INFORMATION SECURITY FRAMEWORK AND NATIONAL CYBER SECURITY

PRESENTED BY

DR. PETER O. OLAYIWOLA, BBA, MBA, Ph.D., CPA, MNIM.
MCPN, FNCS, FCFI, MHTCIA. CLWE, JP+
President, Computer Forensics Institute, Nigeria (CFIN)

@

CONFERENCE ON REGULATORY IMPERATIVES FOR CYBERCRIME AND CYBER SECURITY IN NIGERIA
ORGANIZED BY NIGERIAN COMMUNICATIONS COMMISSION (NCC)
@ INTERNATIONAL CONFERENCE CENTRE, ABUJA, FCT, NIGERIA,
5TH MARCH 2012

AGENDA

- ***Introduction***
- ***Information Security Framework***
- ***National Cyber Security***
- ***Nigeria: Taking a Proactive Approach***
- ***Q & A***
- ***End***

Introduction

ABOUT THE AUTHOR:

- President, Computer Forensics Institute, Nigeria (CFIN)
- Managing Forensics Examiner/CEO, Digital & Computer Forensics Associates (DCFA)
- CEO, Rockshire Computer Technologies Limited
- Former Project Director, Lagos State Global Computerisation Programme
- Former Senior Manager (Information Technology, International Trust Bank – former Gamji Bank PLC
- Former Lecturer, University of Ilorin
- World Bank Consultant, Information Technology
- DFID Consultant, Info. Tech. and Public Financial Management (PFM)
- Fellow, Computer Forensics Institute, Nigeria (CFIN)
- Fellow, Nigeria Computer Society
- Chartered Information Technology Professional
- Member, High Technology Crime Investigation Association
- Certified Live Wire Examiner
- Expert Witness, Election Tribunal
- Former, General Secretary & Chairman, Education Committee, Nig. Computer Society
- Former Council Member, Computer Professionals Registration Council of Nigeria
- etc.

Introduction

ABOUT THE AUTHOR:

- **Conference Director:**
- **First West African Digital and Computer Forensics Conference**
- **organized by Computer Forensics Institute, Nigeria (CFIN) in collaboration with major Stakeholders, to be held**
  - **Venue: International Conference Centre, Abuja**
  - **Dates: Wed. - Friday, 18th - 20th April, 2012**
  - **(http://www.cfinonline.org)**

OUR SERVICES

DIGITAL & COMPUTER FORENSICS ASSOCIATES (DCFA) offers the following:

- Cyber Security Consulting Services
- Digital & Computer Forensics Consulting
- Cyberwarfare Centre Project Management
- Development of Cyberwar Defense Team
- Cyberwarfare Advisory Services
- Information Technology Consulting
- Training in Digital Forensics & Cyber Security

OUR SERVICES (cont'd)

CFIN Training Programme include:

1. Digital & Computer Forensics
2. Information/Cyber Security
3. Biometrics
4. Data Recovery
5. Handwriting & Questioned Documents Analysis,
6. Electronic Evidence Presentation, etc.

Information Security Framework and National Cyber Security: An Introduction

- Why discuss this topic?
- Military and intelligence leaders agree that the next major war is not likely to be fought on the battle-ground but in cyber space.
- The recent attacks on the US and other governments corroborate this claim; and everyday thousands of attempts are made to hack into the world's critical infrastructure and private organizations.

Information Security Framework and National Cyber Security: An Introduction (cont'd)

- William J. Lynn, U.S. Deputy Secretary of Defense, states that "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space.

CYBER WARFARE: DEFENDING AGAINST CYBERATTACKS:

- **DEFINITION**: **CYBER WARFARE**
- "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."
- The *Economist* describes cyber warfare as "the fifth domain of warfare."
- The Shanghai Cooperation Organisation (members include China and Russia) defines cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states".

CYBER WARFARE: DEFENDING AGAINST CYBERATTACKS:

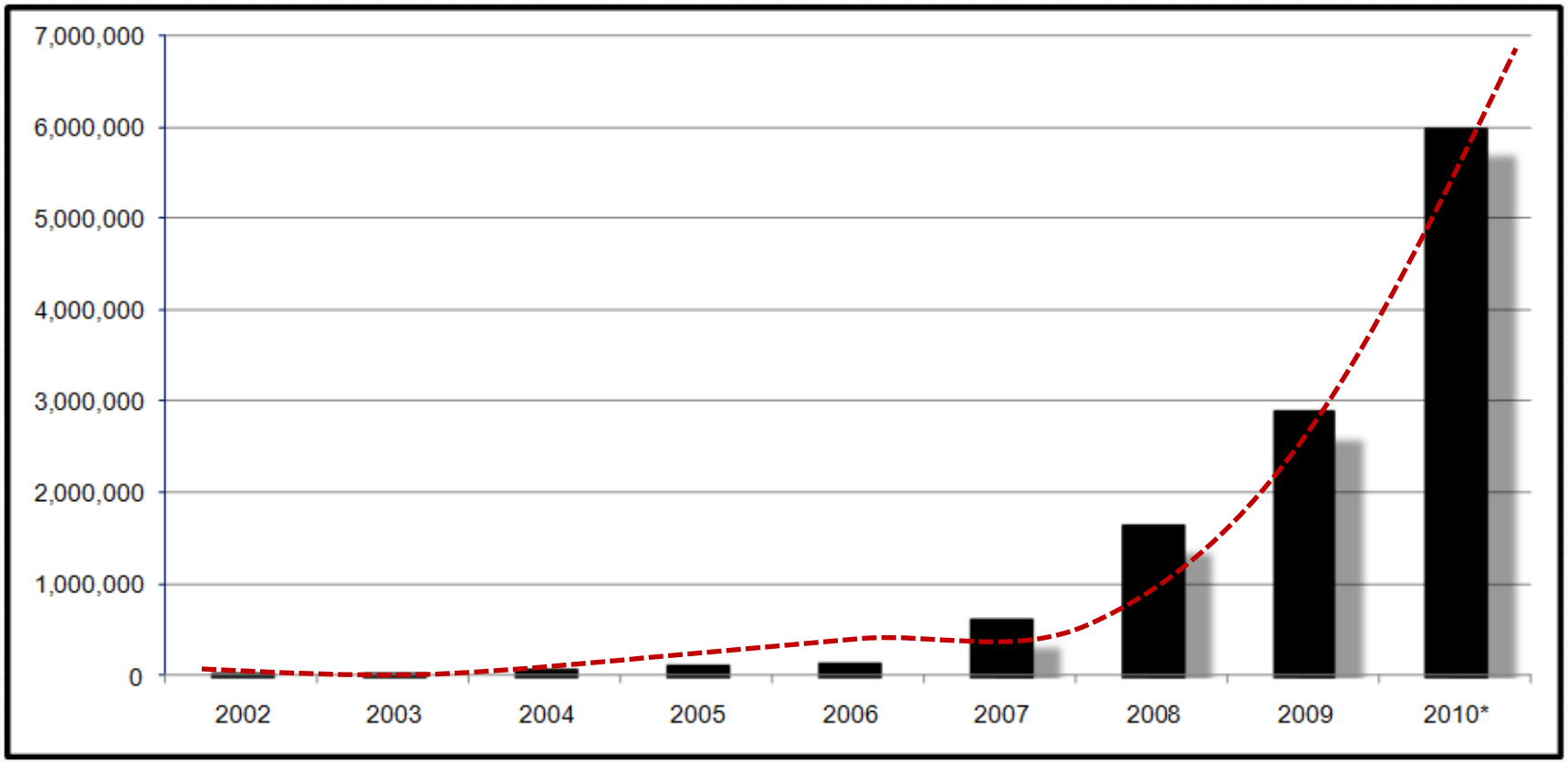
- In 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset."
- In May 2010, the Pentagon set up its new U.S. Cyber Command (USCYBERCOM), headed by General Keith B. Alexander, Director of the National Security Agency (NSA), to defend American military networks and attack other countries' systems.

