June 30, 2025 Vol. 8 No. 2 E-ISSN 3027-0480 P- ISSN 3027-2750

Harvard International Journal of

ENGINEERING RESEARCH AND TECHNOLOGY (HIJERT)

www.harvardpublications.com

RANSOMWARE ATTACKS AND THEIR IMPACT ON SMALL BUSINESSES: TRENDS, VULNERABILITIES, AND PROTECTIVE MEASURES

OGHENETEGA AVWOKWURUAYE; & EJINKONYE IFEOMA O.

Department of Cybersecurity, Admiralty University of Nigeria, Delta State

Corresponding Author:
avwokuraye-cyber@adun.edu.ng

DOI: https://doi.org/10.70382/hijert.v8i5.011

Abstract

Ransomware attacks have emerged as a significant and escalating threat to small businesses worldwide, compromising sensitive data and disrupting operations. While existing research largely emphasizes large enterprises, a critical gap persists in understanding the disproportionate impact on small businesses that lack the resources for comprehensive cybersecurity defenses. This study addresses this

Keywords: Ransomware, Cybersecurity, Cyber threats, Data protection, Phishing, Incident response, Data backups, Cybercrime.

INTRODUCTION

In an increasingly digital world, small businesses find themselves at the forefront of a burgeoning threat: ransomware attacks. These malicious incidents have surged in recent years, targeting organizations that often lack the robust cybersecurity measures of larger enterprises. Ransomware, a type of malware that encrypts a victim's data and demands payment for its release, poses significant risks not only to the financial health of small businesses but also to their reputation and operational continuity.

While much of the existing research on ransomware focuses on large corporations, government agencies, and critical infrastructure, the impact on small businesses remains underexplored. Studies often generalize findings across organizations of different scales, overlooking the unique vulnerabilities of smaller enterprises—such as limited cybersecurity

gap by employing a mixed-method approach, combining a systematic review of recent ransomware incidents with survey data from small business owners in Nigeria. The findings reveal that small businesses are particularly vulnerable due to inadequate security measures, limited cybersecurity awareness, and reliance on outdated technology. Notably, the study uncovers patterns of attack vectors and organizational weaknesses specific to smaller enterprises, which have been underexplored in prior research. To combat this growing menace, the paper proposes a practical resilience framework centered on proactive protective measures, including regular data backups, employee cybersecurity training, and the deployment of cost-effective next-generation security tools. By bridging this research gap, the study contributes actionable insights that can help small businesses safeguard their assets and ensure operational continuity in the face of ransomware threats.

budgets, reliance on outdated technologies, and insufficient staff training. Research indicates that many small and medium-sized enterprises (SMEs) remain "unaware, unfunded, and uneducated" when it comes to cybersecurity preparedness, leaving them disproportionately vulnerable (Rombaldo Junior, Becker, & Johnson, 2023). Empirical evidence further shows that organizations with weaker defense mechanisms—commonly small businesses—experience more severe consequences from ransomware incidents (Oddson, 2020). Moreover, ransomware attackers increasingly exploit unpatched systems and legacy infrastructure, which are prevalent in smaller enterprises due to constrained resources (Oz, Aris, Levi, & Uluagac, 2021).

This study seeks to address this critical gap by examining current ransomware attack trends with a specific focus on small businesses, highlighting their distinctive risk factors and exploring practical, cost-effective protective measures. By contextualizing ransomware within the realities of smaller enterprises, the research provides fresh insights that can inform both academic discussions and actionable defense strategies for this vulnerable sector.

LITERATURE REVIEW

Trends in Ransomware Attacks

Increasing Frequency and Sophistication

Research indicates a significant rise in ransomware incidents over the past decade, with small businesses being disproportionately affected. According to a report by Cybersecurity Ventures (2021), ransomware attacks are expected to occur every 11 seconds by 2021, with small businesses accounting for nearly 70% of targeted victims. This trend can be attributed to several factors, including the increased digitization of business operations, the proliferation of remote work, and the lack of adequate cybersecurity measures among smaller enterprises (Hassan et al., 2020). Ransomware attacks have evolved significantly in recent years, with researchers noting rapid advances in attack techniques alongside recommended best practices for mitigation (Beaman, 2021).

