INFO 6027: Information Security Planning
Winter 2022

Week 2 – Planning, Risk, and BIA

FANSHAWE

Housekeeping

- Check In Time:
  - How are you settling in? Any questions about the program, this course, next week's lottery numbers? ☺
- What did we talk about **last week**?
  - What is information "security"
  - The role of the leader/manager in security planning, management styles
  - Comparing security management and business management
- Any questions from last week?

Agenda

- Housekeeping / News / Current events
- Today's Lesson
  - Planning
  - Risk
  - SWOT Analysis
  - Business Impact Analysis
- Summary and Reminders

Current Events: What is happening in (your) world?

- **Ransomware, Ransomware …**

The most dangerous place on Earth
America and China must work harder to avoid war over the future of Taiwan

Disasters of 2022?

- Covid-19
- **Others?**

Disasters a Factor in Security Planning

•Which threats NORMALLY exist to businesses in California or Australia?

Which threats/risks do you see as a result of:

- Fire damage?
- Smoke damage?
- Suppression efforts?
- Evacuation (shut off hydro, heat, water, etc)?
- Potential for new fires?
- Lightning?
- Human Resources?

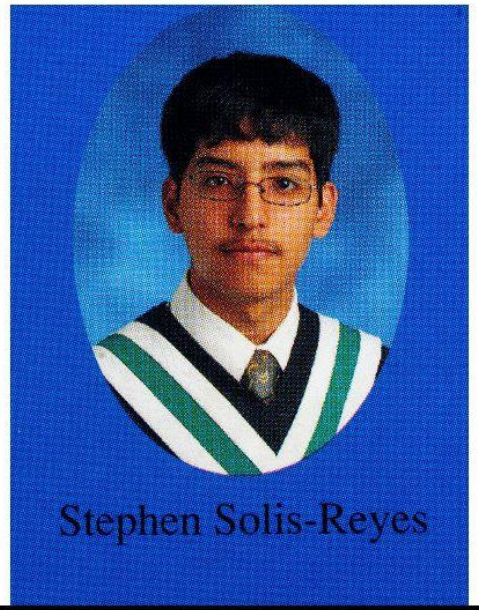
How would you plan for a disaster if you owned a business in California?

Planning for Cyber-Incidents…

NEWS LOCAL

Court hears it took computer whiz kid Stephen Solis-Reyes six seconds to get into the Canada Revenue Agency system

By Jane Sims, The London Free Press
Friday, May 6, 2016 7:51:00 EDT PM



Stephen Solis-Reyes

Recommend 82

Stephen Solis-Reyes is one of those brainiac computer whiz kids who this time, maybe, was a little too smart for his own good.

Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. **Heartbleed** may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client.

Heartbleed - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/**Heartbleed**

https://lfpress.com/2016/05/06/court-hears-it-took-computer-whiz-kid-stephen-solis-reyes-six-seconds-to-get-into-the-canada-revenue-agency-system/wcm/83a120c5-477a-2abb-1a49-553653cb7f80

Today's Discussion - Week 2

1. Risk!!

- Analyzing your environment
- Identifying and analyzing risks
- Threat analysis

2. Business Impact analysis (BIA)

Risk in InfoSec

- **Risk**: is the *likelihood* of a *threat* exploiting a *vulnerability* to have a damaging *impact* on an *asset*
- **Threat**: anything that might have a damaging *impact* on an *asset*. The potential cause of an unwanted incident resulting in harm to a system or organization.
- **Vulnerability** anything that permits a *threat* to impact an *asset*
- **Asset** anything used to create, store, transmit or receive information and data

In other words…

- The **risk** is that X could happen
- the **threat** is what will make X happen.
- the **vulnerability** is *how* the ***threat*** can make X happen to the asset
- The **asset** is what is affected by the X happening

Is information your company's greatest asset?

- **All** organizations depend on information to **survive**
- A valuable organisational **asset** can be:
  - Printed or written on paper
  - Stored electronically
  - Transmitted by post or using electronic means
  - Shown on corporate videos
  - Verbal - spoken in conversations

"…Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected" *(ISO/IEC 27001:2005)*

- ***27001 is NOT just Information Technology (IT). It is ALL types of information and transmission media***

Why does RISK matter? (1)

Consider the ***potential*** of:

- damage to brand or reputation of the organization, or embarrassment if information fell into the wrong hands - forged emails, defaced web site, bad publicity
- damage of relationships with the public and other stakeholders
- going out of business (bankruptcy)
- downtime - reboot the machine/restart services, rebuild/restore from backup
- loss of confidential data, loss of work not backed-up

What Are Some Risks to Businesses?

- Ex. We stop being compliant with a regulatory requirement.

What else?

- An insider shares/sells our trade secrets
- A strike (ie. labour dispute)
- A virus (sick people or sick computers)
- A sustained outage
- A fire
- Someone breaks into our data center
- We lose our backup servers/storage

Why Does RISK matter? (2)

Consider the **threat** of malicious hackers:

- Malicious – sabotage, damage, defacement
- Academic - gaining knowledge
- Industrial espionage – steal/sell secrets
- Ex-employee - delete old logins, cripple or embarrass
- White hacker - ethical hacker (displaying the weaknesses of your system)
- Cyber Warfare – disruption of communications
- Terrorism – Ideologically driven (making a political point)

Cost of protection vs. Value of assets

Costs of *achieving* security

- Prevention
  - ✓ Planning
  - ✓ Training
  - ✓ Tools
- Appraisal
  - ✓ Inspections
  - ✓ Audits
  - ✓ Tests

Costs of *not* achieving security

- Internal failures
  - Scrap
  - Rework
- External failures
  - Warranty
  - Liability
  - Loss of reputation

Can we ever "achieve security"?

Why or why not?

