Cloud Adoption and Digital Transformation Cybersecurity Consideration for SMEs

ISABIRYE EDWARD KEZRON
Department of Information Systems

Abstract- This paper discusses the dual challenge SMEs face: availing the use of technology while parceling on security to counter the constraints in resource use. But it also looks at such threats as advanced with intelligence, the future of AI and quantum computing and its security implications. Cybersecurity is not only an IT problem for SMEs but also a strategic area to maintain digital transformation. Challenges outline key recommendations concluding that cybersecurity has to be updated in order to protect the digital future of SMEs. Cloud solutions and development are fundamental to growth across SMEs in the today's market. Nevertheless, they introduce numerous cybersecurity threats to organizations and their outcomes can negatively affect operational and reputational aspects. This paper focuses on the different issues that SMEs encounter in cloud deployment, digitalization and security risk management and provides recommendations on preventing or overcoming the challenges.

I. INTRODUCTION

Cloud computing has a very important role to digital transformation strategy of Small and Medium Enterprises (SMEs) which greatly impacts the advancement of the businesses and work efficiency. Whereas, prior research focused on the positive impacts that the adoption of cloud brings, this study seeks to look at the positive and negative impacts of cloud technologies with focus on the risk impacting on cyber security. For the SMEs with fewer resources to spend, the cloud solutions can help them find affordable and effective business processes and relations with clients as well as facilitate business decisions. It also means that cloud platforms also facilitate joint work of teams and departments located in different geographic locations. However, this paper recognizes other risks, which are not usually associated with cloud adoption, but upon which the value of clouds greatly depends on such as Cyber security risks.

Thus, this research enables contribution to respective literature and practice by identifying these risks and offering feasible solutions for secure cloud adoption. Even now most SMEs are Struggling with various issues: systems integration, lack of skilled workers or resources, as well as weaknesses like data leakage that can make them susceptible to emergent cyber threats. Cyber security is therefore an essential part of organizational digital transformation.

II. BACKGROUND STUDY

Using cloud computing the organizational performance is improved on the other hand there are new threats to security. The internal capacity or capability of SMEs to safeguard intellectual assets and to manage security concerns appropriately is usually inadequate or is missing (Sharma, Singh & Sharma, 2009). Others are theft that involves loss of data, unauthorized access and phishing. Inggarsono et al (2015) have opined that SMEs of developing nations are at considerable risk as malware protection and IT back-up are negligible in most cases. While many SMEs have security solutions protecting their environment, many of those solutions are not very sophisticated the majority of companies do not employ encryption or access control mechanisms, let alone multi-factor authentication.

Besides, there are other factors that have a negative impact on the cyber security environment for SMEs: regulations and compliance. Every single regulation like GDPR has highly enforced regimes that govern data collection and data management. Non-compliance results in possible Penalties, loss of customers' confidence and business goodwill (Renaud & Ophoff, 2021). The issue with following these regulations lies with the fact that SMEs can seldom afford full compliance departments.

The adoption of cloud technology by business operations, especially SMEs, has created the need for cyber security infrastructure in their business model. Based on the analysis of the current and potential threats, this paper proposes that SMEs should adopt a proactive approach to security to succeed under the cloud technology environment. New threats and compliance are achieved through daily to annual security audits, security policies, efforts to develop secure IT literacy among employees, and an upgraded level of security. The next step in the process is offered by frameworks like ISO/IEC 27001 and NIST which offer actual solutions on how SME shall undertake this process.

The following is an evaluation of the case of SMEs embracing cloud technologies with a view on their security considerations. By providing a synthesis of the literature review with actual case studies and recommendations, the study intends to address this gap effectively to offer possibility practical approaches to meet the cyber security needs of SMEs in their digital transformation agenda.