CYBER WARFARE: DEFENDING AGAINST CYBERATTACKS:

- In February 2010, top American lawmakers warned that the "threat of a crippling attack on telecommunications and computer networks was sharply on the rise."
- According to The Lipman Report, numerous key sectors of the U.S. economy along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations.

Information Security Framework and National Cyber Security: An Introduction (cont'd)

EXPONENTIAL GROWTH IN MALWARE



Information Security Framework and National Cyber Security: An Introduction

Malware:

2,895,802 signatures / year

7,933 signatures / day

330 signatures / hour

5 signatures / minute

1 signature / 12 seconds

CYBER WARFARE: THREATS & REALITIES – GLOBAL COMPUTER HACKING

- In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility.
- The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.

Information Security Framework and National Cyber Security: An Introduction (cont'd)

Information Security Framework and National Cyber Security: An Introduction (cont'd)

- Some of these damages included:
  - unleashing powerful Denial of Service (DOS) attacks,
  - exposing national security secrets, and
  - compromising individual victims' credit card numbers and bank account credentials.

Information Security Framework and National Cyber Security: An Introduction (cont'd)

- Virtually all online users have been affected by botnets, either as helpless recipients of spam emails or as frustrated users attempting to visit an unavailable or dangerous Websites.
- Millions of users have suffered a much worse fate: Recruited unknowingly into a botnet army.
- Perhaps, you are already a victim!

Information Security Framework and National Cyber Security: An Introduction (cont'd)

- The Bredolab botnet alone had infected over 30 million computers and sent an estimated 3.6 billion virus-laden emails every day in late 2009.
- As of early December 2010, over 5,400 botnet command and control servers were identified and active.

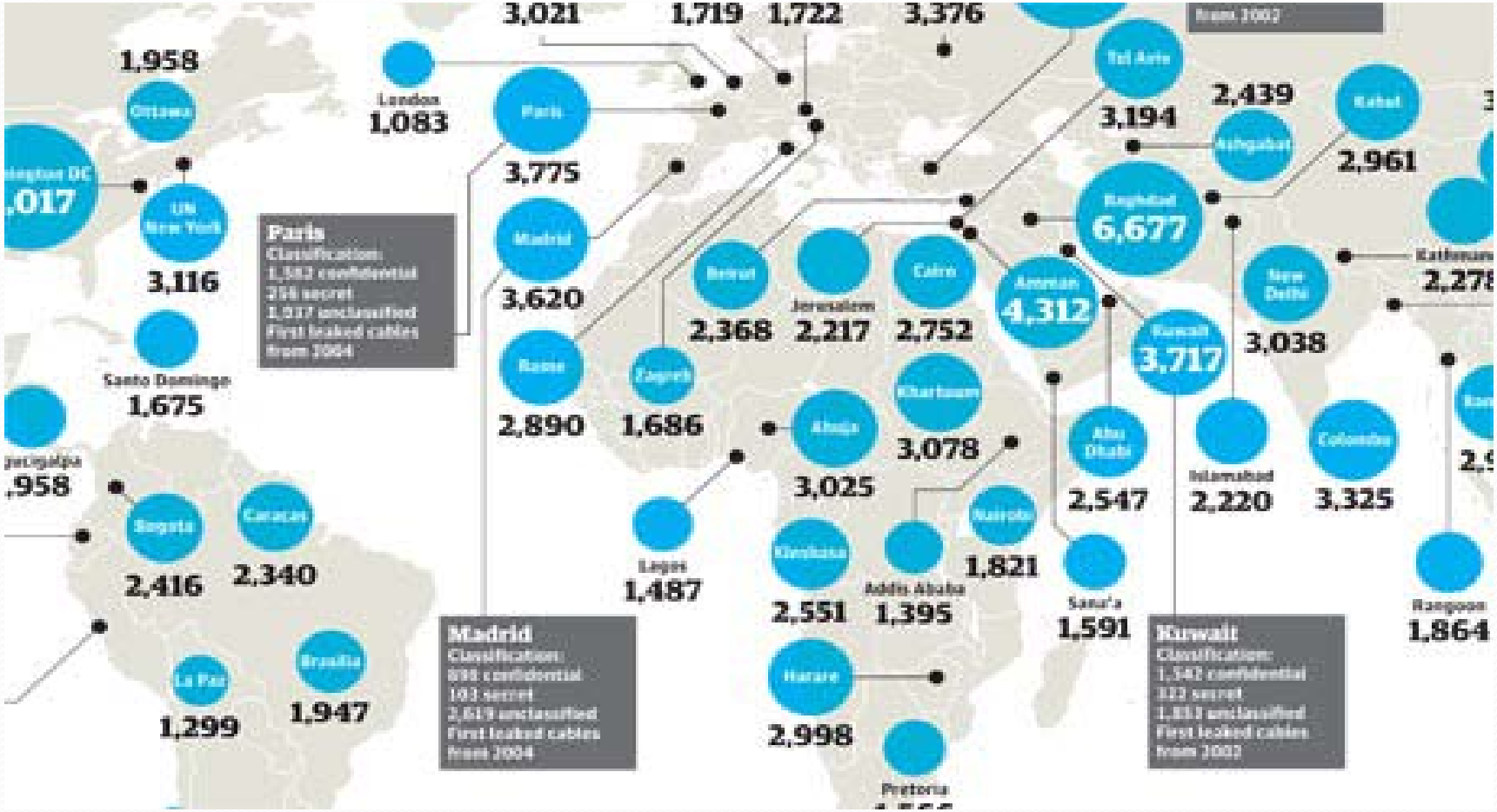
Information Security Framework and National Cyber Security: An Introduction (cont'd)

