

THE NIGERIAN CAPITAL MARKET INFORMATION SECURITY FORUM



**THE Nigerian
STOCK EXCHANGE**

Why Capital Market Executives Should Take Cybersecurity Seriously

Ade BAJOMO

Executive Director
Market Operations and Technology

April 16 2015

Introduction – Cyber security

Cyber security — the protection of valuable intellectual property and business information in digital form against theft and misuse.

— disgruntled employees releasing sensitive electronic information, taking intellectual property to competitors.

The US government has identified cyber security as “one of the most serious economic and national security challenges we face”



Cyber security — is an increasingly critical management issue.

Companies must now fend off ever-present cyber attacks.

While sophisticated companies have recently endured highly public breaches to their technology environments, many incidents go unreported.

Why The Nigerian Capital Market Information Security Forum



Planet of the Phones



“in developing countries every ten extra mobile phones per 100 people increase the rate of growth of GDP-per-person by more than one percentage point—by, say, drawing people into the banking system”

Need to secure and maintain information integrity has never been greater



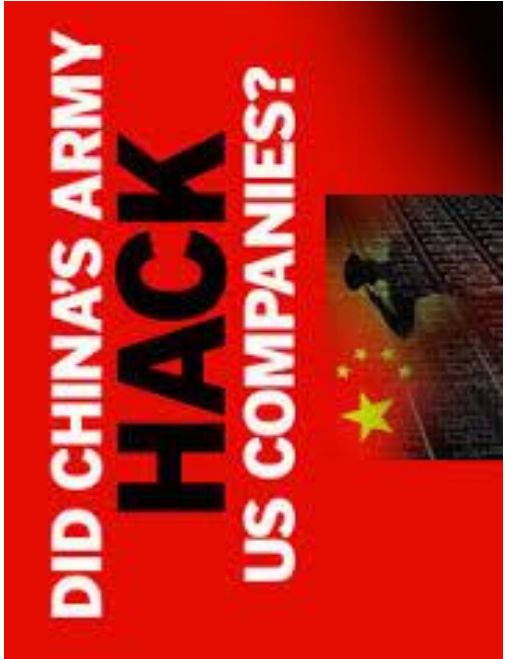
The Statistics that you don't want to be part of

- **SMB Threat Perception:** 77% say their company is safe from cyber threats
- 66% say they are not concerned with hackers, cyber-criminals, or even employees stealing data
- 47% believe a data breach would have no impact on their business

- **SMB Security Program Status:** 87% do not have a formal written security policy
- 59% do not have a security incident response plan for a data breach
- 50% of users still use poor passwords
- 83% do not have a system to require employees to periodically change passwords

- **SMB Threat Reality:** 71% of data breaches target small businesses
- 69% of cyber attacks target retail and restaurants
- 96% of data breaches target payment card data
- 60% of small businesses close within six months of experiencing a data breach
- IOSCO reported a sharp increase in the number of Exchanges and Capital Market operators experiencing information security breaches

Managing Information is now serious business



Keep your friends close and your information closer

Remaining Open for Business



Navigating the Security Maze



The Top Security Concerns for Execs - People



Access Denied



I need to find the bad people



I won't let you be me



Go find some other mug

The Top Security Concerns for Execs - Technology



Hello, are you still there?



I may be lost but not forgotten



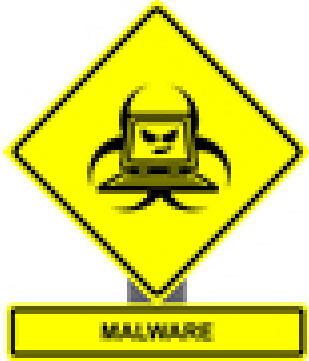
Hey, get off my network



I seek what you leak, so carry on

Keep your friends close,
Your info closer

The Top Security Concerns for Execs – Processes (and People)



Mind what you install,
Don't catch a virus



Email someone else



Don't come fishing with me



It's a jungle out there,
Even in the cloud!

The NCMISF

- Most business transactions in the Capital Market will be done on smart technology
- Maintaining awareness is not an option
- The group's term of reference is on www.nse.com.ng
- Seminars will be at least twice a year
- Members will provide advice across industry
- Membership is free
- Share the news – both good and not so good



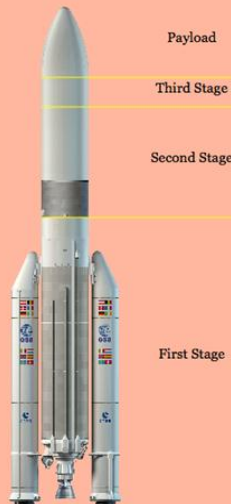
... to conclude

- No such thing as 100% security but execs can take sensible steps to protect their business
- Being secure can be hard work but is not rocket science
- Pay attention to people, technology and processes
- Keep your ears to the ground – native senses work in an information centric age
- Join the NCMISF – Get good advice and early warning wherever possible

Proceed to Launch!