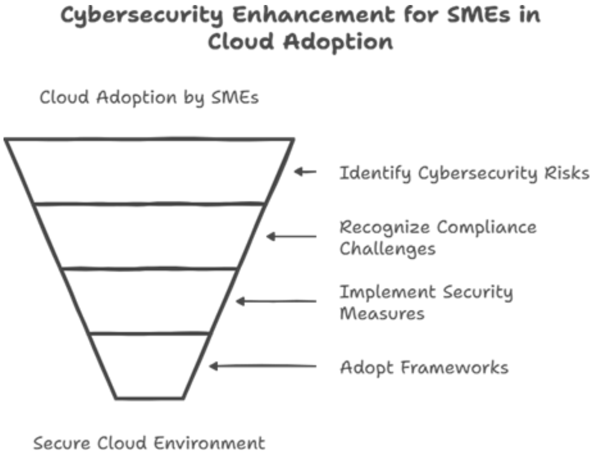
Cybersecurity Enhancement for SMEs in Cloud Adoption
Cloud Adoption by SMEs
Identify Cybersecurity Risks
Recognize Compliance Challenges
Implement Security Measures
Adopt Frameworks
Secure Cloud Environment

Figure 1: Cybersecurity Enhancement for SMEs in Cloud Adoption

III. RESEARCH ELABORATIONS

Recent studies concretely show that the implementation of cloud solutions in SMEs is considered difficult due to high costs, the necessary specific knowledge, and security threats (Yuen & Baskaran, 2023). Though the reliance on cloud increased significantly, the SMEs do not have adequate resource and knowledge to leverage these technologies to maximum extent (Inggarsono et al., 2015). Cyber security is an issue that is critically important because most SMEs are not capable of properly protecting themselves from threats such as phishing scams, ransomware, and data leaks (Sharma, Singh & Sharma, 2009). Most of the prior research revolves around the technological and economical tariffs of cloud usage, whilst the practical cyber security solutions for the SMEs are not studied sufficiently. There are standard lists such as the ISO/IEC 27001 standard and the NIST framework The problem is that these frameworks are adopted in some way, but they are not used enough to address the specific issues facing SMEs in cloud adoption (Mujinga, 2020). To support this research, this study will seek to provide the following objectives: This study seeks to provide the following objectives: This research uses both numerical and non-numerical data: it is conducted using both qualitative and quantitative data collection techniques. From industries such as retail, healthcare, manufacturing, professional services, examples of failures and difficulties of SMEs will be examined. These industries have been selected to represent their potential different readiness for adoption owing to characteristics such as level of technology access, regulation and support as indicated in Gonzalez et al. (2013).

The study will target companies which have implemented cloud solutions effectively and firms that experienced major barriers to Cloud adoption. Proposed as following; by making the comparison of these cases, the study will point out best practice and challenges, which enable to offer practical knowledge for the similar SMEs (Renaud & Ophoff, 2021).

To guide SMEs in adopting effective cyber security strategies, the study will focus on two established frameworks: ISO/IEC 27001 and NIST. These frameworks provide more prescriptive rules of engaging with the cloud and managing issues such as hacking of cloud computing systems or leakage of data. ISO/IEC 27001 framework offers plans that can be adapted to the SMEs practical needs, and NIST's framework focuses on the protection, detection, response, and recovery of SMEs against the threats (Renaud & Ophoff, 2021).

Furthermore, this research will examine how these frameworks assist SMEs in achieving the compliance goal especially GDPR compliance that is compulsory for multinational ventures (Lokuge & Duan, 2021). Nonetheless, these frameworks are critical as indispensable instruments in managing risks and protecting the effectiveness and stability of cloud operations.

The research approach used in the work is a mixed method of qualitative and quantitative analysis of case study findings and survey data allowing for the SMEs to provide practical recommendations on how to approach the cyber security matter proactively while integrating the cloud solutions.