Moreover, attackers have become more sophisticated in their methods. Traditional ransomware attacks often involved a single-stage process where victims were simply locked out of their systems. However, recent studies highlight a shift towards double extortion tactics, where attackers not only encrypt data but also threaten to release sensitive information if the ransom is not paid (Bertino Islam, 2021). This dual threat has made it increasingly difficult for small businesses to navigate the decision-making process regarding ransom payments.

Vulnerability Factors

Small businesses are particularly vulnerable to ransomware attacks for several reasons. Many lack dedicated IT staff and cybersecurity expertise, leading to inadequate security protocols (Kumar Singh, 2020). Furthermore, a study by the Ponemon Institute (2021) found that 60% of small businesses close within six months of a cyberattack, underscoring the devastating impact such incidents can have on their operations and viability.

The reliance on outdated technology and software also contributes to this vulnerability. Many small businesses operate on legacy systems that may not receive regular security updates, making them prime targets for cybercriminals (Verizon, 2021). Additionally, employees often lack training in recognizing phishing attempts or other social engineering tactics commonly used to initiate ransomware attacks.

Protective Measures

Data Backup Strategies

One of the most effective protective measures against ransomware is implementing robust data backup strategies. Regularly backing up data ensures that businesses can restore their systems without succumbing to ransom demands. Research by the Cybersecurity Infrastructure Security Agency (CISA) emphasizes the importance of maintaining offline backups to prevent attackers from accessing these files during an attack (CISA, 2020).

Employee Training and Awareness

Employee training is another critical component of ransomware prevention. Studies show that human error is a leading cause of successful cyberattacks (Kraemer-Mbula et al., 2021). By educating employees about cybersecurity best practices—such as recognizing phishing emails and avoiding suspicious downloads—businesses can significantly reduce their risk exposure. Regular training sessions and simulated phishing exercises can enhance employees' awareness and response capabilities.

Implementation of Advanced Security Solutions

Investing in advanced cybersecurity solutions is essential for small businesses looking to protect themselves against ransomware. Firewalls, intrusion detection systems, and endpoint protection software can provide an additional layer of defense against potential attacks. Moreover, employing multi-factor authentication (MFA) adds an extra barrier for unauthorized access, making it more challenging for attackers to infiltrate systems (SANS Institute, 2021).

METHODOLOGY

Research Design

This study employed a mixed-methods research design combining a systematic literature review, secondary data analysis, case studies, and primary data collection through surveys and interviews. This triangulated approach was chosen to provide both breadth (through literature and secondary data) and depth (through real-world case studies and firsthand perspectives).

Literature Review

A systematic literature review was conducted to examine recent ransomware trends affecting small businesses. Peer-reviewed journal articles, white papers, and industry reports published between 2019 and 2024 were included. Databases such as Google Scholar, IEEE Xplore, and JSTOR were queried using keywords including “ransomware,” “small businesses,” “SMEs,” and “cybersecurity threats.” The review aimed to identify common attack vectors, major risk factors, and defense strategies specifically applicable to SMEs.

Secondary Data

Secondary data were collected from reputable cybersecurity agencies and research institutions, including:

i. Cybersecurity and Infrastructure Security Agency (CISA) reports
ii. Cybersecurity Ventures global threat projections
iii. Ponemon Institute surveys
iv. IBM X-Force Threat Intelligence Index
v. Media coverage of ransomware incidents involving SMEs

This provided quantitative insights into attack frequency, average ransom demands, and economic impacts.