Rocket Design

	Thrust (kNewtons)	Fuel (tonnes)	Cost (\$million)	Mass (tonnes)	
First Stage	1000	500	600	700	Payload
Second Stage	200	100	120	108	Third Stage
Third Stage	30	15	18	15	Second Stage
Boosters	800	400	480	528	First Stage
Totals:			1218	1351	





**THE Nigerian
STOCK EXCHANGE**

THANK YOU

Questions & Answers

Visit our website today!

www.nse.com.ng

“A truly user-friendly experience”

NEW & IMPROVED WEBSITE

- Featuring Intuitive navigation
- Enhanced view of listed securities
- Detailed quotes and charting
- Site-wide search
- Mobile access
- Easy-to-find information
- Social media integration
- Improved site load-time
- Enhanced content





THE Nigerian STOCK EXCHANGE

NIGERIAN CAPITAL MARKET INFORMATION SECURITY FORUM *Protection of Information Assets*

Favour Femi-Oyewole (NSE)

April 16, 2015

- Introduction

- Asset - Overview

- Assessing Values for Information Assets

- Assessing Values for Information Assets

- Access Control

- Balancing Information Security and Access

- Security Management - Challenges

- Manage Identities

- Managing Access Control Attacks

- Recap: Protection of Information Assets

- **What is Information?**
- A collection of organized fact
- A key resource for all enterprises.



- **What is an Asset?**
- Something you own that has value
- can gain value over time
- can lose value over time



This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements

- While hardware and software elements are easily described, the human resources, documentation, and data information assets are not as readily discovered and documented
- These assets should be identified, described, and evaluated by people using knowledge, experience, and judgment
- As these elements are identified, they should also be recorded into some reliable data handling process

- Provides a record of valuable assets for accounting/tracking purposes
- Helps identify areas of potential risk (notebooks storing private data, servers with expired warranties, etc.)
- Important piece of information for business continuity planning
- Provides information useful during technical support or in the event of loss/theft (make, model, serial number)

Information Asset Classification

Examples of these kinds of classifications are:

- confidential data
- internal data
- public data

Information Asset Valuation

- Key questions should be asked to assist in developing the criteria to be used for asset valuation



For People	For Procedures	For Data
<ul style="list-style-type: none">• Position name/number/ID- try to avoid names and stick to identifying positions, roles, or functions• Manager• Security Clearance level• Special skills	<ul style="list-style-type: none">• Description• Intended purpose• What elements is it tied to• Where is it stored for reference• Where is it stored for update purposes	<ul style="list-style-type: none">• Classification• Owner/creator/manager• Size of data structure• Data structure used – sequential, relational• Online or offline• Where located• Backup procedures employed

- Information asset is identified, categorized, and classified, assign a relative value
- The most valuable information assets are given the highest priority, for example:

Which information asset is the most critical to the success of the organization?

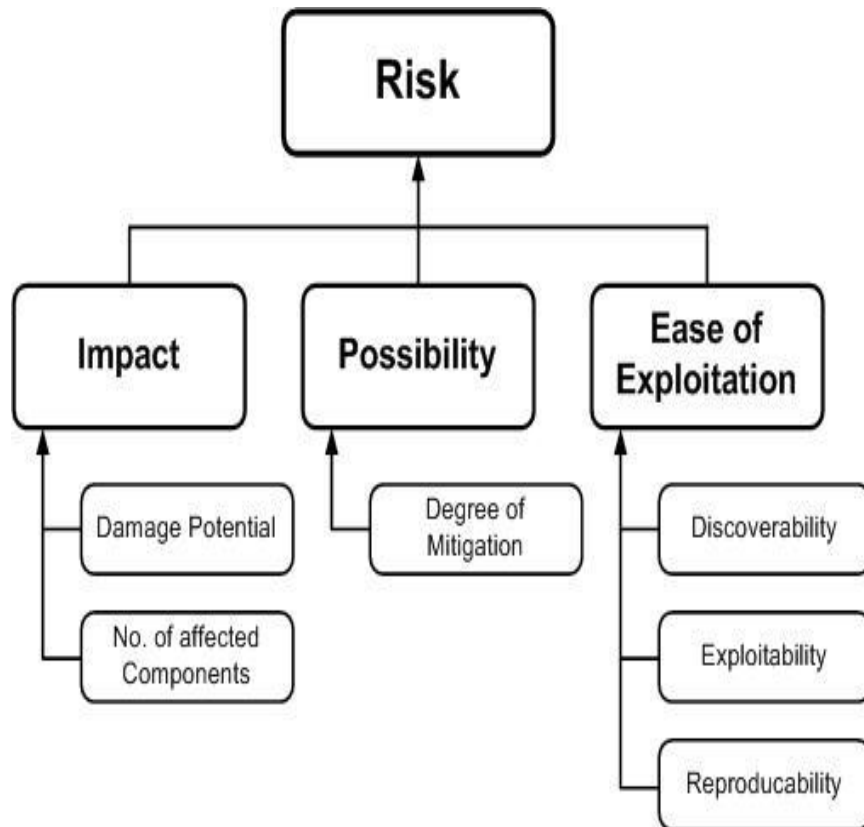
Which information asset generates the most revenue?

Which information asset generates the highest profitability?

Which information asset is the most expensive to replace?

Which information asset is the most expensive to protect?

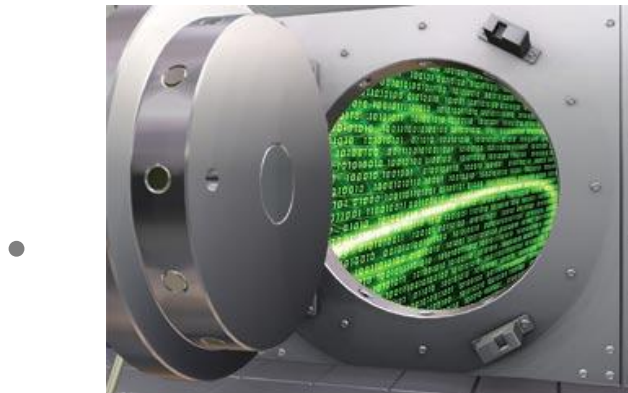
Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?



