Introducing myself

Dr. Zakria

- PhD, Software Engineering

  University of Electronic Science and Technology of China.

- MS, Computer Science and Information Technology

  NED University of Engineering and Technology, Karachi.

- BS, Electrical (Computer) Engineering

  COMSATS University, Lahore, Pakistan

What is Information Security ?

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

What is Information Security ?

- **IT Security** is information security applied to technology

- **Information security** also covers physical security, human resource security, legal & compliance, organizational, and process related aspects

What is Information Security ?

- **IT Security functions:**
  - Network security
  - Systems security
  - Application & database security
  - Mobile security
- **InfoSec functions:**
  - Governance
  - Policies & procedures
  - Risk management
  - Performance reviews

What is Information Security ?

- **What is Cyber Security ?**
  - Precautions taken to guard against unauthorized access to data (in electronic form) or information systems connected to the internet
  - Prevention of crime related to the internet

What is Information Security ?

- Three Pillars of Information Security:
  - **Confidentiality:** keeping information secret
  - **Integrity:** keeping information in its original form
  - **Availability:** keeping information and information systems available for use

Why Is Information Security Needed ?

- **Bangladesh Bank SWIFT Hack – Feb 2016:** Hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests

REF: WIRED.COM

Why Is Information Security Needed ?

Contd…

- Requests sent to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
- USD 81 million stolen
- Total impact could have been USD 1 billion

REF: WIRED.COM

Why Is Information Security Needed ?

Recent Cyber Attack – May 2017

NHS

NHS cyberattack is 'biggest ransomware outbreak in history'

The NHS hack using Wanna Decryptor ransomware has shut down IT systems with 75,000 attacks in 99 countries

Ransomware attack hits 99 countries with UK hospitals among targets – live updates

REF: TELEGRAPH

Why Is Information Security Needed ?

Screenshot of the suspected ransomware message on a GP's computer in the Greater Preston area CREDIT: PA

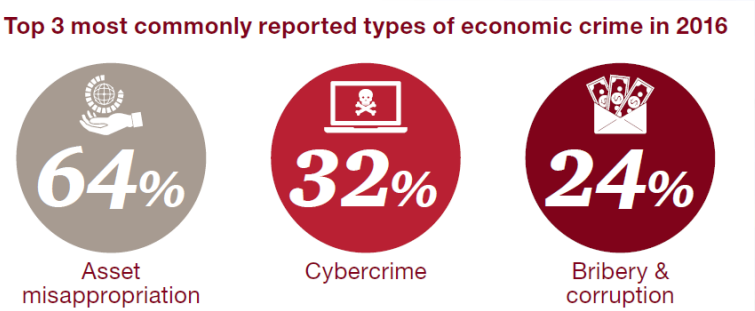
REF: GUARDIAN

Why Is Information Security Needed ?

- **The Importance Of Information**
  - IT is pervasive in our society & critical to the Ops & Mngmt of all organizations
  - IT is an enabler for business and govt
  - Personal information is vital for individuals to function in society
  - Information holds value

Why Is Information Security Needed ?

IMPORTANCE OF INFORMATION SECURITY



- As per PWC Global Economic Crime Report 2016, Cyber Crime was amongst the top 3 most commonly reported types of economic crime

- As per Europol 2013 report, Cyber Crime is now more profitable than the drug trade

Who Is Information Security For ?

- **Personal:**
  - Social media passwords and safe usage
  - Online banking and email account passwords
  - Home PC/laptop security
  - Mobile security