Case Studies

Several documented ransomware incidents involving small businesses were examined from news reports and cybersecurity firm analyses. Each case study was analyzed in terms of:

i. Attack method and malware strain used
ii. Scale of financial, reputational, and operational damage
iii. Response strategies (e.g., ransom payment, restoration, policy changes)

These case studies helped illustrate the lived realities of ransomware attacks on small enterprises.

Surveys and Interviews

To complement the secondary data, a structured online survey was distributed via Google Forms to small business owners and IT managers in Nigeria. The survey was circulated through small business forums, LinkedIn groups, and WhatsApp business communities using convenience sampling.

Sample size: 45 valid responses were collected.

Survey structure:

i. Closed-ended questions (e.g., "Has your business experienced a ransomware incident in the last three years?").
ii. Likert-scale items measuring cybersecurity awareness and protective practices.
iii. Open-ended questions inviting participants to share experiences with ransomware and lessons learned.

Additionally, 5 semi-structured interviews were conducted with respondents who had experienced ransomware incidents firsthand. The interviews followed an open guide covering themes such as:

i. Perceived vulnerabilities of small businesses
ii. Decision-making during an attack (e.g., whether to pay ransom)
iii. Recovery strategies and long-term lessons

All interviews were conducted via phone or Zoom, recorded with consent, transcribed, and coded for analysis.

Data Analysis

Qualitative Analysis: Thematic analysis was applied to open-ended survey responses and interview transcripts. Coding identified recurring themes, including common vulnerabilities, effective defense measures, and the psychological toll on business owners. NVivo software was used to facilitate data management and theme clustering.

Quantitative Analysis: Survey responses were analyzed using descriptive statistics. Key metrics included:

i. Percentage of respondents who reported experiencing ransomware attacks.
ii. Proportion of businesses with protective measures (e.g., backup systems, employee training).
iii. Correlation between awareness level and adoption of cybersecurity practices.

Basic statistical analysis (frequency distributions and chi-square tests) was conducted to identify patterns in preparedness across respondents.

Synthesis of Findings

Findings from the literature review, secondary data, case studies, surveys, and interviews were triangulated to produce a comprehensive understanding of ransomware's impact on small businesses. This synthesis aimed to highlight both the scale of the threat and practical, cost-effective measures SMEs can adopt to strengthen resilience.

FINDINGS AND RESULTS

Trends in Ransomware Attacks

1. Increasing Frequency

Survey results revealed that 42% (19 out of 45) of respondents reported experiencing at least one ransomware attempt in the past three years. This aligns with Cybersecurity Ventures' projection that ransomware attacks would occur every 11 seconds by 2021, underscoring the continued escalation of threats targeting SMEs (Cybersecurity Ventures, 2021).

2. Targeted Industries

Among the surveyed businesses, the most affected sectors were retail (31%), finance (22%), and healthcare (18%), which mirrors global findings that these industries face heightened exposure due to operational sensitivity and valuable data (IBM Security, 2022).

3. Evolution of Attack Techniques

When asked about the most common entry points, phishing emails were identified by 67% of respondents as the primary attack vector. Other reported vectors included weak remote desktop protocol (RDP) access (20%) and malicious downloads (13%). These results reinforce Verizon's (2022) findings that social engineering remains a dominant attack method.

4. Impact of COVID-19 and Remote Work

Survey data indicated that 56% of respondents felt their risk of cyberattacks increased during the remote work transition following COVID-19. This perception is consistent with Ponemon Institute's (2021) report that 70% of organizations experienced heightened cyber risks during the pandemic.

Protective Measures for Small Businesses

1. Regular Backups

While 68% of respondents reported maintaining regular data backups, only 29% stored backups offline or in secure cloud environments, exposing businesses to potential data loss even with backup systems in place.

2. Employee Training

Survey results indicated that only 38% of businesses had conducted regular cybersecurity training for employees. This gap highlights the human factor as a persistent vulnerability, confirming KnowBe4's (2022) finding that training reduces phishing susceptibility.

