Security of Court Electronic Information: Practical Hints

National Workshop for Information & Communication Technology Staff

National Judicial Institute, Abuja, Nigeria

By:
Victor E. Kulugh

Outline

01 ❖Introduction

02 ❖Definition of Key Terms

03 Information Security Goals

04 Achieving InfoSec Goals

05 ❖Roles of parties in Information Security

06 ❖Recommendations

07 ❖End - Q and A

Introduction

- The Internet has significantly improved the life of humans by raising productivity, efficiency and reducing dramatically the cost in time and resources for accomplishing tasks.
- Thus, Electronic Information Systems have become indispensable in our daily endeavours; whether they are social, political, economic etc.
- Electronic information systems thrive on their ability to process, store and transmit data at greater efficiency and reduce cost. Thus data is the oil of now and the future.

Introduction – Cont'd

- However, these systems come with vulnerabilities that are subject to threats and risks, exploitable by different threat actors.
- The motivation of the threats is to illiciately access these data to their gain and lose of the data owners.

Introduction – Motivation for the Training

- The court is a critical government institution in Nigeria (and elsehwhere) that is increasingly depending on ICT infrastructure to deliver services to stakeholders.

- This dependency will increase in the near future due to the Federal government's policy on developing the digital economy through the following frameworks:

•

Introduction – Motivation for the Training

- The NITDA NDPR requires all entities to protectively process the data of Nigerian citizens

- National Digital economy policy and strategy (2020-2030)
- Nigeria e-government interoperability framework and Nigeria e-government roadmap
- Nigeria Digital economy diagnostic report
- Nigerian National Broadband Plan (NNBP 2020-2025)

Introduction – Motivation for the Training

- The courts will increasingly use electronic information resources in their core processes as a result of:
- Admissibility and management of electronic evidence
- The post-pandemic effects will also generally increase ICT usage
- The increased reliance on ICT infrastructure will heighten the information risk that the court will be exposed to

Definitions of Key Terms

- **Data**: This representation of facts, concepts, or instructions in a formalized manner, which should be suitable for communication, interpretation, or processing by human or electronic machine.

- **Information**: is organized or classified data, which has some meaningful values for the receiver. Information is the processed data on which decisions and actions are based.

- **Information Security:** Methods applied to ensure that information infrastructure and resources are not compromised, damaged or abused.

