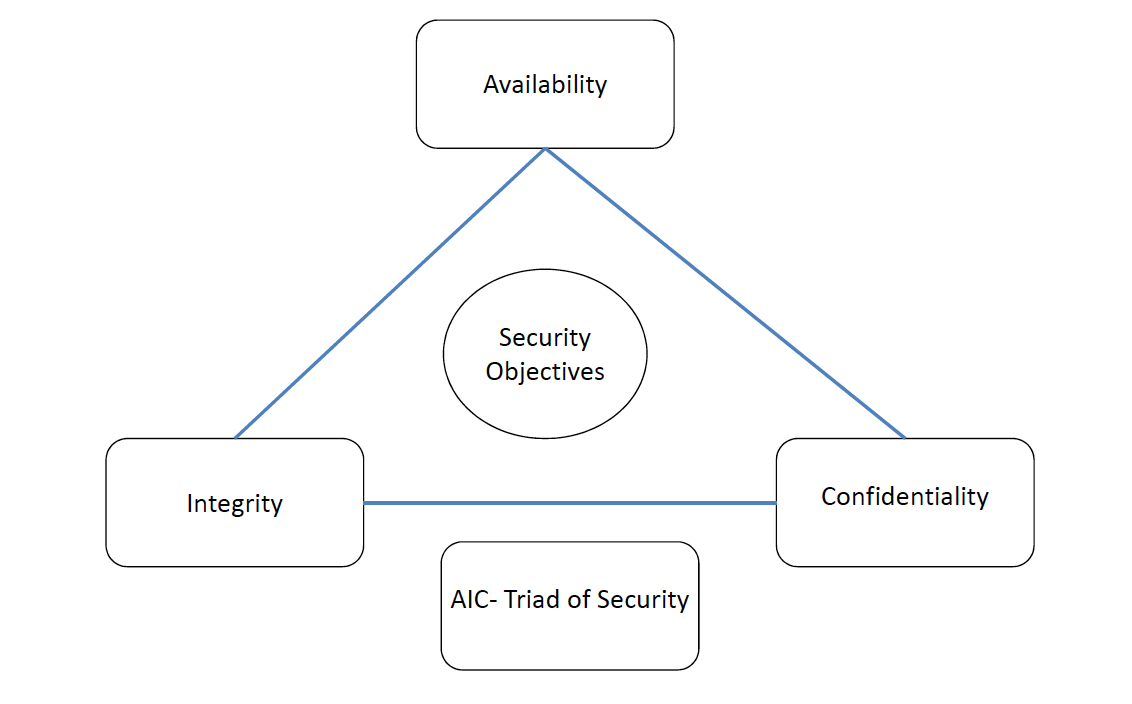
WEEK 1



**Availability** Protection ensures **reliability** and **timely** **access** to **data** and **resources** to **authorised** **individuals.**

**Integrity** Is upheld when the **assurance** of the **accuracy** and **reliability** of **information** and **systems** is **provided** and any **unauthorised** **modification** is **prevented**.

**Confidentiality** Ensures that the **necessary** **level** **of** **secrecy** is **enforced** at **each** **junction** of data **processing** and **prevents** **unauthorised** **disclosure**.

This **level** of **confidentiality** should **prevail** while **data** **resides** on **systems** and **devices** **within** the **network**, as it is **transmitted**, and **once** it **reaches** its **destination**.

Controls to Counter Cyber Attack

**Availability**

* Redundant array of inexpensive disks (***RAID***)
* Clustering
* Load balancing
* Redundant data and power lines
* Software and data backups

**Integrity**

* Hashing (data integrity)
* Configuration management (*system integrity*)
* Change control (*process integrity*)

**Confidentiality**

* Encryption for data at rest (*whole disk, database encryption*)
* Encryption for data in transit (*IPSec, SSL, PPTP, SSH*)
* Access control (*physical and technical*)

**Vulnerability** A lack of a **countermeasure** or a **weakness** in a **countermeasure** that is **in** **place**.

**Threat** A threat is **any** **potential** **danger** that is **associated** with the **exploitation** of a **vulnerability**.

**Threat** (*for business*) The threat is that **someone**, or **something**, will **identify** a **specific** **vulnerability** and **use** it **against** the **company** or **individual**.

**Threat Agent** The **entity** that **takes** **advantages** of a **vulnerability** is referred to as a **threat** **agent**.

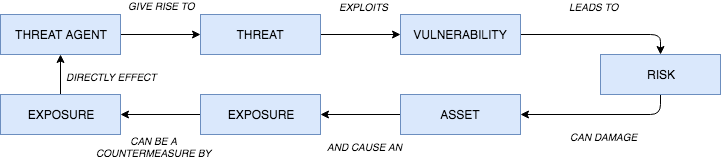
**Risk** A risk is the **likelihood** of a **threat** **agent** **exploiting** a **vulnerability** and the **corresponding** **business** **impact**.