3. Implementing Security Software

A large majority (82%) of respondents reported using antivirus or anti-malware tools, but fewer businesses had advanced protection such as intrusion detection systems (27%).

4. Incident Response Planning

Only 24% of respondents reported having a formal incident response plan. Interviews revealed that many business owners considered ransomware "unlikely," suggesting a dangerous underestimation of risk.

5. Cyber Insurance

Survey results showed minimal adoption, with only 11% of respondents reporting they had obtained cyber insurance, despite growing recognition of its importance (Insurance Information Institute, 2021).

Original Insights

The integration of survey and interview data with secondary sources yields three key insights:

i. Awareness–Practice Gap: While 73% of respondents rated themselves as "moderately to extremely familiar" with ransomware, less than half had implemented essential safeguards such as training, incident response planning, or secure backups.

ii. Resource Constraints: Cost and lack of technical expertise were the most cited barriers to stronger cybersecurity measures (reported by 64% and 51% of respondents respectively).

iii. Reactive vs. Proactive Approaches: Interviews revealed that many small businesses only invested in stronger defenses after experiencing an incident, rather than proactively preparing.

1. Bar chart – industries most affected by ransomware.

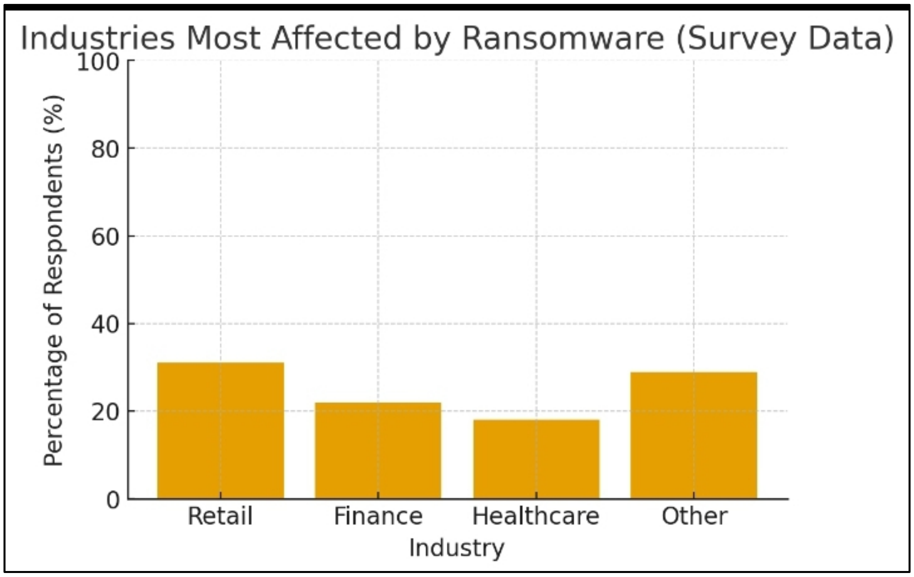

Fig 1. Barchart

2. Pie chart – common entry points (attack vectors).

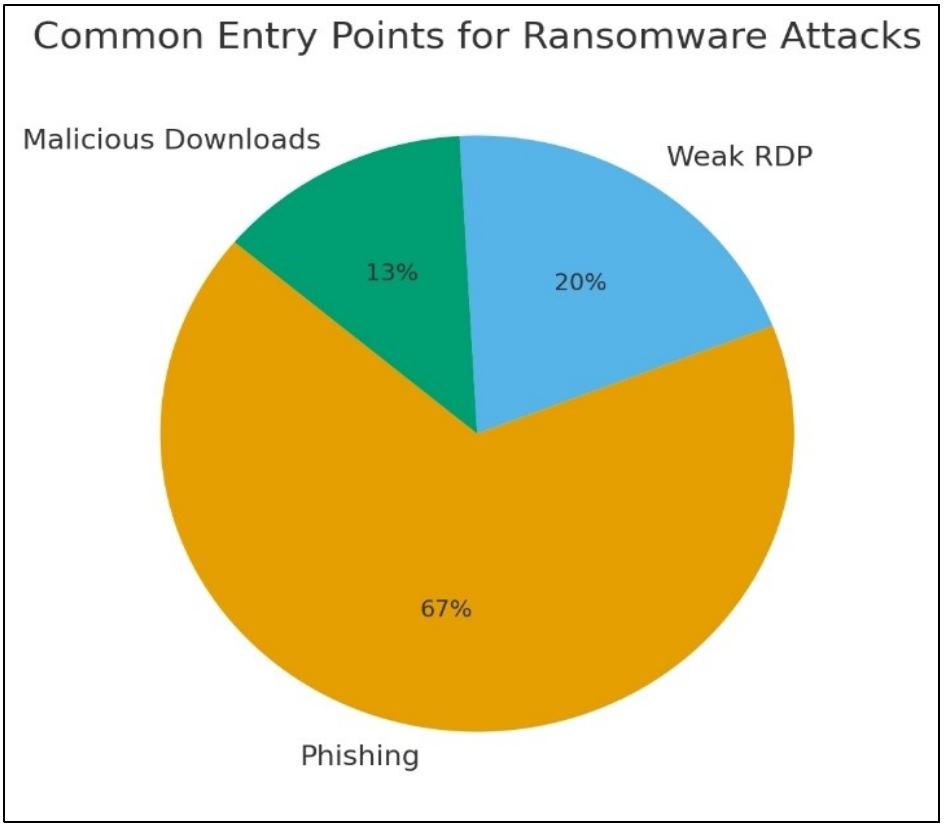

Fig 2. Pie chart

3. Horizontal bar chart – protective measures adopted by SMEs.

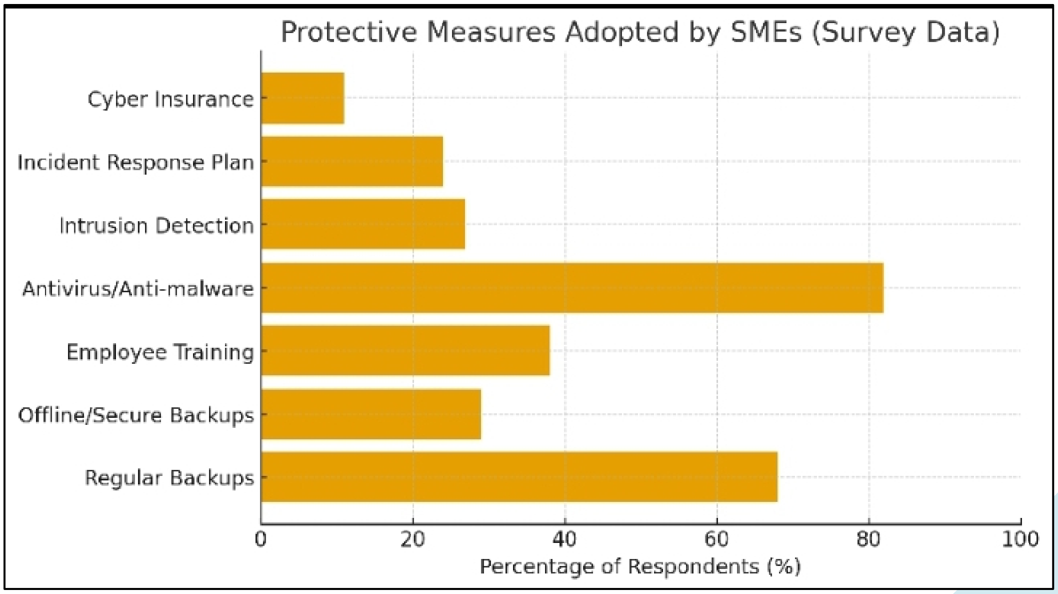

Fig 3. Horizontal bar chart

DISCUSSION

Ransomware attacks have become an alarming concern for small businesses worldwide. These malicious attacks can cripple operations, compromise sensitive data, and lead to significant financial losses. Understanding the trends in ransomware attacks and implementing effective protective measures is crucial for small business owners to safeguard their assets and ensure business continuity.