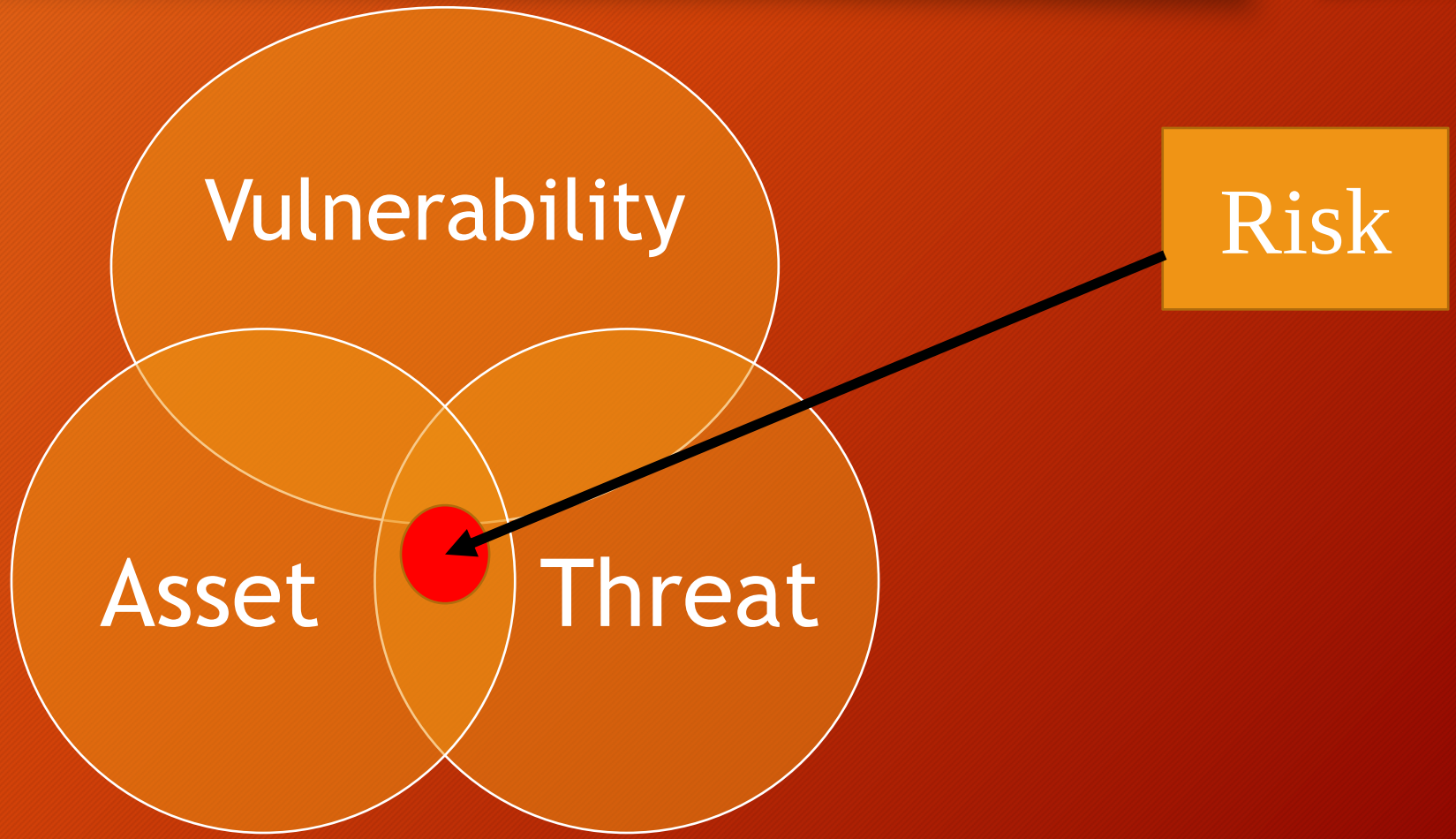
Definitions of Key Terms - Personal Information

- Most individuals and organisations have some form of online presence.
- For your safety on the cyberspace, reveal only what is extremely necessary.
- Note that whatever even you provide can be used to uniquely identify you and link you to your organisation.