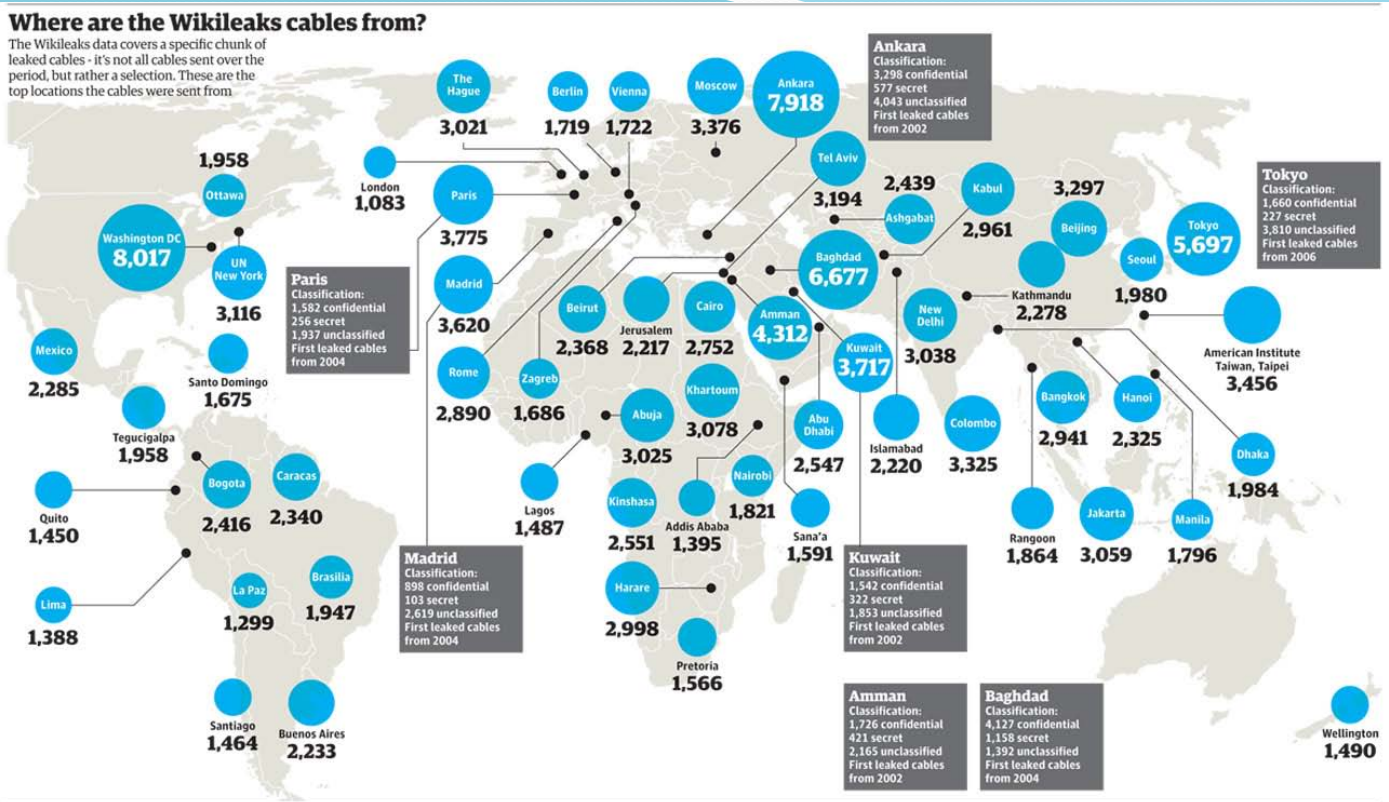
- Wikileaks began on Sunday November 28th publishing leaked United States embassy cables, the largest set of confidential documents ever to be released into the public domain.

Information Security Framework and National Cyber Security: An Introduction (cont'd)

- Wikileaks embassy cables revelations cover a huge dataset of official documents:
  - 251,287 dispatches,
  - from more than 250 worldwide US embassies and consulates.
  - including over 50,000 documents covering the current Obama Administration.

Information Security Framework and National Cyber Security: An Introduction (cont'd) WIKILEAKS





Information Security Framework

- **ISO/IEC 27002** is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled *Information technology - Security techniques - Code of practice for information security management*.
- ISO/IEC 27002:2005 has developed from BS7799, published in the mid-1990's. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards.