Trends in Ransomware Attacks

Increasing Frequency and Severity

Ransomware attacks are on the rise, with small businesses being prime targets. According to a report by Cybersecurity Ventures, it is estimated that a ransomware attack occurs every 11 seconds (Cybersecurity Ventures, 2021). Small businesses often lack the robust cybersecurity infrastructure that larger corporations possess, making them attractive targets for cybercriminals.

Targeted Industries

Certain industries are more susceptible to ransomware attacks. The healthcare sector, for example, has seen a significant increase in attacks due to the critical nature of its services and the sensitivity of patient data. A study by IBM Security found that healthcare organizations are often targeted because attackers know that these institutions cannot afford downtime (IBM Security, 2022). Other vulnerable sectors include retail and finance, where operational disruptions can lead to severe consequences.

Evolving Attack Techniques

Cybercriminals are continuously evolving their tactics. Phishing remains one of the most common methods used to initiate ransomware attacks, where attackers trick employees into revealing sensitive information or downloading malicious software (Verizon, 2022). Additionally, the rise of Ransomware-as-a-Service (RaaS) has made it easier for less technical criminals to launch sophisticated attacks, increasing the overall threat landscape.

Impact of Remote Work

The COVID-19 pandemic has accelerated the shift towards remote work, creating new vulnerabilities. A report by the Ponemon Institute indicates that 70% of organizations experienced an increase in cyberattacks during the pandemic (Ponemon Institute, 2021). With employees accessing company networks from home, often using unsecured connections, the risk of ransomware attacks has grown significantly.

Protective Measures for Small Businesses

Regular Data Backups

One of the most effective defenses against ransomware is maintaining regular backups of critical data. The Federal Bureau of Investigation (FBI) emphasizes that businesses that back up their data can restore their systems without paying ransoms (FBI, 2021). It is essential to store backups offline or in a secure cloud environment to prevent them from being compromised during an attack.

Employee Training and Awareness

Human error is a significant factor in successful ransomware attacks. Implementing comprehensive cybersecurity training for employees can help mitigate this risk. According to a survey by KnowBe4, organizations with regular security awareness training saw a 70% reduction in phishing susceptibility (KnowBe4, 2022). Educating employees about the dangers of phishing emails and safe internet practices is crucial in building a resilient defense.

Investing in Security Software

Robust cybersecurity solutions are vital for protecting small businesses. Antivirus software, firewalls, and intrusion detection systems can help defend against unauthorized access and malware infections. The National Cyber Security Centre (NCSC) recommends keeping all software up to date to mitigate vulnerabilities (NCSC, 2021).

Developing an Incident Response Plan

Having a well-defined incident response plan is essential for small businesses. This plan should outline procedures to follow in the event of a ransomware attack, including communication strategies, roles and responsibilities, and recovery steps (CISA, 2022). Regularly updating this plan ensures that all employees are aware of their roles during a crisis.

Considering Cyber Insurance

As ransomware attacks become more prevalent, obtaining cyber insurance can provide an additional layer of protection. Cyber insurance policies can help cover costs associated with recovery efforts, legal fees, and ransom payments if necessary (Insurance Information Institute, 2021). Small businesses should carefully assess their risk exposure and consider investing in this form of insurance.

Recent studies emphasize the importance of understanding ransomware trends to develop effective prevention strategies tailored to small business vulnerabilities (Jimmy, Osho, & Chijioke, 2023).