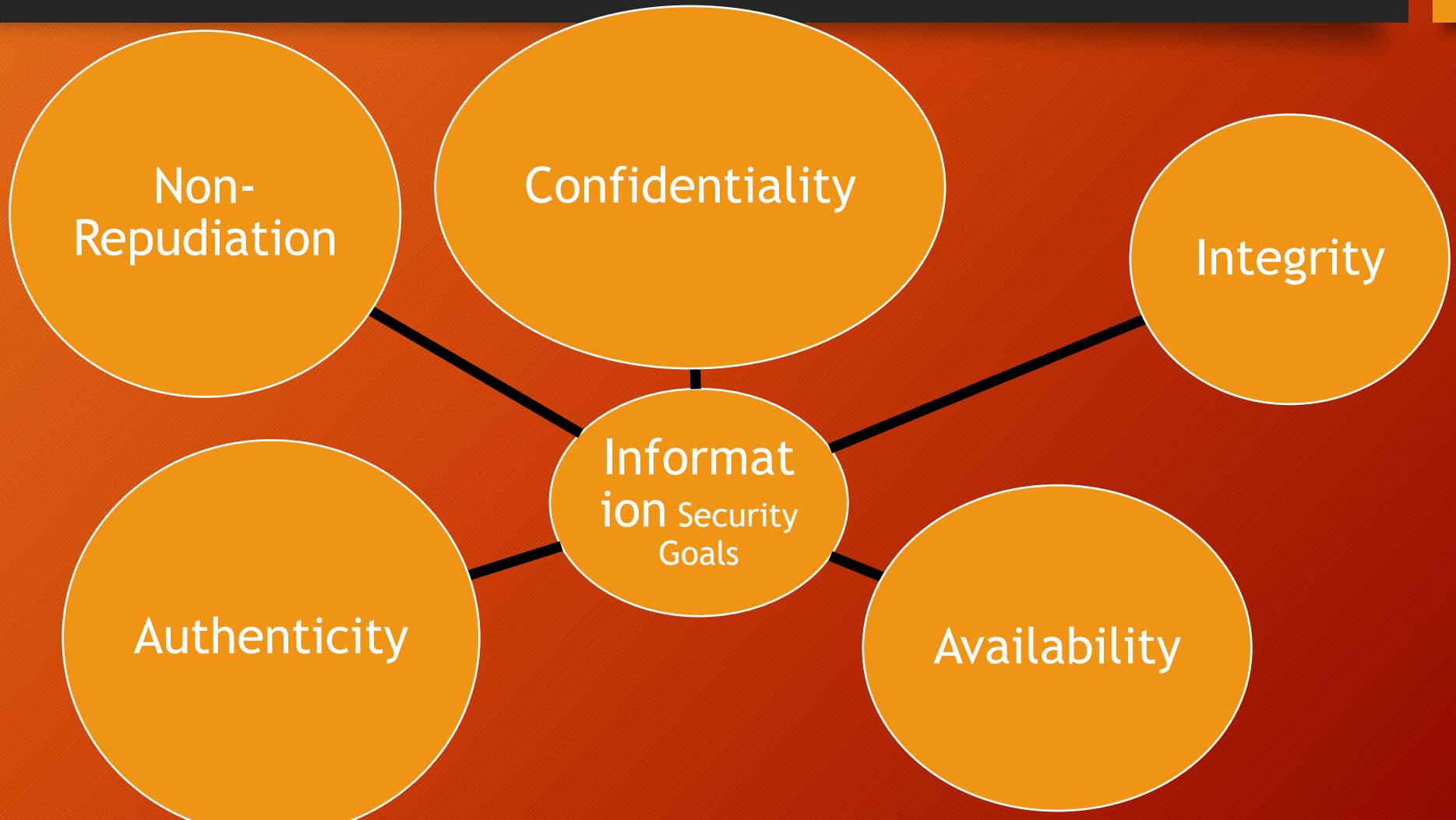
Definitions of Key Terms – Cont'd

- **Vulnerabilities**: Weaknesses, flaws or errors in technology, people or procedures that can be exploited by threat actors to compromise, degrade or abuse information resources.
- **Threats**: Any circumstance or event (Intentional or unintentional) with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- **Risk**: the potential of loss or harm related to technology/cyber infrastructure within an organization

Definitions of Key Terms - Vulnerability, Threats Assets and Risk



Understanding Information Security Goals



Information Security Goals – Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The following measures can be applied:

- Data Classification
- Security of data at rest, on transmission or during processing
- Provide data security policies, standards, frameworks and guidelines
- Education and awareness for data custodians and end-users

Confidentiality Tools

- Encryption
- Access Control
- Authentication
- Authorization
- Physical Security

Information Security Goals – Integrity

The property that data has not been altered in an unauthorized manner or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulations

- Prevent unauthorised users from making modifications to data or programs
- Prevent authorised users from making improper or unauthorised modification
- Maintain internal and external consistency of data and programs

Threats to Integrity

The integrity of data is threatened when the data is exposed to corruption, damage, destruction, or other disruption of its authentic state

Information Security Goals – Availability

Ensuring timely and reliable access to and use of information by authorized users without interference and in all circumstances. Availability can be threatened by:

- Denial of Service (DoS) Attacks from intentional or unintentional sources
- Loss of Information System capabilities maybe because of natural disaster
- Equipment failure