Information Security Framework (cont'd)

- ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).
- Information security is defined within the standard in the context of the C-I-A triad:
  - *the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required).*

Information Security Framework (cont'd)

- Information Security:
  - Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and destruction.
  - Simply put: protecting our data and our systems from those who would wish to misuse them.
  - Protecting our assets.
  - Protecting: Confidentiality, Integrity and Availability – the C-I-A Triad

Information Security Framework (cont'd)

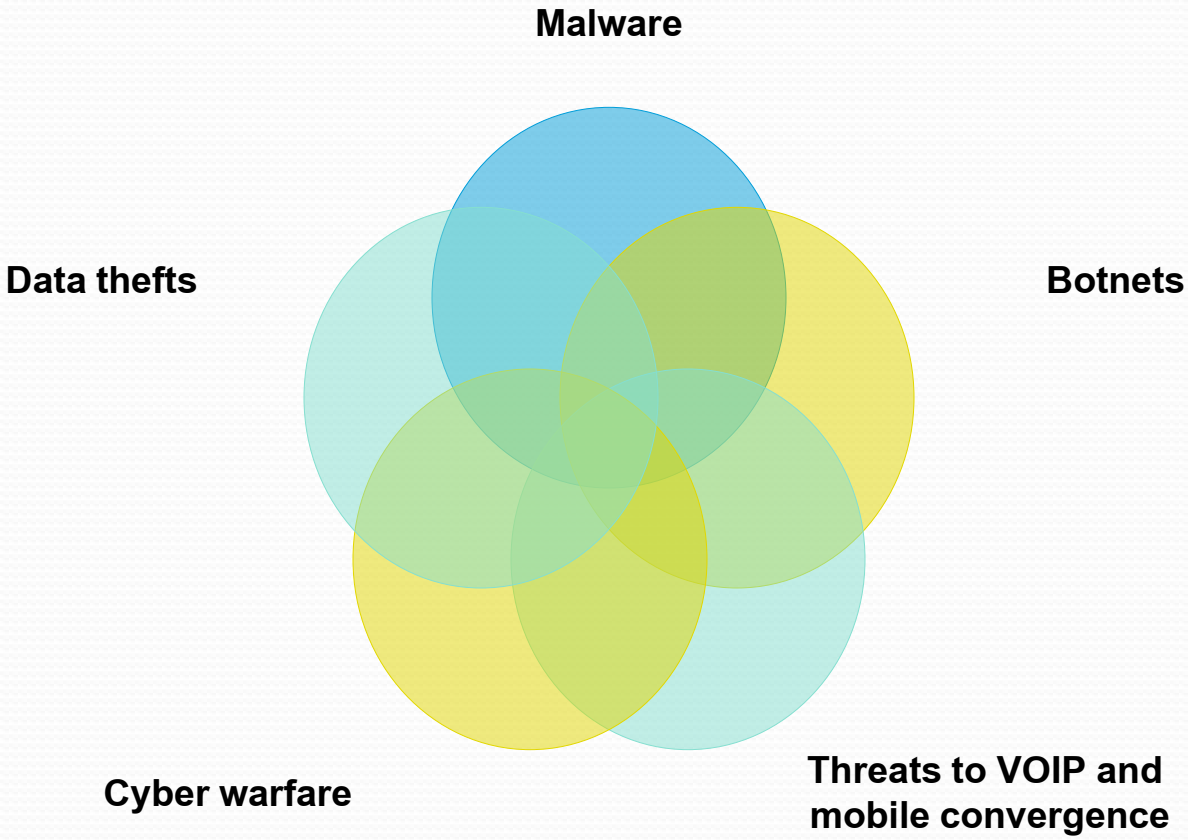
- Types of Attacks:
  - Confidentiality -- Interception
  - Integrity -- Interruption
    -- Modification
    -- Fabrication
  - Availability -- Interruption
    -- Modification
    -- Fabrication

Information Security Framework (cont'd)

- Threats: Something that has the potential to cause us harm
- Vulnerabilities: Weaknesses that can be used to harm us – holes that can be exploited by the threats
- Risk: Likelihood that something bad will occur. Requires both threats and vulnerabilities

Information Security Framework (cont'd)

CYBER THREATS



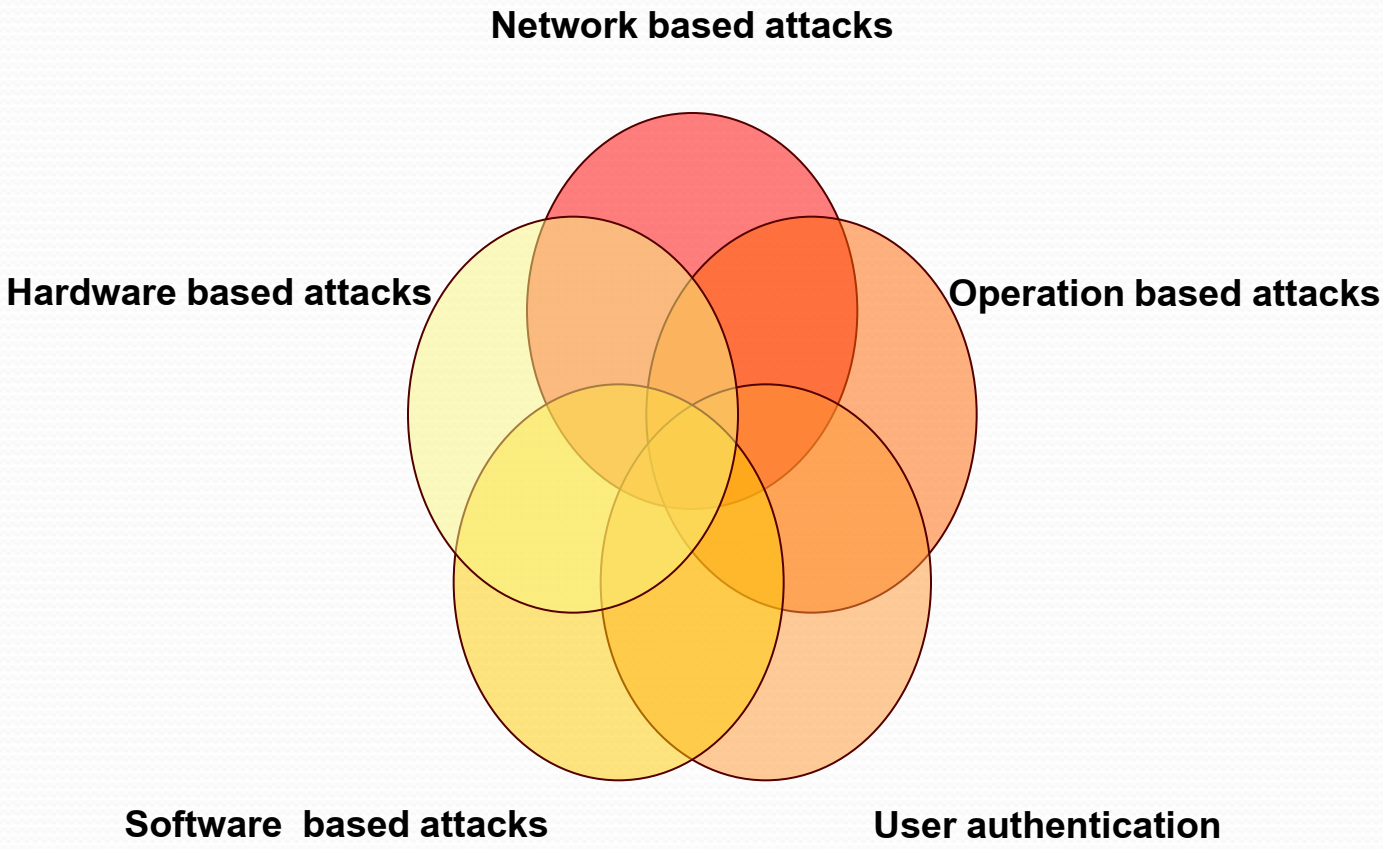
Information Security Framework (cont'd)