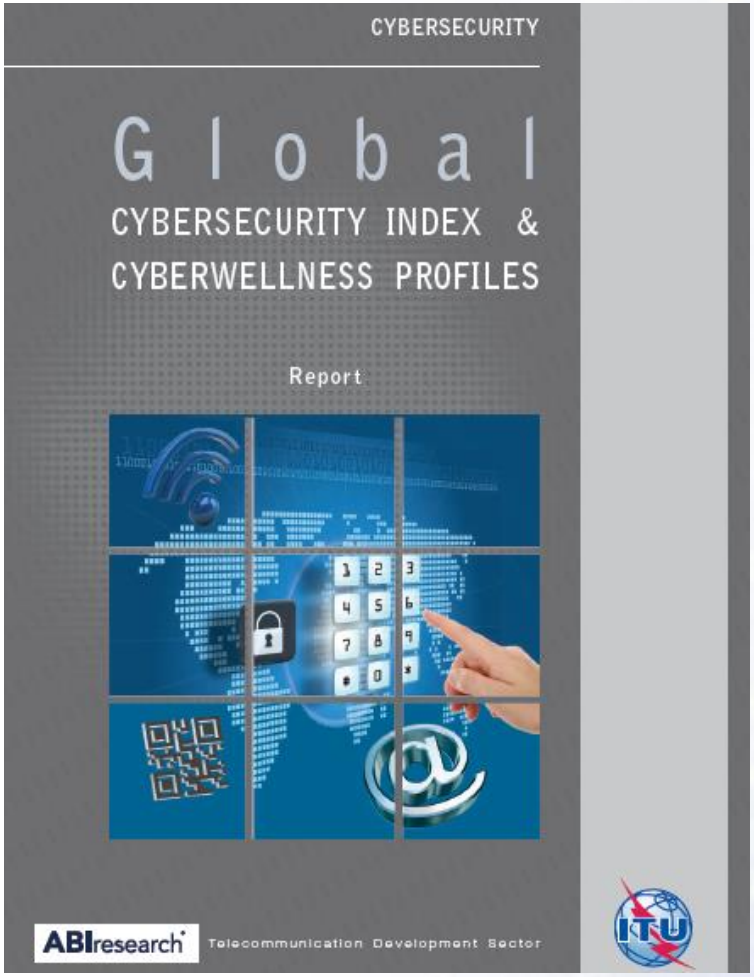
Who Is Information Security For ?

- **Organizational:**
  - Board and executive leadership (management commitment)
  - CISO (responsible to drive security program)
  - IT staff and business users (following information security policies & procedures)

Who Is Information Security For ?

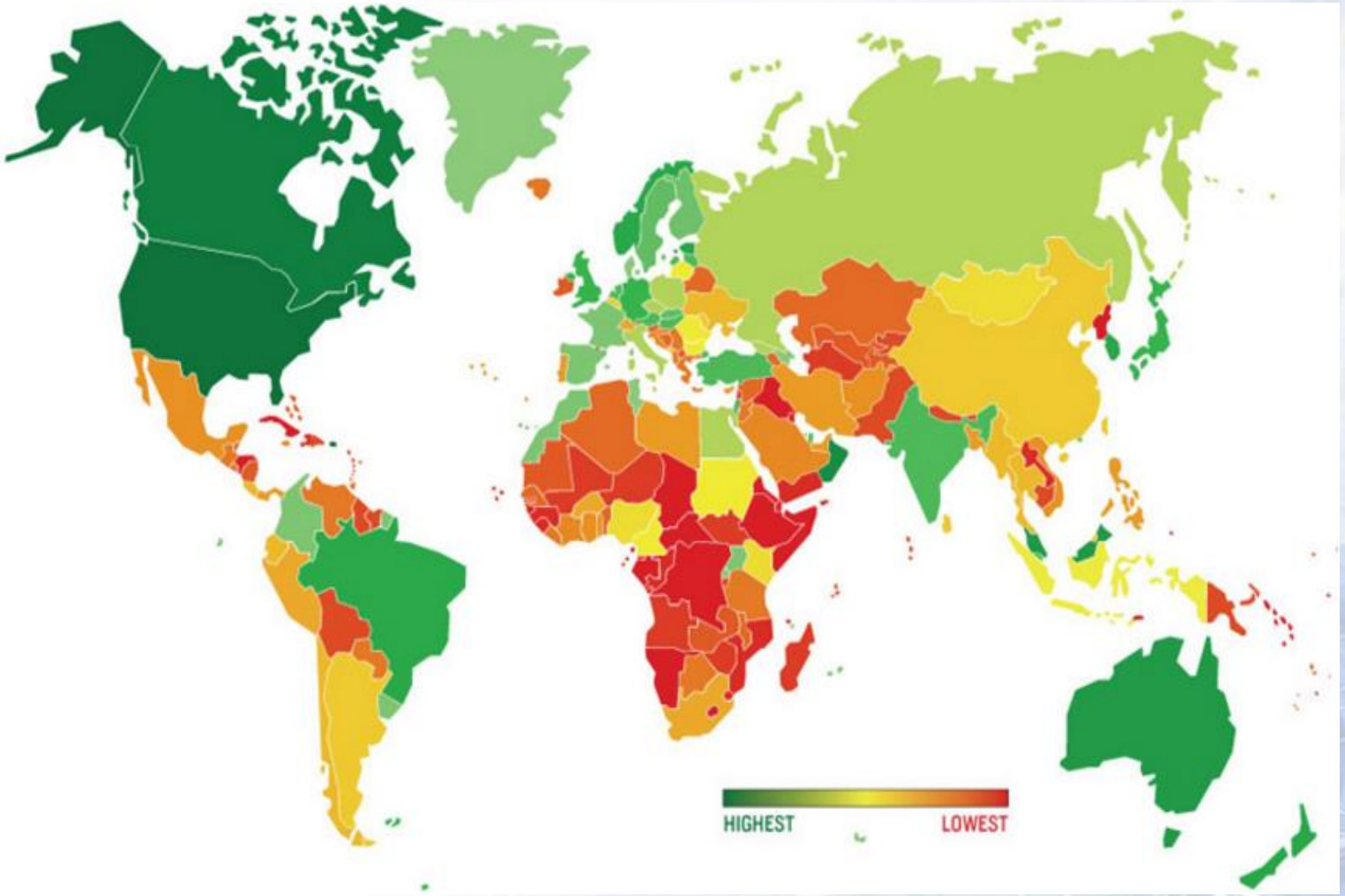
- **Govt and national:**
  - Law enforcement
  - Legal and policy making
  - National database
  - Critical infrastructure
  - Regulation
  - Standards and certification
  - Capacity-building and coordination

