SYSTEMS SECURITY
KASNEB CICT PAPER NO 16

PAPER NO.16 SYSTEMS SECURITY

GENERAL OBJECTIVE

This paper is intended to equip the candidate with the knowledge, skills and attitude that will enable him/her to secure lCT systems in an organization

16.0 LEARNING OUTCOMES

A candidate who passes this paper should be able to:
• Identify types of threats to ICT systems
• Adopt different security mechanisms
• Prepare business continuity planning (BCP) strategies
• Develop and implement a systems security policy
• Undertake basic computer forensic audits
• Demonstrate social-ethical and professional values in computing.

CONTENT

16.1 Introduction to systems security
- Overview of systems security
- Goals of system security
- Security core concepts
- Security mechanisms

16.2 Security threats and controls
- Sources of threats
- Types of threats
- Crimes against lCT and computer criminals
- Controlling security threats
- Ethical hacking

16.3 Systems security
- Classification
- People errors
- Procedural errors
- Software errors
- Electromechanical problems
- Dirty data

16.4 Physical and logical security
- Physical security
- Logical security(authentication, access rights. Others)

16.5 Data/software security

- Use of the normal security systems
- Vulnerability assessment
- Employing virus security precautions
- Employing Internet security precautions
- Vetting of ICT employees

16.6 Transmission security

- Symmetric encryption
- Asymmetric encryption
- Duplicate and alternate routing
- Firewall types and configuration
- Secure socket layer and transport layer security
- IPv4 and 1Pv6 security
- Wireless network security
- Mobile device security
- Wireless protected access

16.7 ICT risk management

- Risk management concepts
- Risk analysis
- Risk assessment framework
- Countermeasures
- Corporate risk document

16.8 Business continuity planning (BCP)

- BCP scope, teams and roles
- Backup types and strategies
- Hot and cold sites
- Disaster recovery plans

16.9 System security policy implementation

- Components of systems security policy
- Systems security policy development
- System security policy implementation
- Systems security strategies
- Audit

16.10 Introduction to computer forensics

- Computer forensics concepts
- Incidence handling

- Investigating desktop incidents
- Investigating network incidents
- Securing and preserving evidence

16.11 Professional values and ethics in computing

- Intellectual property and fraud
- Information systems ethical and social concerns
- Telecommuting and ethical issues of the worker
- Codes of ethics for IT professionals
- Professional ethics and values on the web and Internet
- Objectivity and integrity in computing
- The role of professional Societies in enforcing professional standards in Computing

16.12 **Emerging Issues and trends**

Topic 1

16.1 Introduction to systems security

- ***Overview of systems security***

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Overview

IT security

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

The act of ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

Threats

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an

organization's website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. Hence a key concern for organizations today is to derive the optimal information security investment. The renowned Gordon-Loeb Model actually provides a powerful mathematical economic approach for addressing this critical concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics.

Definitions

Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry

standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

The definitions of InfoSec suggested in different sources are summarized below (adopted from).

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)

3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)

4. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)

5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)

6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)

7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)

8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization’s perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: *confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.*" (Cherdantseva and Hilton, 2013)

Profession

Information security is a stable and growing profession. Information security professionals are very stable in their employment; more than 80 percent had no change in employer or employment in the past year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2015.

- ***Goals of system security***

The real basic goals of information security are

3. Confidentiality
4. Integrity
5. Availability
6. Non-repudiation. Accomplishing these is a management issue before it's a technical one, as they are essentially business objectives.

Confidentiality is about controlling access to files either in storage or in transit. This requires systems configuration or products (a technical job). But the critical definition of the parameters (who should be able to access what) is a business-related process.

Ensuring integrity is a matter of version control - making sure only the right people can change documents. It also requires an audit trail of the changes, and a fallback position in case changes prove detrimental. This meshes with non-repudiation (the change record must include who as well as what and when).

Availability is the Cinderella of information security as it is rarely discussed. But however safe from hackers your information is, it is no use if you can't get at it when you need to. So you need to think about data back-ups, bandwidth and standby facilities, which many people still leave out of their security planning.

- ***Security core concept***

Key concepts

The CIA triad of **confidentiality**, **integrity**, and **availability** is at the heart of information security. (The members of the classic InfoSec triad — confidentiality, integrity and availability are interchangeably referred to in the literature as **security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.**) There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition. It has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts.

Security of Information Systems and Networks proposed the nine generally accepted principles: **Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment**. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.

