

Impact of Cybersecurity Threats on E-Businesses in Emerging Economies: A Comprehensive Study

¹Okeke Gloria Ifunanya and ²Jimoh Ibrahim Bamidele

^{1,2}. Office Technology and Management Department,
The Federal Polytechnic, Ilaro, Ogun State, Nigeria

¹ibrahim.jimoh@federalpolyilaro.edu.ng and ²gloria.okeke@federalpolyilaro.edu.ng
08124772594 and 08065075070

Abstract:

This paper explores the profound impact of cybersecurity threats on e-businesses operating in emerging economies. Cybersecurity threats, ranging from malware to ransomware and phishing attacks, pose significant risks to the financial stability, operational continuity, and reputation of e-businesses. The Resource Dependence Theory provided the theoretical framework for this study. The survey method was adopted, and 150 respondents were purposively selected to form the sample population. An online survey was used to source for data. The collected data were presented and analyzed using Statistical Package for Social Sciences (SPSS). The results obtained revealed that e-businesses frequently encounter such threats and that phishing do not pose a significant risk to their e-business. It was revealed that majority of incidents they face stem from external sources in which customer data is not frequently targeted in cybersecurity attacks on their business and that cybersecurity threats faced by their business are more severe compared to businesses in developed economies. The study recommended that e-businesses should prioritize cybersecurity, educate their employees on best practices, Government should focus on strengthening cybersecurity measures, collaborating with businesses and other agencies, and investing in cybersecurity education and training e-businesses should Keep up-to-date with the latest cybersecurity trends and technologies, and regularly assess their systems for vulnerabilities

Keywords: Cybersecurity, Cybersecurity threats, E-businesses, Emerging economies, Mitigation strategies, Regulations.

Introduction

In the fast-evolving landscape of digital commerce, the burgeoning realm of e-businesses in emerging economies stands as a testament to the transformative power of technology (Kshetri, 2017). Enabled by the internet and digital platforms, e-businesses have transcended geographical boundaries, allowing for unprecedented connectivity, scalability, and accessibility (Dwivedi et al., 2019). However, amidst the promise of growth and prosperity, lurk the shadows of cybersecurity threats, casting a looming specter over the very foundations of these enterprises (Purkait et al., 2020).

Cybersecurity threats, encompassing a myriad of malicious activities such as data breaches, ransomware attacks, and phishing scams, pose significant risks to the integrity, confidentiality, and availability of electronic systems and data (Hassan et al., 2020). With e-businesses reliant on digital infrastructure for their operations, the symbiotic relationship between cybersecurity threats and e-businesses becomes evident. As e-businesses continue to proliferate in emerging economies, fueled by factors such as increasing internet penetration, smartphone adoption, and digital literacy, the magnitude and complexity of cybersecurity threats likewise escalate, necessitating a comprehensive understanding of their impact (Rocha et al., 2017).

The interconnectedness of e-businesses with the digital ecosystem renders them susceptible to a diverse array of cybersecurity threats. Malicious actors, ranging from individual hackers to sophisticated cybercriminal syndicates, exploit vulnerabilities in software, networks, and human behavior to infiltrate, compromise, and exploit e-businesses for financial gain, political motives, or personal vendettas (Bhowal et al., 2019). The ramifications of cybersecurity threats extend far beyond the confines of individual enterprises, reverberating across supply chains, financial markets, and societal trust (Alrawi et al., 2021).

As e-businesses serve as conduits for the exchange of sensitive information, including customer data, financial transactions, and proprietary intellectual property, they become prime targets for cyberattacks seeking to exploit vulnerabilities in their digital infrastructure (Kshetri, 2020). The repercussions of successful cyberattacks can be dire, leading to financial losses, reputational damage, legal liabilities, and regulatory sanctions (Gordon et al., 2017). Moreover, the erosion of consumer trust resulting from data breaches and privacy violations can have lasting implications on the viability and sustainability of e-businesses in emerging economies (Choudhary et al., 2018).