IV. RESULT

The study also pointed out the following important problems observed in cyber security of SMEs during clouds adoption. The following challenges are outlined and their consequences stated in Table 1. Probably the biggest challenge is data confidentiality since most organizations fail to implement proper access control mechanisms, opt for suboptimal encryption, and harbor susceptible third parties (Renaud & Ophoff, 2021; Mujinga, 2020).

The second issue is a shortage of IT specialists; indeed, most SMEs lack dedicated staff, including IT and cyber security specialists. This lack of specialist skills drives reliance on third parties and various risks emerging if these third parties do not meet the security levels that should be on board in learning institutions (Yuen & Baskaran, 2023). Table 1 as also previously highlighted, two particular challenges are thus compliance with all regulatory requirements and the need to ensure quality health services. It can therefore be argued that regulatory frameworks such as the GDPR and the PCI DSS pose a significant amount of difficulty when implementing particularly for Cross-border SMEs (Lokuge & Duan, 2021; Hutchings et al., 2013). Last but not the least, the existing threats of SMEs can be summarized as: The growing and progressive threats including ransomware and phishing attack are also potential threats if cloud vulnerabilities are not managed proactively (Hutchings et al., 2013).

These challenges understate the need for an inclusive and specific cyber security approach for SMEs.

Table 1: Top Cyber security Risks That SMEs Experience as They Move to the Cloud

Cyber Security	Description	Frequency	Impact Level
Data Breaches	Poor encryption and poor controls over accesses resulting to unauthorized access to important Information.	High	Critical
Lack of IT Expertise	Lack of internal skills for proper handling of cloud security, and Risk assessment and management.	Moderate	High
Compliance with Regulations	Legal risks due to inability in Maintaining compliance to the data protection laws including GDPR.	High	High

Based on this work, major measures that can be identified from the SMEs to mitigate cyber security risk during the process of cloud adoption are as follows accomplished. An overall description of these strategies and their benefits are presented in the following table (Table 2).

Among them one of the most recognized ones is the adoption of the zero-trust models through which any request made to the system is tested for authenticity and allowed in even if it comes from within the

Strategy	Description
Zero-Trust Models	Validates the integrity of each user at the time he/she tries to connect, thus limiting threats posed by intrusion activities.
Employee Training	Briefs staff and members on phishes, secure passwords, and practices that will reduce human factor mistakes.
Regular Updates and Patching	Prevents risks by updating systems and Software's regularly from where vulnerabilities are known.
Multi-Factor Authentication	Enhances security access since the user has to submit several types of identification.
Managed Security Services	MSSPs give surveillance and responsiveness to help SMEs strengthen their cybersecurity.

Table 2: Strategies of Managing Cybersecurity Risks in SMEs

organization. This is mostly because any user and device that wants to seek entry to a resource is examined to determine if it has the permission to do so (Renaud & Ophoff, 2021). This is why training programs are very helpful in the management of risks in organizations. By training and making the employees aware, the SMEs effectively reduce the possibility of human error, which is a main root of almost all the cyber threats (Kushwah et al., 2023). This enhances the protection of a system against developed threats that are typical path for the attackers (Mujinga, 2020). This one is also adopted by SMEs and aims at having several ways of confirming one's identity when gaining access. Finally, it is worth noting that the majority of SMEs depend on MSSPs to offer them outsourced, managed security services intended to monitor, detect, and respond to threats occurring in real-time.

This approach provides what SMEs can afford or may not have internally to enhance the security condition for their business (Lokuge & Duan, 2021).

These, as shown in table 2 below, are precaution measures that should be taken by SMEs to mitigate current emergent risks linked to cloud computing.

