Let’s talk about

CYBERSECURITY BASICS

info@africacybersec.com
www.africacybersec.com

CONTENTS

ABOUT THE AUTHORS

Cedric Ngabonziza

has 10 years of experience in Information Security, a reputation for anticipating emerging threats, Cedric has worked with a diverse range of organizations, delivering customized solutions to protect their digital assets.

His ability to communicate complex security concepts in a clear and accessible manner has made him a trusted advisor to both executives and IT teams.

Eric Ngabonziza

has 30 years of experience in Africa and North America, designing, configuring, implementing and deploying various network and data security solutions for companies such as CIE -Côte d'Ivoire, Wassi Technology, Blackberry, IBM, Bell Mobility, NRT Technologies, Vonage Canada, Richardson Wealth etc.

Eric speaks 5 languages fluently including English and French.

INTRODUCTION

Cybersecurity is the practice of protecting network systems, programs and data from criminal or unauthorized users by protecting or defending information and communication systems.
Cybersecurity is a combination of strategies, policies and standards used to protect cyberspace.

What is cyberspace?

- Internet
- internet of things
- Ethernet networks
- Wireless networks
- Broadband networks
- smartphones
- Laptop
- Tablet
- PC

When and how cybersecurity began?

The researcher named Thomas Bob created the creeper virus around the year 1970 and it was leaving a message saying "I'm a creeper, catch me if you can"

In 1972, Ray Tomlinson created the first antivirus software called Reaper to remove creeper.

CHAPTER I

GETTING TO KNOW CYBERSECURITY

Confidentiality

The ability to protect data so that unauthorized parties cannot see the data.

Encryption, Access control can be used to achieve the confidentiality.

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext into incomprehensible text, also called ciphertext.

Access control is a data security process that allows organizations to manage who is authorized to access company data and resources.

Integrity

Fight against the inappropriate modification or destruction of information, and in particular guarantee the non-repudiation and authenticity of information

Hashing, Digital signature and Certificates can be used to verify the integrity of a data.

Hashing is a one-way function that transforms a file or string of text into a single summary of the message.
The hashing value is calculated by a hashing algorithm using the binary data of a particular file.

A digital signature is a cryptographic output used to verify the authenticity of data.

A security certificate is used as a means of providing a website's security level to general visitors, Internet service providers (ISPs), and web servers.

Availability

Means ensuring rapid and reliable access to a data by using Fault Tolerance, Redundancy, Load-balancing or Backup.

Fault tolerance is a process that allows an operating system to respond to hardware or software failure.
Fault tolerance refers to the ability of the system to continue operating despite failures or malfunctions.

Data redundancy refers to the practice of maintaining data in two or more places within a database or data storage system.

Data redundancy ensures that an organization can provide continuous operations or services if something goes wrong with its data, such as data corruption or loss.

Load balancing is the process of distributing network traffic across multiple servers. This ensures that no server supports too many requests.

The goal of **backup** is to deposit data in a separate, secure location, away from devices, where it can be recovered if necessary.

CHAPTER II

CYBERSECURITY PROFESSIONALS

Cybersecurity professionals or information security professionals have a lot of responsibilities, but the core of their duties is to protect online data and infrastructure/networks from compromise.

Cybersecurity professionals protect our most sensitive information like bank account information

If a breach occurs, cybersecurity professionals are responsible for identifying the problem and finding a solution quickly.

Cybersecurity roles and positions

Cybersecurity administrator: Ensures the proper functioning of security systems on a daily basis
Cybersecurity Specialist: Maintain an organization's automated security systems and employee ID card system
Cybersecurity Analyst: Plan and execute flawless security measures
Vulnerability Assessor: Identify system vulnerabilities and provide a solution
Incident Responder: Prevent and protect against threats
Forensic Expert: Protecting the cyber world and helping law enforcement
Cybersecurity Auditor: Find weak points in a security system before hackers do and identify systems misconfiguration
Cryptographer: Responsible for writing code that hackers cannot decipher
Cybersecurity consultant: Advise and implement security solutions
Cybersecurity Manager: Responsible for managing security teams to ensure systems security
Cybersecurity Director: Establish rules, policies, procedures and resolve complex issues
Chief Information Security Officer (CISO): IT security expertise and business acumen