**Exposure** An exposure is an **instance** of **being** **exposed** to **losses**.

**Control** A **control**, or **countermeasure**, is put into place to **mitigate** the **potential** **risk**.

A **countermeasure** may be a **software** **configuration**, a **hardware** **device**, or a **procedure** that **eliminates** a **vulnerability** or that **reduces** the **likelihood** a **threat** **agent** will be able to **exploit** a **vulnerability**.

Relationship Among Different Security Concepts



Types of Attack

1. ***INBOUND ATTACKS***

*Scrambling sequence of data packets*

* **Intrusion Detection Systems** rely on packets coming through the network **sequentially** to identify **patterns** or ‘**signatures**’.
* Destination device reassembles packets on the **inside**.

*Encoding*

* Not all IDS signature detection is normalised.
  + E.g. - Unicode-encoding by changing spaces to “**%20**”

1. ***MALWARE***

* Any software that the user of system admin did not authorise or want on their computer.
* *Spyware, grayware, adware, Trojan horses, key loggers, backdoors, rootkits.*
* Once installed, it’s difficult to detect by **intrusion** **detection** **systems** and **firewalls** **rarely limit egress (*outbound*) traffic**.
* Once inside a system, malware can scan for vulnerabilities and exploit them.

*HOW DOES MALWARE GET ONTO A SYSTEM?*

* **Phishing (Social Engineering)**
  + Emails sent to people who are then:
    - Lured into **downloading** **malicious** **software**.
    - Visit a **website** that **infects** the **system**.
    - Gives up **passwords**.
* **Pharming** 
  + Redirecting a websites traffic to another website
    - **DNS poisoning** - modifying a router’s **DNS** **address**.
    - **Modifying** **OS** local **resolution** hosts **file**.
* **Backdoors**
  + **Secret entry points** into a **program** that **bypass** normal **security** **checks**.
  + **Maintenance hooks** are an example of a **legitimate** form of **backdoor**, to debug and test programs.
  + **Logic Bombs** are embedded in programs and are set to **explode** when certain **conditions** are **met**. - Can alter or delete files.
* **Viruses (Self-propagating)**
  + **Attach** to **programs** of files enabling it to spread.
  + Almost always an **EXE** file.
  + Cannot spread without **human** **action**.
  + *Comprise of three parts:*

1. **Infection Mechanism**
   1. *Means by which is spreads.*
2. **Trigger**
   1. *Event or condition that enacts the virus.*
3. **Payload**
   1. *What the virus does.*

TYPES OF VIRUS

*ENCRYPTED VIRUS*

* A portion of the virus **creates** a **random** **encryption** **key** and **encrypts** the **remainder** of the **virus**.
* When the virus is **invoked**, the **key** is **used** to **decrypt** the virus.
* When the virus **replicates**, a **different** **key** is used.
* **Difficult** to **monitor** bit **patterns** of the **virus**.

*STEALTH VIRUS*

* Explicitly designed to **hide** **itself** **from** **detection**
  + *e.g.* ***compressing itself*** *to be the* ***same******size*** *as the* ***program*** *it has* ***infected****, or detecting virus scans and presenting the original version of the program.*

*POLYMORPHIC VIRUS*

* **Mutates** with every **infection** making **signature** **detection** **impossible**.
* **Functionally** the **same** but **bit patterns are different**.

*METAMORPHIC VIRUS*

* As with polymorphic but the **alteration** of **bit pattern** is **even more complex**.
* **Routines** may also **change** so **behaviour as well as** **bit** **pattern** may **change**.

WORMS

* Unlike a virus, **worms can travel without human action**.
* Uses vulnerabilities of the system to **travel unaided**.
* Can **replicate** **many** **times**, **consuming system memory and/or network bandwidth**.
* Code Red worm (*359k MS IIS Web servers in 1 day (July 2001)*)…patch made available 1 year earlier. Costed at $2.62 billion.

TROJAN HORSES

* “**Hides itself**” **as useful software** but actually **does damage once installed**.
* Can **delete files, corrupt information**.
* Also create “**backdoors**”, giving malicious users access to your system.
* **Do not reproduce**, unlike viruses and worms.
* The software may continue to **perform the task you installed it for**, but **behind the scenes** it is **attacking the system**.
* Alternatively, it may be acting maliciously while operating ask expected e.g. collecting passwords and form data.

