OLEA NEWS

JUNE 2023

OLEA INSURANCE SOLUTIONS AFRICA - www.olea.africa - info@olea.africa

CYBERSECURITY, A MAJOR CHALLENGE FOR YOUR BUSINESSES |
CYBER INSURANCE: PROTECT YOUR BUSINESSES

CYBERSECURITY, A MAJOR CHALLENGE FOR YOUR BUSINESSES

Bryan Rangapanaiken, Group Information Technology Security Manager, OLEA.

What is cybersecurity and what are its challenges?

Cyber security is the set of measures and practices put in place to protect computer systems, networks, data and users from digital threats and attacks.

The growing dependence on digital technologies in Africa has a major impact on the continent's businesses. Rapid advances in information and communication technologies (ICT) have transformed the day-to-day operations of African companies. However, this growing dependence also presents significant challenges. Interpol estimates that cybercrime costs Africa $4 billion a year.

Cybersecurity challenges for African companies are multiple and crucial. They include the protection of sensitive data, the prevention of cyber-attacks, the preservation of confidentiality, integrity, the availability of information, as well as ensuring user confidence and compliance with data protection regulations. Cybersecurity aims to anticipate, detect and respond effectively to security risks and incidents in order to maintain a secure and reliable digital environment for individuals, businesses and organisations.

What are common cyber threats for an African company?

The top five cyber threats in Africa identified in the latest Interpol report are:

1. Online scams: Fake emails or SMS claiming to come from a legitimate source are used to deceive individuals into revealing personal or financial information.

2. Digital extortion: victims are led to share compromising images that are used for blackmail.

3. Business Messaging Compromise: Criminals hack email systems to obtain information about the company's payment systems, then deceive the company's employees to transfer money to their bank account.

4. Ransomware: Cybercriminals block IT systems in hospitals and public institutions, then charge money to restore functionality.
5. Botnets: Compromised machine networks are used as a tool to automate large-scale cyber-attacks.

Source: Interpol African Cyberthreat Assessment Report

How can employees be made aware of cyber threats?

Cyber security awareness is critical to protecting businesses from cyber threats. Here are some effective measures to put in place to raise employee awareness and strengthen company security:

Cybersecurity training: The most important factor is training. Organise regular training sessions to familiarise employees with common cyber threats. By informing them about the techniques used by cybercriminals, you help them detect and prevent potential attacks.

Safety policies: Establish clear safety policies and communicate them to all staff. These policies should address topics such as the use of strong passwords, secure information sharing, access to sensitive data and the use of personal devices in the workplace.

Simulation exercises: Conduct cyber-attack simulation exercises to allow collaborators to apply their cybersecurity knowledge. These simulated exercises may include phishing attacks, intrusion attempts or emergency situations.

Regular communication: Maintain regular and clear communication on cybersecurity news. Send newsletters, alert emails or internal announcements to keep employees informed of the latest developments and safety measures.

In conclusion, cybersecurity awareness is a crucial element in protecting businesses. By implementing measures such as training, security policies, simulation exercises and regular communication, companies can increase the vigilance of their employees and reduce cybersecurity risks.

Cyber awareness must be an ongoing priority and integrated into the corporate culture.

What is OLEA doing to build strong cybersecurity infrastructures?

At OLEA, the founders quickly understood the importance of investing in securing our infrastructure and IT tools. In partnership with one of the leaders in cybersecurity training, we have implemented various organisational measures to increase awareness and accountability among all our employees.

OLEA demonstrates its commitment to optimal security of its infrastructures, in particular by having implemented with its partners and suppliers' security policies for information systems meeting the requirements of several standards and certifications: PCI-DSS certification, ISO/IEC 27001 certification, GDPR certification, SOC 1 TYPE II and SOC 2 TYPE II certifications.

OLEA has also partnered with Microsoft Gold Partner certified partners to secure its cloud infrastructure.

This includes the implementation of security solutions such as:

- 1.Identity Protection
- 2.Email Protection
- 3.Mobile Device Management
- 4.Endpoint Detection and Response
- 5.Mobile Application Manangement
- 6.Data Loss Prevention

By implementing these various security measures, OLEA strengthens the protection of its data and that of its customers, prevents potential threats and guarantees compliance with privacy and security regulations. In addition, OLEA continues to evolve and improve its security practices to meet the changing needs of its customers and current and future security challenges.

CYBER INSURANCE: PROTECT YOUR BUSINESSES

Ayouba Seydou, Group Placement and Reinsurance Director, OLEA.

We are facing more and more data breaches that are making headlines around the world, loss of personal and corporate data that have significant consequences.

The majority of articles relate to the type of data loss that impacts individuals at a personal level: credit card numbers, medical records, dates of birth, etc.

We should also be aware of the impact of the loss of business data and information such as intellectual property that, in the hands of a competitor or even an extortionist, can severely disadvantage the business.

What are the features and benefits of Cyber Insurance?

Cyber insurance allows a company to maintain its activity, reducing the financial impact (loss of turnover, costs and expenses, claims and assets), operational (confidentiality, reliability and availability) but also the consequences for the company's reputation and the information system.

The most frequent covers are of two kinds:

DAMAGE COVERAGE:

- Operating losses
- Costs incurred by the customer
- Protection of Personal Data
- Defence costs and sanctions in the course of an investigation
- Computer extortion attempts

CIVIL LIABILITY GUARANTEES:

- Complaints following a data breach or breach of personal data
- Multimedia warranty

Which companies are eligible for Cyber Insurance?

Virtually all companies process personal data on a daily basis, including ID card numbers, employee profiles, credit card information, and sensitive customer information.

These same companies are faced with responsibilities if this data falls into the wrong hands or into the public domain.

From small companies to multinationals, all are involved and eligible.

