Caroline Irungu

Manager
Advisory
Tel: +25 420 280 6000
Email: cirungu@kpmg.co.ke

Cyber risk management in the East African insurance industry

The insurance sector is undergoing significant transformation, evidenced by the high rate of digital transformation. In addition, data has become a valuable resource, making companies that collect and process data vulnerable to cyberattacks. Insurance companies are often exposed to this risk due to the extent of sensitive customer information collected from policyholders. This article highlights key cyber risk trends prevalent in the East African insurance sector, common cyberattacks and critical strategies to implement to effectively safeguard information assets.

Cyber risk trends

Digital transformation

The use of new technologies has been on the rise with the primary aim to enhance the customer experience. The implementation of digitisation through automated underwriting, claims processing and digital policy management are key areas for strategic growth. However, the increased use of digitisation in these processes increases the extent of vulnerability to cyber risk.

Data privacy and regulatory compliance

The recent implementation of data protection regulations across the region, such as the Kenya Data Protection Act (2019), The Data Protection and Privacy Act of Uganda (2019), Rwanda's Data Privacy Law (2021) and Tanzania's Personal Data Protection Act (2022), demonstrates the importance placed by regulators in the protection of personal information of data subjects.

Cloud solutions

Insurance providers have now begun to use cloud computing for storage and processing of large amounts of data. Cloud solutions provide scalability, savings and operational flexibility. However, this shift increases the exposure to cyberattacks, particularly when organisations fail to enforce strong security measures to protect cloud infrastructure. Misconfigured cloud settings, weak authentication mechanisms and insecure application programming interfaces are common points of exploitation.

Digital fraud

With more digital connections established between internet users in today's world, cyberattackers have turned towards exploiting weaknesses in systems. This results in the perpetration of cyber-enabled fraud, including policy manipulation, false claims and identity theft. This trend is particularly common with mobile insurance services within the region whereby attackers exploit poor authentication processes to file fraudulent claims.

Cyberattacks in the insurance industry

Ransomware

As the cyber threat landscape continues to evolve, ransomware continues to be one of the more prevalent cyber threats faced by insurance companies. Attackers gain access to critical business information such as customer records, policyholder information and claims documentation, after which they encrypt and demand a ransom for decryption. In most instances, organisations are caught between paying the ransom with no guarantee of data retrieval or losing access to vital private and confidential information, resulting in operational losses, system downtime and reputational damage.

Phishing

Phishing attacks also continue to pose a significant risk as fraudsters target internal stakeholders through fake emails. These messages often look genuine, as if they were sent by customers or trusted institutions. When an employee clicks on malicious links or downloads an attachment, attackers open scripts that enable them to gain unauthorised access into the environment. This allows the attacker to steal login credentials, amongst other private information, that would help in perpetuating other forms of attacks such as data breaches or malware dissemination.

Third-party vendor risk

Insurers frequently outsource key processes such as claims processing, IT services or cloud storage to third-party vendors. Vulnerabilities present due to weak cybersecurity at the third-party vendor can be taken advantage of by cyberattackers with a detrimental downstream impact on the insurer.

Data breaches

Insurance companies handle large volumes of personally identifiable information such as names, addresses, identification numbers and financial details. Cybercriminals target this data for a variety of malicious reasons, including identity theft and financial fraud. Not only do data breaches lead to direct financial losses, it also leads to the erosion of trust amongst customers and other key stakeholders, potentially resulting in regulatory penalties.

Strategic initiatives to assist with the protection of information assets

To mitigate the growing risk of cyberattack in East Africa, insurance companies would be encouraged to implement comprehensive cybersecurity strategies. Set out below are key considerations when designing your information asset protection strategy.

Investment in cybersecurity infrastructure

Insurance companies are encouraged to invest in cybersecurity infrastructure such as firewalls, intrusion detection systems, encryption and multi-factor authentication. Regular system updates and patches help reduce vulnerabilities that hackers may exploit.

Cybersecurity training and awareness

Safety awareness is another important lever in designing your cyber risk strategy. All stakeholders, such as employees and vendors who have access to the organisation's infrastructure, should be regularly trained on how to recognise phishing attempts or suspicious emails among other types of social engineering. Regular simulations can help equip stakeholders with the necessary knowledge in responding effectively to potential threats.

Incident response planning

This step involves developing and maintaining an incident response plan which outlines specific steps that must be taken in the event of a cyberattack. This plan must include the identification of key personnel responsible for incident management, communication protocols as well as procedures for minimising attack impacts.

Secure third-party relationships

Insurance companies are encouraged to undertake rigorous vetting processes prior to onboarding third-party vendors, due to hazards posed by vendors that are external entities. This includes conducting third-party risk assessments that will inform the cybersecurity clauses to be incorporated during contracting, carrying out regular security assessments of vendors and setting up self-attestation mechanisms to ensure compliance with industry standards.

Data encryption and access controls

The employment of data encryption is another key control to consider, both at rest and in transit, to ensure that sensitive information remains protected even if it gets into the wrong hands. Additionally, access to critical systems and data should be restricted to authorised personnel, and strong authentication measures should be enforced.

Regular security audits

Routine security audits and penetration testing can help insurance companies identify vulnerabilities within systems and processes. By proactively addressing these weaknesses, insurers can reduce the likelihood of successful cyberattacks.

Cyber insurance

Given the evolving cyber threat landscape, insurers should consider purchasing cyber insurance to mitigate the financial impact of potential attacks. This coverage can help address costs associated with breach response, legal fees and regulatory fines.

Conclusion

Insurance companies are consistently and highly exposed to the risk of cyberattack, considering the extent of information assets held. Awareness of the cyberattack landscape is essential to the design of effective countermeasures. However, this risk can be constructively managed by investing in cyber security infrastructure, conducting regular employee training, implementing incident response planning, and performing third-party risk management assessments. Given the ever-evolving risk landscape, constant vigilance and ease of adaptability have become the new norm.