- Threats change
- Tech changes
- Environment changes
- Budget changes

Information Security Processes

- **Primary**
  - Policy – what do we need to do?
    - Structures
    - Organization
  - Planning – how are we planning to do it?
    - Methodologies

- **Secondary (supporting)**
  - Problem Solving
    - SWOT Analysis (**strengths, weaknesses, opportunities and threats)**
  - ***Asset Determination*** (does this have value to the company?)
  - Threat Determination (from who? from where? on what?)
  - Risk Management (Potential loss, probability vs impact)
  - **Information Assurance** – (protect/defend info) Remember CIA?

Planning

- BCM and BCP
  - All about identifying risks (both internal and external) and planning for them
  - Commonly involves a risk assessment
- Utilize **Methodologies**
  - Cyclical Process (assess, plan, act, check/re-assess)
  - Continuous improvement to meet changing needs
- Soft Science vs. Hard Science
  - Hard Sciences are rigid, inflexible, and absolute (formulas that **always** work).
    - Ex. Math, chemistry, physics
  - Soft science is flexible, dynamic, and adaptable
- InfoSec management processes are_____sciences

POLICY (and process/procedures)

Hint: Define your POLICIES as soon as possible!

- And **re-define** policy as your Sec Plan(s) are created / refined.

- ***Policy describes what the objectives and strategies are, and the process used to achieve them.***
- A deliberate system of principles to guide decisions and achieve rational outcomes.
- A statement of **intent** - implemented as a **procedure** or **protocol**.
- **Like rules with a purpose!** Policy is driven by **goals** and relevant law (cannot conflict), and must be properly structured, supported and administered.

Problem Solving - SWOT Analysis

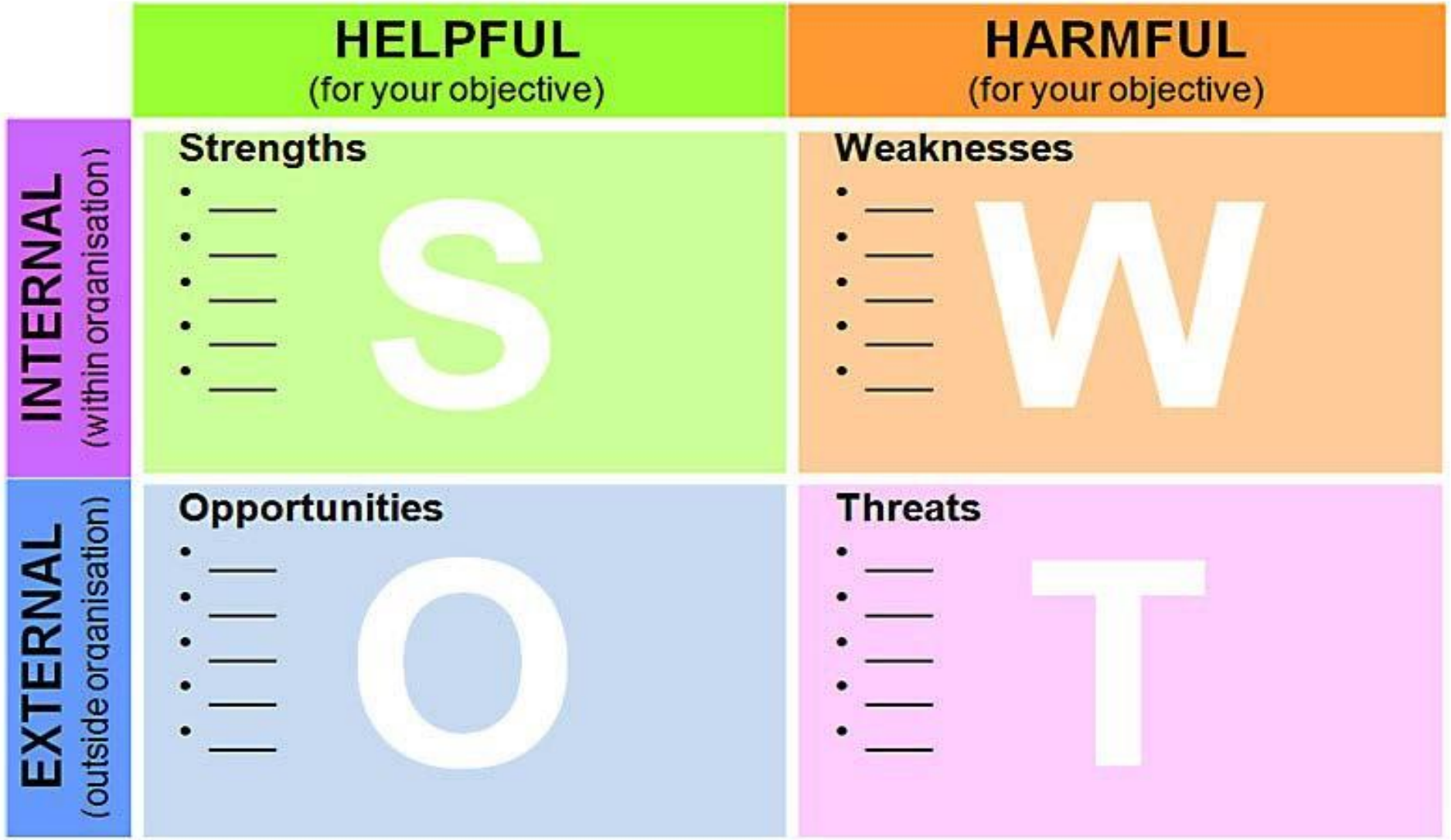
What is SWOT Analysis?

- SWOT analysis is a simple problem solving / planning tool that compare **strengths** and **weaknesses** with **opportunities** and **threats** to **create an action plan**.
- Strengths and weaknesses are **internal** to the business being analyzed while opportunities and threats are **external** factors.
- involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieve that objective
- SWOT can be adapted to **many different planning purposes…..**

SWOT Can be Used For

- **Help make policy decisions**
- Quick way to examine a small business idea
- The basis of a marketing action plan
- Starting point for business contingency planning (CP)
- As tool for involving staff/employees in business planning – e.g. solving particular problems or achieving particular business goals
- as a self-evaluation tool for how you're doing managing staff or running your business
- Admins ask: ***"Is objective attainable, given the SWOT?"***

SWOT Matrix


HELPFUL
(for your objective)
HARMFUL
(for your objective)
INTERNAL
(within organisation)
EXTERNAL
(outside organisation)
Strengths
S
Weaknesses
W
Opportunities
O
Threats
T

SWOT example: a small local business

Sedibeng Breweries is a medium-scale brewery located in the growing industrial centre of Selebi Phikwe, Botswana.