Who Is Information Security For ?

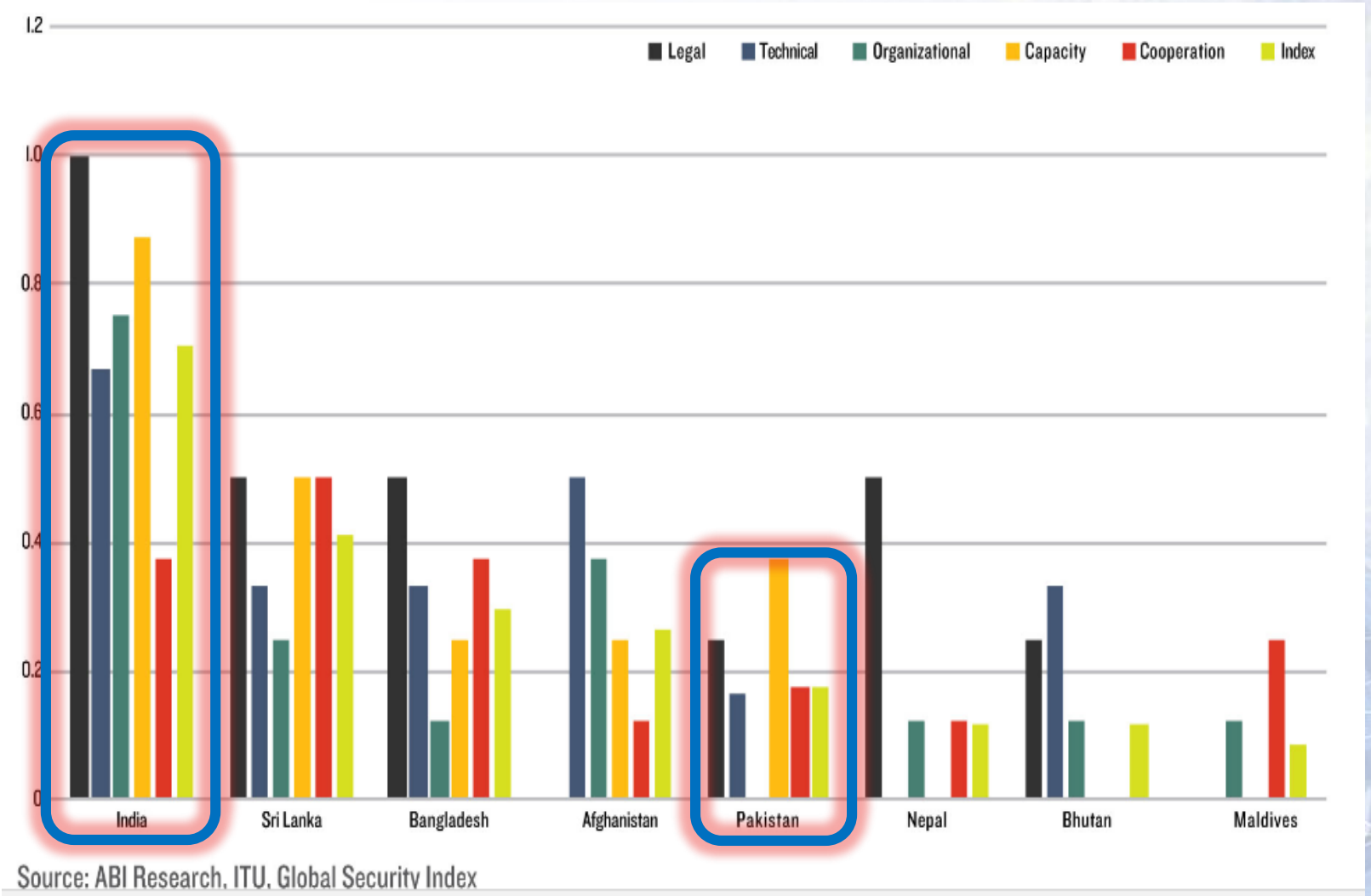


- Legal
- Technical
- Organizational
- Capacity building
- Cooperation

Who Is Information Security For ?



