Cybersecurity Threats – Targets and Perpetrators

A Presentation at the
Two-day Cybersecurity Education and Awareness Seminar
Organized by the Internet Society – Liberia's Chapter
Corina Hotel, 24th Street, Sinkor
March 18-19, 2021

By Hon. Zotawon D. Titus, *GCPP; MPP*
Commissioner of International Gateway Services
Liberia Telecommunication Authority (LTA)
Republic of Liberia
Email: dzotawontitus@gmail.com

Presentation Outline

- ✓Introduction to Cybersecurity
- ✓Understanding Cybersecurity as Part of ICT Ecosystem
- ✓The Vulnerability of Cyberspace Worldwide
- ✓Why Do Some People Commit Cybercrime?
- ✓Some Targets of Cyber Criminals
- ✓Some Measures to Mitigate Cyberattacks
- ✓Reflections of Cyber and Digital Vulnerability in Liberia
- ✓Conclusion

Introduction to Cybersecurity

- **Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes
- **The Budapest Convention/Council of Europe Convention on Cybercrime** (2001) is the first international treaty seeking to address internet and computer crime by harmonizing national laws and increasing cooperation among nations in fighting cybercrime
- **The International Telecommunication Union** (ITU) is leading the global action on Cybersecurity (WSIS Geneva in Dec 10-12 2003; WSIS Tunis Nov 16-18, 2005); ITU has since developed tool kits to aid developing countries in pursuit of this objective
- **ECOWAS Cybersecurity Initiative** – 2010 adopted Supplementary Act on the Protection of Personal Data and in 2011 adopted a directive on the fight against cybercrimes
- **The Malabo Convention** (2014) on Cybersecurity and Personal Data Protection seeks to secure African cyberspace by facilitating the harmonization of national laws
- **Each nation shall** secure its cyberspace to create a safe cyber culture, protect personal data, information infrastructure and online activities consistent with ITU Guidelines
- **Liberia has developed** its national cybersecurity strategy (2021 – 2026) to secure its cyberspace, support digitalization and to promote partnerships in fighting cybercrime

Understanding Cybersecurity as Part of ICT Ecosystem

- Cybersecurity is meaningless if it doesn't protect cyberspace
- Cyberspace refers to the interdependent network of critical national information infrastructure
- These interdependent infrastructure include
  - Terrestrial fiber cable
  - Internet exchange point,
  - Infrastructure of the mobile network operators
  - Data center and
  - Database of institutions
- These networks are prone to different kinds of errors and can become vulnerable
- Criminals can use network vulnerability to cause damage

Vulnerability of Cyberspace Worldwide

The more people are connected digitally, the more risky it is. The 2018 findings of Microsoft provides the following summary:

- 71% of companies worldwide admitted to cyber attack
- Companies loss about 400 billion to cyber attack each year
- By the end of 2020 about 3 Trillion United States Dollars of economic value was lost to cyber crime
- There are about 556 million people that are victims of cyber crime each year
- About 160 million data are compromised each year from different kinds of breaches
- Most cyber attacks go unreported in a number of developing countries

Why Do Some People Commit Cybercrimes?

There are several reasons why people commit cybercrimes. These reasons include the following:

- To benefit some financial gains
- To access a given information system for the purpose of causing disruptions
- To compromise the integrity of a given system
- To negatively influence decision for political reasons
- To engage in cyber terrorism
- To cause personal damage
- other

Some Targets of Cyber Criminals

Cybercriminals target the following

- Individuals
- Banking institutions
- Electoral system
- Government online services
- E-commerce services
- Critical information infrastructure
- Other

Some Measures to Mitigate Cyberattacks

Institutions:

- Put in place a robust security protocol
- Hire competent people of integrity to manage your system
- Invest in capacity building and also in your infrastructure
- Put in place proactive measures to protect your infrastructure

Individuals:

- Purchase digital device with authentic trademark of a reputable manufacturer if you can afford
- Make effort to read the information manual of the device
- Ensure that your digital device is password protected and do not disclose your password to second party
- Update your device regularly

Reflections of Cyber and Digital Vulnerability in Liberia

- What do you know or what have you experienced about your email being hacked?
- Have you received a message in your email from someone claiming to be kinsman of a wealthy person who died and left a treasure behind? and that person asked you to remit some money to redeem such a treasure?
- What about a caller posting to be an agent of a mineral seller stranded on the highway requesting you to send some money to him or her so that you could be a partner in the sales once they arrive in the city?
- What about one pretending to be a representative of a mobile company calling to notify you that your child has won a scholarship but you need to send a few dollars to facilitate delivery?
- Do you have an idea of cyber attack that heavily impacted Liberia in recent times?

Conclusion

- Cybercrime is a global threat and cybersecurity as a solution requires a true global partnership;
- ITU, African Union, ECOWAS etc. support the fight against cybercrimes
- Education on cyber threats will help to promote cybersecurity and secure cyberspace; Such education requires the active support of all stakeholders
- Cyber criminals regularly devise means to carry out cyber attacks, targeting individuals and institutions for financial gains or other reasons; these attacks take place on platforms that have become the target of hackers
- It is therefore important to promote digital and cyber safety in order to minimize the potential risk associated with this growing phenomenon
- Service providers, Civil society organizations, the media and government need to work together to ensure a cyber culture that is not susceptible to hackers

End of Presentation

Cybersecurity Threats – Targets and Perpetrators

Zotawon D. Titus, *GCPP; MPP*

Commissioner of International Gateway Services

Liberia Telecommunication Authority (LTA)

Republic of Liberia

Email: dzotawontitus@gmail.com

I Thank You