- Malicious attackers will install malware on **social networking sites** leading to increased phising scams, or stealing data, etc- browser level protection needed.
- Hackers will install **malcode within video content** which will affect users accessing video clips.
- **Mashup technology** used by web applications to combine data/media from multiple sources, locations and coding styles may lead to increased corporate espionage and other scams
- **Identity thefts** will only increase and **botnets** will be used for corporate espionage and phising scams
- **Polymorphic exploitation -** Polymorphic Malware is malicious software that has the ability to change its signature randomly each time it replicates - creation of unique exploit with each user request –signature based protection engines at network or host level fail

Information Security Framework (cont'd)

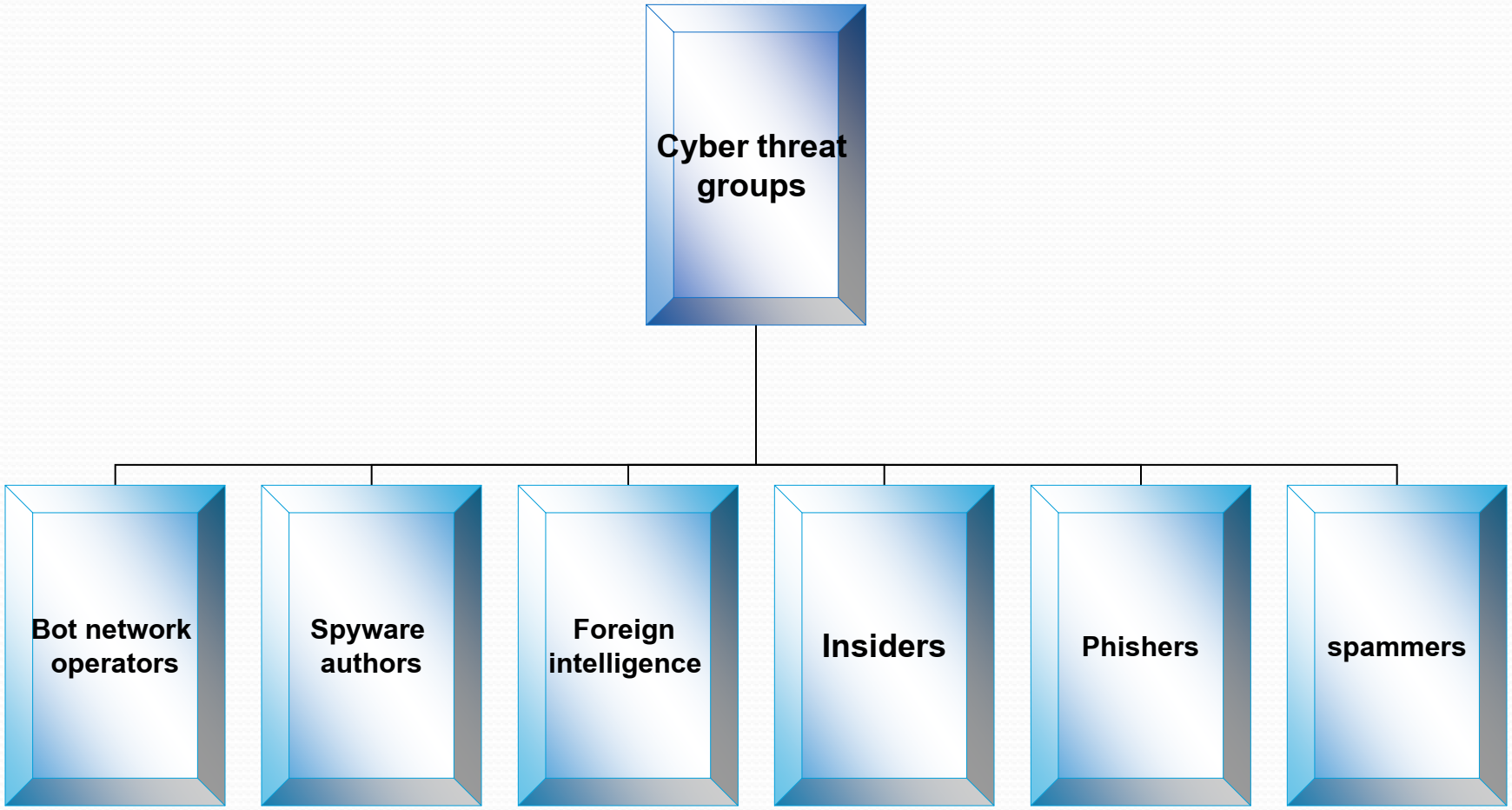
- Growing popularity of VOIP applications - instances of **voice spam and voice phising or smishing** (using SMS) will increase
- **Targeted attacks** - Attack activity through e-mail, Instant messaging, P2P networks will increase
- **Denial of service** affecting voice infrastructure
- **Cyber terrorist** attacks will increase and lead to cyber warfare - threat to nation's sovereignty
- **MMS scams** will be on the rise and raise issues of defamation and invasion of privacy

