Computer Security: Fundamentals

Bachelors in ICT

By

Ezer Osei Yeboah-Boateng, Ph.D.

Outline

- Key Definition(s)
- Essentials Elements of Cyber-Security
- Cyber-Security: Threats
- Cyber-Security: Vulnerabilities

Books & Resources

- Principles of Information Security, 4th Edition, 2011, by Michael Whitman & Herbert Mattord, Cengage Learning.
- A Practical Guide to Security Engineering & Information Assurance, by Debra S. Hermann, CRC Press, 2002.
- A Guide to Computer Security, by Joseph M. Kizza, Springer, 2009.
- Information Security Management Handbook, edited by Ed. Skoudis, CRC Press, 2002.

Food 4 Thought

Learning Outcomes

- To appreciate what the elements of cyber-security are;
- To able to distinguish between threats and vulnerabilities;
- To appraise cyber-risk parameters and how to evaluate it.

Definitions

- Cyber-Security - is to safeguard computer systems and the confidentiality, integrity and availability of the data they contain.

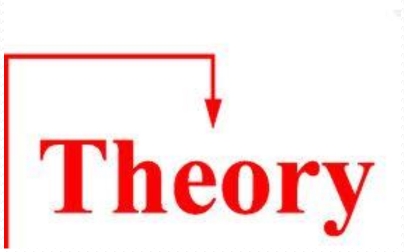
Cyber-Security

Ubiquitous Internet

- has motivated the way we live, work and play today;
- has become the primary conduit for exploiting vulnerabilities;
- has created opportunities, such that cyber-criminals can cause catastrophic impact whilst equipped with only a computer and the knowledge needed to identify and exploit vulnerabilities;
- has created the need for comprehensive research & high-level cyber-security expertise.

Cyber-Security

- ***Essential Elements of Cyber-Security***
  - ITU-T Rec. X.805 stipulates 8 security dimensions, viz: authorization, authentication, availability, communications security, confidentiality, integrity, non-repudiation & privacy.
  - Other authorities have attempted to propose alternatives – Garfinkel, 1994 – PGP & Parker, 2002 – hexad; Dhillion & Backhouse, 2000 – RITE;
  - Universally, the security triad of CIA form the basic bed-rock of any good security initiative.



Cyber-Security

- ***Essential Elements of Cyber-Security***

By definition:

- Confidentiality – is the property that information is not made available or disclosed to unauthorized inidividuals, entities or processes, either in storage or in transmission;
- Integrity - is the property that information has not been altered nor modified in storage and/or in transmission;
- Availability – is the property that information assets are accessible by authorized entities whenever needed.

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Computer Security Objectives

Essential Elements of Cyber-Security

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Cyber-Security

- ***Essential Elements of Cyber-Security***

- Risk is the likelihood of the occurence or realization of a threat. It is given by:

Risk (due to a threat) Ξ Threat (to an asset) X Vulnerability (to that threat)

- Stajano, 2002 posits that cyber-security is essentially risk management – to identify:
  - Assets – any items of economic value to be protected;
  - Threats – any agent, condition or circumstance that can cause harm, loss or damage or compromise an asset;
  - Vulnerabilities – any weaknesses that might facilitate the occurence of a threat;
  - Attacks – any avenues or ways through which a threat is realized.

Cyber-Security

- ***Essential Elements of Cyber-Security***

- Risk – an expected loss caused by an attack, corresponding to the value of the asset involved, and the likelihood that the attack will occur.
- Business impact is evaluated with expert knowledge and historical data.
- Wawrzyniak, 2006 postulated that the impact consists of 2 key elements:
  1. The financial loss upon the threat realization; and
  2. The moral loss affecting the business functionality – corporate image – for a long time.

Cyber-Security

- ***Essential Elements of Cyber-Security***
- Cyber-Risk – we take a holistic view of cyber-risk and allude to a combined definition of cyber-risk as:
- *"the possibility of the occurrence or realization of a threat, due to compromises of the confidentiality, integrity and availability (CIA) of the system and the associated adverse impact on business."*

Cyber-Security

- ***Essential Elements of Cyber-Security***
- It follows that the cyber-risk can be defined mathematically as a fuzzy relational function:

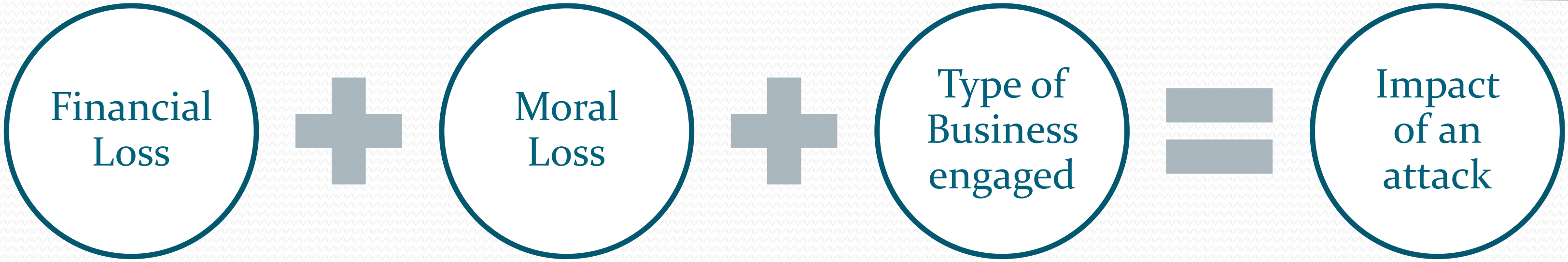
$$\mathit{Risk}_{\text{threat}} \triangleq \tilde{\mathrm{F}}(\text{Threat}_{\text{asset}}, \text{Vulnerability}_{\mathit{threat}}, \text{Asset Value})$$

where:

- Asset Value is the summation of contributing values from the CIA utilities as evaluated in respect of the urgency for restoring a compromised asset and/or its criticality to the business;
- Vulnerability is a weakness within the system that can be exploited by threat agents; and
- Threat is the possibility of exploiting the weakness, given the conditions of motivation or intent, capability, opportunity and attractiveness of the asset.

Cyber-Security

- ***Essential Elements of Cyber-Security***



- **Information** which is ascertained by security classification.
- Below are typical classifications:

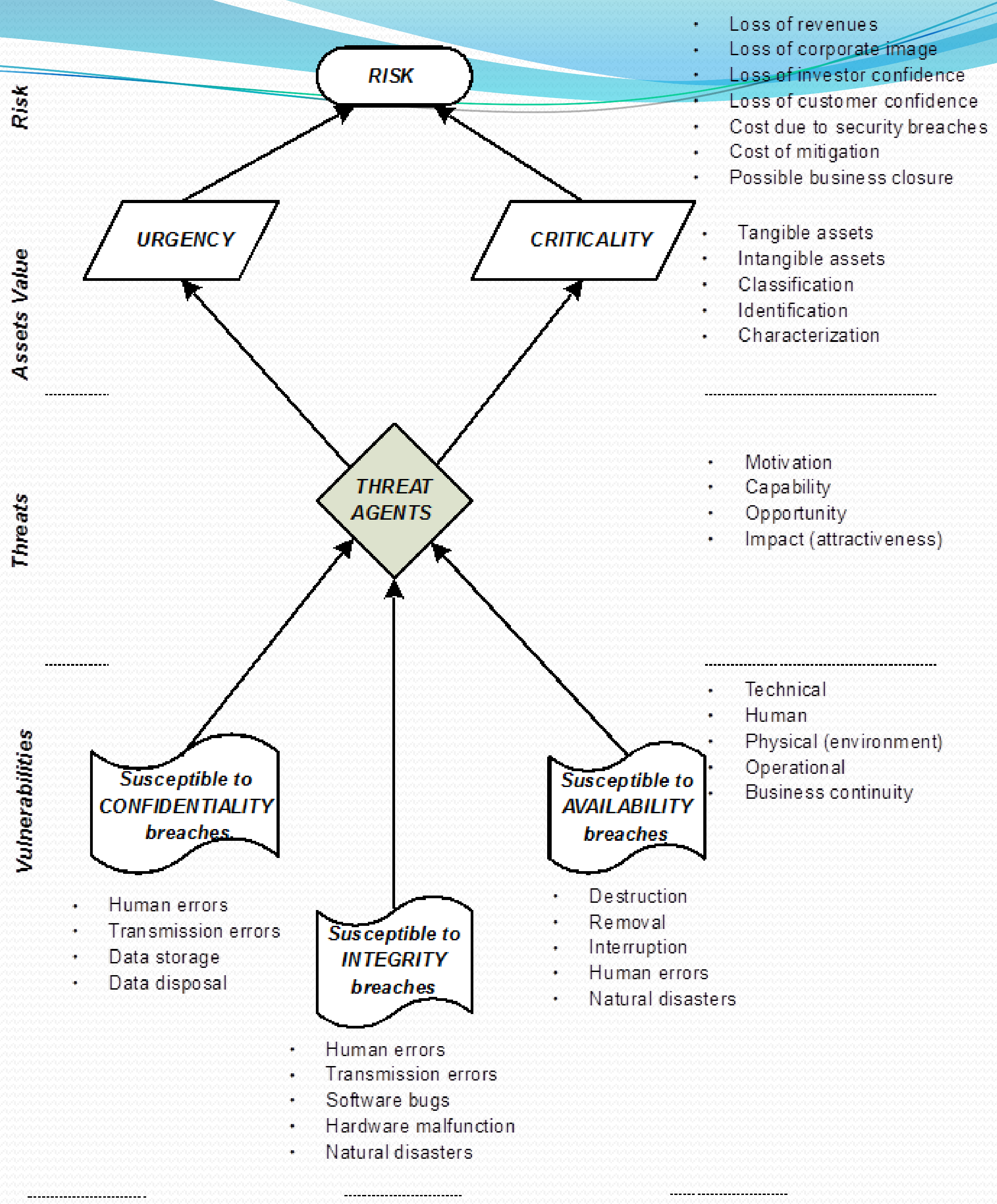
Business
- Public, Sensitive, Private or Confidential