In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy. The completeness and accuracy of the IAS-octave was evaluated via a series of interviews with IAS academics and experts. The IAS-octave is one of the dimensions of a Reference Model of Information Assurance and Security (RMIAS), which summarizes the IAS knowledge in one all-encompassing model.

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes"

Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Note: This is also regarded as part of Integrity.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

The 6 Security Core Concepts

1. **Risk Assessment (RA) & Business Impact Analysis (BIA)** – If you can't (in some form) qualify/quantify your business risks related to your sensitive data, and then determine an estimated cost-of-loss related to data theft or unavailability, how will you know how much to spend on security? Put simply; if the cost of security outweighs the value of the data, don't do it (this includes compliance). This does NOT mean you should do nothing at all, it just means you need to re-evaluate how you perform some of your business functions. The first question is not "How do I protect it? "It's "Do I need it?"
2. **Security Control Selection & Implementation** – The RA, done correctly, will show you where you can make improvements in your security posture. This does not necessarily involve capital expenditure – which should always be the LAST resort – it can be something as simple as destroying every instance of redundant data. Regardless, at some point you will probably purchase technology, but even here you should be careful – now I have to write another blog – and ensure that this new technology meets all of the business needs defined in the RA.
3. **Security Management Systems** – There's not much point putting security controls in place if you don't manage them properly to *keep* them in place. This is where standards like ISO 2700X come into play. This is the day-to-day procedures used to maintain the operational aspect of your security infrastructure. Obviously this will vary dramatically by organisation; from a simple check-list for your corner sandwich shop, to a full time job for larger more complex organisations. The trick is doing only what's appropriate, without going overboard.
4. **Governance & Change Control** – Ask 100 people what Governance is, and you'll get 105 different answers. I believe governance provides a function that trumps all others; it allows the business side of an organisation to talk to the IT side in the ***same*** language. Business: "I want this new functionality. "IT: "Sure, but do it this way." is the perfect conversation. IT, and especially IT security, are typically seen as roadblocks, but this is just a symptom of immature Governance processes. As for change control, that's just common sense. If things don't change, the only increase in security risk is from external sources. The threat landscape changes almost daily, why make things worse by screwing up internally as well?
5. **Incident Response (IR) & Disaster Recovery (DR)** – Fairly self-explanatory; what's the point of being in business if you don't intend *staying* in business? For example; if you are an e-

commerce company, you should know from the RA what your maximum downtime is, and both your security controls and IR & DR processes need to fit according.

6. **Business Continuity Management (BCM) & Business As Usual (BAU)** – You may ask why this is broken out from IR & DR. This because BCP and BAU are more related to the business side of the table, and IR & DR are on the IT side. IT never leads, IT enables, it's the business side that needs to lay down the plans for staying in business, as well as how to do so efficiently, and cost effectively.

It's a bold statement, but if you follow these core concepts, it won't matter the compliance regime, the data type, of even the type / location your business is in, you'll be covered …mostly.

Yes, this is a lot of work, and the up-front costs in both capital and resource terms can be significant, but it's a damned sight cheaper than the cost of non-compliance, fines, and particularly; being breached. In the extreme, what if it's the difference between you being in business or not?

- ***Security mechanisms***

We use several layers of proven security technologies and processes to provide you with secure online access to your accounts and information. These are continuously evaluated and updated by experts to ensure that we protect you and your information. These include:

- Secure Socket Layer (SSL) Encryption
- Authentication
- Firewalls
- Computer Anti-Virus Protection
- Data Integrity
- Ensuring Your Online Safety

Secure Socket Layer (SSL) Encryption

When you successfully login to Online Banking or another secure website using an authentic user ID and password, servers will establish a secure socket layer (SSL) connection with your computer. This allows you to communicate privately and prevents other computers from seeing anything that you are transacting – so you can conduct online business safely. SSL provides 128-bit encrypted security so that sensitive information sent over the Internet during online transactions remains confidential.

Authentication

To protect our users, we provide secure private websites for any business that users conduct with us. Users login to these sites using a valid client number or username and a password.

Users are required to create their own passwords, which should be kept strictly confidential so that no one else can login to their accounts.

Firewalls

We use a multi-layered infrastructure of firewalls to block unauthorized access by individuals or networks to our information servers.

Computer Anti-Virus Protection

We are continuously updating our anti-virus protection. This ensures we maintain the latest in anti-virus software to detect and prevent viruses from entering our computer network systems.