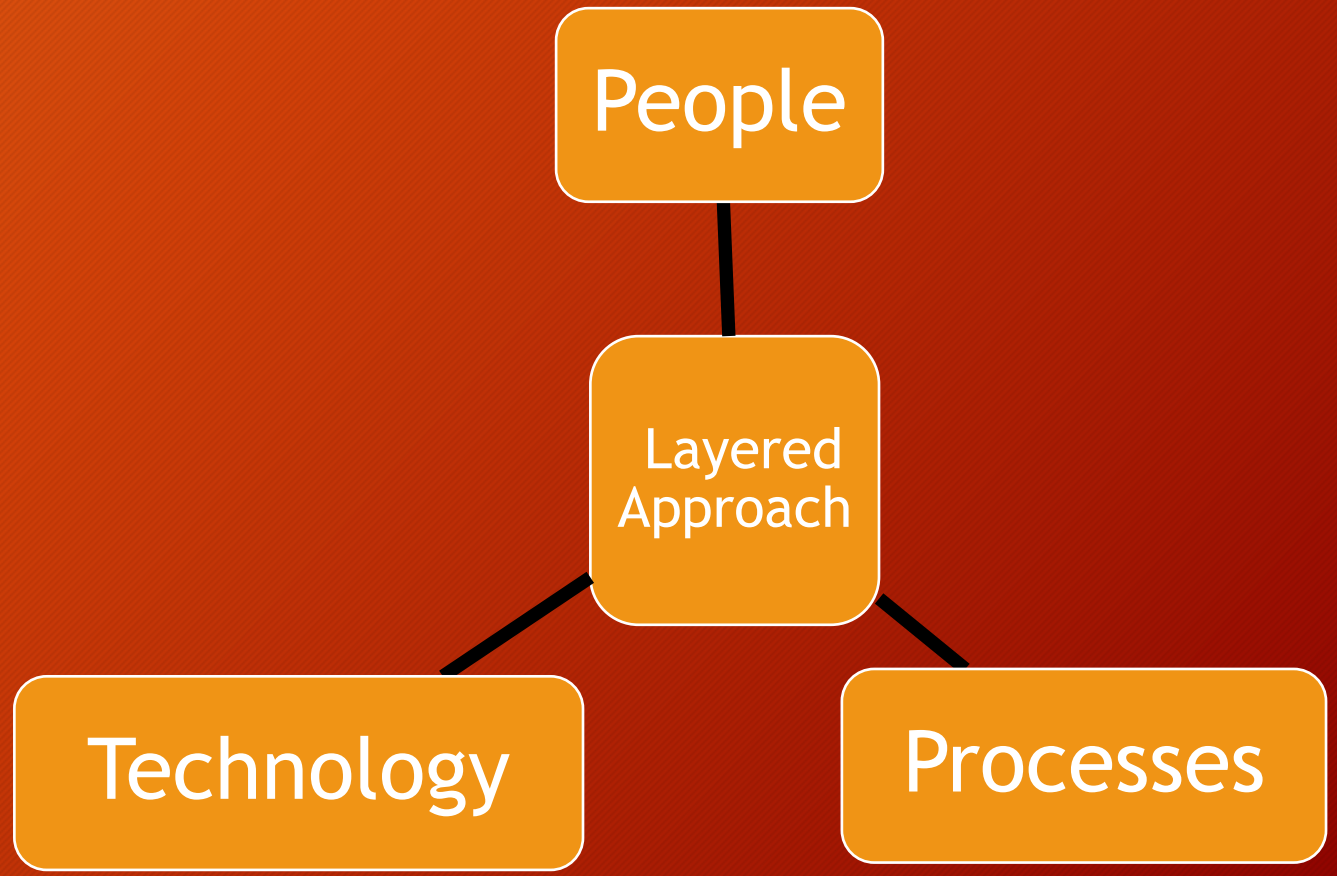
Information Security Goals – Authenticity and Non-Repudiation

Authenticity: The assurance that the information communicated is genuine

Non-Repudiation: The assurance that the sender cannot deny sending a message neither can the receiver deny receiving the message

Layered Approach to Achieving Information Security Goals

There are vulnerabilities at each of these layers that threats can exploit



Layered Approach - People

People: The weakest link on the security chain as a result of human weakness. Thus, they are vulnerable to:

- Social Engineering;
- Good password etiquette
- Patches updates on OS and applications
- Avoid installation of software from unknown or unapproved sources;
- Ensuring that backups are done at the set times;
- Reporting any strange circumstances to the appropriate authorities immediately;

Social Engineering

Social engineering is an attempt by attackers to fool or manipulate humans into giving up access, credential, banking details, or other sensitive information. This is done using sophisticated trickery and emotional manipulation.

Social Engineering - Stages

Reconnaissance - The art of researching on the target to gather information such as organizational structure, roles, behaviours etc. This may be done via organisations' websites, social media profiles and even in-person visits

Planning - using the information they gathered, the attacker selects their mode of attack and designs the strategy and specific messages they will use to exploit the target individuals' weaknesses.