Who Is Information Security For ?



Source: ABI Research, ITU, Global Security Index

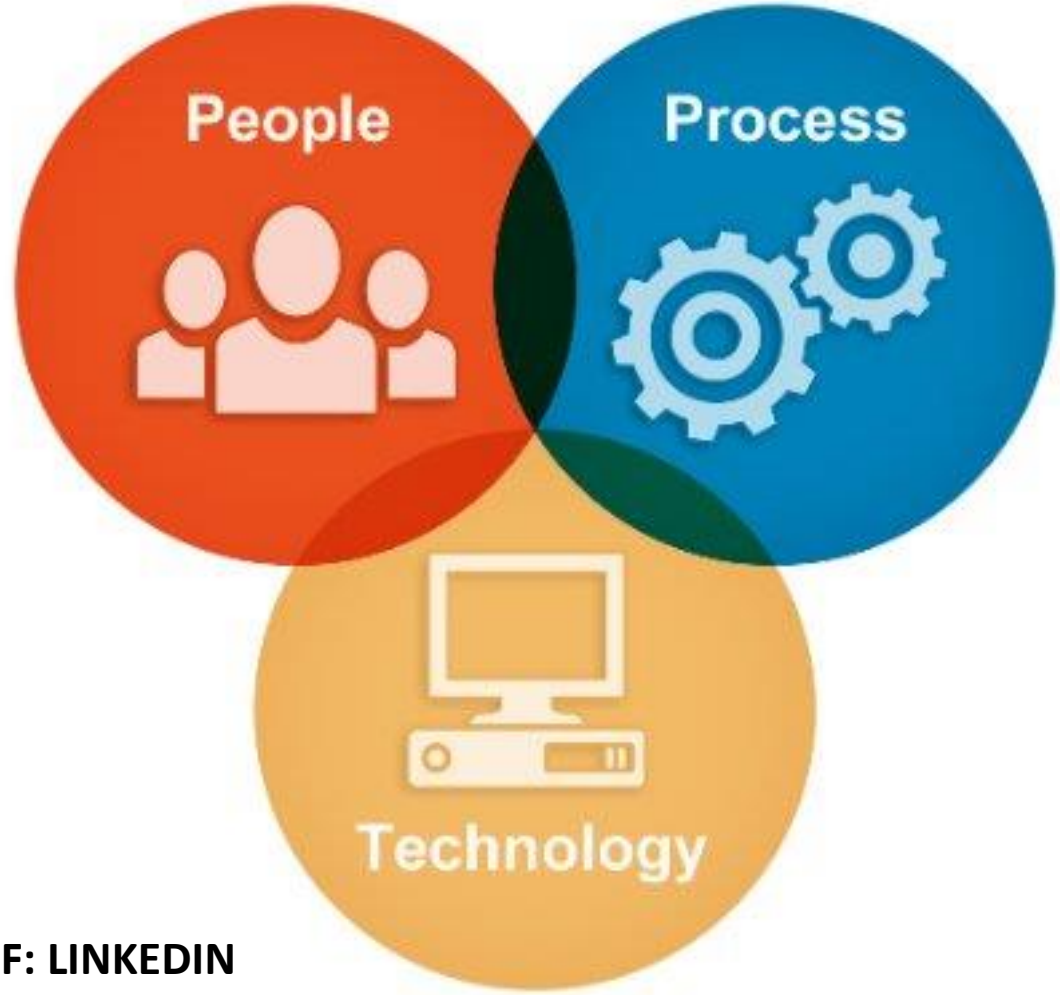
Who Is Information Security For ?