Their primary market advantages are: their company culture, consistent “quality” branding, traditional recipes, and commitment to rural distribution.

Strengths	Weaknesses
Capital stock: We’ve established and maintained a strong capital base. **Marketing:** Aggressive and focused marketing campaign with clear goals and strategies. **Management team:** Together have wide experience in product and business know-how.	**Not tech-savvy:** Establishing a reputation on the internet will be challenging. **Quick expansion:** There are a lot of new hires to train and organizational structures to learn. **New:** Don’t have the reputation or money for big breweries.
Opportunities	**Threats**
Packaging: New generation of consumers appreciate high-end bottling and labels. **Craft beer niche:** There is a growing community of craft beers appreciators in Botswana. **Government programs:** Promotions of and initiatives to support Botswana exports.	**Vertical integration:** Major breweries are establishing control of supply and distribution channels to corner the market. **Price fluctuation:** Huge fluctuations in prices of supplies may occur. **Competitor market:** Competition could develop expensive new marketing campaigns.

Internal	**Strengths**	**Weaknesses**
	✔ Your specialist marketing expertise ✔ A new, innovative product or service ✔ Location of your business ✔ Quality processes and procedures ✔ Any other aspect of your business that adds value to your product or service	✔ Lack of marketing expertise ✔ Undifferentiated products or services (i.e. in relation to your competitors) ✔ Location of your business ✔ Poor quality goods or services ✔ Damaged reputation
External	**Opportunities**	**Threats**
	✔ A developing market such as the Internet ✔ Mergers, joint ventures or strategic alliances ✔ Moving into new market segments that offer improved profits ✔ A new international market ✔ A market vacated by an ineffective competitor	✔ A new competitor in your home market ✔ Price wars with competitors ✔ A competitor has a new, innovative product or service ✔ Competitors have superior access to channels of distribution ✔ Taxation is introdused on your product or service

Active Learning Exercise! In Breakout Groups

- Remember your fictional business?
- Your business is considering using **social media for marketing purposes**.
- Complete a SWOT analysis
- Save it as an image and attach it to your Week 2 discussion post ☺

Break?

FANSHAWE

An **ASSET** – what is it?

- a useful or valuable thing, person, or quality.
- **property** owned by a person or company, regarded as having value and available to meet debts, commitments, or legacies.
- resources or things of value that are owned by a company.

An example:

- **Consider your business**. What are some of its assets? Take a moment to list some of the assets your business might have
- Does the type of business you create change what your assets might be? How so?

What is Information Assurance?

- Managing the Risk to the Asset
  - Company wants to be ASSURED that their information is safe at every state of its life cycle.
  - Protection of the AAA/CIA triad and uses physical, technical, and administrative controls to accomplish these tasks.
- The IA Life Cycle includes:
  - Creation
  - Modification
  - Processing
  - Storing
  - Transmitting
  - Deletion
- All forms of data – including data in transit and data at rest

This figure shows the relationship among some of these terms.

We start with the concept of a system resource, or asset, that users and owners wish to protect.