Types of Access Controls

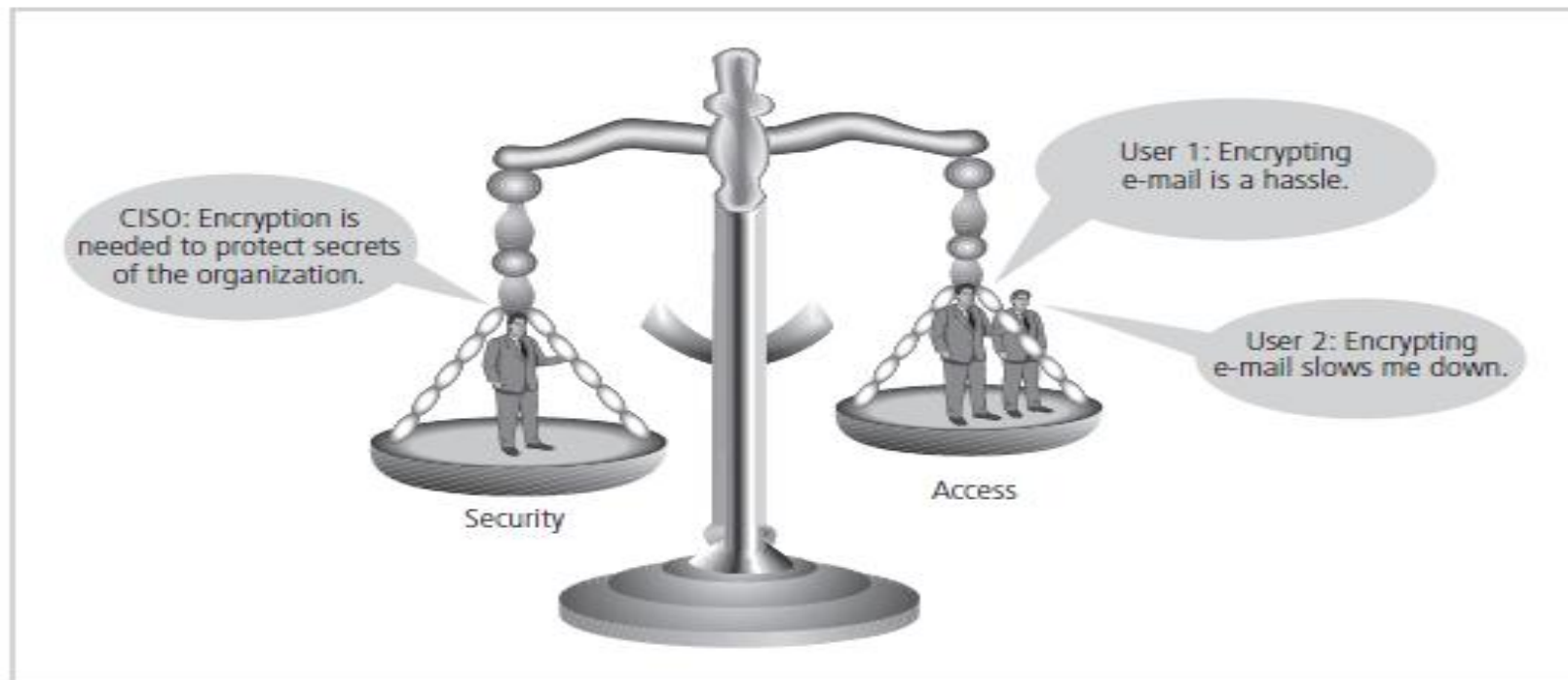
- Discretionary Access Controls (DAC)
- Mandatory Access Controls (MACs)
- Nondiscretionary Controls

- Should everyone have an access button?



Should information be kept in a vault?

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability



- Do you:
 - **Control who** has access to which resources
 - **Know what** is happening in your environment
 - **Know what** to do about it
 - Have the tools necessary to **take action**

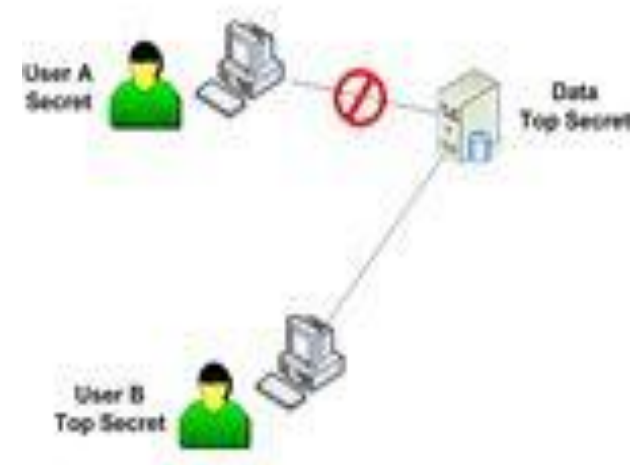


- **Mandatory**

- Enforces corporate security policy
- Compares sensitivity of information resources