Information Security Framework (cont'd)



Information Security Framework (cont'd)

CYBER THREATS GROUPS



Information Security Framework (cont'd)

- **Controls:**
  - Physical Control e.g. locks, fence, guards, cameras, etc.
  - Logical Control (or technical control) e.g. passwords, encryption, firewalls, IDS
  - Administrative Control: based on laws, rules, policies, procedures, guidelines and other items that are paper in nature. Rules on how we expect the users in our environment to behave. Critical ingredient is ability to enforce compliance.

Information Security Framework (cont'd)

- **Defense in depth:**
- Formulating a multilayered defense that will allow us to mount a successful defense should one or more of our defensive measures fail.
- Layers:
  - External Network
  - Internal Network
  - Host
  - Application
  - Data

Information Security Framework (cont'd)

Information Security Framework (cont'd)

- Information Security Management (ISM):
  - a systematic approach to encompassing people, processes, and Information Technology (IT) systems that safeguards critical systems and information, protecting them from internal and external threats
- Information Security Framework considers global, national, organizational, and employee standards to guide ISM.
- IS framework is intended to promote a cohesive approach which considers a process view of information within the context of the entire organizational operational environment.

Information Security Framework (cont'd)

- Information Security Framework establishes security policy and practices
- Policies provide general, overarching guidance on matters affecting security that the management and staff are expected to follow.
- Practices document methods and minimum compliance activities as appropriate to ensure that policy objectives are met.

Information Security Framework (cont'd)

- Security policy applies to all:
  - Hardware
  - Software
  - Data
  - Information
  - Network
  - Personal computing devices
  - Support personnel, and
  - Users
- These components of information technology are covered by the umbrella term of "Information Resources."

Information Security Framework (cont'd)

- **Contents of the Framework:**
- **Security Policy**: the scope of policy, roles and responsibilities
- **Organizational Security**: Addresses security responsibilities of the workforce, third parties, and outsourcers
- **Risk Assessment and Treatment**: Documents the process the government (or corporation) will use to identify and assess risk as well as treat the risk through controls and practices.
- **Asset Classification**: Assures appropriate protection of government (or corporate) physical assets.
- **Human Resources Security**: Addresses the considerations with government (or corporate) staff prior to employment, during employment, and after termination

Information Security Framework (cont'd)

- **Physical and Environmental Security**: Deals with the protection of physical areas and equipment from physical threats and unauthorized access.
- **Communications and Operations Management**: Addresses the many facets of information technology operations
- **System Access Controls**: Tackles access restrictions for users at network, operating system, application and mobile computing levels
- **System Development and Maintenance**: Deals with the many aspects of application development and maintenance security concerns
- **Information Security Incidents**: Addresses the reporting and management requirement for security incidents.

Information Security Framework (cont'd)

- **Business Continuity**: Plans for interruptions of government or corporate business activities
- **Compliance**: Addresses the government's (or the corporation's) compliance with laws and statutes, security policies, controls and practices as well as audit considerations.

Information Security Framework (cont'd)

- GOALS AND OBJECTIVES:
- To reduce vulnerability of country's cyberspace
- To protect critical infrastructure and critical information systems and services
- To improve interdepartmental coordination mechanisms for prevention, rapid response and recovery from attacks
- To advance legal mechanisms that support the goals of the cyber security strategy
- To create a Computer Emergency Response Team (CERT)
- To launch awareness programs on cyber security
- To enhance international cooperation, promoting cyber security culture and international agreements

National Cyber Security

"In this cyberspace world, the distinction between "crime" and "warfare" in cyberspace also blurs the distinction between police responsibilities, to protect societal interests from criminal acts in cyberspace, and military responsibilities, to protect societal interests from acts of war in cyberspace."

Source: Emerging Challenge: Security And Safety In Cyberspace by Richard O. Hundley and Robert H. Anderson in IEEE Technology and Society, pp. 19–28 (Winter 1995/1996)

National Cyber Security (cont'd)

- Certain infrastructures deemed "critical" have been identified as essential to the nation's defense and economic security and the health, welfare, and safety of its citizens
- Their incapacity or disruption could have a debilitating impact on governments and the private sector
- Assuring these infrastructures and the information systems and networks on which they more and more depend for operations represents a complex and long-term undertaking

National Cyber Security (cont'd)

- **ESPIONAGE AND NATIONAL SECURITY BREACHES**
- Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.

National Cyber Security (cont'd)

- **ESPIONAGE AND NATIONAL SECURITY BREACHES (cont'd)**
- Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world.
- General Alexander notes that the recently established US Cyber Command is currently trying to determine whether such activities as commercial espionage or theft of intellectual property are criminal activities or actual "breaches of national security."

National Cyber Security (cont'd)

- **SABOTAGE**
- Military activities that use computers and satellites for coordination are at risk of equipment disruption.
- Orders and communications can be intercepted or replaced.
- Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption.

National Cyber Security (cont'd)

- **SABOTAGE (cont'd)**
- The civilian realm is also at risk
- Security breaches have already gone beyond stolen credit card numbers,
- Potential targets can also include:
  - electric power grid,
  - trains, or
  - the stock market.

National Cyber Security (cont'd)

- **SABOTAGE (cont'd)**
- In mid July 2010, security experts discovered a malicious software program that had infiltrated factory computers and had spread to plants around the world.
- It was considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," noted the *New York Times.*

National Cyber Security (cont'd)

- **ELECTRICAL POWER GRID**
- The federal government of the United States admitted that the electric power transmission is susceptible to cyberwarfare.
- The government is also working to ensure that security is built-in as the next generation of "smart grid" networks are developed.