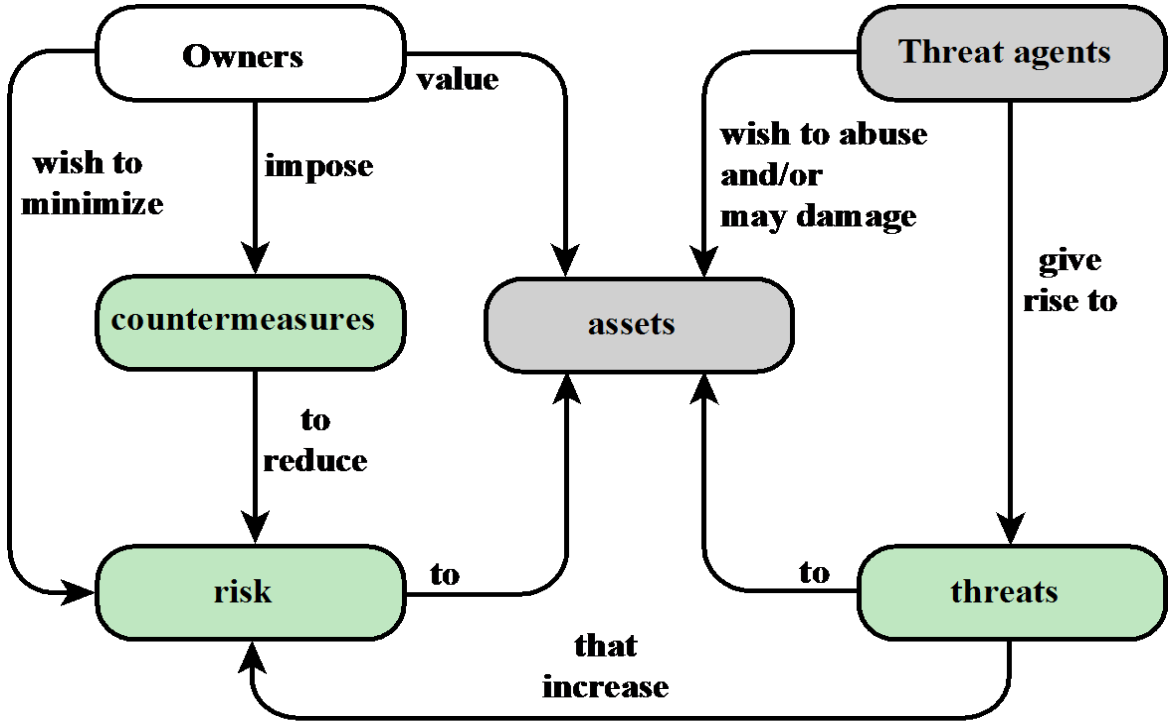
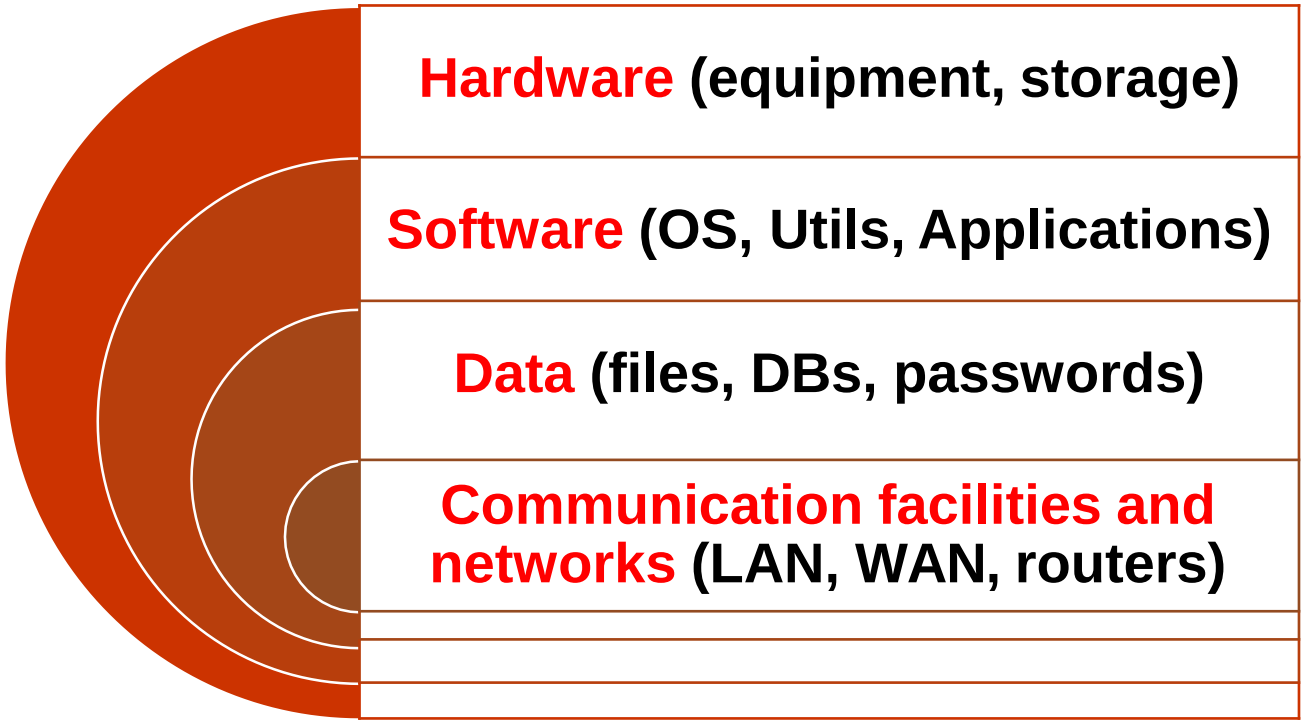


Figure 1.1 Security Concepts and Relationships

Assets of a Computer System?

are any data, devices, or other component of the environment that support **information**-related activities.



Computer and Network **Assets** (with examples of threats to those assets)

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities - CIA
  - Corrupted (loss of integrity), Leaky (loss of confidentiality),
  - Unavailable or very slow (loss of availability)
- Threats – a source of potential security harm to an asset.
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out) based on the **origin of the attack**
- **Passive** – attempt to learn or make use of information from the system that does not affect system resources
  - **Active** – attempt to alter system resources or affect their operation
  - **Insider** – initiated by an entity inside the security parameter
  - **Outsider** – initiated from outside the perimeter
- **Vulnerability is the *bridge* *between the* *threat* *and the* *asset*. It is the means through which a threat can act on an asset**

Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

Threat Analysis – A Data Center

What are some **threats** to the data centre?

- Perhaps it's a natural disaster-related damage threat (earthquake, hurricane, tornado, flooding).

Risk Assessment

1. What would be the **impact** of the threat?
   - The impact could be anything from the systems being down for a few hours to total destruction of the data centre.
3. What's the threat's **frequency/likelihood**?
   - In Florida, hurricanes seem to occur almost on a yearly basis. In the Midwest, the likelihood of a tornado is higher than on the West Coast. It stands to reason that a data centre built on an earthquake fault in California is not ideal. While the frequency of an earthquake is perhaps one every 10 years, all you need is one good earthquake to destroy the data centre.

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **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. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Threat Consequences, and the Types of Threat Actions That Cause Each Consequence

Based on RFC 4949 Glossary

Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Security Requirements

(FIPS PUB 200)

(page 1 of 2)

Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Security Requirements

(FIPS PUB 200)

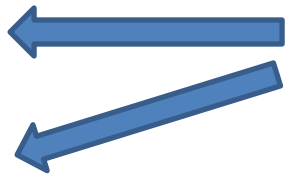
(page 2 of 2)

Risk Management Steps

- Identify risks – *Who or what could cause harm to the asset? How could this occur?*
- Analyze risks – use a Risk Assessment matrix to determine risk level
- Evaluate risks – is this a risk that requires action/treatment?
- Treat risks – determining the order in which risks get treated

Risk Treatment Options

- Accept risks – do nothing. This has consequences!
- Avoid risks – not proceed with activity or system
- Transfer risks – share resp. with others (ex. Insurance)
- Reduce Consequence - ex. off-site backup, DRP, or multi-site replication
- Reduce Likelihood – make asset more secure (ex. Deploy firewalls, access tokens, password policies)



These are both Risk Mitigation strategies

Risk Assessments

- Determines the level of risk for each asset's vulnerabilities
- Assigns a Risk Rating – helps for prioritizing actions/treatments