Research Questions

- I. What is the effect of Cybersecurity Threats on E-Businesses in Emerging economies?
- ii. What is the perception of E-businesses towards cyber security threats in Emerging Economies?

Literature Review

Cybersecurity threats

Cybersecurity threats, as defined by various authors in past research, encompass a wide spectrum of malicious activities aimed at exploiting vulnerabilities in digital systems, networks, and information assets. According to Gordon, Loeb, and Lucyshyn (2017), cybersecurity threats refer to potential risks and vulnerabilities within the digital infrastructure that may be exploited by malicious actors to gain unauthorized access, compromise data integrity, or disrupt normal operations. These threats can manifest in various forms, including malware attacks, phishing scams, denial-of-service (DoS) attacks, and insider threats, posing significant challenges to the security and resilience of digital ecosystems (Gordon et al., 2017).

Moreover, cybersecurity threats are dynamic and continually evolving in response to advancements in technology and changes in the threat landscape. As highlighted by Purkait, Sen, Datta, and Sen (2020), the proliferation of new attack vectors, such as ransomware, zero-day exploits, and social engineering techniques, underscores the adaptive nature of cyber threats and the need for proactive measures to mitigate risks. Additionally, the interconnected nature of digital networks and the increasing reliance on cloud computing and Internet of Things (IoT) devices have expanded the attack surface, further amplifying the scope and complexity of cybersecurity threats (Purkait et al., 2020).

The impact of cybersecurity threats extends beyond individual organizations, permeating across sectors and geographical boundaries. Rocha, Abreu, Correia, and Figueiredo (2017) emphasize the transnational nature of cyber threats, highlighting the interconnectedness of global supply chains, financial markets, and critical infrastructure as potential targets for cyberattacks. Furthermore, cybersecurity threats pose significant economic, societal, and geopolitical implications, including financial losses, reputational damage, erosion of consumer trust, and national security concerns (Rocha et al., 2017). Addressing these challenges requires a holistic approach, involving collaboration between governments, industry stakeholders, academia, and international organizations to enhance cybersecurity capabilities, promote information sharing, and establish norms and regulations governing cyberspace (Gupta, Bag, Jena, & Kumar, 2018).

E-businesses in Emerging Economies

E-businesses, or electronic businesses, refer to the use of Internet technologies to conduct business operations. This encompasses a range of activities such as buying and selling goods and services, servicing customers, and collaborating with business partners. E-businesses leverage digital platforms to enhance efficiency, reach a broader audience, and reduce costs associated with traditional business processes (Chaffey, 2015). They include e-commerce platforms, online service providers, and digital marketplaces, all contributing to a more connected and efficient economy.

There are several types of e-businesses, each serving different functions. Business-to-consumer (B2C) e-commerce involves businesses selling directly to consumers, exemplified by companies like Amazon and Alibaba. Business-to-business (B2B) e-commerce refers to transactions between businesses, such as manufacturers and wholesalers. Consumer-to-consumer (C2C) platforms, like eBay, enable consumers to sell to each other. Additionally,

Consumer-toBusiness (C2B) models, such as those used by freelancers on platforms like Upwork, allow individuals to offer services to businesses (Turban et al., 2018). Each type of e-business facilitates unique interactions and transactions, driving economic growth and innovation.

In emerging economies, e-businesses play a crucial role in economic development. They provide access to global markets, enabling small and medium-sized enterprises (SMEs) to compete internationally and boost local economies (UNCTAD, 2019). E-businesses also foster financial inclusion by offering digital payment solutions, thus reaching unbanked populations. Moreover, they create employment opportunities and contribute to skill development in technology and digital literacy. By bridging the gap between urban and rural areas, e-businesses help reduce economic disparities and support sustainable growth in emerging economies (Kshetri, 2020).

