



The Significance of Cybersecurity in Somali Businesses and Government Organizations

Abdiweli Mohamed Halane
Information Security Adviser
Hormuud Telecom

Contents

- Introduction
- Why Cyber Security is Important for business and government
- Cyber Security Goals
- What is cyber security
- What kind of attacks does the business encounter
- Targets of cyber attacks
- Purpose of Cyber Attacks
- Security Controls
- Problems Somalia is now having with cyber security
- Recommendations
- Conclusion

Introduction

Ref: <https://aag-it.com/the-latest-cyber-crime-statistics>



In 2021, 1 in 2 American internet users experienced account breaches.



1 billion emails were compromised, impacting 1 in 5 internet users 2022.



In 2022, data breaches cost companies \$4.35 million on average.



Globally, there were over 236.1 million attacks involving ransomware in the first half of 2022.



According to statistics 39% of UK companies, a cyberattack occurred in 2022.



Phishing is the most frequent cyberthreat that companies and people encounter.

Why Cyber Security is Important for business and government

- *Our world today rules by the technology, and we can't do without it at all. From booking our flight tickets, efficient operation of computer systems, communication, education, transactions, online booking leisure, and shopping, to catching with old friend technology plays significant role on it.*
- *However, the same technology may expose you when its vulnerable and could lead to loss essential data. Cyber security alongside with physical commercial security, has thus become one of the most important factor of industry and governmental organisations.*



- Cybersecurity is essential to businesses because it protects data from threats like data theft and/or misuse and keeps systems safe from viruses.
- The importance of cyber security increases as more and more business is conducted over networks of networks.
- Cybercriminals have always attacked information systems, and it is expected that these attacks will only grow in the future as information security increases. Nevertheless, there are reasonable precautions that businesses may take to reduce the dangers of cyberattacks.



Cyber Security Goals



Confidentiality:

Making information accessible only to those authorized to use it.



Integrity

Safeguarding the accuracy and completeness of information and processing methods



Availability:

Ensuring that information is available

What is cyber security



Protecting networks, data, computers, servers, mobile devices, electronic systems, and cyberspace against attackers is known as cyber security includes.



Network security: Is protecting a computer network against opportunistic malware, targeted attackers, and intrusions.



Application security: focuses on keeping software and devices free of threats.



Information security: Protects the integrity and privacy of data, both in storage and in transit.



Operational security: Is a processes and decisions for handling and protecting data assets including policies and procedures how and where data can be exchanged or stored, as well as the permissions users have when they access a network.



Disaster recovery and business continuity: How the company gets back to full operating capability after an incident by restoring information and operations. Business continuity refers to the strategy that a business uses to try to function in the absence of specific resources.



End-user education: Is the technique of defending computers, laptops, mobile phones, and tablets against malicious threats and cyberattacks is known as endpoint security.

What kind of attacks does the business encounter?

**Business
Email
Compromise**

Phishing

Malware

**Insider
Threats**

**Remote
Network
Vulnerabilities**

Ransomware

Data theft

**Social
Engineering**

**Man-in-the-
Middle Attack**

Targets of Cyber Attackers



Computer networks



Personal Computers



Critical infrastructure

Purpose of Cyber Attacks

1

*Bring down
systems*

2

*Disable
Networks*

3

*Disrupt/disable
essential
networks*

4

*Cripple
financial
networks*

5

*Steal or Alter
data*



So how do we secure
our information assets?

?

Implement Controls



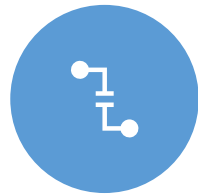
Cyber security awareness for the employee



Make sure your systems and software are up to date.



Ensure Endpoint Protection



Install a Firewall



Backup your data



Control access to your systems



Wi-fi Security

Cont:



Employee personal accounts
Separate logins for each staff




Access Management
Creating Central login system



Different passwords on the different application



Problems Somalia is now having with cyber security


- Due to its prolonged period of civil unrest, Somalia is currently dealing with additional issues related to cyber security including.
 - An increase in cyber-crimes and an absence of laws governing cybersecurity.
 - Insufficient knowledge about information security in Somalian government and businesses
 - Insufficient funding for cyber security business, education intuitions and government
 - Sales of information security tools to Somalia are prohibited internationally.
 - lack of digital literacy
- 



How do we Solve the
problems?

?

Recommendations business and Government

- Controllers should be implemented in critical infrastructure to stop cyberattacks:
 - Application control
 - Employee cyber security awareness
 - Patch applications and Operating systems.
 - User application hardening
 - Restrict administrative privileges
 - Patch operating systems
 - Multi-factor authentication
 - Regular backups.
 - Use firewalls and anti-intrusions systems
 - Use license software
 - Use antivirus software
- 

Cont:

- System managers in the public and private sectors need to receive qualified cyber security training.
- Business and government should prioritize cybersecurity investments and resources for greatest impact.
- Cybersecurity education should be offered at higher education institutions.
- Teaching Digital literacy
 - Teaching students how to evaluate the information they find online. ...
 - Discuss online privacy with students. ...
 - Help students understand online etiquette. ...
 - Teach digital writing. ...
 - Discuss AI tools and academic integrity.



Government Responsibility for Information Security

Creating security agencies such as:

National Cyber agency (NCA).

- *Defining and driving the cyber security agent of the entire country and developing national and international cyber security strategy.*

National Critical Infrastructure Agents (NCIA).

- *Protecting critical infrastructure and creating national critical infrastructure protection program.*

National Incident Response and Recovery plan

- *Develop national incident response plan to mitigate the effects of the cyber incidents.*
- *Active monitoring for attacks*
- *Multiple sources of threat intelligence*

Cont:

Defined laws pertaining to all crimes.

- *Develop cyber security laws to prevent, investigate and take actions against cybercrimes.*
- *Establish international cooperation and collaboration.*

A vibrant cybersecurity ecosystem

- *Develop the capabilities professionals and raise citizens cyber awareness by focusing: Accreditation cyber security cybersecurity providers, training providers and entrepreneurs.*

**T
a
k
e
a
w
a
y
s**

- *Security is valuable because it ...*
 - *Protects information against various threats*
 - *Ensures Government and business continuity*
 - *Minimizes image and financial losses and other impacts*
 - *Optimizes return on investments*
 - *Creates opportunities to do business safely*
 - *Maintains privacy and compliance*
 - *We all depend on information security*

Thank
you!

