TECH4DEV

INFORMATION SECURITY: A CRITICAL INFRASTRUCTURE FOR A NATION'S GROWTH

PRESENTED BY:
CYBERGUARDIANS

TEAM MEMBERS

RESEARCHERS

Lizzy Njoku
Ezinne Kalu
Mercy Momoh
Gladys Mwangi

EDITORS

Ifeoma Ibisi
Blessing Obasi
Matina Williams
Ibilola Odusegun

DESIGNER

Janet Oluwatoyin Olabode

PROBLEM

Mybusiness.com reported that 60% of small businesses close down six months after a cyber attack.

The Commonwealth Telecommunications Organization (CTO said that small businesses contribute 60% of total employment and up to 40% of national income (GDP) in emerging economies.

This report highlights why small businesses need to protect themselves against common cyber attacks as they can affect and disrupt security and personal data. A country with security systems will reduce the risk of privacy invasion of its citizens, thereby facilitating secure online transactions within the growing digital economy.

SOURCE: WEFORUM

IMPACT

A Nation or business can be impacted by cyberattacks in various ways. The impact does differ based on the type and extent of these cyberattacks.

Cyberattacks that are aimed at online businesses in a nation can lead to:

- Significant financial harm
- Operational disruption: business downtime
- Breach of national security: stunted economic growth
- Data breaches: theft of personal and financial information
- Electrical breakouts: failure of equipment, servers, software
- Reputational damage: loss of integrity, customers, and earnings
- Penalties & Fees: due to the release of customer information, court cases

SOURCE: TRYHACKME

FRAMEWORKS

CTO has been promoting the adoption of smaller cyberstandards such as Cyber Essentials, as existing standards such as ISO 27001 be too onerous for smaller organizations. Such cyber standards can help organizations protect themselves against common cyber attacks and thereby facilitate secure online transactions within the growing digital economy.

ASSETS

- Employees
- Contractors
- Hardware
- Software
- Information

VULNERABILITIES

- Unsecured APIs
- Misconfigurations
- Weak Credentials
- Outdated Software
- Broken Access Control

THREATS

- Malware
- Phishing Attacks
- Physical Theft & Vandalism
- Distributed Denial Of Service
- Inside Threat & Malicious Intents

SOURCE: CTO

CYBERGUARDIANS

SOLUTIONS

Confidentiality

- Encryption
- Authorization
- Access control
- Authentication
- Physical Security

Integrity

- Backups
- Checksums
- Install SSL Certificate
- Codes For Data Correction

Availability

- Physical Protection
- Computer Redundancy

The CIA triad security model aims to direct security leaders and teams with their data security and infrastructure. It is based on the principles of confidentiality, integrity, and availability.
The triad's objective is to assist businesses in creating their security strategy, rules, and controls, as well as a fundamental basis for new products, and technology.

CYBERGUARDIANS

BENEFITS

- Identify risks and reduce vulnerabilities
- Reduce threats and allow cyber security outcomes
- Prevent unauthorized access to sensitive information
- Reduce the likelihood of business and operation disruption
- Reducing the risk of data breaches and attacks in IT systems.
- Preventing disruption of services, e.g., denial-of-service attacks.
- Protecting IT systems and networks from exploitation by outsiders.
- Ensuring business continuity through data protection of information assets.
- Providing peace of mind by keeping confidential information safe from security threats.

SOURCE: REDTEAMSECURE

EFFECTIVENESS

- Confidentiality: By putting permissions, authentication, and authorization procedures in place to prevent unwanted access, this principle contributes to the security of customer and external data, thereby securing the nation's information.

- Integrity: This principle guarantees the accuracy of information. To uphold data integrity, it is necessary to encrypt data in transit, hash passwords, use version controls, and make use of intrusion detection systems.

- Accessibility: This guarantees that data is readily available and usable to meet business requirements. Lack of accessibility can cause business processes to stall or slow down, as well as prevent customers from accessing their information or associated software.

CYBERGUARDIANS

CONTRIBUTION SDGs 9.a

In fulfilling this, information security plays an important role in validating United Nations’ 2030 Sustainable Development Goals (SDGs) 9.a approach, according to which international trade contributes to the promotion of sustainable development.

- Information Technology enables better management of infrastructure and provides additional business opportunities through online services.
- Infrastructure is controlled and optimized by ICTs, power networks, water supplies, transportation systems, or telecommunication networks
- ICTs contribute to making cities smarter and more sustainable to improve the quality of life, concerning economic, social, environmental as well as cultural aspects
- Industrialization and the increase in productivity highly depend on the effective use of Information Technologies

CYBERGUARDIANS

THANK YOU

We are The CyberGuardians!!!

SECURITY PROJECT