Secure Tomorrow

Minet

AON | Global Network Correspondent

MINET THOUGHT LEADERSHIP

Minet is a trusted pan-African advisor that meets the uncertainties of tomorrow by delivering risk and human capital solutions today. As the largest Aon Global Network Correspondent, Minet has access to a network of over 50,000 colleagues in 120 countries as well as to proprietary data, research and analytics which enable us to manage and secure the risks of tomorrow and provide clients with an unrivaled advantage. For more information, please visit www.minet.com

Risk. Reinsurance. People.

THE ROLE OF INSURANCE IN CYBERSECURITY RISK MANAGEMENT: TRENDS AND BEST PRACTICES IN AN AFRICAN CONTEXT

July 4th, 2023

Africa is the world's second-largest continent in terms of geographic area and population and has in recent years emerged as a fast-growing digital giant thanks to a young population.

With the recent COVID-19 pandemic, lockdowns imposed across the continent resulted in a surge in remote connectivity services as organizations in Africa rapidly built and continue building infrastructure and services to ensure business continuity. At the same time, internet penetration and smartphone access accelerated the adoption of digital technologies. This increase in the level of digital growth however comes with a potent increase in the level of cybercrime necessitating cybersecurity.

In today's digital era, cybersecurity has become a critical concern for organizations across the globe, and Africa is no exception. With the increasing number of cyber threats and attacks targeting businesses of all sizes, it is essential for organizations in Africa to adopt robust cybersecurity risk management strategies. One vital component of such strategies is the role of insurance in mitigating and managing cyber risks. In this article, we will explore the trends and best practices surrounding insurance in cybersecurity risk management specifically in an African context.

Several countries in Africa have witnessed a significant rise in cybercrime activities in recent years. The rapid digital transformation, increased internet penetration, and the proliferation of mobile devices have all created new opportunities for cybercriminals. According to the WEF Global Cyber Security Outlook 2022, there was a 31 percent year-on-year increase in cyberattacks in 2021 compared to 2020. With these developments, managing cybersecurity and privacy in a dynamic and vulnerable environment remains a major challenge for African enterprises. Africa is continuing to strengthen its data protection legal and regulatory framework with the adoption of cyber security policies and regulations across Africa currently being at 66 percent. To date, 36 of 54 African countries have data protection laws and/or regulations. 16 countries have signed the African Union Convention on Cyber Security and Personal Data Protection ("Malabo Convention") and 13 countries have ratified it.

Secure Tomorrow

Minet

Cyber Insurance.

Cybersecurity Insurance has emerged as a valuable tool in managing cybersecurity risks. Cybersecurity insurance, also known as cyber insurance or cyber risk insurance, is a specialized form of insurance coverage designed to protect organizations from financial losses and liabilities resulting from cyber-attacks, data breaches, and other cybersecurity incidents. It provides financial protection to organizations in the event of a cyber incident, covering costs associated with data breaches, ransomware attacks, business interruption, legal expenses, and regulatory fines. It also extends to cover any expenses related to incident response, forensic investigations, and data recovery.

In terms of trends, cyber insurance in Africa is experiencing a surge in demand: As more awareness about cyber threats grows, more and more organizations are recognizing the importance of cyber insurance. According to a 2022 study, the global demand for cyber insurance is projected to grow from $16.66 billion in 2023 to $84.62 billion by 2030 exhibiting a compounded annual growth rate of 26.1%.

There is also customization of policies to address the needs of organizations in Africa. Insurance intermediaries are working with clients and insurance providers to offer more customized policies to address the specific needs and risk profiles of organizations in Africa. This shift and flexibility allow organizations to have coverage that aligns with their unique cybersecurity challenges and budgets. In Nigeria, the Cybersecurity Alliance for Mutual Progress (CAMP) has partnered with risk carriers to offer affordable cybersecurity insurance coverage to small and medium-sized enterprises (SMEs). This initiative aims to enhance the resilience of Nigerian organizations against cyber threats. In South Africa, several insurance companies have introduced cyber insurance products tailored to the needs of specific industries such as healthcare, financial services, and retail. These industry-specific policies address the unique cybersecurity challenges faced by organizations in those sectors.

There is also evident collaboration with governments and regulatory bodies: African governments and regulatory bodies are increasingly emphasizing the importance of cybersecurity and promoting the adoption of cyber insurance. Examples of initiatives like this include the South African Insurance Association (SAIA) which has been actively engaging with government entities to develop frameworks that encourage businesses to adopt cybersecurity insurance.

As organizations become increasingly aware of cyber threats, cyber risks, and the existence of relevant and tailor-made insurance products, it is imperative that they implement best practices such as assessment and mitigation. Insurance alone is not a panacea for cybersecurity risks. Organizations must implement robust cybersecurity measures, conduct regular risk assessments, and develop incident response plans to complement their insurance coverage. Insurance providers often require evidence of effective risk mitigation practices before providing coverage, emphasizing the importance of a proactive approach to cybersecurity. It is necessary that before purchasing cyber insurance, organizations conduct a thorough risk assessment to identify potential vulnerabilities and develop a robust internal cybersecurity strategy. Risk carriers often require evidence of effective risk mitigation practices before providing cyber coverage.

Upon understanding the potential vulnerabilities and developing sound cyber security strategies, organizations may then seek cyber insurance coverage. Organizations must carefully review and understand the coverage offered by different insurance policies. It is crucial to ensure that the policy covers a broad range of cyber risks, including data breaches, ransomware attacks, business interruption, and reputational damage. A prudent and experienced intermediary such as Minet will be able to help the organization obtain comprehensive coverage for its cyber security needs.

Thirdly, organizations should have a well-defined incident response plan. This is critical for minimizing the impact of any cyber incidents. Most Cyber insurance policies will require organizations to have documented incident response procedures in place.
Lastly, organizations should continuously monitor and update their cyber risk programme and strategy. With the prompt development of technology, cyber threats are also evolving more rapidly. It is important that organizations regularly review and update their cybersecurity measures. Some risk carriers may furthermore require regular assessments and security audits to maintain coverage.

In conclusion, as Africa continues its digital transformation journey and embraces the opportunities presented by technology, the importance of cybersecurity and insurance cannot be overstated. The role of insurance in cybersecurity risk management in the African context is crucial in mitigating financial losses and ensuring business continuity in the face of cyber threats. By understanding the trends and adopting best practices, African organizations can effectively navigate the complex cybersecurity landscape and protect themselves against potential damages.
Furthermore, the collaboration between insurance providers, governments, and regulatory bodies in promoting cybersecurity insurance highlights the recognition of its significance on the African continent. This partnership encourages businesses to prioritize cybersecurity and invest in comprehensive insurance coverage tailored to their specific needs and risk profiles.

Keith Enoch Wabwire | Claims Handler | Minet Uganda

References

1. https://www.fortunebusinessinsights.com/cyber-insurance-market-106287
2. United Nations Conference on Trade and Development
3. WEF Global Cyber Security Outlook 2022
4. https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45#:~:text=The%20Personal%20Data%20Protection%20Act,Electronic%20and%20Postal%20Communications%20Act.
5. https://www.forbes.com/sites/forbestechcouncil/2022/08/02/africas-chaotic-legal-and-regulatory-cybersecurity-landscape-requires-harmonization/?sh=e6d17011a9ab
6. KPMG Africa Cyber Security Outlook Report 2022