Probability	Impact: Low	Impact: Medium	Impact: High
High	low	medium	high
Medium	low	medium	medium
Low	low	low	low

Stevestedman.com

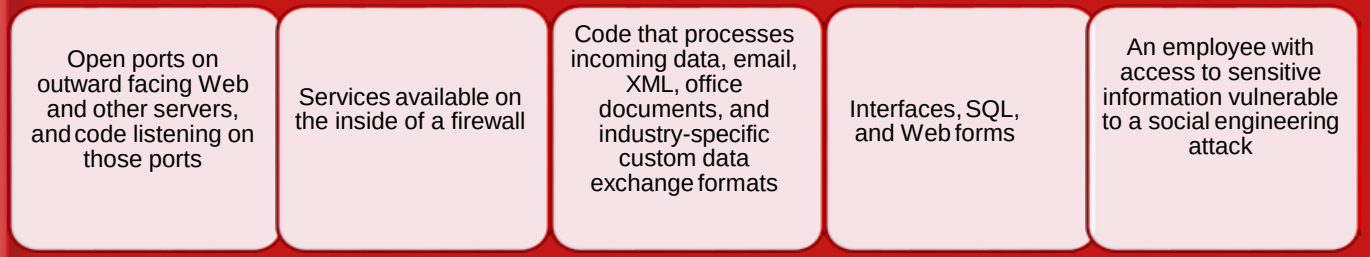
What is a Risk Assessment

- **Quantitative and qualitative risk assessments?**
  - Quantitative – measurable. Numbers, facts, evidence-based
  - Qualitative – opinion-based, personal experience, training
- **How to reduce Likelihood/Probability?**
  - Through **CONTROLS**
  - Controls are the things we do to lower either the impact or the likelihood of a harmful event.
  - For example reducing how many people have access, their training, etc
  - Some probabilities we can control/predict, others we cannot
    - Ex. ***Could anyone have predicted Covid-19?***

Attack Surfaces: This is your **exposure**.

Consist of the reachable and exploitable vulnerabilities in a system

Examples:



Where are you exposed?

How are you protecting/limiting that exposure?

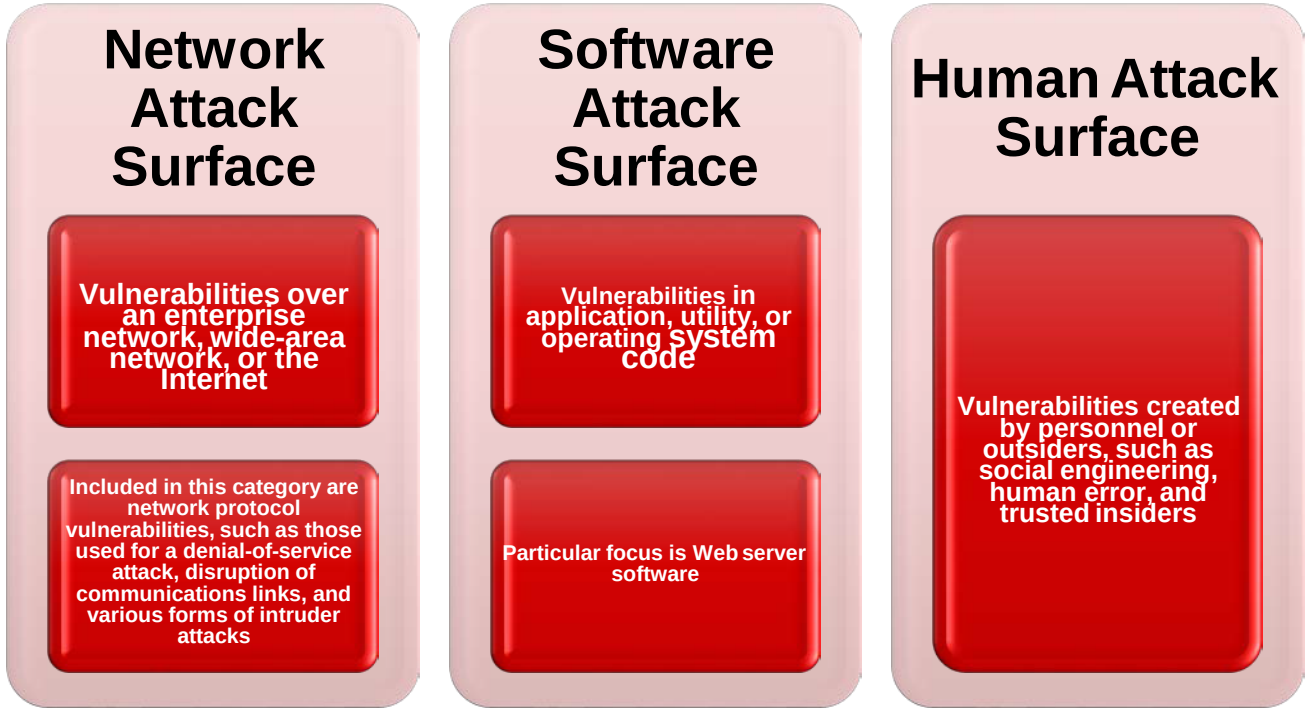
Attack Surface: What is exposed/presented to the threat agent

Awfully hard to hit a target you can't see!!

Identifying Possible Attack Surfaces:

- Do we have reachable/exploitable vulnerabilities in a system?
- do we have a public-facing website?
- do we allow VPN connections?
- do we welcome the public into our facilities and computers?
- Do we provide information security training to our staff?

Attack Surface Categories



Reduce Social Engineering: how much of your identity is online and freely accessible to the public?