National Cyber Security (cont'd)

- **ELECTRICAL POWER GRID (cont'd)**
- In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former US national security officials.

National Cyber Security (cont'd)

- **ELECTRICAL POWER GRID (cont'd)**
- The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack.
- Massive power outages caused by a cyber attack, could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

National Cyber Security (cont'd)

- **MILITARY**
- In the U.S., General Keith B. Alexander, first head of the recently formed USCYBERCOM, told the Senate Armed Services Committee that computer network warfare is evolving so rapidly that there is a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."
- Cyber Command is the newest global combatant and its sole mission is cyberspace, outside the traditional battlefields of land, sea, air and space.“

National Cyber Security (cont'd)

- **MILITARY (cont'd)**
- USCYBERCOM will attempt to find and, when necessary, neutralize cyberattacks and to defend military computer networks.
- Alexander sketched out the broad battlefield envisioned for the computer warfare command, listing the kind of targets that his new headquarters could be ordered to attack, including "traditional battlefield prizes – command-and-control systems at military headquarters, air defense networks and weapons systems that require computers to operate."

National Cyber Security (cont'd)

- THE COMPLEXITY
- The distributed nature of internet based attacks means that it is difficult to determine motivation and attacking party, meaning that it is unclear when a specific act should be considered an act of war.

National Cyber Security (cont'd)

- **PRIVATE SECTOR**
- Computer hacking represents a modern threat in ongoing industrial espionage and as such is presumed to widely occur.
- It is typical that this type of crime is underreported.
- According to McAfee's George Kurtz, corporations around the world face millions of cyberattacks a day.
- "Most of these attacks don't gain any media attention or lead to strong political statements by victims."
- This type of crime is usually financially motivated.

National Cyber Security (cont'd)

- The United States Department of Defense sees the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security.
- One U.S. agency, the Joint Forces Command, describes some of its attributes:
- Cyberspace technology is emerging as an "instrument of power" in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information.

National Cyber Security (cont'd)

- With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad.
- Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies.

National Cyber Security (cont'd)

- In February 2010, the U.S. Joint Forces Command released a study which included a summary of the threats posed by the internet:
- "With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests.
- "Cyberspace will become a main front in both irregular and traditional conflicts.

National Cyber Security (cont'd)

- On March 28, 2009, a cyber spy network, dubbed GhostNet, using servers mainly based in China tapped into classified documents from government and private organizations in 103 countries … but China denied the claim.

National Cyber Security (cont'd)

- **CIVIL SOCIETY**
- Potential targets in internet sabotage include all aspects of the Internet from the backbones of the web, to the Internet Service Providers, to the varying types of data communication mediums and network equipment.
- This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the desktops and laptops in businesses and homes.
- Electrical grids and telecommunication systems are also deemed vulnerable, especially due to current trends in automation.

National Cyber Security (cont'd)

- From the phone in your pocket to the military's most sophisticated weapons system, cyber espionage and computer hacking represent an economic and national security threat to Nigeria.
- What will happen when Cyber threats strike?

Cyberwar Defence Team

National Cyber Security (cont'd)

- In the U.S., Cyber Command was set up to protect the military
- Government infrastructures are primarily the responsibility of the Department of Homeland Security
- Corporate infrastructures are the responsibility of the private companies

National Cyber Security

- **WHAT TO DO?**
- The Presidency, in full collaboration with the private sector, and with the enlightened guidance and support of the National Assembly, should establish a national Legislative and Regulatory Framework with the following attributes:
  - the focus must be on deciding "what must be protected?"
  - Since everything can not be protected, we must *establish a hierarchy* of "Critical Assets"
  - In its simplest form, we must identify and focus our attention on those things to which the description "unbelievable" would certainly apply were we to lose them.
  - National Policy level input is the essential element in determining these "Critical Assets".

National Cyber Security (cont'd)

- We must adopt a *proactive, not reactive, approach* to identifying those Critical Assets and to formulating a *national level strategy* to integrate and focus our efforts.
- The new regime for infrastructure protection - across all elements of national vulnerability—must *leverage all appropriate elements of the government.*
- The heart of leveraging, and its most thorny element, is *information, information, information . . .*
- The barriers to a significantly enhanced exchange of information across the traditionally uncommunicative stove pipes of government must be removed without providing an undue advantage to our adversaries in the process.