- **Discretionary**

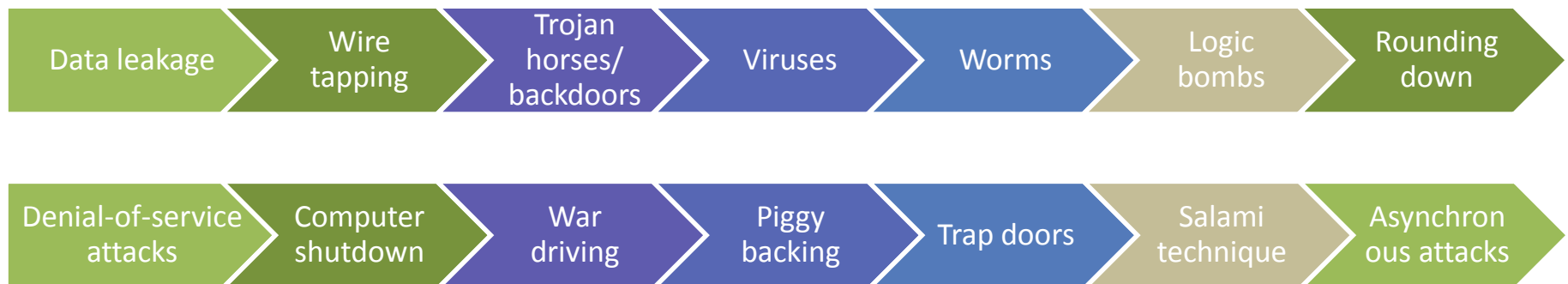
- Enforces data owner-defined sharing of information resources



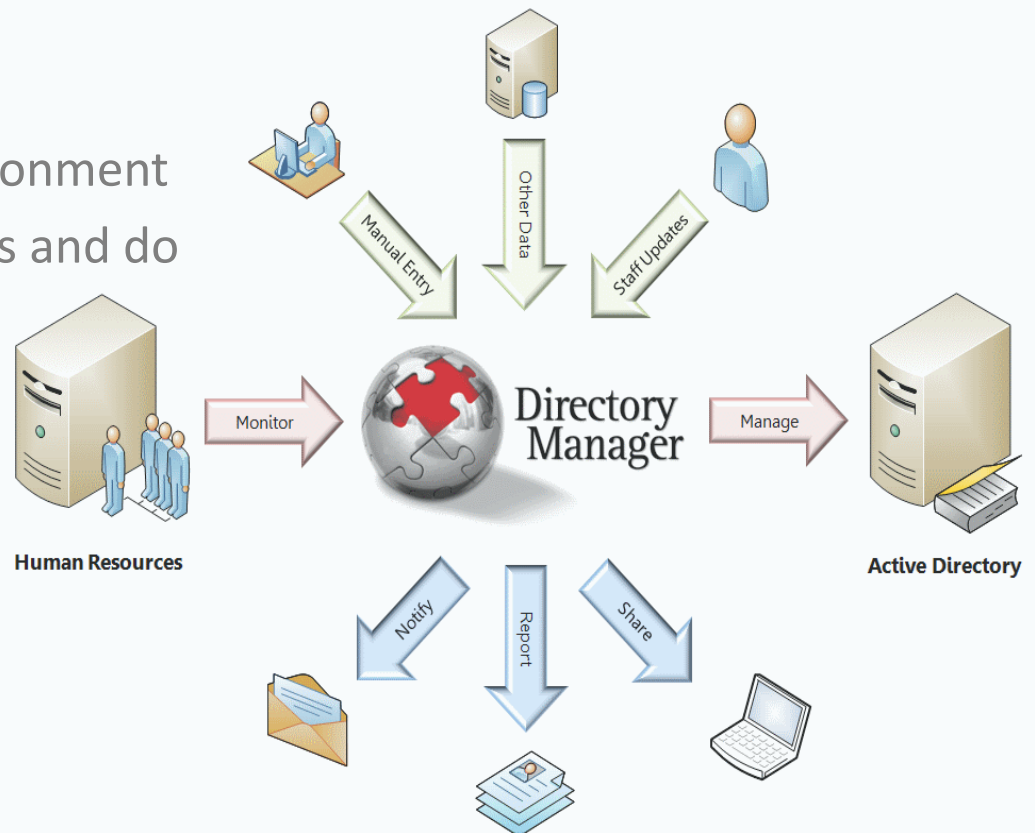


Logical access controls are the primary means used to manage and protect information assets.

Logical Access Exposures



- Identity and Access management is critical to total security management
- Identities must be managed
 - Manage who is in your environment
 - Control what they can access and do
 - Know what users have done



- What is a password? (someone tell me because I forgot...)

	Description
Password Problems	People write down passwords, People use weak passwords
Create good passwords	Use a phrase and take attributes of a phrase, transpose characters
Attacks on Password	Sniffing (Electronic Monitoring), Brute force attacks
Passwords and the Operating System	The Operating System should enforce password requirements like Aging, Reuse of old passwords, numbers of characters, Limit login attempts
Password protection	System should NOT store passwords in plaintext, encrypt hashes Passwords salts
Cognitive passwords	Used to verify who you are talking to without giving out password
One Time Password (OTP)	Not vulnerable to electronic eavesdropping, but vulnerable to loss of token
OTP Type	Synchronous: uses time to synchronize between token and authentication server Asynchronous: Challenge response



I&A common vulnerabilities

- Weak authentication methods
- Lack of confidentiality and integrity for the stored authentication information



Best practices for logon IDs and passwords

- Passwords should be minimum of 8 characters, combination of alpha, numeric, upper and lower case and special characters