Think of Defence in Depth as a Battlefield or a Castle. Think of the LAYERS of security

DID is *one* option for Information Assurance

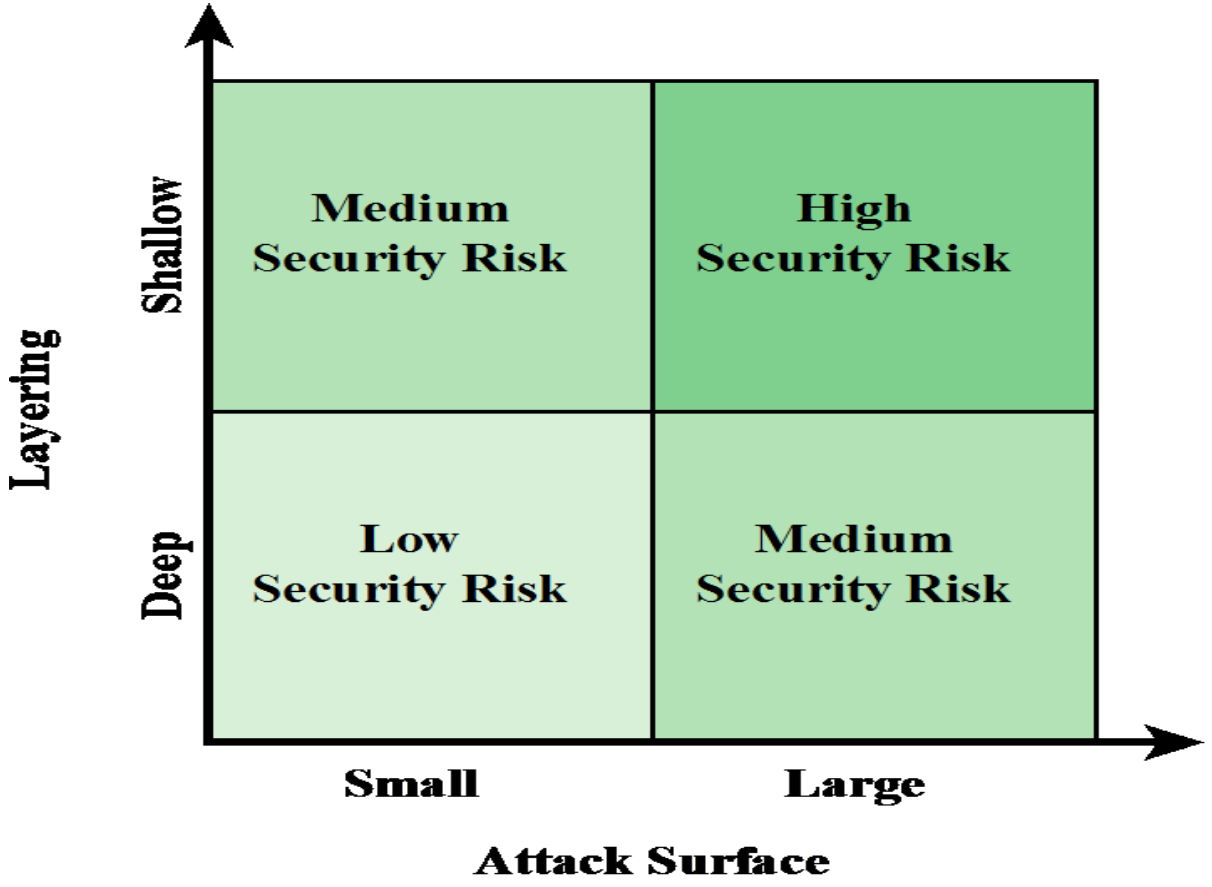
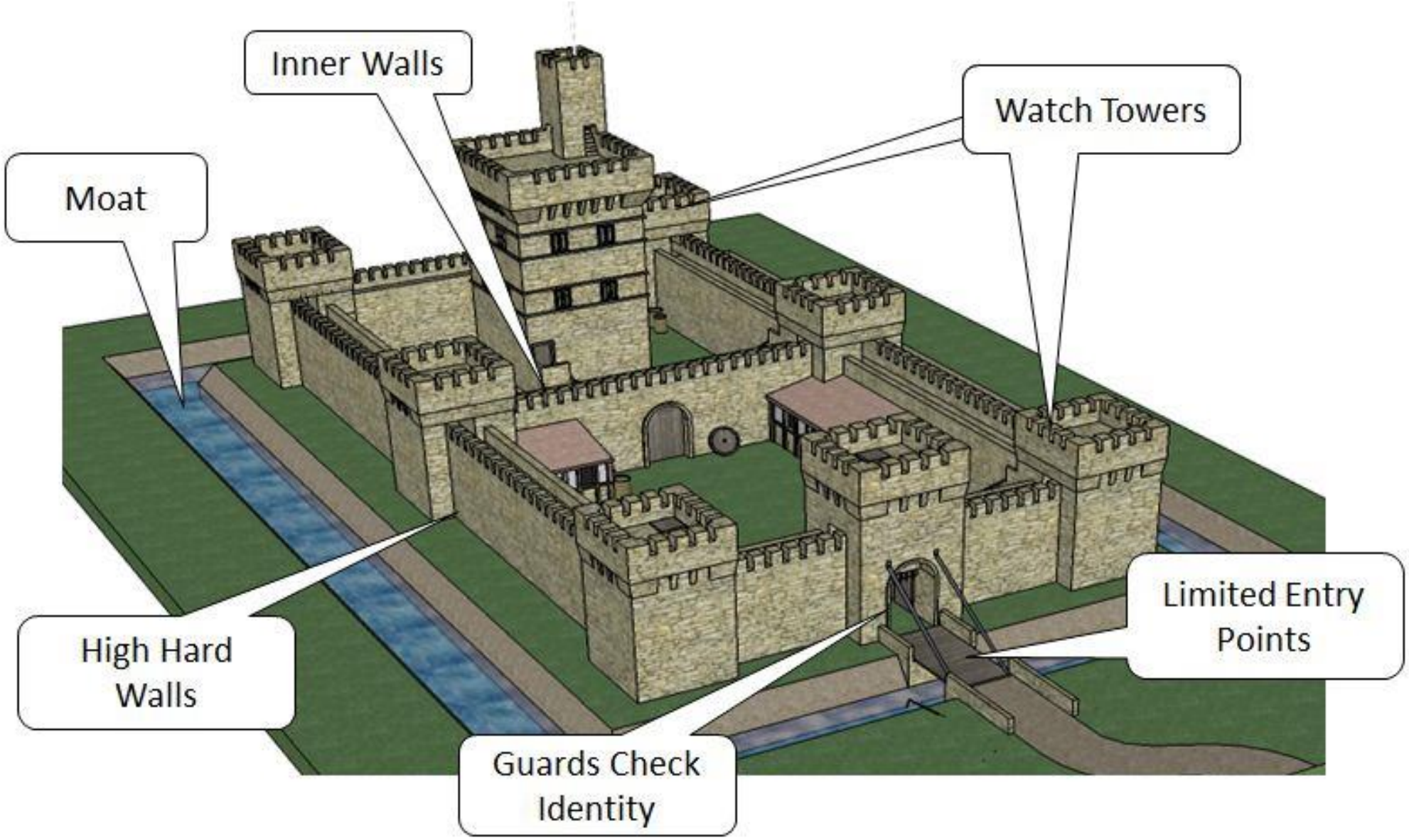