Data Integrity

The information you send to one of our secure private websites is automatically verified to ensure it is not altered during information transfers. Our systems detect if data was added or deleted after you send information. If any tampering has occurred, the connection is dropped and the invalid information transfer is not processed.

Ensuring Your Online Safety

Find out how these security mechanisms safeguard your communication.

TOPIC 2

16.2 Security threats and controls

Threats classification

Threats can be classified according to their type and origin:

- Type of threat
  - Physical damage
    - fire
    - water
    - pollution
  - natural events
    - climatic
    - seismic
    - volcanic
  - loss of essential services
    - electrical power
    - air conditioning
    - telecommunication
  - compromise of information
    - eavesdropping,
    - theft of media
    - retrieval of discarded materials
  - technical failures

        - equipment
        - software
        - capacity saturation
    - compromise of functions
        - error in use
        - abuse of rights
        - denial of actions
- Origin of threats
    - Deliberate: aiming at information asset
        - spying
        - illegal processing of data
    - accidental
        - equipment failure
        - software failure
    - environmental
        - natural event
        - loss of power supply
    - Negligence: Known but neglected factors, compromising the network safety and sustainability.

Note that a threat type can have multiple origins.

Threat model

People can be interested in studying all possible threats that can:

- affect an asset,
- affect a software system
- are brought by a threat agent

Threat classification

Microsoft has proposed a threat classification called STRIDE, from the initials of threat categories:

- **S**poofing of user identity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure (privacy breach or Data leak)
- **D**enial of Service (D.o.S.)
- **E**levation of privilege

Microsoft used to risk rating security threats using five categories in a classification called DREAD: Risk assessment model. The model is considered obsolete by Microsoft. The categories were:

- **D**amage – how bad would an attack be?
- **R**eproducibility – how easy it is to reproduce the attack?
- **E**xploitability – how much work is it to launch the attack?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy it is to discover the threat?

The DREAD name comes from the initials of the five categories listed.

Associated terms

Threat agents or actors

Threat agents
Individuals within a threat population; practically anyone and anything can, under the right circumstances, be a threat agent – the well-intentioned, but inept, computer operator who trashes a daily batch job by typing the wrong command, the regulator performing an audit, or the squirrel that chews through a data cable.

Threat agents can take one or more of the following actions against an asset

- Access – simple unauthorized access
- Misuse – unauthorized use of assets (e.g., identity theft, setting up a porn distribution service on a compromised server, etc.)
- Disclose – the threat agent illicitly discloses sensitive information
- Modify – unauthorized changes to an asset
- Deny access – includes destruction, theft of a non-data asset, etc.

It's important to recognize that each of these actions affects different assets differently, which drives the degree and nature of loss. For example, the potential for productivity loss resulting from a destroyed or stolen asset depends upon how critical that asset is to the organization's productivity. If a critical asset is simply illicitly accessed, there is no direct productivity loss. Similarly, the destruction of a highly sensitive asset that doesn't play a critical role in productivity won't directly result in a significant productivity loss. Yet that same asset, if disclosed, can result in significant loss of competitive advantage or reputation, and generate legal costs. The point is that it's the combination of the asset and type of action against the asset that determines the fundamental nature and degree of loss. Which action(s) a threat agent takes will be driven primarily by that agent's motive (e.g., financial gain, revenge, recreation, etc.) and the nature of the asset. For example, a threat agent bent on financial gain is less likely to destroy a critical server than they are to steal an easily pawned asset like a laptop.

It is important to separate the concept of the event that a threat agent get in contact with the asset (even virtually, i.e. through the network) and the event that a threat agent act against the asset.

The term *Threat Agent* is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company.

Threat Agent = Capabilities + Intentions + Past Activities

These individuals and groups can be classified as follows:

- Non-Target Specific: Non-Target Specific Threat Agents are computer viruses, worms, Trojans and logic bombs.
- Employees: Staff, contractors, operational/maintenance personnel, or security guards who are annoyed with the company.
- Organized Crime and Criminals: Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- Corporations: Corporations are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- Human, Unintentional: Accidents, carelessness.
- Human, Intentional: Insider, outsider.
- Natural: Flood, fire, lightning, meteor, earthquakes.

- ***Sources of threats***

A threat sources are those who wish a compromise to occur. It is a term used to distinguish them from threat agents/actors who are those who actually carry out the attack and who may be commissioned or persuaded by the threat actor to knowingly or unknowingly carry out the attack.