Government
- Unclassified, Sensitive but Unclassified, Restricted, Confidential, Secret or Top Secret

Results & Analysis

Schematic Description of the CSVA Model

Multi-faceted Cyber-Security Vulnerabilities Assessment (CSVA) Model (Yeboah-Boateng, 2013)



Risk

Assets Value

Threats

Vulnerabilities

RISK

- Loss of revenues
- Loss of corporate image
- Loss of investor confidence
- Loss of customer confidence
- Cost due to security breaches
- Cost of mitigation
- Possible business closure

URGENCY

CRITICALITY

- Tangible assets
- Intangible assets
- Classification
- Identification
- Characterization

THREAT AGENTS

- Motivation
- Capability
- Opportunity
- Impact (attractiveness)

- Technical
- Human
- Physical (environment)
- Operational
- Business continuity

Susceptible to CONFIDENTIALITY breaches

- Human errors
- Transmission errors
- Data storage
- Data disposal

Susceptible to INTEGRITY breaches

- Human errors
- Transmission errors
- Software bugs
- Hardware malfunction
- Natural disasters

Susceptible to AVAILABILITY breaches

- Destruction
- Removal
- Interruption
- Human errors
- Natural disasters

Cyber-Threats

- Do you want to have absolutely, positively 100% security against all vulnerabilities and exploits? - known and unknown?

- It's simple! Leave your computer in the box – once ON, functionality (convenience) versus security …
  - Many features – sources of vulnerabilities
  - The essence of sharing – as conduit for vulnerabilities, e.g. viruses, worms us same communication channel as shared files and folders;

Cyber-Threats

- Malware – capturing passwords, credit card numbers. Sending out malware to other computers or to email addresses of people you know, DoS from your computer, etc.
- Weak passwords – guess or crack your password, gain access to confidential information, steal your identity, install and execute programs using your account, etc.
- Network “neighbors” – computers within the same range of IP addresses, easy to communicate , e.g. DSL, cable modem, etc.

Cyber-Threats

- a **threat** is the potential for one or more unwanted consequences caused by a circumstance, capability, action or event that could be harmful to a system or person.
- Threats can be caused naturally, accidentally or intentionally.
- In essence, a threat is a ubiquitous phenomenon.

Cyber-Threats

- The US President’s Information Technology Advisory Committee (PITAC) posits that the innovations in ICT have created a whole new industry through the “ubiquitous interconnectedness
  - – first exhibited by the Internet and further extended in local area networks, wide area networks, [etc.]
  - – has generated whole new industries, rejuvenated productivity in older ones, and opened new avenues for discourse and education and an unprecedented era of collaborative science and engineering discovery worldwide.”
- PITAC continues that “that is indeed good news. The bad news is that ubiquitous interconnectivity provides the primary conduit for exploiting vulnerabilities on a widespread basis.” (PITAC, 2005)
- Innovations in ICT created the ubiquitous Internet, which is an embodiment of “openness, inventiveness and [assumes] goodwill” (PITAC, 2005)

Cyber-Threats

- Today’s interconnectivities or the Internet, are constantly under attack by hackers or crackers, who engage in spoofing, phishing, denial of service attacks via worms, Trojans, viruses and other assorted malware, including spyware, adware and spam.
- Malware has been an unfortunate feature of daily life on the Internet and, lately, with advanced mobile phones.
- Often, malware is aimed at uncovering and exploiting personal and confidential data.

