Internet Safety and Security:
Strategies for Building an Internet Safety Wall

Sylvanus A. EHIKIOYA, PhD
Director, New Media & Information Security
Nigerian Communications Commission
Abuja, NIGERIA

Internet Security

- The Internet as a platform for almost all forms of activities --- social, economic, governance, education, health, etc

- It is attractive for perpetuating crimes

- Effects of Internet Security breaches are far-reaching.

Examples of Criminality on the Internet

- Cyber Terrorism
- Cyber warfare
- Cyber espionage
- Phishing
- Malware, worms, virus, Trojan horses, etc
- Denial of Service, spam, botnets and zombies
- Frauds (financial, social, intellectual Property, etc)
- Distribution of X-rated content and CoP

Security Vulnerability, Threats, and Risk

- Vulnerability is a term that describes the weakness in a system, network, application, or process that can be exploited by a threat to create an adverse effect.

- Vulnerabilities can either be technical or physical in nature, and can be identified through assessment activities and continual situational awareness

Threats

- A threat is any indication, circumstance or event with the potential to cause loss or damage to an asset.

- To access vulnerability and risk, threats need to be characterized in some more detail.

Some important threats characteristics

- Type (e.g., insider, terrorist, military, or environmental (e.g. hurricane, tornado)),
- Intent or motivation,
- Triggers (i.e., events that might initiate an attack),
- Capability (e.g., skills, specific knowledge, access to materials or equipment),
- Methods (e.g., use of individual suicide bombers, truck bombs, assault, cyber), and
- Trends (what techniques have groups used in the past have experimented with, etc.).

Risk

- A risk can be described as the chance of a loss or damage and the resulting consequences.
- Risks are often characterized qualitatively as high, medium, or low.
- The level of risk varies among different components of cyberspace, and some may, therefore, deserve more attention than others in the development of an effective framework.
- Some components are considered to be particularly vulnerable, some are viewed by different groups of attackers as particularly tempting targets, and some would, if compromised, have particularly large impacts.

Examples of Threats

- A hacker remotely copying confidential files from a company network.
- A worm seriously degrading the performance of a wide-area network.
- A system administrator violating user privacy.
- Probe – access a target in order to determine its characteristics.
- Scan – access a set of targets sequentially in order to identify which targets have a specific characteristic.
- Flood – access a target repeatedly in order to overload the target's capacity.
- Bypass – avoid a process by using an alternative method to access a target.
- Spoof – masquerade by assuming the appearance of a different entity in network communications.
- Read – obtain the content of data in a storage device or other data medium.
- Steal – take possession of a target without leaving a copy in the original location.
- Modify – change the content or characteristics of a target.
- Delete – remove a target or render it irretrievable.

A Quick Take Away

- Security vulnerability of cyber infrastructure exists when there is possibility to manipulate the assets of cyber infrastructure and cause doubts in the ***confidentiality, integrity and availability*** (CIA) of data and information contents of the cyber infrastructure.

- Ensuring the CIA of data and information contents of the cyber infrastructure at all times is the pivot of Internet Security.

Strategic Initiatives

- Cyber and information security awareness training.
- Develop relevant and improve cyber and Information Security Regulatory Framework
- Monitor compliance to framework
- Regular organisation of cyber and information security for a
- Establishment of national CERT and cyber Forensic Labs
- MoUs for National Monitoring of Ips
- Enact relevant regulatory laws

Key Policy Considerations

- The cyber security policy is an evolving task, which need to be regularly updated and refined putting into consideration the technological trends and security challenges posed by such technology directions.

- The security of cyber space is not an optional issue but an imperative need in view of its impact on national security, public safety and economic well-being.

- The issue of cyber security needs to move beyond traditional technological measures such as anti-virus and firewalls. It needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks.

- Cyber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.

- Effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations.

- There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.

- Security is all about what people, process and technology and as such there is a clear need for focusing on people and processes while attempting to use the best available technological solutions, which otherwise could prove ineffective.

- Use of adequately trained and qualified manpower along with suitable incentives for effective results in a highly specialized field of cyber security.

- Security needs to be built-in from the conceptual design stage itself when it comes to developing and deploying critical information infrastructure, as opposed to having security as an afterthought.

Priorities for Actions

- Creation of necessary situational awareness regarding threats to Information and Communication Technology (ICT) infrastructure for determination and implementation of suitable response

- Creation of a conducive legal environment in support of safe and secure cyber space, adequate trust and confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders and effective prosecution

- Protection of IT networks and gateways and critical communication & information infrastructure

- Putting in place a daily mechanism for cyber security emergency response and resolution and crisis management through effective predictive, preventive, protective response, and recovery actions

- Policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology and people) and incentives for compliance.

- Indigenous development of suitable security techniques and technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products and processes

- Creation of a culture of cyber security for responsible user behaviour and actions

- Effective cyber-crime prevention and prosecution actions

- Proactive preventive and reactive mitigation actions to reach out and neutralize the sources of trouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral and multi-lateral agreements with overseas CERTs, security agencies and security vendors.

- Protection of data while in process, handling, storage and transit and protection of sensitive personal information to create a necessary environment of trust.

Questions?

Contact:

ehikioya@ncc.gov.ng

ehikioya@gmail.com

+234-803-606-2390