Social Engineering Stages - Cont'd

Execution - the attacker carries out the attack usually by sending messages by email or another online channel. In some forms of social engineering, attackers actively interact with their victims; in others, the kill chain is automated, typically activated by the user clicking on a link to visit a malicious website or execute malicious code

Social Engineering - Techniques

Phishing: An attacker uses a message sent by email, social media, instant messaging clients or SMS to obtain sensitive information from a victim or trick them into clicking a link to a malicious website. Vishing is the voice variant of phishing attacks

Call to action: Eg your bank account/ATM has been blocked, click to access COVID-19 grant

Thrives on targets/victims' emotion and spoofing identities of organisations or colleagues.

Social Engineering – Techniques – Cont'd

Whaling attack: Is a variant of phishing attack that is targeted at individuals with privileged access to systems or to highly valuable sensitive information. Eg senior executives, wealthy individuals, or network administrators.

Others are:

Pretexting, Baiting, Scareware, Diversion theft, Honey trap, Tailgating

Social Engineering - Prevention

Security Awareness Training: Conducting continuous security awareness among staff in the first line of defence against social engineering.

Antivirus and Endpoint Security Tools: Modern endpoint protection tools can:

- ❑Identify and block obvious phishing messages;
- ❑or any message that links to malicious websites;
- ❑IPs listed in threat intelligence databases.

They can also intercept and block malicious processes as they are executed on a user's device.

Social Engineering - Prevention

- **Penetration**: Allowing individuals with ethical hacking skillset to identify and exploit weaknesses in your organisation. This will help you identify personnel and systems you need to focus on

Good Password Etiquette

Passwords are common forms of authentication and must be chosen and managed in a manner protects the user and the organisation

- Do not choose passwords based on personal information that are easy to remember. E.g Date of birth, address, phone numbers, names of children or spouse.
- Avoid using dictionary words as password
- Ensure to change default passwords to your personalised ones

Good Password Etiquette – Steps

- Step 1: words that relate to a memory that is unique to you. e.g. mybirthdayisnexttomorrow
- Step 2: Use uppercase and lowercase letters MybirthdayisNEXTtomorroW
- Step 3: Replace some letters with numbers and symbols to make it even harder to crack. e.g. Myb1rthd@y1sN3XT2m0rr0W
- Step 4: Add special characters and numbers at the end e.g. Myb1rthd@y1sN3XT2m0rr0W@11

Other aspects of people approach.

- Patches updates on OS and applications: Must be updated as soon as they are released.
- Avoid installation of software from unknown or unapproved sources – Ensure softwares sources are known and approved before installation
- Ensuring that backups are done at the set times: Organisations must define back-up policies that must be adhered to (Daily, weekly etc)

Layered Approach - Processes

- **Processes**: This layer ensures that documented strategies are in place that address the security of electronic information

  - Information assets identification, classification and prioritisation (identify most critical information assets)
  - Define responsibilities, functions and relationships between functions
  - Relationship between the various functions and the ICT department

Layered Approach – Processes – Cont'd

- Define Access control – (virtual and physical) access control policy
- Principle of least privilege (On a need-to-know bases
- Define, design and document Incident response plans
- Define and design Back-up policy and how regular the back-up should be tested

