**Topic- Developing Secure Information Systems, Application Development Security, Information Security Governance & Risk Management, CCTV and Intrusion Detection Systems, Backup Security Measures.**

**Backup security Measures**

**1.-what is data security and backup?**

**Security**

Data security refers to the protection of data from unauthorized access, use, change, disclosure and destruction and includes network security, physical security, and file security.

**Storage & Backup**

Data storage refers to holding your data files in a secure location that you can readily and easily access. Data backup, in contrast, refers to saving additional copies of your data in separate physical or virtual locations from data files in storage.

**2.-Why should you secure and backup your data?**

Your data is the basis of your research. If you lose your data, recovery could be slow, costly, or impossible. It is important that you secure, store, and backup your data on a regular basis. Securing your data will help to prevent:

1. -Accidental or malicious damage/modification to data
2. -Theft of valuable data
3. -Breach of confidentiality agreements and privacy laws
4. -Premature release of data, which can void intellectual property claims
5. -Release before data have been checked for accuracy and authenticity

Keeping reliable backups is an important part of data management. Regular backups protect against the risk of damage or loss due to hardware failure, software or media faults, viruses or hacking, power failure, or even human errors.

**3.-Guidelines for data security & backup**

**Security**

Security needs to be considered for all copies of your data, including your working data set, backup copies and archived copies.

1. **Network security** 
   1. Keep confidential data off the Internet
   2. Put sensitive materials on computers not connected to the internet
2. **Physical Security** 
   1. Restrict access to buildings and rooms where computers or media are kept
   2. Only let trusted individuals troubleshoot computer problems
3. **Computer Systems & Files** 
   1. Keep virus protection up to date
   2. Don’t sent confidential data via e-mail or FTP - use encryption, if you must send data
   3. Use good passwords on files and computers

**Storage & Backup**

One of the most important data management tasks is keeping backups of your data. There is a real risk of losing data through hard drive failure or accidental deletion.

**Remember to use the Backup 3-2-1 Rule**

1. 3 copies of your data - 2 copies are not enough
2. 2 different formats - i.e. hard drive+tape backup or DVD (short term)+flash drive
3. 1 off-site backup - have 2 physical backups and one in the cloud

**Backup options**

1. Hard drives - personal or work computer
2. Departmental or institution server
3. External hard drives
4. Tape backups
5. Discipline-specific repositories
6. University archives
7. Cloud storage

**4.- Security & backup resources**

1. **Creating Good Passwords**
   1. These password tips were created by CMU’s Information Security Office and provide recommendations on how to securely maintain and manage passwords.
2. **Storing Your Data**
   1. The UK Data Archive provides additional guidelines on data storage, backup and security.
3. **Data Backup Best Practices**
   1. Best practices for data backups presented by DataONE.

**CCTV and Intrusion Detection System**

Intrusion or Burglar alarms are systems designed to detect unauthorized entry into a building or area. It consists of an array of sensors, a control panel, alerting system and interconnections. Sensors detect intruders by many methods such as monitoring door and window contacts, by passive infrared motion detectors, ultrasound, vibration, electric or magnetic fields, or microwaves. Sensors may be directly wired to a control panel that provides sensor power or may communicate wireless.

Intellicon offers Intrusion Detection solutions which are robust and may also be combined with closed circuit television surveillance systems to automatically record the activities of intruders, and may interface to access control systems for electrically locked doors. Systems range from small, self-contained noisemakers, to complicated, multi-zoned systems with color-coded computer monitor outputs. Systems work without interruption for long periods and under extreme conditions.

**What is an intrusion?**

Any set of actions that attempt to compromise the confidentiality, integrity, or availability of a computer resource.

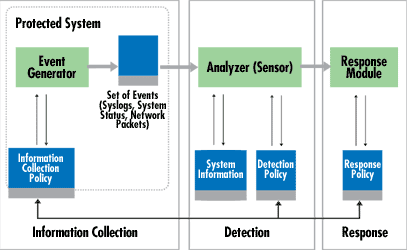
**Types of Intruders**

• In an early study of intrusion, Anderson identified three classes of intruders:

1. **Masqueraders**: An individual who is not authorized to use the computer and who penetrates a system’s access controls to exploit a legitimate user’s account.
2. **Misfeasor:** A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
3. **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit actions.

**Intrusion Detection Systems (IDS)**

1. Intrusion detection is the process of identifying and responding to malicious activity targeted at resources
2. IDS is a system designed to test/analyze network system traffic/events against a given set of parameters and alert/capture data when these thresholds are met.
3. IDS uses collected information and predefined knowledge-based system to reason about the possibility of an intrusion.
4. IDS also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion, etc.

[](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwipirHDx7LeAhWRfysKHQWpAv8QjRx6BAgBEAU&url=http%3A%2F%2Ftechgenix.com%2Fintrusion_detection_systems_ids_part_i__network_intrusions_attack_symptoms_ids_tasks_and_ids_architecture%2F&psig=AOvVaw314DXv8a4XTTaZK2ZpsKva&ust=1541139865799339)

Intrusion Detection System

**Components of IDS**

Basically there are three components or modules in an Intrusion detection System:

1. Sensor: Responsible for capturing packets and sending to the Console class.
2. Console: Responsible for analyzing packets captured by Sensor class.
3. It is the class responsible for displaying GUI and generating alerts.

**Functions of IDS**

1. An IDS detects attacks as soon as possible and takes appropriate action.
2. An IDS does not usually take preventive measures when an attack is detected.
3. It is a reactive rather than a pro-active agent.
4. It plays a role of informant rather than a police officer.

**Information Security Governance & Risk Management Domain**

The Information Security Governance and Risk Management domain entails the identification of an organization’s information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, roles, and responsibilities of individuals in identifying and securing organization’s information assets; the development and use of policies stating management’s views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary, and private information; third party management and service level agreements related to information security; employment agreements, employee hiring and termination practices, and risk management practices, and tools to identify, rate, and reduce the risk to specific resources.

**Information Security & Risk Management Domain**

* Information Security Concept
* Information Security Management
* Information Security Governance
* Information Classification
* System Life Cycle (SLC) and System Development Life Cycle (SDLC)
* Risk Management
* Certification & Accreditation •  Security Assessment
* Configuration Management
* Personnel Security
* Security Education, Training, and Awareness
* Project Management