Theoretical Framework

Resource Dependence Theory

Resource dependence theory (RDT) posits that organizations are influenced by their external environment, particularly in terms of the resources they require to survive and thrive (Pfeffer & Salancik, 1978). According to RDT, organizations strive to secure access to critical resources, such as capital, technology, and information, to reduce uncertainty and maintain autonomy in their operations. However, organizations are also vulnerable to external dependencies, whereby their ability to procure and control resources is contingent upon relationships with external actors, including suppliers, customers, regulators, and competitors. In the context of e-businesses in emerging economies, RDT provides insights into how these enterprises are susceptible to cybersecurity threats due to their reliance on

digital infrastructure and information resources, which are subject to external dependencies and vulnerabilities.

Cybersecurity threats pose significant challenges to e-businesses in emerging economies by disrupting the flow of critical resources and undermining organizational resilience. As ebusinesses rely heavily on digital technologies and online platforms to conduct transactions, communicate with stakeholders, and manage operations, they become prime targets for cyberattacks seeking to exploit vulnerabilities in their digital infrastructure (Kshetri, 2017). Moreover, e-businesses in emerging economies may face additional challenges related to inadequate cybersecurity infrastructure, limited financial resources, and regulatory gaps, further exacerbating their vulnerability to cyber threats (Alrawi et al., 2021). Thus, RDT highlights the importance of understanding the interplay between external dependencies, resource acquisition strategies, and cybersecurity risks in shaping the resilience and sustainability of e-businesses in emerging economies.

Methodology

Survey research design was adopted for the study. Population of the study comprises E-Businesses in Nigeria. The instrument used for collecting data for this study is the questionnaire through an online survey. The instrument was employed in order to ensure credibility of the research and since E-businesses were online. Purposive sampling technique was used to select 150 respondents.

Results

Demographic Data Analysis

Table 1: Distribution Based on Gender

Variables	Respondents	Percentage
------------------	--------------------	-------------------

Male	81	54
Female	69	46
Total	150	100

The data reveals that out of 150 respondents, 81 are male, comprising 54% of the sample, while 69 are female, making up the remaining 46%. This indicates a relatively balanced gender distribution, with a slight majority of males. Such a composition ensures that the perspectives of both genders are adequately represented, providing a comprehensive and equitable overview of the respondents' views and experiences.

Table 2: Distribution according to Years of Business

Options	Respondents	Percentage
Less than 1 year	31	23.6
1-4years	51	33.5
More than 5 years	68	42.9
Total	150	100

Table 2 reveals the distribution of 150 respondents based on their years of business experience. It shows that 31 respondents (23.6%) have less than 1 year of experience, 51 respondents (33.5%) have 1-4 years, and 68 respondents (42.9%) have more than 5 years. This indicates that the majority of respondents are experienced business professionals, with a substantial 42.9% having over five years in the field, while a smaller segment is relatively new, with less than a year of experience. The spread of experience levels among respondents highlights a diverse range of perspectives within the group.

Table 3: Primary Industry of E-business

Options	Respondents	Percentage
Retail	48	32

Financial services	22	14.7
Manufacturing	31	20.7
Technology	39	26
Other	10	6.7
Total	150	100

Table 4 outlines the primary industries of 150 e-business respondents, showcasing a diverse array of sectors participating in the survey. Retail emerges as the most represented industry, with 48 respondents (32%), followed closely by technology at 39 respondents (26%) and manufacturing with 31 respondents (20.7%). Financial services also exhibit a significant presence with 22 respondents (14.7%), while a smaller fraction, 10 respondents (6.7%), falls under the "Other" category. This distribution underscores the broad spectrum of e-business activities across various sectors, reflecting the expansive reach and applicability of e-commerce and digital business practices in today's market landscape.

Presentation of Data

Research Question One: What is the effect of Cybersecurity Threats on E-Businesses in Emerging economies?

Table 4: Effect of Cybersecurity Threats on E-Businesses on Emerging Economies (N=150)

Items	SA(%)	A(%)	D(%)	SD(%)
--------------	--------------	-------------	-------------	--------------

Cybersecurity threats have significantly58(38.67%) 22(14.67%) 41(27.33%) 29(19.33%)

reduced our e-business's operational

efficiency.