Layered Approach – Processes – Cont'd

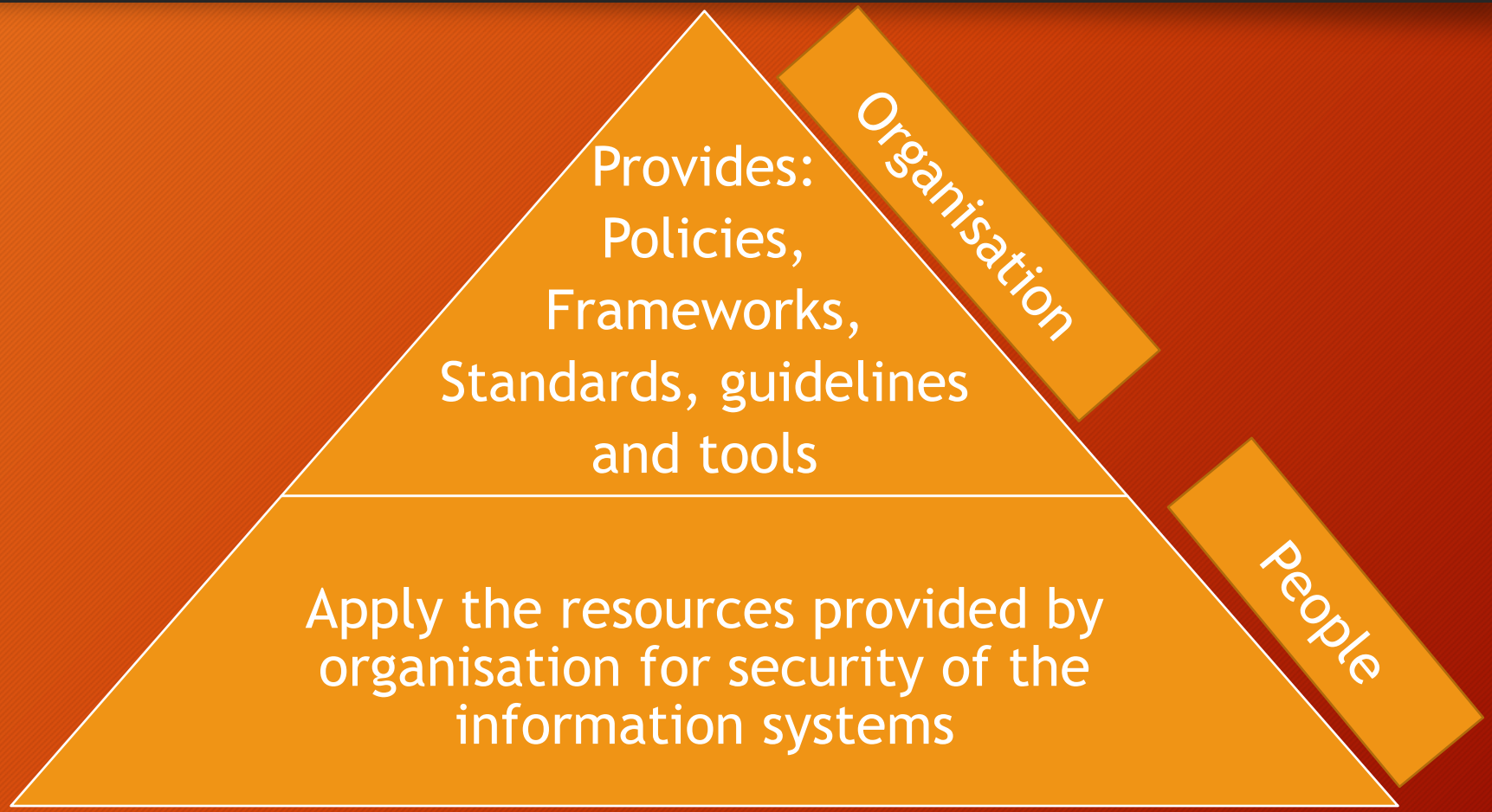
- Malware Management policy
- Update and patches policy and guidelines
- Password policy
- Define sanction grids in failure to follow strategies/policies

Layered Approach -Technology – Security Landscape

- Network Security
- Application Security
- End-point Security
- Data Security
- Identity Management
- Mobile Security
- Cloud Security
- Disaster Management & BCP

Technology – Securing the Technology layer

Roles in the security of electronic information



Recommendations

- Ensure the establishment of Information Security Department in the court to build the kind of capacity that is required for the future
- Develop policy frameworks, adopt and tailor information security standards, frameworks and guidelines
- Create a balanced availability of people, processes and technology

Recommendations – Cont'd

- Regularly engage personnel in information security training and awareness programmes to address SE concerns.
- Responsibility must be taken at every level (Organisation or individual)
- Depending on the sensitivity of information, add supplementary authentication methods. E.g Multi-Factor Authentication and biometric.

Recommendations – Cont'd

- Regularly test your incident response plan
- Conduct regular penetration testing
- Test your back-ups regularly to ensure they are in place
- Be strict with negligent users who expose the organisation's information resources to avoidable risk.

End

Thank You