The delivery of cloud solutions has provided substantial and complex changes in the business processes and security solutions of the SMEs and other enterprises to achieve the best level of effectiveness and adaptability and security. One of those changes is moving from static on premise installations to more complex and less expensive cloud-based systems. It has resulted to savings of the SME cost in terms of operational costs for performing key operations with more focus on operations as they attain high levels of technological facilities than the large companies (Yuen & Baskaran, 2023). The cloud solutions have also improved the availably of data and also revolute the manner in which SMEs engage in sharing of information. One can list such features as real- time data exchange, which also allows for different forms of remote collaboration, which would help SMEs extend and improve their daily activities; the opportunity to have work accomplished by a distributed team without concerns about distance (Mujinga, 2020). Similar benefits include application for reception of people and penetration into better markets that create new opportunities for SMEs. In other words, cloud adoption has dramatically changed how cyber security should be approached.

Another advantage of relying on cloud solutions is that, contrary to traditional solutions, these functions are arranged by the cloud providers, thereby when engaging cloud solutions for their businesses, the above listed functions of data encryption, update frequencies as well as threat detection mechanisms are already incorporated into the SME's cloud solutions, making their management easier (Lokuge & Duan, 2021). These capabilities have enabled small enterprises in particular to detect emerging threats early enough and deal with them in the best way possible thereby enhancing on their cyber security status. However, the use of cloud also raises the issue of moving in the understanding of the security of information networks.

Cloud computing is being adopted more used by SMEs for their operations, and they are applying various strategies like ordinary audits, compliance to relevant legislations and laws, and the latest forms of authentication to protect their cloud environments (Renaud & Ophoff, 2021). This shift in SME attitude can be attributed to a heightened understanding of the fact that these companies need to embrace more proactive and adaptive form of cyber security due to increase in new threats. In total, cloud solutions turned not only into the powerful tool that greatly changed the flexibility and efficiency of SME operations but also into the proper source of the systematic approach to the key problem of the modern world cyber security

DISCUSSION

Therefore, the results of this study lie in the acknowledgement of cloud solutions by the SMEs and recognition of the role of the cloud technology as a strategic resource for business growth in the current environment. The utilization of cloud solutions enables SMEs to reduce their operational expenses while growing their businesses and increasing the general level of performance as a factor that may help them remain viable in the constantly evolving markets (Yuen & Baskaran, 2023). These novelties make a lot of possibilities for SMEs from the position of similar services and applications that can offer only the large companies because of the monetary and technical facilities.

From a cyber-security perspective, the study reveals a dual aspect: as much as cloud computing provides a number of advantages, it also gives rise to many risks. These security aspects which are offered by CSPs; encryption, automatically updates, and threat detection enhance SMEs' security (Lokuge & Duan, 2021). However, to address the management of vulnerabilities while improving the protection, SMEs need to go beyond these capabilities. The study further reveals the aspect of staff training and compliance to widely accepted cyber security frameworks as other approaches that can be implemented (Renaud & Ophoff, 2021). Such strategies are not preventive but are fundamental in creating a holistic security approach that flex with emerging risks. It also influences the whole economy and society by the adoption of cloud technologies even further.

SMEs, through adopting the cloud computing technology, an opportunity to foster economic stability and incomes generation. Also, the adoption of cloud solutions promotes an environment for embracing technology innovation—paramount in today's dynamic commercial environment (Mujinga, 2020). The above cultural change propels organizations to develop new ideas that increase competitiveness in the modern global economy.

One of the largest concentrations of this research is on the policy fabric and the accessibility of knowledge-based tools to help SMEs manage obstacles, including a deficit of IT staff and much legal compliance information. Overcoming these barriers is critical to SME's engaging and sustaining value in cloud solutions and putting the company in a competitive place in the digital business environment.

CONCLUSION

Cloud solutions are now a major step in the digital transformation process of SMEs in the global level. There are many advantages of utilizing cloud computing which include high flexibility, cost saving and access to new innovative solutions, but there are some disadvantages, which consist of high security risks. The risk environment due to the shift to the cloud means that SMEs need to consider their security positions as they seek to secure their information and Organizations' reputation.