CHAPTER III

CYBERSECURITY COMPTENCIES

Interpersonal Skills

Displaying the skills to work effectively with others by doing the followings:

Showing sincere interest in others and their concerns
Demonstrating sensitivity to the needs and feelings of others
Interpreting the verbal and nonverbal behavior of others
Recognizing when relationships with others are strained
Demonstrating flexibility for change based on the ideas and actions of others
Maintaining open lines of communication with others
Encouraging others to share problems and successes
Establishing a high degree of trust and credibility with others
Demonstrating sensitivity, flexibility, and open-mindedness when dealing with different values, beliefs, perspectives, customs, or opinions

Integrity

Displaying strong moral principles and work ethic.

Abide by a strict code of ethics and behavior
Choose an ethical course of action and do the right thing, even in the face of opposition
Encourage others to behave ethically
Use company time and property responsibly
Perform work-related duties according to laws, regulations, contract provisions, and company policies
Understand that behaving ethically may go beyond what the law requires
Treat others with honesty, fairness, and respect
Make decisions that are objective and reflect the just treatment of others
Take responsibility for accomplishing work goals within accepted timeframes
Accept responsibility for one's decisions and actions and for those of one's group, team, or department
Learn from mistakes

Professionalism

Maintaining a professional presence.

Maintain composure and keep emotions in check
Deal calmly and effectively with stressful or difficult situations
Accept criticism tactfully and attempt to learn from it
Dress appropriately for occupational and worksite requirements
Maintain appropriate personal hygiene
Refrain from lifestyle choices which negatively impact the workplace and individual performance
Remain free from substance abuse
Project a professional image of oneself and the organization
Demonstrate a positive attitude towards work
Take pride in one's work and the work of the organization

Initiative

Demonstrating a commitment to effective job performance by taking action on one's own and following through to get the job done.

Persist and expend extra effort to accomplish tasks even when conditions are difficult or deadlines are tight
Persist at a task or problem despite obstacles or setbacks
Go beyond the routine demands of the job

Adaptability and Flexibility

Displaying the capability to adapt to new, different, or changing requirements.

Remain open to considering new ways of doing things
Actively seek out and carefully consider the merits of new approaches to work
Embrace new approaches when appropriate and discard approaches that are no longer working
Take proper and effective action when necessary without having all the necessary facts in hand
Easily adapt plans, goals, actions or priorities in response to unpredictable or unexpected events, pressures, situations and job demands
Easily shift gears and change direction when working on multiple projects or issues

Dependability and Reliability

Displaying responsible behaviors at work.

Behave consistently and predictably
Come to work on time and as scheduled
Arrive on time for meetings or appointments
Comply with organizational rules, policies, and procedures
Ask appropriate questions to clarify any instructional ambiguities

Lifelong Learning

Demonstrating a commitment to self-development and improvement of knowledge and skills.

Demonstrate an interest in personal and professional lifelong learning and development
Identify when it is necessary to acquire new knowledge and skills
Take steps to develop and maintain knowledge, skills, and expertise necessary to perform one's role successfully by
Integrate newly-learned knowledge and skills with existing knowledge and skills

Reading

Understanding written sentences, paragraphs, and figures in work-related documents.

Understand the purpose of written materials
Comprehend meaning and identify main ideas
Note details and facts
Detect inconsistencies
Identify implied meaning and details
Identify missing information
Review written information for completeness and relevance
Integrate what is learned from written materials with prior knowledge
Apply what is learned from written material to new situations

Communication

Listening, speaking, and signaling so others can understand.

Receive, attend to, understand, interpret, and respond to verbal messages and other cues
Recognize important information in verbal messages
Comprehend complex instructions
Identify feelings and concerns within verbal messages
Consider others' viewpoints and alter opinion when it is appropriate to do so
Apply active listening skills using reflection, restatement, questioning, and clarification
Effectively answer questions of others or communicate an inability to do so and suggest other sources of answers
Gain commitment and ensure support for proposed ideas
Attend to nonverbal cues and respond appropriately
Attend to visual sources of information (e.g., video)
Ascertain relevant visual information and use appropriately

CONCLUSION

You can get into Cybersecurity even if you don't have an IT background