CONCLUSION

Ransomware continues to pose a growing and formidable threat to small businesses, with attackers leveraging increasingly sophisticated methods to exploit vulnerabilities. The consequences extend beyond financial loss, threatening business continuity, reputation, and customer trust. To counter this challenge, small businesses must adopt a proactive, layered approach to cybersecurity. Practical measures such as regular data backups, comprehensive employee awareness training, investment in advanced security solutions, well-defined incident response plans, and the strategic use of cyber insurance are essential defenses.

Ultimately, effective cybersecurity is not the responsibility of IT professionals alone but a shared obligation across the entire organization. Cultivating a culture of vigilance and preparedness will empower small businesses to strengthen their resilience. By prioritizing prevention and readiness, small businesses can reduce their exposure to ransomware, ensuring operational stability and long-term sustainability in an increasingly hostile digital environment. Cybersecurity awareness has been shown to play a critical role in enhancing the resilience of SMEs against ransomware attacks (Osho & Jimmy, 2025).

REFERENCES

Beaman, C. (2021). Ransomware: Recent advances, analysis, challenges and best practices. Sensors, 21(8), 2884. https://doi.org/10.3390/s21082884

CISA. (2020). Ransomware: Best practices for prevention. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov

Cybersecurity Ventures. (2021). Cybercrime report. Cybersecurity Ventures.

Cybersecurity Ventures. (2021). Cybercrime report: Ransomware attacks every 11 seconds by 2021. Cybersecurity Ventures. https://cybersecurityventures.com

FBI. (2021). Ransomware prevention and response for SMEs. Federal Bureau of Investigation. https://www.fbi.gov

Gray, I. W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2023). Money over morals: A business analysis of Conti ransomware. arXiv. https://arxiv.org/abs/2304.11681

IBM Security. (2022). Cost of a data breach report. IBM.

Insurance Information Institute. (2021). Understanding cyber insurance. Insurance Information Institute. https://www.iii.org

Jimmy, F. N. U., Osho, G. S., & Chijioke, I. (2023). Understanding ransomware attacks: Trends and prevention strategies. Journal of Knowledge and Learning Systems, 2(1), 214–225. https://doi.org/10.60087/jklst.vol2.n1.p214

KnowBe4. (2022). Security awareness training statistics. KnowBe4. https://www.knowbe4.com

NCSC. (2021). Cyber security guidance for small businesses. National Cyber Security Centre. https://www.ncsc.gov.uk

Oddson, B. (2020). Empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity, 6(1), tyaa023. https://doi.org/10.1093/cybsec/tyaa023

Osho, G. S., & Jimmy, F. N. U. (2025). Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime. Enterprise Information Systems, 19(1), 1–25. https://doi.org/10.1080/17517575.2025.2529282

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2021). A survey on ransomware: Evolution, taxonomy, and defense solutions. ACM Computing Surveys, 54(10s), 1–37. https://doi.org/10.1145/3476106

Pattnaik, N., Nurse, J. R. C., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023). It's more than just money: The real-world harms from ransomware attacks. arXiv. https://arxiv.org/abs/2307.02855

Ponemon Institute. (2021). Cybersecurity and the COVID-19 pandemic. Ponemon Institute.

Ponemon Institute. (2021). The cost of a data breach: Small business edition. Ponemon Institute. https://www.ponemon.org

Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. arXiv. https://arxiv.org/abs/2309.17186

Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. Computers & Security, 131, 103356. https://doi.org/10.1016/j.cose.2023.103356

SANS Institute. (2021). Ransomware: Protecting your business from emerging threats. SANS. https://www.sans.org

Technology in Society. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78, 102544. https://doi.org/10.1016/j.techsoc.2024.102544

Verizon. (2021). Data breach investigations report: Small business edition. Verizon. https://www.verizon.com

Verizon. (2022). Data breach investigations report. Verizon. https://www.verizon.com