BOTNETS

* **Zombie** = when a **system gets infected** with malware and **falls under external control**.
* Botnet (*roBOT NETwork*) = collection of zombies under command and control of a hacker.
* Vint Cerf (2007) – Up to 25% of PCs part of a botnet.
* Today there are c.1.2 billion computers on the Internet.
* Feb 2000 – schoolboy brings down Dell, CNN, Amazon, eBay and Yahoo website using 200 university networks in the US to launch distributed denial of service (DDoS) attacks.
* **DDoS** = **hundreds of systems** requesting a new session with a website – servers cannot handle the requests and crash.

HACKNG WEB SERVICES

*Web services act as* ***middleware to connect distributed systems*** *and* ***share data****.*

*Vulnerable to attacks:*

* **Cross-site scripting (XSS)**
  + Attackers “**inject**” **malicious** **scripts** **into** **web pages** (*e.g. posting a message on a social network that includes a script to collect session cookies, hidden inside <script> elements…readers of the message have their cookie stolen*).
* **Cross-site request forgery**
  + **Attackers uses user cookies** (e.g. while logged into bank) to authorize attacks (e.g. transfer money to account X) without user’s knowledge.
* **Browser flaws**
  + A form of **malicious** **code** that takes advantage of a **flaw or vulnerability in an operating system or piece of software** with the intent **to breach browser security** to **alter** a **user's browser settings without their knowledge**.
  + Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code.

SEARCH ENGINE MANIPULATION

*Search engines are manipulated to:*

* **Present false results** that link to malicious sites.
* **Rank malicious** **sites** at the **top** of the **results**.
* **Manipulate** **adverts** to direct to malicious sites.

***Search engines use (secret) page ranking algorithms but word count, result click-thru, and the number of sites linking to a result often supersedes these.***

*Botnets are used to:*

* **Add references to hacked sites** to **boost search engine rankings** of malicious sites.
* Add **keywords** to **pages**, **relating to current** **events**, celeb, political, natural disasters – links to malicious page

Virtualization and the Cloud

Virtual machines now allow **hundreds of instances** of **an operating system** to **run on a single server**.

*What happens if the virtualization software is compromised?*

* Happened in 2009 when over 100,000 websites hosted in a virtual environment were destroyed by a hacker, using a **zero day exploit** to **gain** **root access**.
* Less than half the customers had a full backup.

CONTROL TYPES

***Administrative***

* Commonly referred to as “**soft controls**” because they are **more** **management oriented**.
  + Examples of administrative controls are **security documentation, risk management, personnel security, and training**.

***Technical***

* **Software** or **hardware** components, as in **firewalls, IDS, encryption, identification and authentication mechanisms**.

***Physical***

* Items put into place to protect facility, personnel, and resources.
  + *Examples of physical controls are* ***security guards, locks, fencing, and lighting****.*

FUNCTIONALITIES OF SECURITY CONTROL

**DETERRENT** Intended to **discourage a potential attacker**.

**PREVENTIVE** Intended to **avoid an incident from occurring**.

**CORRECTIVE** **Fixes components** or **systems after** an **incident** has occurred.

**RECOVERY** Intended to bring the **environment** **back to regular operations**.

**DETECTIVE** Helps **identify** an **incident’s activities** and **potentially an intruder**.

**COMPENSATING** **Controls** that **provide** an **alternative measure of control**.

SECURITY METRICS

*Risk can be measures by two ways:*

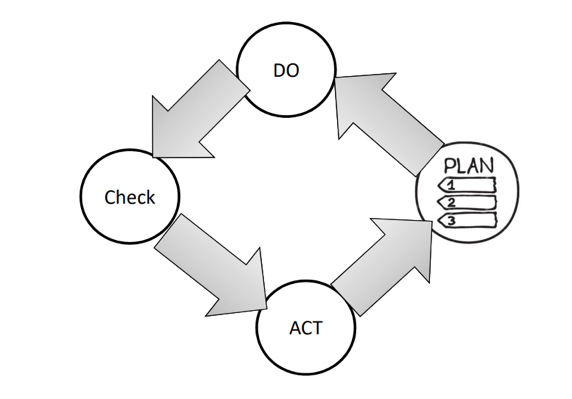
1. ***Quantitative risk analysis*** 
   1. Used to **assign monetary and numeric values** to **all elements of the risk analysis process**.
2. ***Qualitative risk analysis***
   1. Uses a **“softer” approach** to the **data elements** of a **risk analysis**. It **does not quantify that data**, which means that it **does not assign numeric values** to the data **so that** **they can be used in equations**.

WEEK 2

COMMON SECURITY FRAMEWORKS

ISO/IEC 27000

* ISO/IEC 2700 was adapted from British standard 7799 (*BS7799*).
* BS7799 was developed to guide organizations on how to **design**, **implement** and **maintain** **policies**, **process**, and **technologies** to **manage** **risk**.
* It consisted on **two** **parts**:
  + Part **one** outlined **control** **objectives** and how to **achieve** **them**.
  + Part **two** outlines how a **security** **program** can be **set** **up**.
* It laid foundation on how security should cover:
* Information security policy for the organization.
* Creation of information security infrastructure.
* Asset classification and control.
* Personal security.
* Communication and operation.
* Access control.