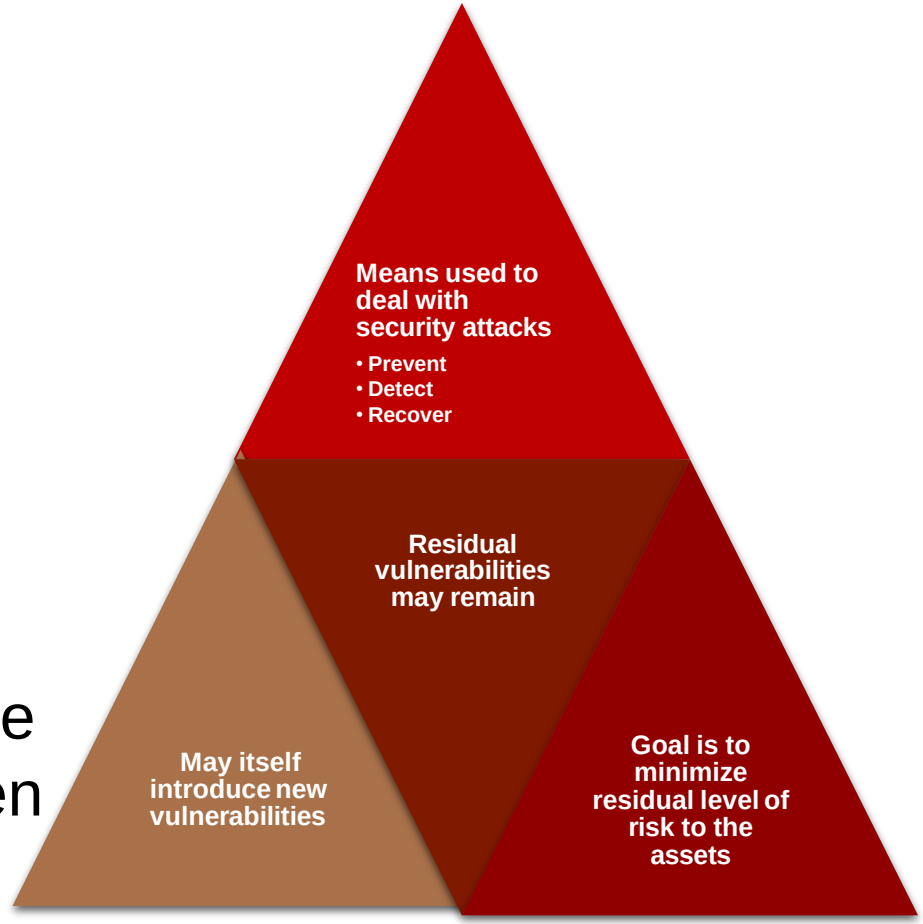
Figure 1.3 Defense in Depth and Attack Surface

DEFENCE IN DEPTH



Countermeasures

- **When is a countermeasure used? Before, during, or after an attack?**
  - Usually **during** an attack, but can be before
- A countermeasure is any means taken to deal with a security attack (pending or in progress).
- Ideally, a countermeasure can be devised to prevent a particular type of attack from succeeding. (See Kaspersky lab exercise)
- When **prevention** is not possible, or fails in some instance, the goal is to **detect** the attack and then **recover** from the effects of the attack



Active Learning Exercise (10 minutes)

- Read this short paper (4 pages) from Kaspersky Lab (2016)
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07184523/Descriptions_of_attacks_eng.pdf
- Read the phases of the 3 attack types and the countermeasures.
- What do you notice? Or what stands out to you?

- **Share your findings in class or in the week 2 discussion forum**

BREAK TIME?

BIA is next!

FANSHAWE

What is Contingency Planning?

- The overall process of preparing for unexpected events.
  - "If things don't happen the way we want them to, what is our backup?"
- The process by which the IT and InfoSec communities **prepare for, detect, react to, and recover from** events that threaten the security of information resources and assets, both human and natural.
- Main goal of CP is to **restore normal modes of operation** with **minimal cost and disruption to normal business activities** after an unexpected event.
  - get things back to the way they were as cheaply and quickly as possible

CP – Three Major Components

1. Business Impact Analysis (BIA)
2. Incident Response Plan (IR Plan)
3. Disaster Recovery Plan (DR Plan)

Introducing:
Business Impact Analysis

- Understanding the organisation that you protect
- Identify and quantify the value of assets
- Identify the risks to assets and how to avoid them
- Work out, *not guess*, how quickly each activity would need to be resumed in the event it is disrupted (despite DA efforts).

- The clue to what a BIA really is in the title:

Analysis of the impact on your business's assets.