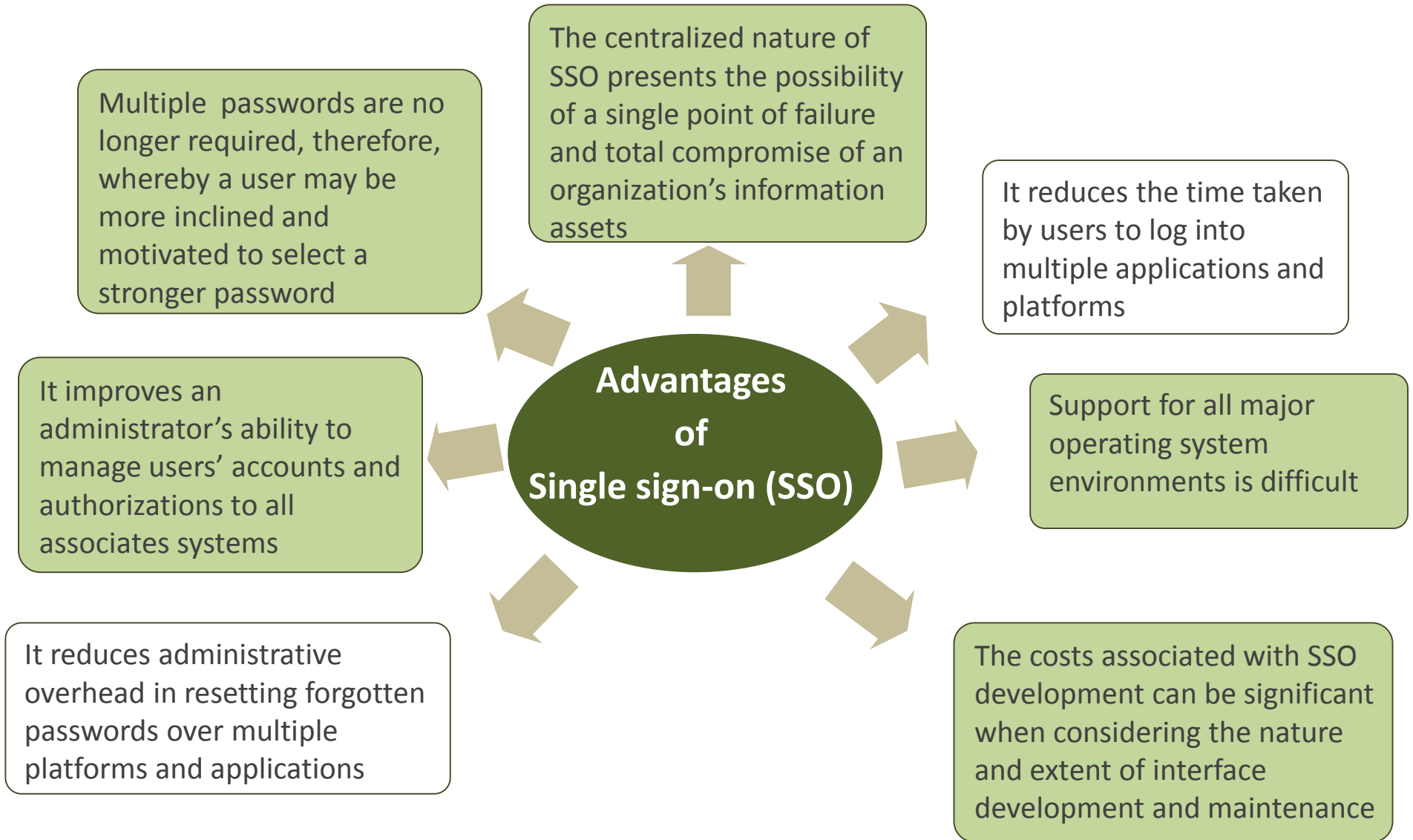


Single sign-on (SSO)

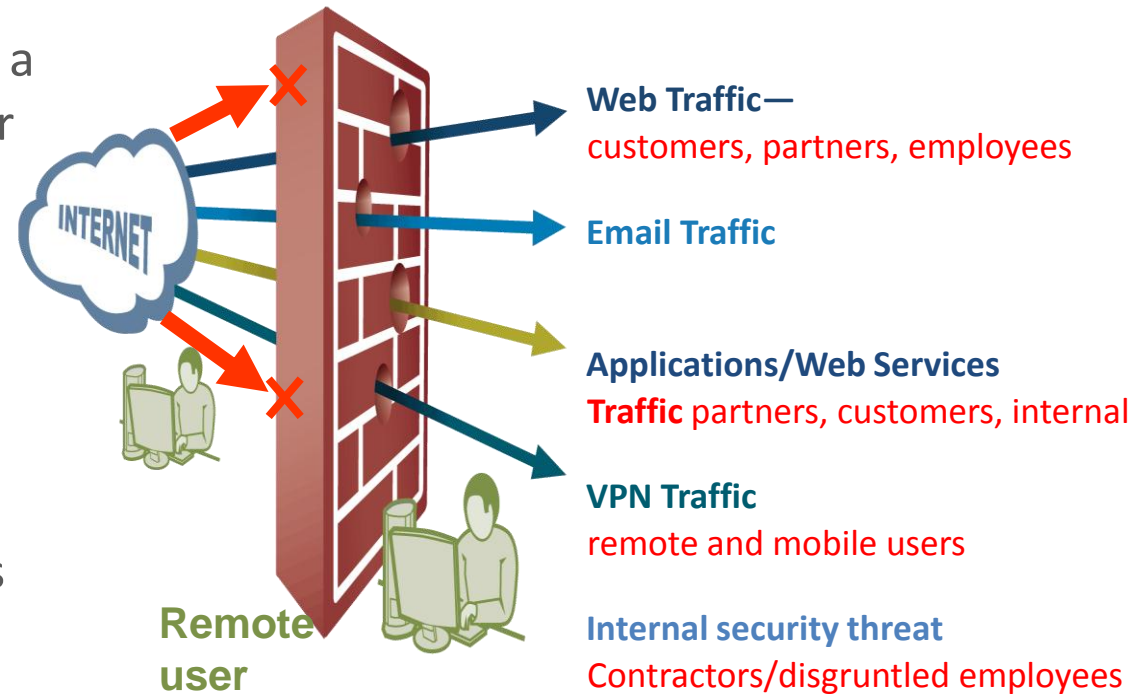
- This is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications.