Why don't companies massively subscribe to Cyber Insurance?

In my opinion several reasons:

1.The lack of awareness of threats, despite all the attacks we see in the media. Many think that this is limited to data loss or even operating loss.

2.The lack of awareness of guarantees, for many covers, or even the cyber offer is unknown. The focus is on visible risks, global damage, civil and professional liability.

3.Many companies believe that a good antivirus with a firewall is enough to prevent this risk.

4.The complexity of cyber questionnaires, which are very specific and require collaboration between the business and IT technicians.

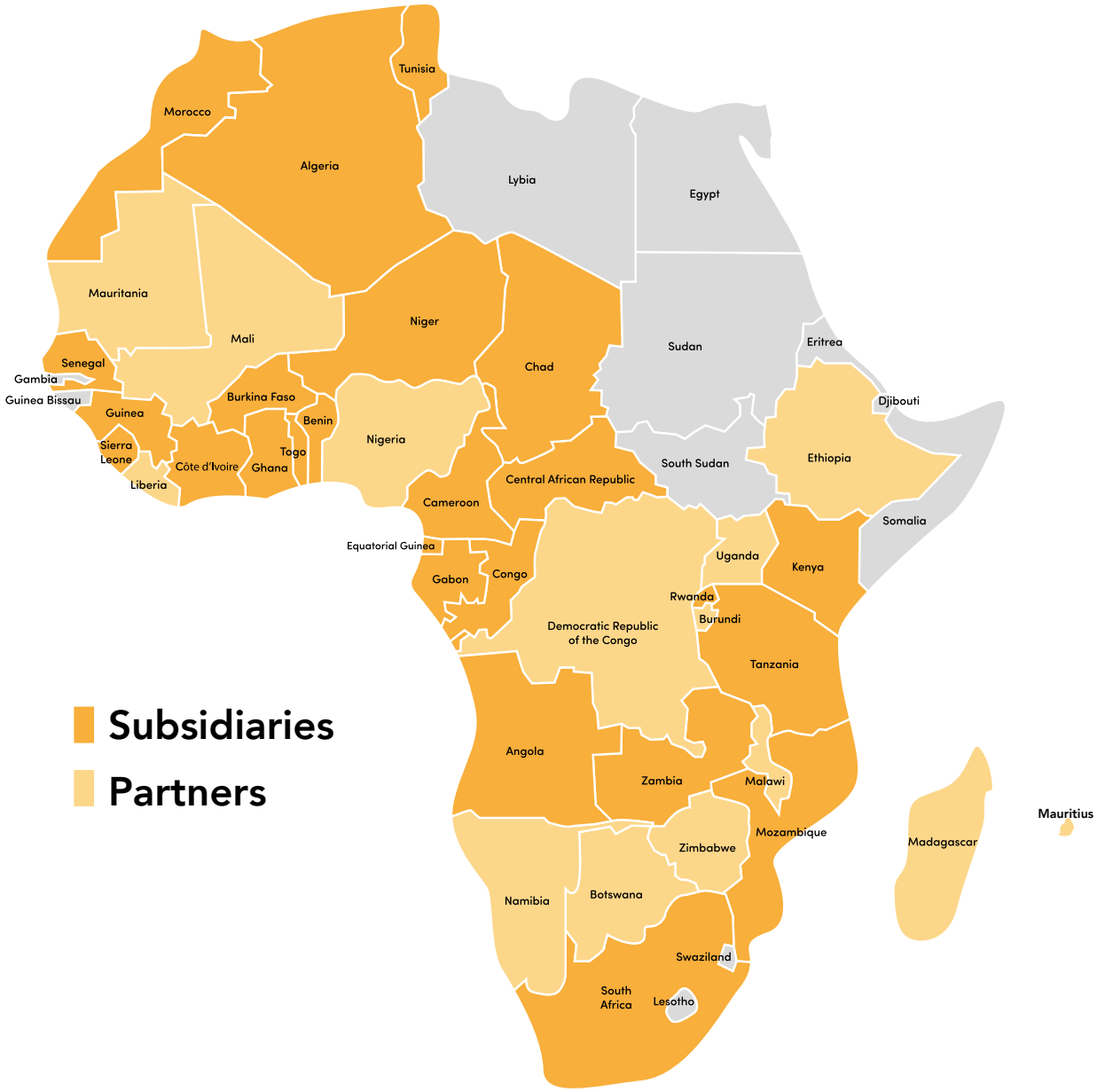
5.Finally, the maturity of IT systems architectures. Indeed, even when companies are aware of the importance of coverage, they do not meet the criteria required by insurers in terms of prerequisites. It should also be noted that the vast majority of intrusions, security vulnerabilities are the result of human errors, which require almost continuous training/ awareness of teams to remain vigilant. The results on these training transfers are extremely positive.

That is OLEA's main strength. We assist businesses that want to sign up for Cyber Insurance very early by conducting security assessments to compile a list of all the requirements. We also provide entertaining, engaging, and ongoing online trainings to improve team awareness for our clients.

For an insurer to agree to rate this risk on behalf of our clients, these factors and this «upgrade» must exist.

DO NOT HESITATE TO CONTACT US FOR ALL YOUR NEEDS RELATED TO THE SUBSCRIPTION OF THIS «CYBER» INSURANCE.
INFO@OLEA.AFRICA

THE OLEA GROUP
AND ITS 24 SUBSIDIARIES IN AFRICA



South Africa | Algeria | Angola | Benin | Burkina Faso | Cameroon | Central African Republic | Congo | Côte d'Ivoire | Gabon | Ghana | Guinea | Kenya | Morocco | Mozambique | Niger | Rwanda | Senegal | Sierra Leone | Tanzania | Chad | Togo | Tunisia | Zambia