- Pakistan ranked almost at the bottom of the table in International ranking by ITU
- Information security is everyone's responsibility
- Pakistan Cyber Security Association (PCSA) formed to address Pakistan's international ranking

How Is Information Security Implemented ?

- Three pillars of information security:
  - People
  - Process
  - Technology

How Is Information Security Implemented ?



REF: LINKEDIN

How Is Information Security Implemented ?

- **Leadership commitment:**
  - Information security policy and objectives
  - Assigning responsibility and authority
  - Resource allocation
  - Performance reviews
  - Ensuring accountability

How Is Information Security Implemented ?

- **Information Security Manager or CISO:**
  - Heads department responsible for implementing information security program
  - Directs planning, implementation, measurement, review, and continual improvement of program

How Is Information Security Implemented ?

- **IT user:**
  - Understand policies
  - Conduct security/risk assessment
  - Design effective security architecture
  - Develop SOPs and checklists
  - Implement controls
  - Report incidents
  - Conduct effective change management

How Is Information Security Implemented ?

- **Business user:**
  - Security awareness and training
  - Follow information security policy
  - Develop and implement secure business processes
  - Role-based access control and periodic reviews
  - Reporting incidents

How Is Information Security Implemented ?

- **Information security program**
  - Assessing security risks and gaps
  - Implementing security controls
  - Monitoring, measurement, & analysis
  - Management reviews and internal audit
  - Accreditation/testing

Who Are The Players In Information Security ?

- Government
- Industry & sectors
- International organizations
- Professional associations
- Academia and research organizations
- Vendors and suppliers

Who Are The Players In Information Security ?

- **Government:**
  - Policy making
  - Law enforcement
  - Legal system
  - National cyber security strategy and standards
  - International coordination
  - Computer Incident Response Team (CIRT)

Who Are The Players In Information Security ?

- **Industry & sectors:**
  - Financial institutions
  - Telecoms
  - Armed forces
  - Federal and provincial IT boards
  - Enterprises
  - Various other sectors (manufacturing, automotive, health, insurance, etc)

Who Are The Players In Information Security ?

- **International organizations:**
  - APCERT (www.apcert.org)
  - European Union Agency for Network & Information Security - ENISA (www.enisa.org)

Who Are The Players In Information Security ?

- **International organizations:**
  - ITU IMPACT (http://www.impact-alliance.org)

https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf

Who Are The Players In Information Security ?

- **Professional associations:**
  - ISACA (isaca.org)
  - ISC2 (www.isc2.org)
  - OWASP (www.owasp.org)
  - Cloud Security Alliance
  - Pakistan Cyber Security Association (PCSA)

http://cybersecurityventures.com/cybersecurity-associations/

Who Are The Players In Information Security ?

