annual cost of cybercrime study* (Annual report) (Accessed: 2024-09-17). Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Kim, J., et al. (2019). Consumer reactions to data breaches. *Journal of Consumer Research*, *46*(4), 123–140.

Cost of a data breach report 2020 [Accessed: 2024-09-17]. (2020). Ponemon Institute. https://www.ibm.com/security/data-breach

Forum, W. E. (2020). *The global risks report 2020* (Accessed: 2024-10-22). https://www.weforum.org/reports/the-global-risks-report-2020

Gartner. (2020). *Cybersecurity predictions 2020* (Accessed: 2024-10-22). https://www.gartner.com/en/newsroom/press-releases/2020

Sharma, S. K., & Lijuan, W. (2020). The effects of online service quality of e-commerce websites on user satisfaction. *The Electronic Library*, *38*(3), 549–564. https://doi.org/10.1108/EL-10-2019-0240

Deloitte. (2021). *The impact of cybersecurity on consumer behavior* (Accessed: 2024-10-22). https://www2.deloitte.com/global/en/pages/risk/articles/cybersecurity-consumer-behavior.html

IBM. (2021). *Cost of a data breach report 2021* (Accessed: 2024-10-22). https://www.ibm.com/security/data-breach

Kurpjuhn, T. (2021). Cybersecurity as a competitive advantage for smes. *Journal of Business Strategy*, *42*(5), 34–45.

Tawileh, W., et al. (2021). Cybersecurity challenges for smes. *Journal of Cybersecurity*, *5*(2), 123–145.

Verizon. (2021). 2021 data breach investigations report [Accessed: 2024-10-22]. https://www.verizon.com/business/resources/reports/dbir/

Alharbi, A., et al. (2022). Transparency in data handling and consumer trust. *Journal of Business Ethics*, *30*(1), 89–105.

Company, M. bibinitperiod. (2022). *Holistic cybersecurity strategies for smes* (Accessed: 2024-10-22). https://www.mckinsey.com/business-functions/risk/our-insights/holistic-cybersecurity-strategies-for-smes