Cyber-Threats

- Hardware failure – data loss (e.g. power outage, hard disk failure, firewall malfunction, router failure, access point failure)
- Natural disaster – data loss (e.g. fire, flood, rains)
- Human sabotage (employees, ex-employees, consultants, contractors, etc.) – internal & external

Cyber-Threats

- Ransomware
- Spam – many firms (SMEs) receive so much of this unwanted email that it shuts down email servers and causes delays in business. This is a compromise of the availability part of the CIA triad.
- Virus – destroys data (integrity)
  - A virus is hidden, self-replicating software that propagates by infecting – i.e., inserting a copy of itself into and becoming part of – another program. A virus cannot run by itself; it requires a host program to be activated.
- Worms – integrity, availability (so much traffic is caused or sent such that the systems shut down)
  - A worm is software that can run independently, can propagate a complete working version of itself onto other hosts in a network, and may consume computer resources destructively.
- Spyware – integrity, confidentiality (e.g. keyloggers)
- Phishing – integrity, confidentiality

Cyber-Threats

- Botnets – denial-of-service (DoS) (availability), spams (availability), stealing of data (integrity & confidentiality)
- A Trojan is software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.
- Phishing means tricking the user into providing identity or banking data by asking the user to confirm his personal data on a fake web site which pretends to be a legitimate site, and often looks exactly like a web page of, for example, a user’s bank.
- Denial of service (DoS) is the prevention of authorized access to a system resource or the delaying of system operations and functions, e.g., the attacker sends a huge number of extra messages to a target service provider and in doing so denies access by others.

Cyber-Vulnerabilities

- A **vulnerability** is a flaw or weakness in a system's design, its implementation, operation or management that could be exploited to violate the system and, consequently, cause a threat.
- Vulnerabilities may have different dimensions: technical, functional or behavioral.

Cyber-Vulnerabilities

- The Vulnerabilities survey shall address the following attributes – their Type, Source and Severity:
  - a weakness in a system that can be exploited to violate the system's intended behavior relative to confidentiality, integrity and availability;
  - vulnerabilities are inherent in the design, operation, or operational environment of a system;
  - vulnerabilities result from errors of omission, error of commission, and operational errors during the life of a system.

Cyber-Vulnerabilities

- Vulnerabilities – are weaknesses of flaws in a systems: design; implementation; operation; management
- Vulnerabilities – may be technical, functional or behavioral.
- Human vulnerabilities – lack of ICT staff, small ICT budgets, un-patched systems, improperly configured systems, etc.
- Wireless networks – ease of bypass (data loss), vulnerable to attacks

Cyber-Vulnerabilities

- ***System complexity, false positives and unpredictable failures***
- Systems complexity may pose the risk of:
  - unpredictable system behavior
  - malicious attacks due to security holes caused by the interaction of components.
- Interactions between operational systems may hinder :
  - customer applications functionality or slow down
  - antivirus software functionality, which may increase the risk of successful virus attacks.
- False positives may arise if the system authenticates and authorizes the wrong person or entity to perform some functions – the system has failed.

Cyber-Security

- ***Lack of user-friendly security and configuration software***
- What techniques are used to authenticate users? For example:
  - Single factor (e.g. user ID + password)
  - Software second factor (e.g. digital certificates + tokens)
  - Hardware second factor (e.g. smartcards)
  - Third factor (i.e. biometrics)
  - Some systems with no authentication.

Cyber-vulnerabilities

- ***Component examples***

i. Component design:
  - Inadvertently flawed component design
  - Intentionally flawed component design
  - Excessive component functionality
  - Open or widely spread component design
  - Insufficient or incorrect documentation

ii. Component procurement:
  - Insufficient component validation
  - Delivery through insecure channel

iii. Component integration:
  - Mismatch between product security levels
  - Insufficient understanding of integration requirements

Cyber-Vulnerabilities

- ***Systems examples***

i. System Internet connection:

- Increased external exposure
- Intrusion information and tools easily available
- Executable content
- Outward channel for stolen information

ii. System use:

- Unintended use
- Insufficient understanding of functionality

iii. System maintenance:

- Insecure updating
- Unexpected side effects
- Maintenance of trap doors

Summary

- We have discussed the elements of cyber-security;
- We have distinguished between threats and vulnerabilities;
- We have defined cyber-risk and its parameters; with examples on its impact on business.

- Next Lecture: Building a Secure Organization.

Thank You All!!!

- Any comments & contributions????