This study focuses on how and why cloud adoption and digital transition are connected to the threats SMEs encounter. Nevertheless, it should be crucial to understand that achieving business objectives does require cloud solutions, but they must be provided with a proper cyber-security strategy. SMEs can achieve cloud environment safety with three recognized standards, including ISO/IEC 27001, NIST-CSF, and CIS Controls. These frameworks are not only protections, but accelerators of change, to ensure that security does not stifle innovation in this digital age.

However, it has been seen that due to the aspects of cloud computing, many SMEs are still struggling with the issue of cyber security. As with most things security-related, delaying decisions in this area is unadvisable and waiting for a security mishap to happen may be downright disastrous. SMEs must focus on three key areas: improving cyber security knowledge, choosing proper frameworks, and profiting from constant security assessment. Such actions will minimize risks and create appropriate security-oriented organizational climate that will boost further, continuous and sustainable business development. Last, cyber security is the foundation of successful and sustainable business within the current complex digital environment for SMEs. For any SME to lacked a strong cyber security posture, they can become entrapped by cyber risks that bring negative impacts to operations and customers. With SMEs moving more of their IT infrastructure to the online platform and investing in the cloud as their businesses grow, they will need to focus on security to unlock their growth and innovate successfully in a competitive global environment.

Future studies should investigate the effects of those frameworks on resilience of SMEs and innovative ways of mitigating new risks such as AI attacks and quantum decryption. Managing these challenges is the key to an SME's survival and success in today's fast growing and increasingly globalized economy. They can become entrapped by cyber risks that bring negative impacts to operations and customers. With SMEs moving more of their IT infrastructure to the online platform and investing in the cloud as their businesses grow, they will need to focus on security to unlock their growth and innovate successfully in a competitive global environment.

Future studies should investigate the effects of those frameworks on resilience of SMEs and innovative ways of mitigating new risks such as AI attacks and quantum decryption. Managing these challenges is the key to an SME's survival and success in today's fast growing and increasingly globalized economy.

REFERENCES

[1] Adam, I. O., & Musah, A. (2015). Small and medium enterprises (SMEs) in the cloud in developing countries: A synthesis of the literature and future research directions. *Journal of Management and Sustainability, 5*(1), 115–130. https://doi.org/10.5539/jms.v5n1p115

[2] Hutchings, A., Smith, R., & James, L. (2013). Cloud computing for small business: Offenses and security risks and how they can be prevented. *Trends and Issues in Crime and Criminal Justice, May* (456), 1–8.

[3] Inggarsono, Y., Goman, M., Paembonan, A. P., & Asri, M. (2015). Small and medium enterprises (SMEs) in the cloud in developing countries: A synthesis of the literature and future research directions. *Journal of Management and Sustainability, 5*(1), 115–130. https://doi.org/10.5539/jms.v5n1p115

[4] Lokuge, S., & Duan, S. X. (2021). Towards understanding enablers of digital transformation in small and medium-sized enterprises. *Proceedings of the 32nd Australasian Conference on Information Systems (ACIS 2021)*. https://doi.org/10.1080/08874417.2024.2386532

[5] Mujinga, M. (2020). Cloud computing inhibitors among small and medium enterprises. *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 1–5. https://doi.org/10.1109/ICISS49785.2020.9315905

[6] Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People, 1*(1), 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

[7] Sharma, K., Singh, A., & Sharma, V. P. (2009). SMEs and cybersecurity threats in e- commerce. *EDPACS: The EDP Audit, Control, and Security Newsletter, 39*(5-6), 1–49. https://doi.org/10.1080/07366981.2009.10798347

[8] Whitehead, G. (2020). Investigation of factors influencing cybersecurity decision-making in Irish SMEs from a senior manager/owner perspective (PhD thesis). National College of Ireland, Dublin. https://trap.ncirl.ie/4310/

[9] Yuen, T. M., & Baskaran, S. (2023). Going digital for SMEs: Strategies to operate and develop business models for sustainability and to take opportunities for achieving