Threat communities

The following threat communities are examples of the human malicious threat landscape many organizations face:

- Internal
  - Employees
  - Contractors (and vendors)
  - Partners
- External

- Cyber-criminals (professional hackers)
- Spies
- Non-professional hackers
- Activists
- Nation-state intelligence services (e.g., counterparts to the CIA, etc.)
- Malware (virus/worm/etc.) authors

Threat action

Threat action is an assault on system security.
Complete security architecture deals with both intentional acts (i.e. attacks) and accidental events. Various kinds of threat actions are defined as subentries under "threat consequence".

Threat analysis

Threat analysis is the analysis of the probability of occurrences and consequences of damaging actions to a system. It is the basis of risk analysis.

Threat consequence is a security violation that results from a threat action. It includes disclosure, deception, disruption, and usurpation. The following subentries describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

1 **Unauthorized disclosure** (a threat consequence)
A circumstance or event whereby an entity gains access to data for which the entity is not authorized. (See: data confidentiality.). The following threat actions can cause unauthorized disclosure:
Exposure: A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:
Deliberate Exposure: Intentional release of sensitive data to an unauthorized entity.
Scavenging: Searching through data residue in a system to gain unauthorized knowledge of sensitive data.
* Human error
Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data
* Hardware/software error
System failure that results in an entity gaining unauthorized knowledge of sensitive data
Interception: A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations. This includes:
Theft: Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
Wiretapping (passive): Monitoring and recording data that is flowing between two points in a communication system (See: wiretapping.)
Emanations analysis

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: Emanation.)
Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. This includes:
Traffic analysis: Gaining knowledge of data by observing the characteristics of communications that carry the data.
Signals analysis: Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: Emanation.)
Intrusion: A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. This includes:
Trespass: Gaining unauthorized physical access to sensitive data by circumventing a system's protections.
Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
Reverse engineering: Acquiring sensitive data by disassembling and analyzing the design of a system component
Cryptanalysis: Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes.

2 Deception (a threat consequence)

A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. The following threat actions can cause deception:
Masquerade
A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity
Spoof: Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
Malicious logic
In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) 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.
Falsification
A threat action whereby false data deceives an authorized entity.(See: active wiretapping.)
Substitution
Altering or replacing valid data with false data that serves to deceive an authorized entity.
Insertion
Introducing false data that serves to deceive an authorized entity
Repudiation
A threat action whereby an entity deceives another by falsely denying responsibility for an act
False denial of origin
Action whereby the originator of data denies responsibility for its generation

False denial of receipt
Action whereby the recipient of data denies receiving and possessing the data

3 Disruption (a threat consequence)

A circumstance or event that interrupts or prevents the correct operation of system services and functions (See: denial of service.) The following threat actions can cause disruption:
Incapacitation
A threat action that prevents or interrupts system operation by disabling a system component
Malicious logic
In context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources.
Physical destruction
Deliberate destruction of a system component to interrupt or prevent system operation
* Human error
Action or inaction that unintentionally disables a system component
* Hardware or software error
Error that causes failure of a system component and leads to disruption of system operation
* Natural disaster
Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component
Corruption
A threat action that undesirably alters system operation by adversely modifying system functions or data
Tamper
In context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.
Malicious logic
In context of corruption, any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data.
* Human error
Human action or inaction that unintentionally results in the alteration of system functions or data
* Hardware or software error
Error that results in the alteration of system functions or data
* Natural disaster
Any "act of God" (e.g., power surge caused by lightning) that alters system functions or data
Obstruction
A threat action that interrupts delivery of system services by hindering system operations.
Interference
Disruption of system operations by blocking communications or user data or control information
Overload
Hindrance of system operation by placing excess burden on the performance capabilities of a system component (See: flooding.)

4 Usurpation (a threat consequence)

A circumstance or event that results in control of system services or functions by an unauthorized entity. The following threat actions can cause usurpation:

Misappropriation

A threat action whereby an entity assumes unauthorized logical or physical control of a system resource

Theft of service

Unauthorized use of service by an entity

Theft of functionality

Unauthorized acquisition of actual hardware, software, or firmware of a system component

Theft of data

Unauthorized acquisition and use of data

Misuse

A threat action that causes a system component to perform a function or service that is detrimental to system security.

Tamper

In context of misuse, deliberate alteration of a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

Violation of permissions

Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.