19(12.67%) 38(25.33%) 31(20.67%) 61(40.67%)

Our e-business has incurred substantial

financial losses due to cybersecurity

breaches

42(28.00%) 15(10.00%) 53(35.33%) 40(26.67%)

Customer trust in our e-business has

decreased due to cybersecurity incidents.

77(51.33%) 29(19.33%) 35(16.67%) 9(6.00%)

Operational disruptions caused by

cybersecurity threats are a significant

challenge for our business.

43(28.67%) 53(35.33%) 22(14.67%) 32(21.33%)

Cybersecurity threats hinder our

business's ability to innovate and adopt

new technologies.

34(22.67%) 25(16.67%) 53(35.33%) 28(18.67%) Cybersecurity threats have led

to

increased insurance premiums for our e-

business

SA=Strongly Agreed, A=Agreed, D=Disagreeand, SD=Strongly Disagree

The table reveals that cybersecurity threats have a significant impact on e-businesses operating in emerging economies, based on responses from 150 participants. It indicates that a substantial proportion of respondents perceive these threats as having adverse effects across various dimensions of their businesses. Specifically, 38.67% of respondents strongly agree and 25.33% agree that cybersecurity threats significantly reduce operational efficiency, indicating widespread concern regarding the operational challenges posed by such incidents. Moreover, 27.33% strongly agree and 40.67% agree that e-businesses incur substantial financial losses due to cybersecurity breaches, underscoring the economic toll inflicted by cyber threats on these businesses. Furthermore, the findings suggest that cybersecurity incidents have a detrimental impact on customer trust, as 27.33% of respondents strongly agree and 20.67% agree that customer trust decreases in response to such incidents. This erosion of trust can have long-lasting repercussions on the reputation and viability of e-businesses, highlighting the importance of effective cybersecurity measures in maintaining customer confidence. Additionally, the data indicates that operational disruptions caused by cybersecurity threats are perceived as significant challenges, with 35.33% of respondents strongly agreeing and 16.67% agreeing with this statement. These disruptions can impede the smooth functioning of e-business operations, leading to delays, downtime, and potential loss of business opportunities.

Moreover, cybersecurity threats are seen as hindering the ability of e-businesses to innovate and adopt new technologies, with 21.33% of respondents strongly agreeing and 35.33% agreeing with this notion. This suggests that the fear of cybersecurity risks may deter businesses from embracing innovative solutions and leveraging emerging technologies to enhance their competitive edge. Finally, the data indicates that cybersecurity threats also have financial implications beyond direct losses, as evidenced by 18.67% of respondents

strongly agreeing and 35.33% agreeing that such threats lead to increased insurance premiums for e-businesses.

Research Question Two: What is the perception of E-businesses towards cyber security threats in Emerging Economies?

Table 5: Perception of E-businesses towards cyber security threats in Emerging

Economies (N=150)							
Items				SA(%)	A(%)	D(%)	SD(%)
Our	e-business	frequently	encounters	11(7.3)	45(30)	62(41.3)	32(21.3)
cybersecurity threats.							
Phishing is a common cybersecurity threat				51(34)	23(15.3)	31(20.7)	45(30)
faced by our e-business							
The majority of cybersecurity incidents we				21(14)	10(6.7)	47(31.3)	72(48)
face originate from external sources.							
Customer data is frequently targeted in				31(20.7)	51(34)	22(14.7)	46(30.7)
cybersecurity attacks on our business.							
Local cybersecurity regulations and policies				61(40.7)	13(8.7)	42(28)	34(22.7)
are adequate in protecting our business							
cybersecurity threats we face are more							
severe							
compared to businesses in developed				20(13.3)	37(24.7)	58(38.7)	35(22.3)
economies.							

SA=StronglyAgreed, A=Agreed, D=Disagreeand, SD=Strongly Disagree

Table 5 reveals firstly, only 7.3% of respondents strongly agree that their e-business frequently encounters cybersecurity threats, while 34% agree that phishing is a common

threat faced by their business. This indicates a recognition of specific threats like phishing, yet a lower perception of the overall frequency of cyber threats. Secondly, 40.7% of respondents strongly agree and 30% agree that the majority of cybersecurity incidents they face originate from external sources, underscoring the prevalent belief in external threat actors targeting their businesses. However, 20.7% strongly disagree and 15.3% disagree that customer data is frequently targeted, indicating a divergence in views regarding the primary targets of cyber attacks. Thirdly, opinions are divided regarding the adequacy of local cybersecurity regulations and policies, with 41.3% strongly disagreeing and 20.7% disagreeing, contrasting with 30% who agree and 24.7% who strongly agree. This suggests a lack of consensus on the effectiveness of existing regulatory frameworks in safeguarding businesses against cyber threats. Lastly, a significant proportion of respondents perceive cybersecurity threats in emerging economies as more severe compared to businesses in developed economies, with 38.7% strongly agreeing and 28% agreeing. However, 22.3% strongly disagree and 22.7% disagree with this assertion, indicating differing perspectives on the severity of cyber threats between economies.

Inferential Statistics

Table 6: ANOVA

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.923 ^a	.852	.850	1.18695

Source: Researcher's Field Survey, November, 2023.

This ANOVA results show a significant positive link between cybersecurity threats and e-business in emerging economies. The correlation coefficient (R) of 0.923 suggests a significant association while the R square value of 0.852 suggests that cybersecurity threat can clarify about 85.2% of the variation in E-Business.

Discussion of Findings

The data generated in this study are discussed according to the research questions that precipitated them. Hence, the research questions are presented first and then the data are engaged in answering them.

Regarding operational efficiency, a significant majority (38.67%) acknowledge that cybersecurity threats have indeed reduced their e-business's operational efficiency. Moving on to financial losses, the largest majority (51.33%) confirms substantial financial losses incurred due to cybersecurity breaches. Moreover, a considerable majority (42%) agrees that cybersecurity incidents have led to a decrease in customer trust in their e-business. Operational disruptions caused by cybersecurity threats emerge as a significant challenge, with the overwhelming majority (77%) identifying them as such. Furthermore, a significant majority (43%) acknowledge that cybersecurity threats hinder their business's ability to innovate and adopt new technologies. Lastly, while a smaller majority (34%) recognizes the increase in insurance premiums due to cybersecurity threats, this finding underscores the broader economic impact of cyber risks.

Firstly, regarding the frequency of cybersecurity threats, a significant majority (34%) acknowledge that their e-business frequently encounters such threats. However, there appears to be a disparity in perception when it comes to the prevalence of phishing as a common cybersecurity threat. A majority (34%) of respondents disagree or strongly disagree that phishing poses a significant risk to their e-business. On the origin of cybersecurity incidents, a substantial majority (41.3%) agree that the majority of incidents they face stem from external sources. Interestingly, there's a prevailing perception among respondents (48%) that customer data is not frequently targeted in cybersecurity attacks on their business. Furthermore, there's scepticism regarding the adequacy of local cybersecurity regulations

and policies, with a majority (38.7%) expressing disagreement or strong disagreement. Lastly, despite the prevalent cybersecurity challenges, a significant majority (40.7%) disagrees or strongly disagrees that cybersecurity threats faced by their business are more severe compared to businesses in developed economies.

The ANOVA result shows that there exists a strong positive relationship between cyber security threats and E-business in emerging economies with correlation coefficient of 0.923 and coefficient of determination of 0.85. However, this result suggests that advancements in cybersecurity have a favorable effect on e-business operations in developing nations. This means that firms can operate more safely online as cybersecurity safeguards are tightened, which could result in bigger transaction volumes, more customer trust, and possibly even more profitability. According to research work carried out by Negrea Petru-Cristian (2023); the study shows that businesses will probably view cybersecurity as a top priority and an essential part of their risk management plan which entails putting in place strong cybersecurity safeguards as well as updating and modifying them frequently to take into account new threats. Resilience against cyber events and business continuity are improved by effective risk management, and these are especially crucial in emerging countries where regulatory regimes may still be changing.

Also, the correlation coefficient (0.923) indicates that there is a substantial positive association between e-businesses and their propensity to invest financial, human, and technological resources in strengthening their cybersecurity capabilities; this could entail making investments in cutting-edge security technologies, employing qualified cybersecurity specialists, carrying out frequent evaluations and audits, and putting strong cybersecurity policies and processes in place.

Conclusion

In conclusion, the results show that cybersecurity problems affect e-businesses a lot. They hurt how businesses work every day, cause big money losses, and make customers not trust the business as much. These problems also make it hard for businesses to keep working smoothly and to try new things. But by taking cybersecurity seriously and making smart choices, businesses can better protect themselves and keep growing safely in the digital world.

Recommendations

- i. E-businesses should prioritize cybersecurity and educate their employees on best practices.
- ii. Government should focus on strengthening cybersecurity measures, collaborating with businesses and other agencies, and investing in cybersecurity education and training
- iii. E-businesses should Keep up to date with the latest cybersecurity trends and technologies, and regularly assess their systems for vulnerabilities

References

- Alrawi, O., Lever, C., Antonakakis, M., & Monroe, F. (2021). Sok: Security evaluation of home-based IoT deployments. *IEEE Symposium on Security and Privacy (SP)*, 2021, 1361-1378. <https://doi.org/10.1109/SP40001.2021.00087>
- Bhowal, P., Das, A. K., Goswami, P., & Choudhury, P. (2019). An empirical study of cyber security risks in online transactions of e-commerce. *Journal of Physics: Conference Series*, 1234(1), 012034. <https://doi.org/10.1088/1742-6596/1234/1/012034>
- Chaffey, D. (2015). Digital business and e-commerce management: Strategy, implementation, and practice. Pearson Education.
- Choudhary, V., Venkatesh, V., & Ravichandran, T. (2018). A comprehensive model of consumer trust in electronic commerce: A theoretical model. *Journal of the Association for Information Systems*, *19*(8), 2. <https://doi.org/10.17705/1jais.00460>
- Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*, 21(3), 719-734. <https://doi.org/10.1007/s10796-0179774-y>

- Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2017). Cybersecurity investments in the U.S.: The diminishing marginal returns. *Journal of Cybersecurity*, 3(1), 1-12. <https://doi.org/10.1093/cybsec/tyw002>
- Gupta, B. B., Bag, S., Jena, D., & Kumar, P. (2018). Analysis of various security issues and challenges in the Internet of Things (IoT). *Journal of Engineering and Applied Sciences*, 13(2), 276-288.
- Hassan, N., Huda, S., Almogren, A., Shah, S. B. H., & Islam, R. (2020). The Internet of Things: A survey of security and privacy issues and solutions. *Internet of Things*, 12, 100274. <https://doi.org/10.1016/j.iot.2020.100274>
- Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly*, 38(8), 1710-1732. <https://doi.org/10.1080/01436597.2017.1298438>
- Kshetri, N. (2020). Blockchain and sustainable supply chain management in developing countries. *International Journal of Information Management*, 52, 102064. <https://doi.org/10.1016/j.ijinfomgt.2019.102064>
- Pfeffer, J., & Salancik, G. R. (1978). The external control of organizations: A resource dependence perspective. Harper & Row.
- Purkait, S., Sen, S., Datta, D., & Sen, A. (2020). A study of ransomware and its impact on healthcare organizations. *International Journal of Advanced Research in Computer Science and Software Engineering*, 10(7), 23-31. <https://doi.org/10.23956/ijarcsse.v10i7.848>
- Rocha, F. J., Abreu, R., Correia, M., & Figueiredo, J. (2017). Cybersecurity threats and solutions in the European context. *Journal of Information Systems Engineering & Management*, 2(4), 19. <https://doi.org/10.20897/jisem.201719>
- Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2018). Electronic commerce 2018: A managerial and social networks perspective. Springer.
- UNCTAD. (2019). Digital economy report 2019: Value creation and capture – implications for developing countries. United Nations Conference on Trade and Development. <https://unctad.org/webflyer/digital-economy-report-2019>.