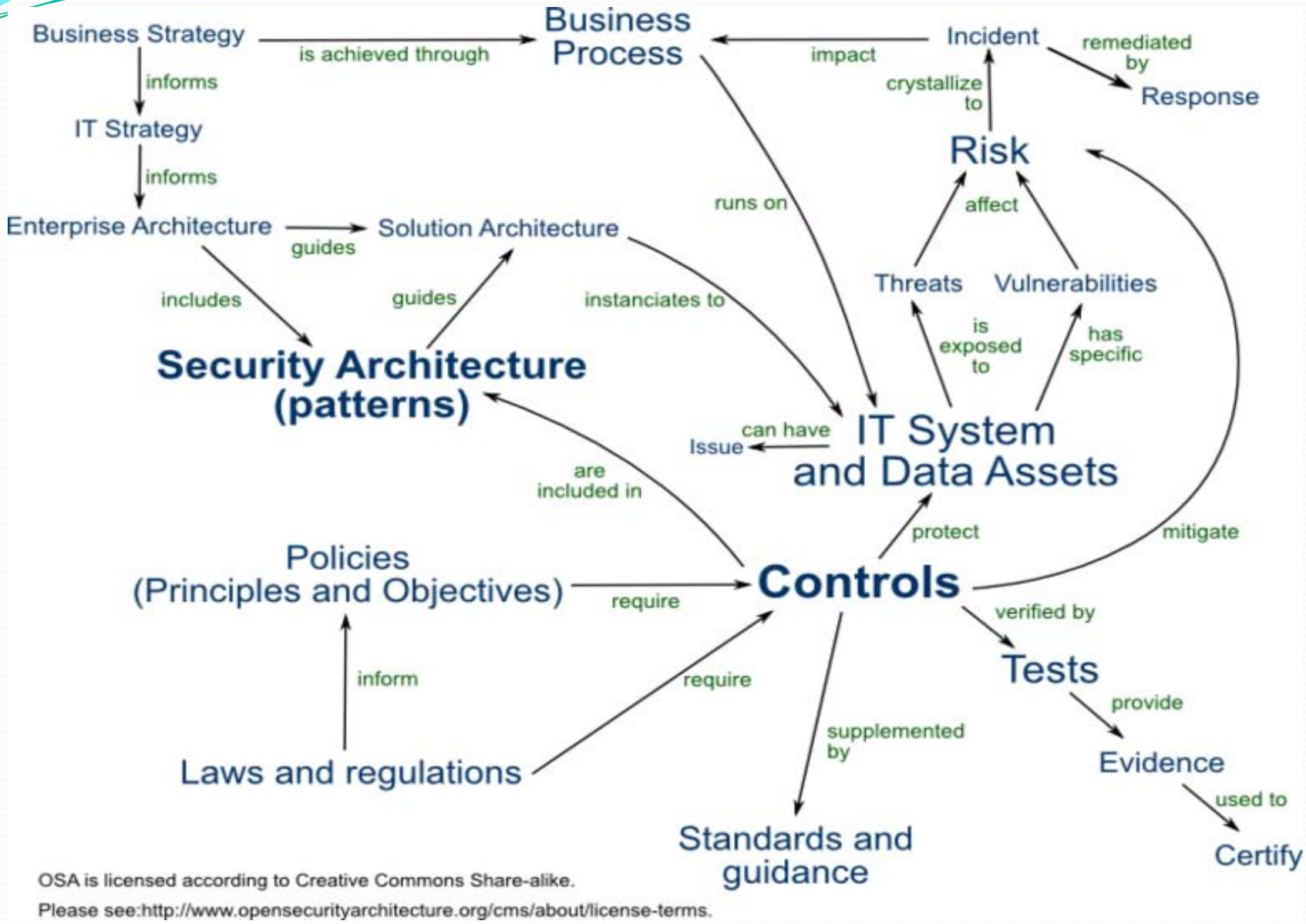
National Cyber Security (cont'd)

- The tensions and barriers between the government and private sector must be replaced by a regime which permits collaboration while, at the same time, protects the secrets and proprietary information and privacy of both
- The National Strategy must form the basis for government – private sector interaction
- Government must be accountable for performance against National Strategy and that accountability must be clear to the entire range of national policy level participants

CYBER SECURITY RISK MANAGEMENT

A Continuous Interlocked Process—Not an Event

OPEN SECURITY ARCHITECTURE (OSA)



National Cyber Security (cont'd)

- Several governments around the world have come to understand that the same assets they have spent millions and billions of dollars to protect physically are now under different types of threats
- The tanks, planes, weaponry, power plants, communication networks have to be protected because they are all now run by and are dependent upon software

National Cyber Security (cont'd)

- The software can be hacked into, compromised, or corrupted
- Coordinates of where bombs are to be dropped can be changed
- Individual military bases still need to be protected by surveillance and military police, which is physical security
- Surveillance uses satellites and airplanes to watch for suspicious activities taking place from afar, and security police monitor the entry points in and out of the base

National Cyber Security (cont'd)

- These types of controls are limited in monitoring *all* of the entry points into a military base
- Because the base is so dependent upon technology and software—as every organization is today—and there are now so many communication channels present (Internet, intranets, wireless, leased lines, shared WAN lines, and so on)
- There has to be a different type of "security police" that covers and monitors all of these entry points in and out of the base.

National Cyber Security (cont'd)

- As a result, cyber security has become more strategic as organisations invest greater resources in developing strategies, defining architectures, and carrying out risk assessments.
- Organizational priorities now include creating awareness among employees, developing policy and standards and training staff in digital forensics and cyber security.

National Cyber Security (cont'd)

- Digital and Cyber Forensics is a tool for people who are interested in extending or perfecting their skills to defend against such attacks and damaging acts.
- You cannot properly protect yourself from threats you do not understand.

Conclusion

- In conclusion, it is the opinion of this paper that:

1. Effective Governance is imperative for success in cyber security efforts. There should be a centralized coordination of national cyber security initiatives
2. There is need to develop a National Cyber Security Technology Framework that specify cyber security requirement controls and baselines for CNII elements, and evaluation and certification of cyber security products and services

Conclusion (cont'd)

3. Then appropriate Legislative and Regulatory Framework to back up the policies, standards, best practices should be put in place.
4. The roles to be played by various actors, such as NSA's Office, NCC, NITDA, CBN, etc. must be clearly defined. (In the USA, most of the standards are set by NIST or utilising ISO/IEC 27002)

Conclusion (cont'd)

5. There is a need to establish the Cyber Emergency Response Team-Nigeria. Fortunately, more and more Nigerians are now becoming certified professionals in digital, cyber or computer forensics and cyber security.
6. Government should promote effective cooperation with the private sector to actualize the above

Conclusion (cont'd)

7. There is a need for capacity building and training in digital, cyber or computer forensics and cyber security, and in the culture of security
8. Compliance and enforcement mechanism should be developed
9. Government should encourage international cooperation in cyber security

Conclusion (cont'd)

It is our hope that with the above suggestions, Nigeria's Critical National Information Infrastructure (CNII) will be secure, robust, and dependable.

Also, imbibing the culture of security will not only promote Nigeria's stability but also her socio-economic growth and development.

THANK YOU

END

Dr. Peter O. Olayiwola, BBA, MBA, Ph.D., CPA, MASM, MNIM, MCPN, FNCS, FCFI, MHTCIA, CLWE, JP+

Managing Forensics Examiner/CEO, Digital & Computer Forensics Associates (DCFA)

President/Chairman, Computer Forensics Institute, Nigeria (CFIN)

CEO, Rockshire Computer Technologies Limited

E-Mail: peterolayiwola@yahoo.com

chairman@cfinonline.org

Phone: 0803-853-3157, 0702-544-1173, 0802-320-8780

Website: www.cfinonline.org