- Token devices, one-time passwords
- Biometrics
 - Physically-oriented biometric
 - Behaviour-oriented biometric



- ✓ Authorization is the process where a system determines if a specific user has access to a particular resource
- ✓ The intent of authorization is to ensure that a user only accesses system functionality authorized
- ✓ Role based access control (RBAC) is commonly used to manage permissions within an application



Access Control

Elevation of privileges

Disclosure of confidential data

Compromising admin-level accounts often results in access to user's confidential data

Data tampering

Privilege levels do not distinguish users who can only view data and users permitted to modify data

Who is reviewing the log?

Confirm review documentation

What activity/data is logged?

(1) Log Size (2) Reviewing Time

To provide assurance that the enterprise security architecture

viz - *policies, standards, procedures, and controls*

ensure the **CONFIDENTIALITY, INTEGRITY, and AVAILABILITY** of information assets.

- the **design, implementation, and monitoring of logical access controls** should ensure the **confidentiality, integrity, availability** and **authorized** use of information assets.
- the **network infrastructure security** should ensure **confidentiality, integrity, availability** and **authorized** use of the network and the information transmitted.
- the **design, implementation, and monitoring of environmental controls** should prevent or minimize loss.
- the **design, implementation, and monitoring of physical access controls** should ensure that information assets are adequately safeguarded.
- the **processes and procedures used to store, retrieve, transport, and dispose of confidential information** assets.



**THE Nigerian
STOCK EXCHANGE**

THANK YOU

Questions & Answers

Visit our website today!

www.nse.com.ng

“A truly user-friendly experience”

NEW & IMPROVED WEBSITE

- Featuring Intuitive navigation
- Enhanced view of listed securities
- Detailed quotes and charting
- Site-wide search
- Mobile access
- Easy-to-find information
- Social media integration
- Improved site load-time
- Enhanced content





Information Security Made Simple



**THE Nigerian
STOCK EXCHANGE**

Defending Against The Digital Invasion

Presenter: Obadare Peter Adewale

Nigerian Capital Market Information Security Forum (NCMISF)

16th April 2015

PROFESSIONAL CERTIFICATIONS

- **Fellow British Computer Society (FBCS)**
- **Chartered I T Professional (CITP)**
- **COBIT 5 CERTIFIED ASSESSOR**
- **COBIT 5 Foundation Certificate**
- **Payment Card Industry Professional (PCIP)**
- **Payment Card Industry Qualified Security Assessor**
- **ISO 27001 Lead Implementer**
- **ISO 27001 Lead Auditor**
- **ISO 2000 Lead Auditor**
- **ISO 22301/ BS 25999 Lead Auditor**
- **Integrated Management System Lead Auditor**
- **Computer Hacking Forensics Investigator (CHFI)**
- **Ec- council Certified Secure Programmer (ECSP)**
- **Ec- council Licensed Penetration Tester (LPT)**
- **Ec- council Security Analyst (ECSA)**
- **Ec- council Certified Ethical Hacker (CEH)**
- **Master Security Analyst (MSA)**
- **Certified Security Analyst (CSA)**
- **Qualys Guard Certified Specialist (QCS)**
- **Cisco Certified Internetwork Expert (CCIE Written)**
- **Security Networks with ASA Advance (SNAA)**
- **Cisco Certified Design Professional (CCDP)**
- **Cisco Certified Network Professional (CCNP)**
- **Cisco Certified Network Associate (CCNA)**
- **Cisco Certified Design Associate (CCDA)**



**HARVARD
BUSINESS SCHOOL**
Executive Education

**LEADING PROFESSIONAL
SERVICE FIRMS**

LPSF CLASS OF 2014



**MIT Sloan
Executive
Education**

Global Executive Academy

GEA CLASS OF 2014

Honors and Awards

Titans of Tech Centennial Award

Technology Africa

June 2014

Centennial Information Security Company of The Year

FATE ALUMNI MODEL ENTREPRENEUR TOP 3 SELECTIONS

FATE FOUNDATION

November 2013

The FATE Alumni Model Entrepreneur Award is a business and entrepreneurial Award that recognizes and rewards high performing FATE trained entrepreneurs with a track record of business excellence and high social impact.

Global CyberLympics: Africa Regional Champion

International Council of E-Commerce Consultants (EC-Council)

October 2012

CyberLympics is an International Capture-the-Flag Ethical Hacking Competition organised by EC-Council. TeamNaija won the Award for the overall best team for the African Region out of a total of 24 teams.

Distinguished Visitor

Miami-Dade County Office of the Mayor and Board of County Commissioners

November 2010

The Distinguished Visitor award was given during the Global Entrepreneurship Week of an exchange programme to Miami Florida coordinated by Barry-ADPED and sponsored by US Department of State.

Agenda

What are we protecting?

- Company Data
- Personal Data
- Critical systems-email, network, file storage, online services

What are we protecting against?

- Information exposure (Confidentiality)
- Malicious Editing (Integrity)
- DOS-Denial of Service (Availability)

How do these things happen?

- **INSIDER THREAT: ENEMY BY THE WATER DISPENSER**
Internal Malicious user gets remote access to email passwords
- **OUTSIDER THREAT: SHOW ME THE MONEY ”**
Hackers gets access to company's Internet banking
- **OUTSIDER with INSIDER knowledge: DEAL OR NO DEAL**
Social Engineering / video

IT Security vs Information Security

- ♣ IT security deals with protecting the network whilst information security deals with protecting the information transmitted over the network
- ♣ Information security solutions have focused on preventing external threats such as viruses, hackers and worms through perimeter solutions that include firewalls and antivirus software. While still aware of outside threats, companies are now coming to understand they can no longer ignore inside violations concerning data at rest. So information security and privacy is of utmost importance whether it is internal or external
- ♣ IT Security is difficult to comprehend but easy to implement, Information Security is easy to comprehend but difficult to implement

Components of an Information System

Each component has its own security requirements

♣ Software

- Applications, operating systems, utilities
- Exploitation of programming errors accounts for a substantial portion of information attacks
- Easy target for accidental or intentional attacks

♣ Hardware

- Physical components of IS
 - Physical security deals with protection of physical assets
 - from theft, vandalism, destruction
- Issue: security for laptop and notebook computers

Components of an Information System (Contd)

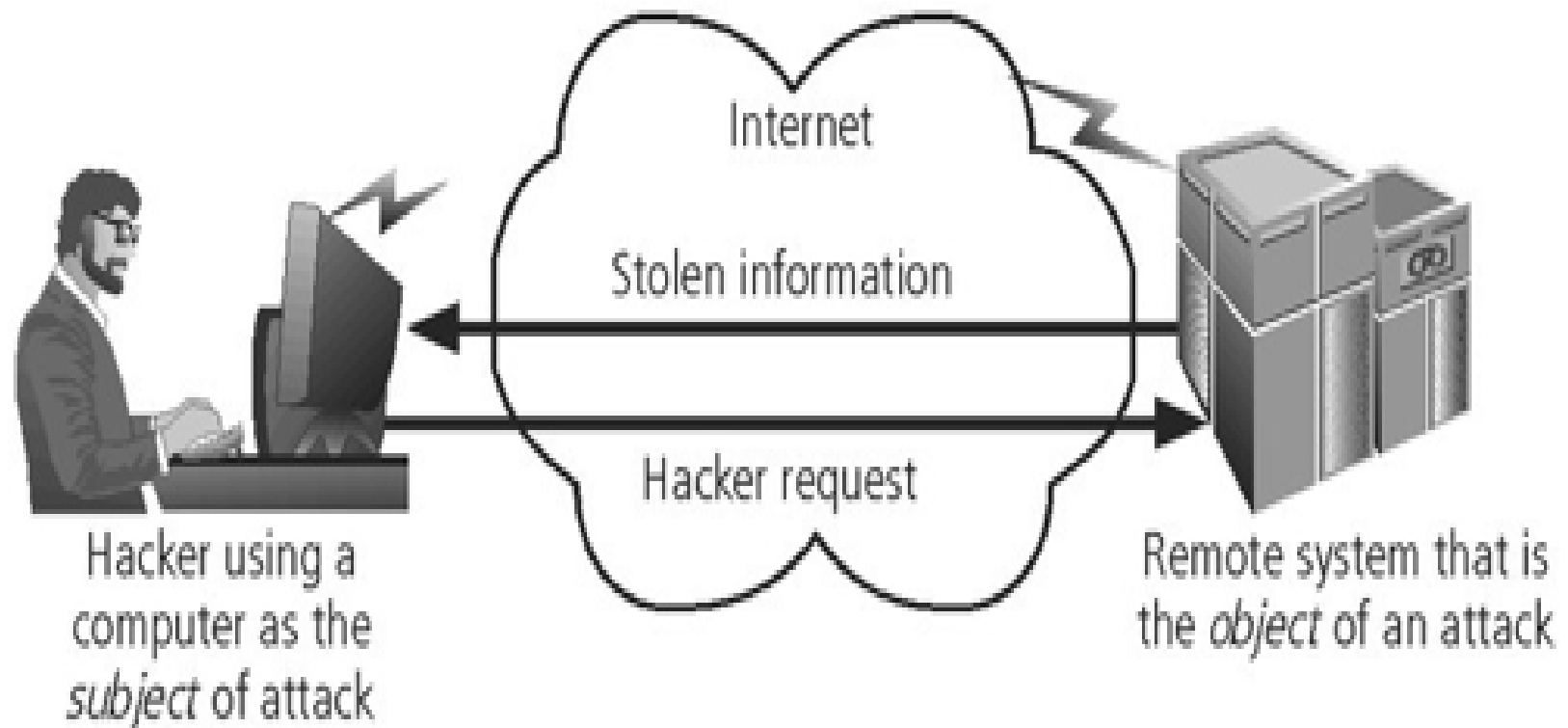
♣ Data

- Often the most valuable asset possessed by an organization and main target of deliberate attacks
- Proper development and use of database management systems increases data security

♣ People

- Can be the weakest link (greatest threat) to security in an organization
- Policy, education and training, awareness and technology are all used to prevent people from accidentally or intentionally damaging or losing information
- **Social engineering** can be used to manipulate the actions of people to obtain access information about a system