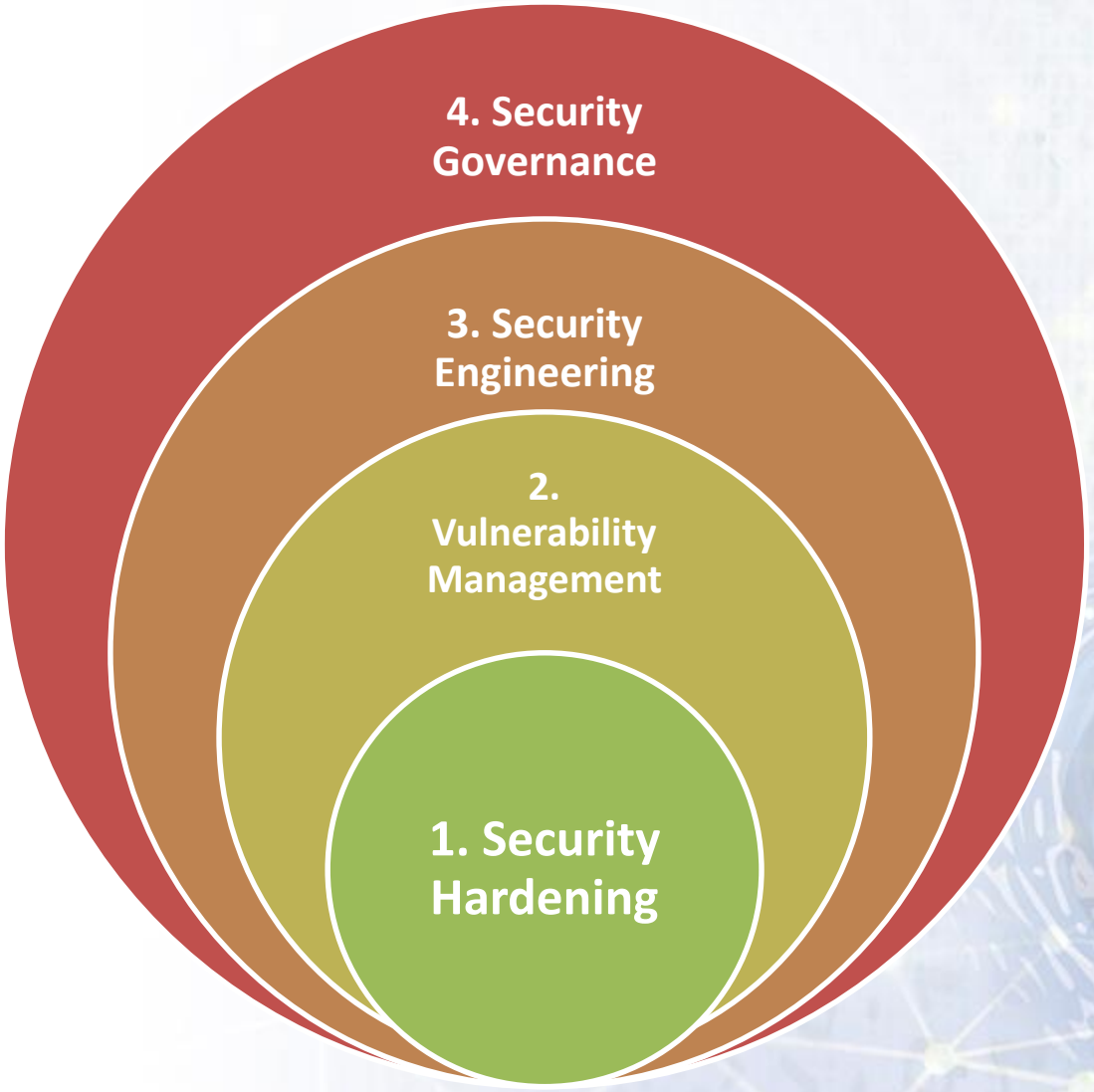
- **Academia & research organizations:**
  - Universities and research programs
  - SANS (www.sans.org)
  - Center for Internet Security (www.cisecurity.org)

http://cybersecurityventures.com/cybersecurity-associations/

Infosec Transformation Framework 4 Layers

1. Security hardening
2. Vulnerability management
3. Security engineering
4. Security governance

Infosec Transformation Framework 4 Layers



Infosec Transformation Framework 4 Layers

- **1: Security hardening:**
  - Compile IT assets
  - Establish minimum security baseline (MSB)
  - Research security controls and benchmarks
  - Pilot (test)
  - Implement controls
  - Monitor and update controls

Infosec Transformation Framework 4 Layers

- **2: Vulnerability management:**
  - Purchase internal tool (NESSUS, Qualys, etc)
  - Conduct vulnerability assessment
  - Prioritize and remediate
  - Report
  - Repeat cycle on quarterly/monthly basis

Infosec Transformation Framework 4 Layers

- **3: Security engineering:**
  - Assess risk profile
  - Research security solutions
  - Design security architecture
  - Implement security controls & solutions
  - Test and validate security posture

Infosec Transformation Framework 4 Layers

- **4: Security governance:**
  - Policies and procedures
  - Risk management
  - Core governance activities (change management, incident management, internal audit)
  - Training & awareness
  - Performance reviews