ISO/IEC 27000: PLAN

* Define the **scope** of the ISMS.
* Define ISMS **policy.**
* Define **approach** to risk assessment.
* **Identify** the **risks.**
* **Analyse** and **evaluate** the risks.
* **Identify** and **evaluate** options for the **treatment** of risk.
* Management **approves** **residual** **risks.**
* Management **authorizes** **ISMS.**
* Select control **objectives** and **controls.**

ISO/IEC 27000: DO

* **Formulate** risk treatment **plan**.
* **Implement** risk treatment **plan**.
* **Implement** **controls**.
* Implement **training** and **awareness** programs.
* Manage **operations**.
* Manage **resources**.
* Implement procedures to **direct**/**respond** to **security** **incidents**.

ISO/IEC 27000: CHECK

* **Execute** **monitoring** procedures.
* Undertake regular **reviews** of ISMS effectiveness.
* Measure **effectiveness** of controls.
* Review **level** of **residual** and **acceptable** risk.
* Conduct **internal** ISMS **audit**.
* Regular management **review**.
* **Update** security **plans**.
* Record **actions** and **events**.

ISO/IEC 27000: ACT

* Implement identified **improvements**.
* Take **corrective**/**preventative** **action**.
* Apply **lessons** **learned** (*including other organizations*).
* **Communicate** **results** to interested parties.
* Ensure **improvements** to **achieve** **objectives**.

ISO/IEC 27000: PROVIDES

* **Information security policy for the organization:**
  + **Map** of **business** **objectives** to **security**, management’s **support**, security **goals**, and **responsibilities**.
* **Creation of information security infrastructure**
  + **Create** and **maintain** an organizational security **structure** through the use of a security **forum**, a security **officer**, defining security **responsibilities**, **authorization** **processes**, **outsourcing**, and independent **reviews**.
* **Asset classification and control**
  + Develop a security infrastructure to protect organizational **assets** through **accountability** and **inventory**, **classification**, and **handling** **procedures**.
* **Personnel security**
  + Reduce risks that are inherent in human interaction by **screening** **employees**, defining **roles** and **responsibilities**, **training** employees properly, and **documenting** the **ramifications** of not meeting expectations.
* **Physical and environmental security**
  + Protect the organization’s assets by properly choosing a facility **location**, **erecting** and **maintaining** a security **perimeter**, implementing **access** **control**, and **protecting** **equipment**.
* **Communications and operations management**
  + Carry out operations security through **operational** **procedures**, proper **change** **control**, **incident** **handling**, **separation** of **duties**, **capacity** **planning**, **network** **management**, and **media** **handling**.
* **Access control**
  + Control access to assets based on **business** **requirements**, **user** **management**, **authentication** **methods**, and **monitoring**.
* **System development and maintenance**
  + Implement security in **all phases of a system’s lifetime** through **development** of security **requirements**, **cryptography**, **integrity** protection, and **software** development **procedures**.
* **Business continuity management**
  + Counter **disruptions** of normal operations by using **continuity** **planning** and **testing**.
* **Compliance** 
  + Comply with **regulatory**, **contractual**, and **statutory requirements** by using **technical** **controls**, system **audits**, and **legal** **awareness**.

ISO/IEC 27000 SERIES

**ISO/IEC 27000 Overview** and **vocabulary.**

**ISO/IEC 27001** ISMS **requirements.**

**ISO/IEC 27002** Code of **practice** for **information security management.**

**ISO/IEC 27003** **Guideline** for **ISMS implementation.**

**ISO/IEC 27004** **Guideline** for information security management **measurement** and **metrics** **framework**.

**ISO/IEC 27005** Guideline for information security **risk** **management.**

**ISO/IEC 27033-1**  Guideline for **network security.**

ISO/IEC 27001 REQUIREMENT

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
   1. Understanding the organization and its context.
   2. Understanding the needs and expectations of interested parties.
   3. Determining the scope of the information security management system.
   4. Information security management system.
5. Leadership
   1. Leadership and commitment.
   2. Policy.
   3. Organizational roles, responsibilities and authorities
6. Planning
   1. Actions to address risks and opportunities.
   2. Information security objectives and planning to achieve them.
7. Support
   1. Resources.
   2. Competence.
   3. Awareness.
   4. Communication.
   5. Documented information.
8. Operation.
   1. Operational planning and control.
   2. Information security risk assessment and treatment.
9. Performance evaluation
   1. Monitoring, measurement, analysis and evaluation.
   2. Internal audit and management review.
10. Improvement
    1. Nonconformity and corrective action.
    2. Continual improvement.