- ***Types of threats***

External

- Strategic: like competition and customer demand...
- Operational: Regulation, suppliers, contracts
- Financial: FX, credit
- Hazard: Natural disaster, cyber, external criminal act
- Compliance: new regulatory or legal requirements are introduced, or existing ones are changed, exposing the organisation to a non-compliance risk if measures are not taken to ensure compliance

Internal

- Strategic: R&D
- Operational: Systems and process (H&R, Payroll)
- Financial: Liquidity, cash flow
- Hazard: Safety and security; employees and equipment
- Compliance: Actual or potential changes in the organization’s systems, processes, suppliers, etc. may create exposure to a legal or regulatory non-compliance.

- ***Crimes against ICT and computer criminals***

Most cybercrimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "professional" criminals find new ways to commit old crimes, treating cybercrime like a business and forming global criminal communities.

Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.

It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber-attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country.

Attack Techniques

Here are a few types of attacks cyber criminals use to commit crimes. You may recognize a few of them:

- Botnet - a network of software robots, or bots, that automatically spread malware
- **Fast Flux** - moving data quickly among the computers in a botnet to make it difficult to trace the source of malware or phishing websites
- Zombie Computer - a computer that has been hacked into and is used to launch malicious attacks or to become part of a botnet
- **Social Engineering** - using lies and manipulation to trick people into revealing their personal information. Phishing is a form of social engineering
- Denial-of-Service attacks - flooding a network or server with traffic in order to make it unavailable to its users
- **Skimmers** - Devices that steal credit card information when the card is swiped through them. This can happen in stores or restaurants when the card is out of the owner's view, and frequently the credit card information is then sold online through a criminal community.

Some identity thieves target organizations that store people's personal information, like schools or credit card companies. But most cyber criminals will target home computers rather than trying to break into a big institution's network because it's much easier.

By taking measures to secure your own computer and protect your personal information, you are not only preventing cyber criminals from stealing your identity, but also protecting others by preventing your computer from becoming part of a botnet.

Social Engineering

Social engineering is a tactic used by cyber criminals that uses lies and manipulation to trick people into revealing their personal information. Social engineering attacks frequently involve very convincing fake stories to lure victims into their trap. Common social engineering attacks include:

- Sending victims an email that claims there's a problem with their account and has a link to a fake website. Entering their account information into the site sends it straight to the cyber-criminal (phishing)
- Trying to convince victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software)
- Pretending to be a network or account administrator and asking for the victim's password to perform maintenance
- Claiming that the victim has won a prize but must give their credit card information in order to receive it
- Asking for a victim's password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password
- Promising the victim they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information

Like other hacking techniques, social engineering is illegal in the United States and other countries. To protect yourself from social engineering, don't trust any emails or messages you receive that request any sort of personal information. Most companies will never ask you for personal information through email. Let a trusted adult know when you receive an email or message that might be a social engineering attack, and don't believe everything you read.

Reformed Criminals: Grey Hat Hackers

For a hacker who wants to come clean and turn away from crime, one option is to work for the people they used to torment, by becoming a security consultant. These hackers-turned-good-guys are called Grey Hat Hackers.

In the past, they were Black Hat Hackers, who used their computer expertise to break into systems and steal information illegally, but now they are acting as White Hat Hackers, who specialize in testing the security of their clients' information systems. For a fee, they will attempt to hack into a company's network and then present the company with a report detailing the existing security holes and how those holes can be fixed.

The advantage of this is that they can use their skills for a good cause and help stop other cyber criminals. Keeping up with security and cyber criminals is a full-time job, and many companies can't afford to have someone completely dedicated to it. Grey Hat Hackers have real-world hacking experience and know more methods of infiltrating networks than most computer

security professionals. However, since they used to be criminals there's always going to be a question of trust.

- ***Controlling security threats***

Controls

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally they are ways of protecting the confidentiality, integrity or availability of information.

1. Administrative

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

2. Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the **principle of least privilege**. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The

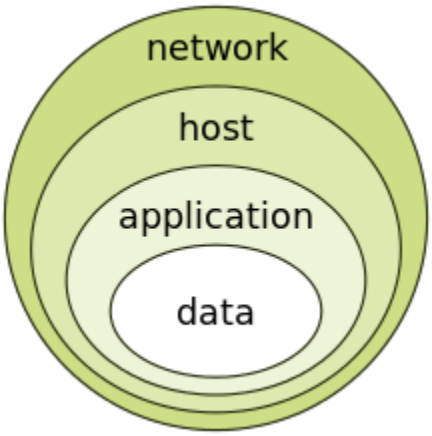
access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

3. Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.

An important physical control that is frequently overlooked is the **separation of duties**. Separation of duties ensures that an individual cannot complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated from one another.

Defense in depth



The onion model of defense in depth

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in-depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

Security classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, and Confidential**.
- In the government sector, labels such as: **Unclassified**, **Unofficial**, **Protected**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
- In cross-sectorial formations, the Traffic Light Protocol, that consists of: **White, Green, Amber**, and **Red**.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the

information and to ensure the security controls required by the classification are in place and are followed in their right procedures.

Access control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Access control is generally considered in three steps: Identification, Authentication, and Authorization.

Identification

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to".

Authentication

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe—a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that they are the person the username belongs to.

There are three different types of information that can be used for authentication:

- Something you know: things such as a PIN, a password, or your mother's maiden name.
- Something you have: a driver's license or a magnetic swipe card.
- Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans.

Strong authentication requires providing more than one type of authentication information (two-factor authentication). The username is the most common form of identification on

computer systems today and the password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called **authorization**. Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms—some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The **non-discretionary** approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The **discretionary approach** gives the creator or owner of the information resource the ability to control access to those resources. In the **Mandatory access control approach**, access is granted or denied basing upon the security classification assigned to the information resource.

Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.

Access controls are security features that control how users and systems communicate and interact with other systems and resources.
Access is the flow of information between a subject and an object.
A subject is an active entity that requests access to an object or the data within an object. E.g.: user, program, process etc.
An object is a passive entity that contains the information. E.g.: Computer, Database, File, Program etc.
Access controls give organization the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality

Access Control Challenges

- *Various types of users need different levels of access* - Internal users, contractors, outsiders, partners, etc.
- *Resources have different classification levels*- Confidential, internal use only, private, public, etc.
- *Diverse identity data must be kept on different types of users* - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords, etc.
- *The corporate environment is continually changing*- Business environment needs, resource access needs, employee roles, actual employees, etc.

Access Control Principles

- *Principle of Least Privilege*: States that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e. Default no access
- *Separation of Duties*: Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.
- *Need to know* : It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

Access Control Criteria

The criteria for providing access to an object include

- Roles
- Groups
- Location
- Time
- Transaction Type

Access Control Practices

- Deny access to systems by undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unneeded system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Ensure that logon IDs is non-descriptive of job function.
- Remove redundant resource rules from accounts and group memberships.
- Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions and review reports periodically.
- Protect audit logs.

Security Principles

- Fundamental Principles (CIA)
- Identification
- Authentication
- Authorization
- Non Repudiation

Identification Authentication and Authorization

Identification describes a method of ensuring that a subject is the entity it claims to be. E.g.: A user name or an account no.

Authentication is the method of proving the subjects identity. E.g.: Password, Passphrase, and PIN

Authorization is the method of controlling the access of objects by the subject. E.g.: A user cannot delete a particular file after logging into the system

Note: There must be a three step process of Identification, Authentication and Authorization in order for a subject to access an object

Identification and Authentication

Identification Component Requirements

When issuing identification values to users or subjects, ensure that

- Each value should be unique, for user accountability
- A standard naming scheme should be followed
- The values should be non-descriptive of the users position or task
- The values should not be shared between the users.

Authentication Factors

There are 3 general factors for authenticating a subject.

- Something a person knows- E.g.: passwords, PIN- least expensive, least secure
- Something a person has – E.g.: Access Card, key- expensive, secure
- Something a person is- E.g.: Biometrics- most expensive, most secure

Note: For a strong authentication to be in process, it must include two out of the three authentication factors- also referred to as two factor authentication.

Authentication Methods

Biometrics

- Verifies an individual's identity by analyzing a unique personal attribute or behavior
- It is the most effective and accurate method for verifying identification.
- It is the most expensive authentication mechanism
- Types of Biometric Systems
    - *Finger Print*- are based on the ridge endings, bifurcation exhibited by the friction edges and some minutiae of the finger

THIS IS A FREE SAMPLE OF THE ACTUAL NOTES

TO GET FULL/COMPLETE NOTES:

Call/Text/Whatsapp:0713440925

You can also write to us at: topexamskenya@gmail.com
or info@mykasnebnotes.com

To download more resources visit: http://www.mykasnebnotes.com

For updates and insights like us on Facebook