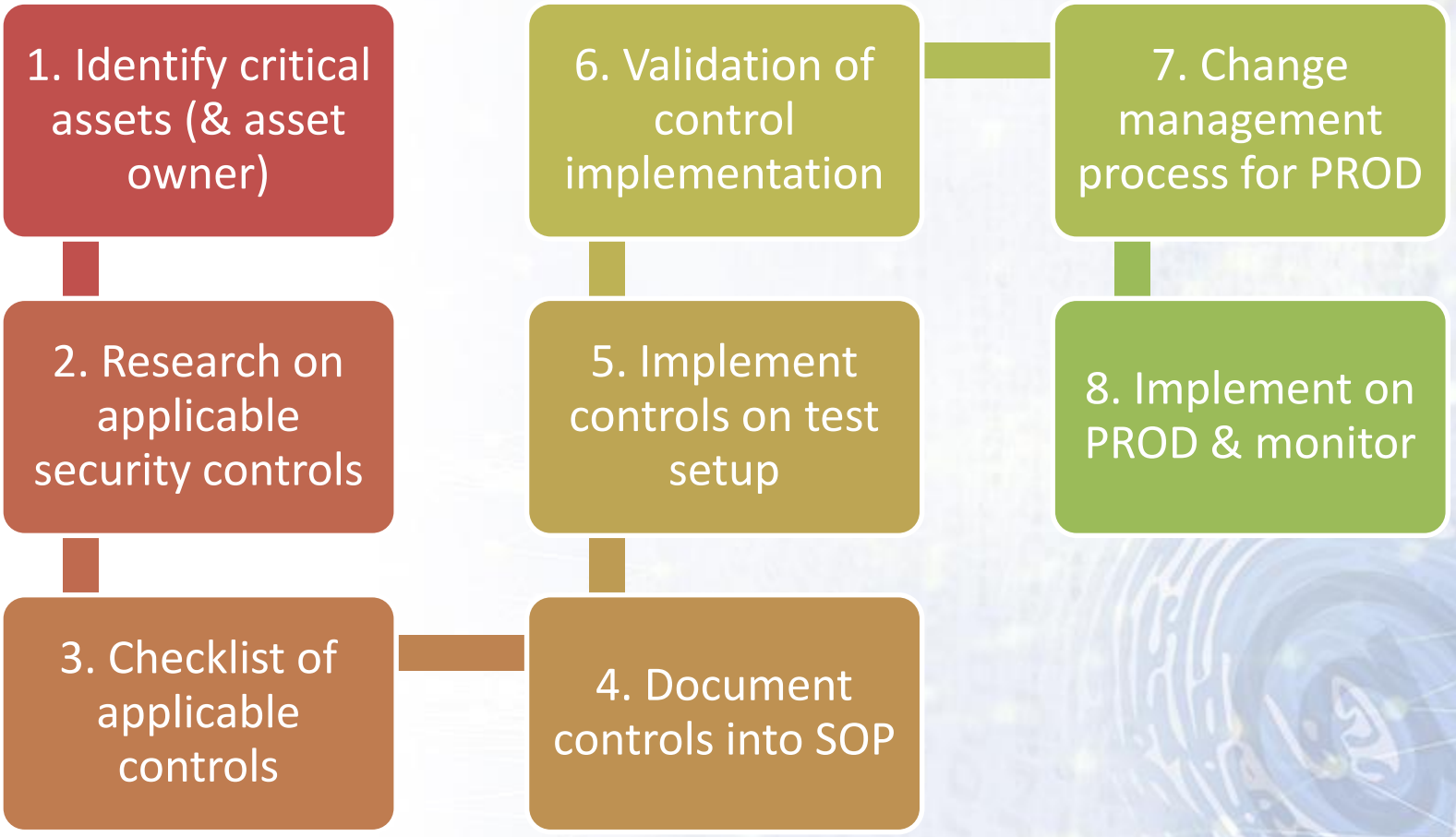
What Is Information Security Hardening ?

- **IT assets** (network, systems, application, databases, mobile, physical security) come with default settings which are not suitable for security
- **Security hardening** is the process of configuring IT assets to maximize security of the IT asset and minimize security risks

What Is Information Security Hardening ?

- **Security in the "trenches:"**
  - Security at the most fundamental operational layer
  - Security where it matters most
  - Usually (but not always) involves junior staff who need extra guidance, training, and scrutiny

What Is Information Security Hardening ?