Purpose of a BIA

The purpose of the BIA is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

- Helps the organization determine which business functions and information systems are the most critical to the success of the organization
- Process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency
- is an extension of the risk assessment process
- is considered to be the first stage of the contingency planning process
- cannot analyze impact unless we know what is affected (assets)

Goals of a BIA

1. Establish a solid foundation for your **planning** process
2. Meet **regulatory** and audit **requirements**
3. Garner **support** from upper management (build consensus for what is most important)
4. **Top ranked risk items** with plans to protect, assign, accept or eliminate the threat
5. Creation of a plan that uses the **outcome of the BIA to establish a priority for recovery**

Active Learning Exercise

Read the next 11 slides on Business Impact Analysis, then:

- Use your business as the context and create a scenario where a BIA needs to be conducted
- List the factors to consider when creating your BIA
- List the benefits and challenges to creating a BIA

- **Post your work on week 2's discussion forum**
  - *Don't forget to comment on the posts of others*

Business Impact Analysis, (contd.)

- BIA begins with the list of threats and vulnerabilities identified in the risk management process
  - Enhances the list by adding information needed to respond to the adversity
- When undertaking the BIA, an organization should consider the following:
  - *Asset & value*
  - *Threat*
  - *Risk & potential loss*
  - *Trigger*
  - *Probability*

Business Impact Analysis, (contd.)

- A BIA is conducted in **three stages**:
  1. Determine mission/business processes and recovery criticality **R C A** (recognition, classification, and assessment of risk)
  2. Identify *resource requirements*
  3. Identify recovery *priorities* for system resources

BIA – Stage 1

- Use RCA: Recognition, Classification, Assessment of risk (root cause analysis) & Application of methods
- **R**ecognition
  - Identify the Asset at Risk
  - Perform Business Impact Analysis

  Or if risks are not yet apparent:
  - Identify Potential Threat
  - Perform Business Impact Analysis on Asset(s) that would be at Risk

BIA – Stage 1, (contd.)

- **C**lassification
  - Identify Risks by category:
    - Risks to input
    - Risks to Output
    - Risks from business tools
    - Human risks
    - Natural Events
    - Technological Risks
    - Terrorism, accidents, cyber terrorism
- **A**ssessment of Risk – **A**pplication of methods
  - Probability
  - Impact

BIA – RCA: - Tools

- Matching Assessed Risk with Strategies
  - RISK is: the **likelihood** of the occurrence of a vulnerability multiplied by the **value** of the information asset minus the percentage of risk mitigated by **current controls** plus the uncertainty of current knowledge of the vulnerability.

- Risk Recognition
- Risk Typing & Categorization
- Systematically assign resources
- Identify Ownership & responsibility
- Prioritize Plan Type

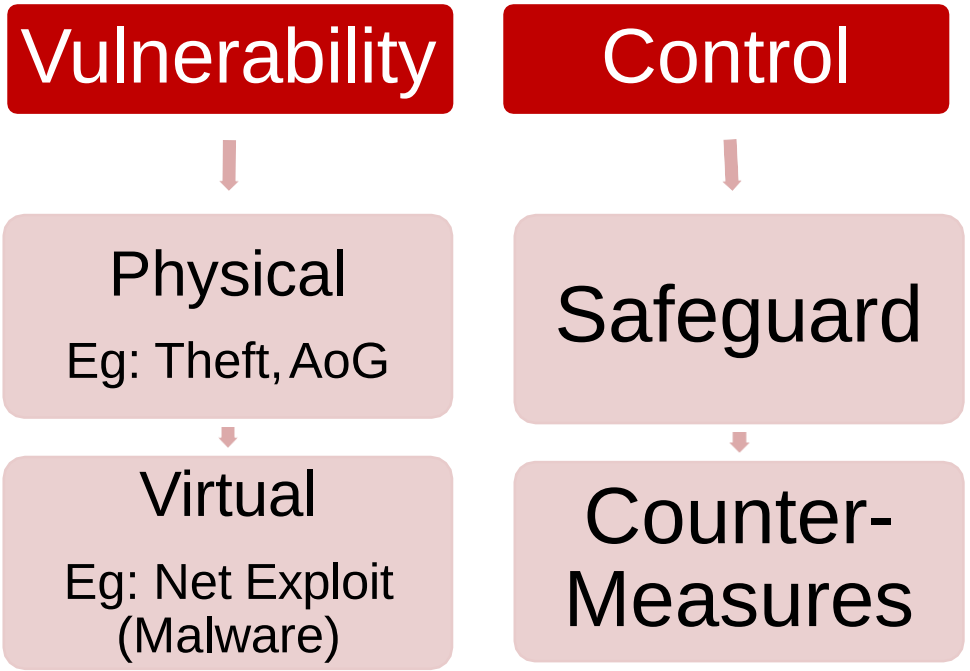
BIA – RCA: Recognize

- Typing or categorization
- Assign Resources
- Look for triggers in common
- Risk Control Strategy – once classified:
  - Avoidance
  - Transference
  - Mitigation
  - Acceptance

BIA – RCA: Categorize

- ICT Threats and Solutions
  - Categorization

InfoSec Hierarchy



BIA – RCA: **Assess/Apply**

- Come to an assessment conclusion
- Apply a methodology
- Assign Resources
- A solution using a system
- Get Information – like SWOT
- Use Information – like **C T F I T D**

  (Cost, Time, Fit, Implementation, Testing and Duration)

Business Impact Analysis

- Application of Methodologies – (e.g. SWOT, CTFITD)
- Answer Each Area
- Information Gathering
  - Surveys, Interviews, Scorecards, Existing Policy / Procedures, Targets, Health & Safety, History, Records
- Disaster Avoidance (DA)
  - Always cheaper and less disruptive
- Disaster Recovery (DR)
  - Always more costly, critical
- Both?
  - When DAP is not 100%

Business Impact Analysis

- **A**pplication of Methodologies – CTIFD
  - **CTFITD** = 6 Application Criteria
  - Costing
    - Acquisition
    - Replacement
    - Availability / Substitution
  - Timeline
    - When to start
    - Permanent or Temporary
    - Cycles
  - Fit
    - Technology
    - Personnel
    - