International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 14, Issue 2, 2026

Cybersecurity: Practices and Incident Response Management in SMEs

Makafui Ofori[1], George K. Agordzo[2], Edinam Agbemava[3], Meshach Tettey[4], Klu K. Proposer[5]
Ho Technical University, Ho.
E. P. College of Education, Amedzofe, Ghana.
Mail Id; makafofori@gmail.com[1], k.agordzo@ymail.com[2], eagbemava@htu.edu.gh[3]
tetteymeshach@gmail.com[4], pkklu@htu.edu.gh[5]
Article Received: 27-02-2026, Accepted 17-03-2026

Abstract.
This research examines Ghanaian SMEs' cybersecurity and incident response. The major goals are to identify and evaluate these SMEs' cybersecurity measures, examine their problems in developing and sustaining effective cybersecurity practices, assess their cybersecurity incident response capabilities, and give practical recommendations for improvement. This study administered surveys to 200 small and medium-sized enterprise (SME) owners and IT managers in Accra and Kumasi, collecting in-depth responses from key stakeholders, and analyzing secondary data sources. SMEs in Ghana are becoming more aware of cybersecurity, but preventative and reactive measures are weak. Only 35% of SMEs employ encryption, and 25% undertake security assessments, although 85% use antivirus software. Financial constraints prevented 60% of SMEs from improving cybersecurity, whereas 40% had a basic incident response strategy and 10% had a whole staff. The study reveals that budgetary constraints, a lack of experienced people, and cybersecurity expertise prohibit SMEs from adopting full cybersecurity measures. Many SMEs lack incident response methods and infrastructure to identify, contain, and recover from cyber attacks, which is difficult. To assist SMEs in establishing and maintaining effective cybersecurity defenses, the report advises targeted marketing, government support for financial and training resources, and the adoption of cybersecurity frameworks like the NIST Cybersecurity Framework, PCI DSS, and CMMC. The survey suggests Ghanaian SMEs need stronger cybersecurity and incident response. SMEs can protect their digital assets, maintain consumer trust, and maintain business continuity in the face of growing cyber risks by bridging these gaps with established frameworks and teamwork.

Keywords: *Cybersecurity, Incident Response, SMEs, Ghana, Cyber Threats, Data Protection.*

Introduction

Small and medium-sized companies (SMEs) all over have a quick digital transformation that has changed business processes and made their competitiveness both locally and globally possible. However, as digital technology is applied increasingly, SMEs have come under several security concerns. SMEs might not have the means or expertise necessary to build strong cybersecurity systems (Arora, Hall, Pinto, Ramsey, & Telang, 2017). Targeting SMEs, cybercriminals attack customer data, intellectual property, and sensitive information, including bank records. In underdeveloped countries where cybersecurity knowledge is limited and preventative steps are judged as nonessential, this danger is especially large (Mukhopadhyay, Chatterjee, & Saha, 2021). Many SMEs in developing nations are unprepared for cyberattacks due to insufficient technical infrastructure, a lack of competent workers, and poor cybersecurity practices (Mukhopadhyay et al., 2021). Among SMEs, there are plenty of phishing, social engineering, ransomware, and advanced persistent threats. These mistakes can cause financial loss, harm to reputation, and regulatory sanctions. Notable cyberattacks such as the WannaCry ransomware assault and massive business data dumps make evident how urgently effective incident response management is needed. Good incident response helps minimize cyber events, quickly recover, and maintain business continuity (Ahmad, Webb, Desouza, & Boorman, 2019). Along with immediate financial losses, SMEs might experience long-term effects like consumer distrust and legal obligations. SMEs must thus create and use comprehensive cybersecurity plans comprising preventative activities and incident response procedures suitable for their risk profiles and needs.

Like other developing nations, Ghanaian SMEs have particular cybersecurity issues. The rapid advancement of digital technology has outpaced the security projects of many small businesses. Their financial status reduces their capacity to buy expensive cybersecurity tools. Many small companies lack the technical capacity to create and sustain robust cybersecurity defenses (Boateng, Heeks, Molla, & Hinson, 2017). The problem is exacerbated by SMEs' misunderstanding of cyber

DOI: https://doi.org/10.62647/IJITCEV14I2PP1-9

dangers for their staff members and themselves. Many SMEs think hackers more often target larger, more profitable companies. False sense of security and inadequate cybersecurity funding expose these businesses to attackers. The lack of comprehensive cybersecurity laws and norms in Ghana makes it harder for SMEs to standardize their operations (Boateng et al., 2017). This article analyzes cybersecurity and incident response techniques applied by Ghanaian SMEs, therefore bridging this gap. The main goals of this study are to comprehend and enhance the cybersecurity environment among Ghanaian SMEs. First, the study seeks to pinpoint and assess the present cybersecurity systems used by SMEs. This entails looking at the kinds of policies, tools, and technology they apply to guard their digital resources and lower cyber vulnerabilities. Second, the study aims to examine the difficulties SMEs have in keeping strong cybersecurity policies in use. The study will also evaluate SMEs' degree of preparedness for handling cybersecurity events. Crucially for reducing harm and guaranteeing company continuity is their capacity to successfully identify, react to, and recover from cyber events. At last, depending on the results, the study seeks to offer useful suggestions for strengthening incident response management among Ghanaian SMEs and cybersecurity policies. These suggestions will be catered to the particular requirements and difficulties found, therefore enabling SMEs to improve their resilience against cyber risks and cybersecurity posture. Based on the main goals of the study, the following research questions are formulated to guide the investigation:

This article examines Ghanaian cybersecurity strategy and incident response management for SMEs in several industries. SME involvement in Ghana boosts growth, innovation, and employment. To meet SMEs' cybersecurity needs, this study includes banking, healthcare, retail, manufacturing, and IT. Ghana's case study permits the research to address developing nation SMEs' specific challenges and opportunities. Like Ghana's fast-growing digital economy, SMEs in similar nations confront cybersecurity issues. This study will benefit Ghana and other developing nations by exposing vital SMEs exposed to cyberattacks. The study will include quantitative survey data and qualitative interviews with SMEs, IT managers, and cybersecurity experts. This thorough strategy will help Ghanaian SMEs analyze their cybersecurity and make targeted improvements.

Literature Review

Cybersecurity and Common Practices in SMEs

For SMEs, the increasing automation of corporate activities has elevated cybersecurity to a top priority. Though they understand the need for cybersecurity, SMEs often find it difficult to apply thorough security measures because of factors including limited financial resources, lack of experience, and inadequate understanding of developing threats (Yeboah-Boateng & Appiah-Nketiah, 2016). The belief that SMEs are not the main targets for cyberattacks aggravates the matter and results in a lazy attitude toward cybersecurity spending. To guard their digital resources, most SMEs depend on simple cybersecurity practices. These comprise frequent software updates, antivirus software, and firewalls. Employee training programs are also widely used to teach personnel about spotting phishing efforts and other social engineering assaults (Ab Rahman & Choo, 2015). These steps are generally inadequate against modern threats, though, and SMEs can lack the sophisticated tools and strategies employed by bigger companies.

Advanced Measures and Emerging Trends

In addition to basic security tools, some SMEs have begun adopting more advanced cybersecurity measures such as encryption, intrusion detection systems (IDS), and multifactor authentication (MFA). *2.3 Frameworks and Best Practices*

To provide a structured approach, frameworks like NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001 are widely referenced. These can enhance SME resilience, though adoption is often hindered by cost and complexity (Johnson, Goetz, & Pfleeger, 2017).

2.4 Incident Response Management

Incident response is critical for minimizing damage. An efficient plan helps companies reduce recovery time, costs, and future risks (Lallie et al., 2020). Organizations without a clear plan often face confusion, delays, and more harm (Fenz, Heurix, Neubauer, & Pechstein, 2014). SMEs, due to limited resources, struggle with these phases (Soomro, Shah, & Ahmed, 2016).

2.4.1 Challenges in Developing Countries

Developing nations face limited funding, poor infrastructure, and a lack of awareness (Mukhopadhyay et al., 2021). In Ghana, outdated software and weak investment hinder SMEs (Hinson, Boateng, & Madichie, 2010; Asante, Osei, & Boateng, 2019).

Methodology

This study uses a case study methodology, which works especially well for investigating complicated events in practical environments. This methodology enables a thorough

investigation of the particular cybersecurity policies and incident response management techniques embraced by SMEs in Accra and Kumasi, Ghana's main cities and economic centers. Employing comprehensive, contextual insights into their cybersecurity concerns and the solutions they use, the case study approach helps a thorough investigation of the several issues these SMEs encounter (Yin, 2018). The necessity to grasp not only the quantitative but also the qualitative, complex experiences of SME owners and IT managers in these important economic hubs justifies this methodology approach.

Data Collection and Samples

We sought comprehensive data using mixed methodologies, integrating qualitative and quantitative methods. This technique ensured cybersecurity awareness for Accra and Kumasi-based Ghanaian SMEs, aligning with the need for holistic approaches in cybersecurity research (Soomro, Shah, & Ahmed, 2016). A representative sample of Accra and Kumasi SME owners and IT managers received structured questionnaires. The surveys sought quantifiable data on cybersecurity practices, including security technology, security events, cybersecurity policy, and cyber crisis preparation. Structured questionnaires made data collection rigorous, making it easier to analyze SME cybersecurity practices and incident response planning trends. Semi-structured interviews with SME managers and cybersecurity experts further provided depth, as recommended in SME cybersecurity studies (Bada & Nurse, 2019).

Other secondary sources included scholarly articles, government studies, and industrial reports. These resources contextualize surveys and interviews. Academic articles covered theoretical and empirical cybersecurity and incident response management in SMEs (Mukhopadhyay, Chatterjee, & Saha, 2021), while industry reports and government publications covered national and sector specific cybersecurity concerns and policies. Secondary data complemented primary data by offering an outside viewpoint on Ghanaian SMEs' cybersecurity practices, allowing a more comprehensive analysis of current issues. The sample was stratified to include SMEs of varied sizes with different technology adoption and cyber hazard exposure. Understanding the multiple cybersecurity concerns SMEs in different industries face and identifying sector-specific best practices and vulnerabilities requires diversity. To ensure a representative sample, 400 SMEs were selected, 200 from each city (Accra and Kumasi). The study participants were chosen based on their willingness to participate and their company's relevance to the research aims. This sample method allowed the research results to be extended to the wider population of SMEs in Ghana at large.

Data Analysis and Statistical Model for Analysis

To analyze the data collected, a combination of qualitative and quantitative data analysis techniques was employed. This mixed-methods approach allowed for a comprehensive understanding of the data, capturing both the statistical trends and the underlying reasons behind those trends. The logistic regression model is represented as:

$$Logit(P) - \beta\alpha + \beta_1 (Company\ Size) + \beta_2 (Industry\ Type) + \beta_3 (Cybersecurity\ Investment)$$

Where:

- P is the probability of an SME being prepared for cyber incidents.
- B_o is the intercept term.
- • β_1, β_2, β_3, are the coefficients for each predictor variable.
- $\in$ is the error term.

$$Investment) + \beta_2 (Frequency\ of\ Incidents) + \beta_3 (Training\ Programs) + €.$$

By using these statistical models, the study provided detailed insights into the factors that influence cybersecurity practices and incident response readiness among SMEs in Accra and Kumasi. These analyses not only identified key predictors of cybersecurity resilience but also offered empirical evidence to inform policy recommendations and strategic decisions for enhancing the cybersecurity posture of SMEs in Ghana. The mixed methods approach, combined with rigorous statistical analysis, ensured the validity and reliability of the study findings, contributing to a deeper understanding of the cybersecurity landscape in Ghanaian

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

SMEs as shown in Figure 1 below.

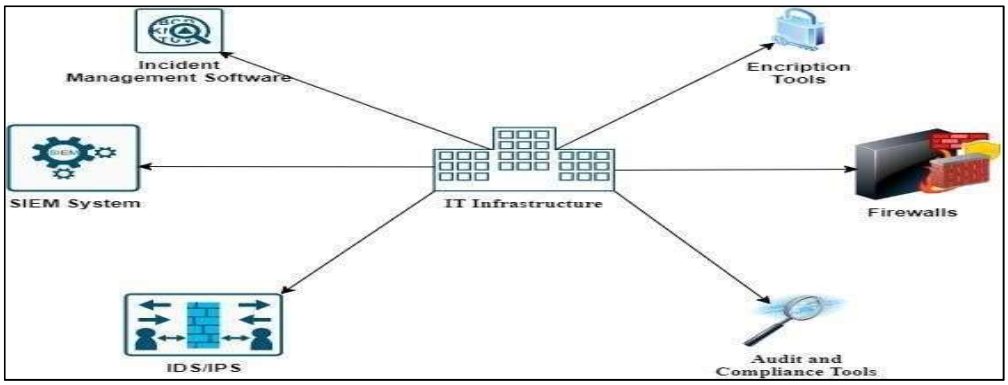

Figure 1: Technology View for Cybersecurity Risk Management

Results

Current Cybersecurity Practices

The survey results indicate varying levels of cybersecurity practice adoption among SMEs in Ghana. Basic cybersecurity measures such as antivirus software and firewalls are relatively common, while more advanced practices like encryption and regular security audits are less prevalent. The data can be visualized using a bar chart to show the percentage of SMEs implementing different cybersecurity measures.

Table 1: Cybersecurity Measures by SMEs in Ghana

Cybersecurity Measure	Percentage of SMEs (%)
Antivirus Software	85
Firewalls	70
Encryption	35
Regular Security Audits	25
Formal Cybersecurity Policy	30
Employee Training	20

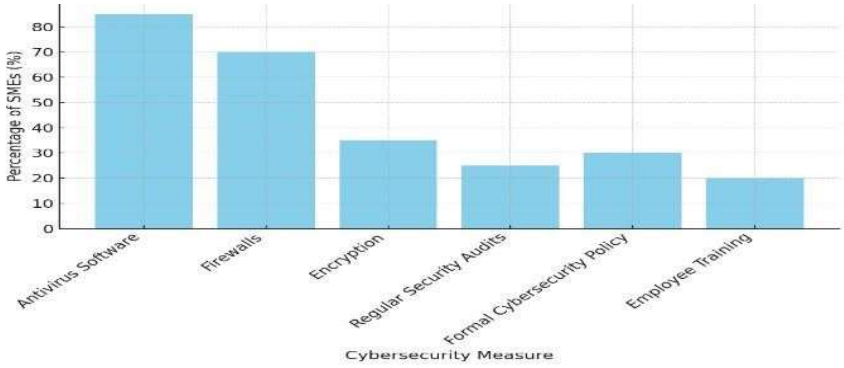

Figure 2: Adoption of Cybersecurity Measures by SMEs in Ghana

The survey results indicate that while most SMEs in Ghana have implemented basic cybersecurity measures, such as antivirus software and firewalls, more advanced practices, such as encryption and regular security audits, are less common. As shown in Figure 2, 85% of SMEs use antivirus software, and 70% use firewalls. However, only 35% of SMEs have adopted encryption technologies, and even fewer (25%) conduct regular security audits. Additionally, just 30% of SMEs have a formal cybersecurity policy, and only 20% provide regular employee training on cybersecurity awareness.

Incident Response Readiness

Incident response readiness among SMEs in Ghana is generally low, with many SMEs lacking comprehensive plans and the necessary infrastructure to handle cybersecurity incidents effectively. A bar chart can illustrate the percentage of SMEs with various levels of incident response preparedness.

Table 2: Incident Response Readiness among SMEs

DOI: https://doi.org/10.62647/IJITCEV14I2PP1-9

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

Incident Response Measure	Percentage of SMEs (%)
Basic Incident Response Plan	40
Advanced Detection Systems	20
Regular Incident Response Drills	15
Comprehensive Incident Response Team	10

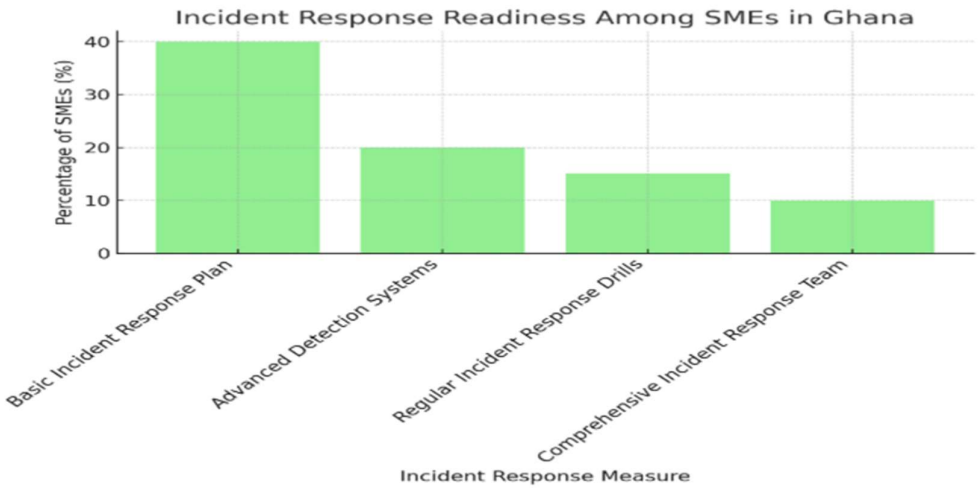

Figure 3: Incident Response Readiness among SMEs

The results show SMEs' lack of readiness to manage cybersecurity events. Only 20% of SMEs have sophisticated detection systems, 15% have frequent issue response exercises, 40% have a basic incident response strategy, and just 10% have a complete incident response team. This discrepancy in incident response readiness emphasizes the necessity of better training and resources to provide SMEs with the skills and expertise to control cybersecurity events properly.

Findings

Many Ghanaian SMEs use firewalls and antivirus software to protect their digital infrastructure, but they ignore more advanced solutions. We underutilize security standards like encryption and auditing. This indicates a disparity in the adoption of comprehensive cybersecurity techniques to secure networks and protect private data. Basic precautions may give the idea of security, but sophisticated cyberattacks require stronger protections. Five main obstacles prohibit SMEs from improving cybersecurity, according to the poll. Financial issues are major. Many small and medium-sized enterprises (SMEs) have limited resources and often overlook cybersecurity, leading to underinvestment in tools and technology. The shortage of skilled workers is another issue. Given the high demand for cybersecurity specialists from larger companies with better compensation and benefits, SMEs may struggle to recruit and keep them. A lack of cybersecurity awareness among SME workers and owners leads to complacency and weak digital resource defense.

Insufficient incident response strategies and teams. Many SMEs cannot control cybersecurity incidents because they lack the infrastructure, protocols, and qualified individuals to detect, contain, and recover from assaults. This diversity in incident response capabilities exposes SMEs to data breaches, operational delays, and financial losses. SMEs risk compounding cyber damage and struggling to restart regular operations without a disciplined incident response strategy. These findings show that Ghana's SMEs must quickly enhance cybersecurity policy and incident response. Industry, government, and SMEs must collaborate to close these gaps. Providing SMEs with training, support, and resources improves their cybersecurity. Cooperative programs may include financial incentives for cybersecurity investments, government-sponsored training courses to build in-house knowledge, and awareness campaigns to educate SMEs on cybersecurity. These methods can help SMEs safeguard their digital assets, preserve consumer confidence, and maintain business continuity against escalating cyber threats. SMEs need cybersecurity advancements to secure their digital assets, preserve consumer confidence, and ensure business continuity. SME challenges—limited financial resources, lack of qualified staff, and

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

insufficient cybersecurity awareness—make specialized regulations crucial. SMEs may improve cybersecurity by taking these sensible
These methods ensure the robustness of their business operations, defend against cyberattacks, and assist SMEs to considerably enhance their cybersecurity posture. Cybersecurity is not only a technical issue but also an essential component of company strategy and risk management. This study on Ghanaian SMEs shows that, in terms of cybersecurity investment and readiness, SMEs typically lag behind larger businesses; the results of this analysis closely follow international trends. Many times, poor technological understanding, limited resources, and ignorance of the significance of cyberattacks cause this gap. For Ghana especially, these global problems are aggravated by distinct socioeconomic factors. Many Ghanaian SMEs operate in environments without advanced cybersecurity solutions or expertise in technology. These constraints make it far more difficult for SMEs to build and maintain robust cybersecurity defenses, hence raising their vulnerability to assaults (Mukhopadhyay et al., 2021).

Recommended Cybersecurity Frameworks for SMEs

By structuring cybersecurity risk management, cybersecurity frameworks may assist SMEs. These frameworks provide SME-specific advice and best practices.

1. NIST Cybersecurity Framework: The flexibility and scalability of this widely used framework make it suited for SMEs and other sectors. It emphasizes the interdependence of five basic functions—Identify, Protect, Detect, Respond, and Recover—and the necessity for continual development to maintain effective cybersecurity defenses (NIST, 2018).
2. PCI DSS (Payment Card Industry Data Security Standard): This framework protects cardholder data and is mandatory for SMEs processing credit cards. A secure network, data protection, vulnerability management, access restrictions, and constant monitoring are required (PCI Security Standards Council, 2018).
3. CMMC certification: SMEs benefit from CMMC's tiered strategy, created for DOD contractors. It provides a clear roadmap to enhancing cybersecurity procedures by defining five maturity levels from basic to advanced (CMMC Accreditation Body, 2020).

Proposed Framework

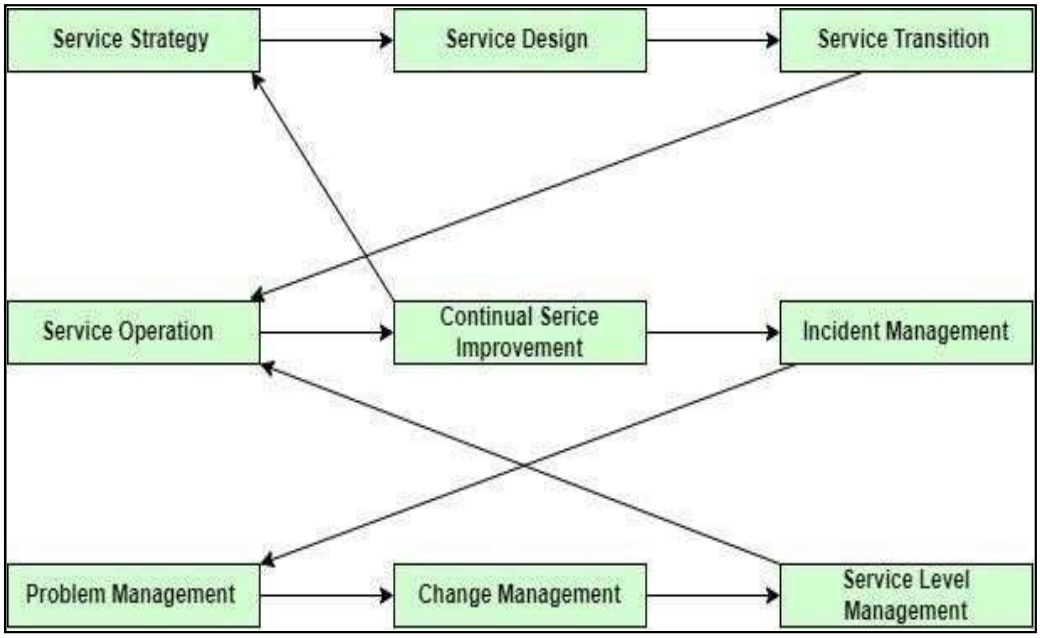

Figure 4: Comprehensive Framework to Cybersecurity Management for SMEs

The ITIL-based, in Figure 4 above provides a comprehensive approach to cybersecurity management for Ghanaian SMEs, addressing the issues identified in the Fault Tree Analysis (FTA). It includes the following key ITIL processes:

1. **Service Strategy**: Focuses on aligning cybersecurity initiatives with business objectives, managing risks, identifying critical assets, and ensuring appropriate budget allocation.
2. **Service Design**: Involves creating robust cybersecurity policies and controls, such as secure

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

configuration management, and access control policies, and designing effective incident response plans.

3. **Service Transition**: Covers the implementation of security measures, including technology deployment (e.g., encryption, IDS/IPS), conducting employee training programs, and rolling out cybersecurity policies.

4. **Service Operation**: Focuses on the daily monitoring and management of cybersecurity, including threat detection, incident logging, and incident response procedures.

5. **Continual Service Improvement (CSI)**: Emphasizes the continuous review and enhancement of cybersecurity practices through regular security audits, post-incident analysis, and updating policies and training.

This ITIL-based approach ensures that all aspects of cybersecurity are addressed systematically, improving resilience against cyber threats and enhancing overall security posture. Arrows are strategically placed to show the flow between these processes, emphasizing how each process interacts and contributes to effective IT service management.

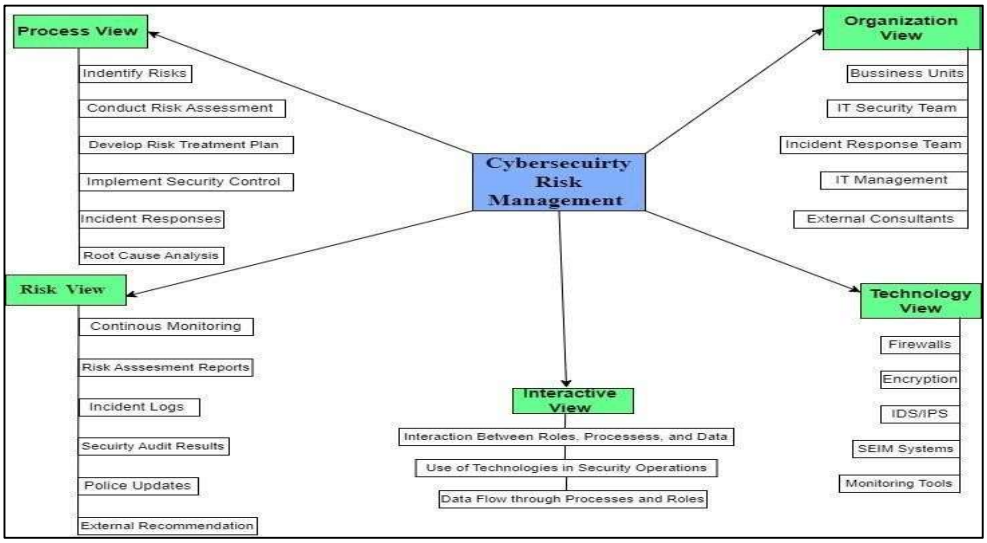

Figure 5: Cybersecurity Risk management Modeling

This multi-view modeling approach ensures that all critical dimensions of cybersecurity are considered, enabling organizations to manage cybersecurity risks effectively and ensure robust protection of their digital assets as shown in the above in figure 5.

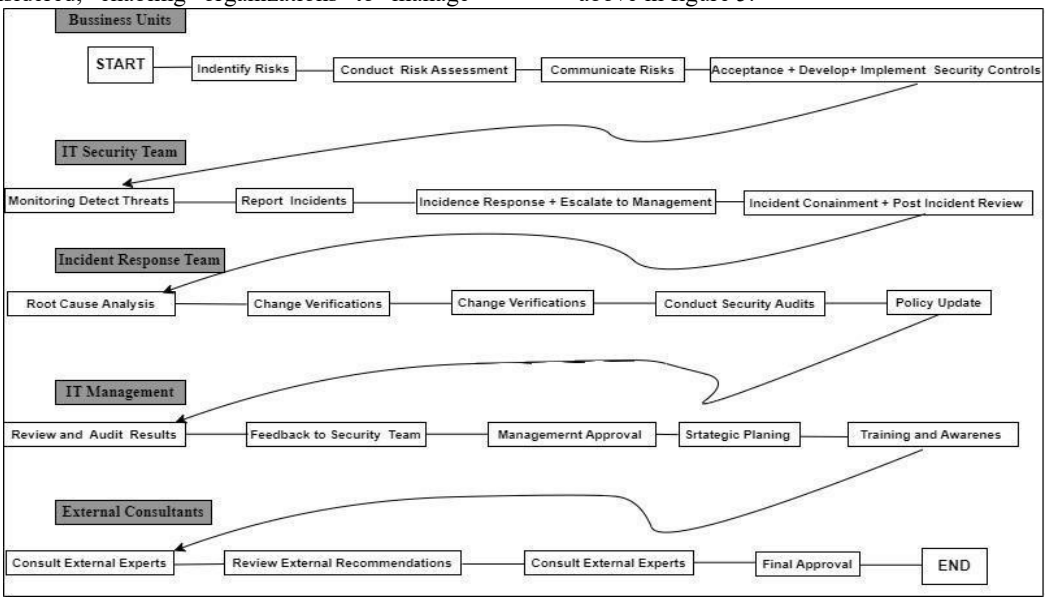

Figure 6: BPMN for Cybersecurity Risk Management

Figure 6 illustrates the interdependencies between different roles and processes, providing a comprehensive view of how organizations can manage cybersecurity risks effectively. It emphasizes the importance of continuous monitoring, collaboration, strategic planning, and ongoing improvement in maintaining a robust cybersecurity posture.

Conclusion

Ghana's SMEs' cybersecurity strategies and incident response management are thoroughly examined in this paper. The results show gaps in proactive and reactive cybersecurity practices, threatening organizational continuity, financial stability, and public confidence. According to the report, Ghanaian SMEs are growing more aware of cybersecurity, but they have not yet adopted robust cybersecurity procedures. Firewalls and antivirus software are popular, but encryption and periodic security assessments are not. Without adequate cybersecurity procedures, many SMEs are vulnerable to data breaches, ransomware attacks, and other cybercrime. The paper also identified key barriers to prudent cybersecurity measures. Most typically, budgetary constraints prevented 60% of SMEs from investing in cybersecurity technology and services. A lack of skilled people and an understanding of shifting cyber dangers make SMEs unable to counter modern assaults. The lack of cybersecurity event preparation is another key concern highlighted by this research. Since just 10% of SMEs have a comprehensive incident response team and 40% have a basic strategy, cyber disasters might cause considerable disruption and harm. Lack of crisis response skills hurts these organizations' immediate operations long-term reputation and consumer confidence. The report proposes many mathematical solutions to these differences. Cybersecurity awareness must be raised through targeted advertising and education. These initiatives should strive to make cybersecurity a strategic priority rather than an expense. Second, SMEs need government support for financial and training resources to build and maintain robust cybersecurity defenses. This may include subsidies, tax incentives, and public-private coalitions to improve SME cybersecurity capabilities. SME adoption of CMMC, PCI DSS, and NIST Cybersecurity Framework is also recommended. These platforms can help SMEs build effective cybersecurity policies and practices and manage cybersecurity risks in a scalable manner. These approaches help SMEs become proactive in cybersecurity, ensuring they can halt cyberattacks and respond swiftly and forcefully. Ghanaian SMEs' cybersecurity must improve to maintain consumer confidence, secure digital assets, and ensure firm continuity. Addressing the gaps with awareness, training, and best practices will protect SMEs against cyberattacks and help them grow and survive in a digital world. SMEs, government agencies, and industry players may work together to develop a robust cybersecurity ecosystem that supports SMEs in Ghana and beyond.

References

1. Ab Rahman, N. H., & Choo, K.-K. R. (2015). *A survey of information security incident handling in the cloud.* Computers & Security, 49, 45–69. https://doi.org/10.1016/j.cose.2014.11.006
2. Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). *Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack.* Computers & Security, 86, 402–418. https://doi.org/10.1016/j.cose.2019.07.001
3. Yeboah-Boateng, E. O., & Appiah-Nketiah, A. B. (2016). *MultiTenancy Issues with Service Delivery in Developing Economies: Privacy, Trust and Availability Concerns.* arXiv preprint, September 5, 2016.
4. Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. (2017). *An ounce of prevention vs. a pound of cure: How can we measure the value of IT security solutions?* Decision Support Systems, 100, 53–62. https://doi.org/10.1016/j.dss.2017.04.006
5. Bada, M., & Nurse, J. R. C. (2019). *Developing cybersecurity education and awareness programmes for Small- and Medium-sized Enterprises (SMEs).* Information & Computer Security, 27(3), 385–402. https://doi.org/10.1108/ICS-07-2018-0080
6. Boateng, R., Heeks, R., Molla, A., & Hinson, R. (2017). *Advancing e-commerce beyond readiness in a developing country: A Ghanaian case study.* International Journal of Electronic Commerce, 21(3), 419–447. https://doi.org/10.1080/10864415.2017.1304316
7. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). *Current challenges in information security risk management.* Information Management & Computer Security, 22(5), 475–493. https://doi.org/10.1108/IMCS-07-2013-0053
8. Hinson, R. E., Boateng, R., & Madichie, N. O. (2010). *Corporate social responsibility activity reportage on bank websites in Ghana.* International Journal of Bank Marketing, 28(7), 498–518. https://doi.org/10.1108/02652321011085176
9. Johnson, C. S., Goetz, E., & Pfleeger, S. L. (2017). *Security through information risk*

DOI: https://doi.org/10.62647/IJITCEV14I2PP1-9

management. Communications of the ACM, 60(3),
42–44. https://doi.org/10.1145/3013007
10. (Replaced with #5 above in list)
11. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyberattacks during the pandemic.* Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2020.102248
12. (Replaced with #3 above in list)
13. Mukhopadhyay, A., Chatterjee, S., & Saha, D. (2021). *Cybersecurity in developing economies: Challenges and opportunities.* Information
Systems Research,
32(2), 421–439.
https://doi.org/10.1287/isre.2020.0974
14. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review.* International Journal of Information Management, 36(2),
215–225.
https://doi.org/10.1016/j.ijinfomgt.2015.11.009
15. Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods.* Sage Publications.
16. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Retrieved from NIST website.
17. PCI Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures (Version 3.2.1).* Retrieved from PCI Security Standards Council.
18. CMMC Accreditation Body. (2020). *Cybersecurity Maturity Model Certification (CMMC) Model Overview.* Retrieved from CMMC Accreditation Body.
19. Ghana Chamber of Young Entrepreneurs. (2022). *43% of SMEs in Ghana suffer cyber-attacks in their business operations.* GCYE News Archive.
20. Cyber Security Experts Association Ghana. (2021). *Strengthening Ghana's Cyber Security through Capacity Building.* Ghana News Agency.