Subject and Object of Attack

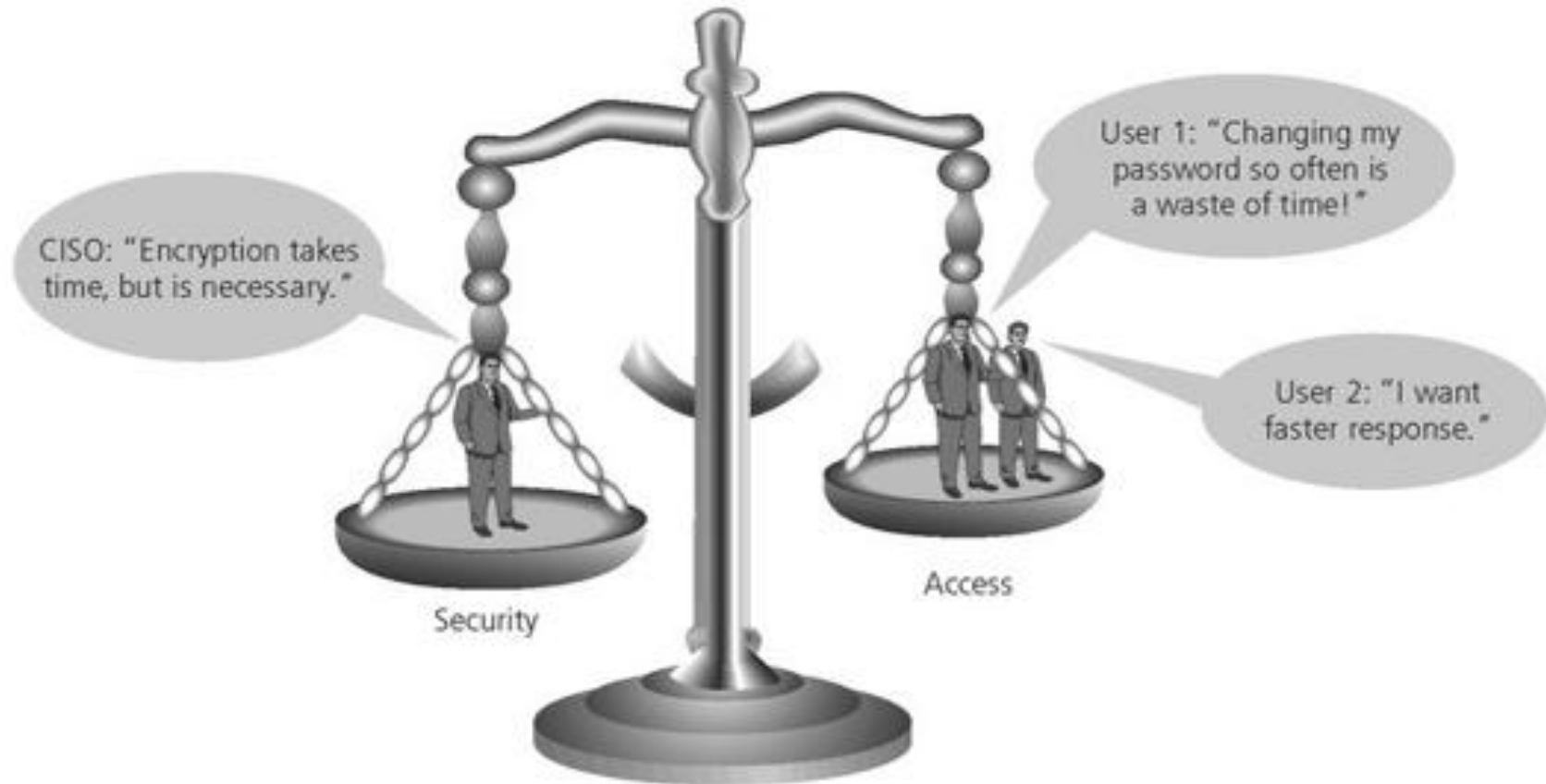


Computer as an Object and Subject of Attack

Balancing Security and Access

- ♣ It is impossible to obtain perfect security
 - Information security is a **process**, not a **goal**
Information security must balance **protection** and **availability**
 - **Unrestricted access**
 - system is available to anyone at any time
 - dangerous to the integrity of the information
 - insufficient control
 - **Total security**
 - would not allow anyone access.
 - **Balance**
 - Operate system to the satisfaction of the users AND the security professional
 - Must allow **reasonable access** to authorized users.
 - Must provide **reasonable protection** against security threats.

Balancing Security and Access



Balancing Security and Access

Approaches to Implementing Security

- ♣ An ongoing process that requires coordination, time, and patience
- ♣ **Bottom-up approach**
 - Starts as grassroots effort with system administrators attempting to improve system security
 - Rarely works, lacks organizational support
- ♣ **Top-down approach**
 - Initiated by upper-level managers
 - Issue policies, procedures, and processes
 - Define the goals and expected outcomes Establish
 - accountability.
 - Has strong upper-management support, dedicated funding, clear planning and implementation process, and means for influencing organizational culture.

Approaches to Security Implementation



Approaches to Security Implementation

DEMO 1: PASSWORD SNIFFING ON THE LAN

INSIDER THREAT: ENEMY BY THE WATER DISPENSER

Network Sniffing & LAN Poisoning

DEMO 2: APPLICATION COMPROMISE

OUTSIDER THREAT: SHOW ME THE MONEY

**Session Hijacking, Simple Phishing attack, Simple SQL Injection attack,
Privilege Escalation**

DEMO 3: HUMAN SECURITY

OUTSIDER THREAT / INSIDER INFO: DEAL OR NO DEAL

Social Engineering / Video

Information Security: Art and Science

♣ Security as Art

- No hard and fast rules or universally accepted solutions
- Requires knowledge and experience of systems and goals to build the solution that best fits the organization's needs

♣ Security as Science

- Technology is a major component of information security solutions
- Requires knowledge of technologies, and use of accepted standards and practices

♣ Security as Social Science

- People are a critical component in the organization and in the security of the organization
- Security must consider and address human factors

Conclusion

THANK YOU



Information Security Made Simple