What Is Information Security Hardening ?

- **Why is security hardening at the first step in the security transformation model ?**
  - Most basic security settings
  - If not adequately addressed here, rest of the security measures hardly matter

What Is Information Security Hardening ?

- **Short example of Cisco router security hardening:**
  - Remote access through SSH and not through telnet
  - Turn of all unused services
  - Session timeout and password retry lockout

http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

What Is Information Security Governance ?

- Information security governance in simpler terms just means effective management of the security program
- Responsibility for governance is associated with the Board and senior management

What Is Information Security Governance ?

- **IT Governance Institute Definition:**
  - "Security governance is the set of responsibilities and practices exercised by the board and executive management, with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

What Is Information Security Governance ?

- **ISO27001:2013 – ISMS (Information Security Management System)** is the world's leading and most widely adopted security governance standard

What Is Information Security Governance ?

- **ISO27001** "provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

What Is Information Security Governance ?

- Ten short clauses and a long Annex with 114 controls in 14 groups
- 27000+ certifications globally in 2015

Difference Between Policy, SOP, & Guideline

- **Policy:**
  - Formal and high level requirement for securing the organization and its IT assets (mandatory)

Difference Between Policy, SOP, & Guideline

- **Policy:**
  - Scope is across organization so should be brief and focusing on desired results
  - Signed off by senior management

Difference Between Policy, SOP, & Guideline

- **Procedure / SOP:**
  - More detailed description of the process; who does what, when, and how
  - Scope is predominantly at a department level having specified audience
  - May be signed off by departmental head

https://www.slu.edu/its/policies

Difference Between Policy, SOP, & Guideline

- **Guideline:**
  - General recommendation or statement of best practice
  - Not mandatory
  - Further elaborates the related SOP

https://www.slu.edu/its/policies

Difference Between Policy, SOP, & Guideline

- **Standard:**
  - Specific and mandatory action or rule
  - Must include one or more specifications for an IT asset or behavior
  - Yardstick to help achieve the policy goals

https://www.slu.edu/its/policies

Difference Between Policy, SOP, & Guideline

- **In practice:**
  - Policy recommended to be a single document applicable at the organizational level (wide audience)
  - Sub-policies may be defined at a departmental level
  - Policies and standards are mandatory

Difference Between Policy, SOP, & Guideline

- **Examples:**
  - Information security policy
  - System administrator password sub-policy
  - User ID & Access Management SOP
  - Vulnerability Management standard
  - Social engineering prevention guideline

Role of People, Process, and Tech In InfoSec

- People, process, and technology are together referred to as the Information Security Triad
- All three aspects help to form a holistic view of Information Security
- All three are important and cannot be overlooked in an Information Security program or activity

Role of People, Process, and Tech In InfoSec

- **People:**
  - People must be trained to effectively & correctly follow policies, information security processes, and implement technology
  - **Social engineering and phishing** are aspects that people must be trained to handle appropriately

Role of People, Process, and Tech In InfoSec

- **Processes** are fundamental to effective information security
  - User access management
  - Backups
  - Incident management
  - Change management
  - Vulnerability management
  - Risk management

Role of People, Process, and Tech In InfoSec

- **Technology** plays a central role in the Information Security program:
  - Firewalls
  - Antivirus
  - Email anti-spam filtering solution
  - Web filtering solution
  - Data loss prevention (DLP) solution

Role Of An Information Security Manager

- The Information Security Manager (Head Of Information Security or CISO) is delegated and authorized by senior management to run the Information Security program and meet its objectives

Role Of An Information Security Manager

- The Information Security Manager develops a policy to regulate the Information Security program which is signed off by senior management
- Assigned resources and authority to plan, assess, implement, monitor, test, and accredit the Information Security activities

Role Of An Information Security Manager

http://www.shortinfosec.net/2009/11/role-of-information-security-manager.html

Role Of An Information Security Manager

- InfoSec Manager Tasks:
  - Develop policy
  - Training & awareness
  - Design security architecture
  - Design security controls
  - Ensure controls are implemented
  - Conduct risk assessment

Role Of An Information Security Manager

- InfoSec Manager Tasks (Contd):
  - Conduct security testing
  - Monitor vulnerability management program
  - Facilitate incident management process
  - Sign-off critical change management activities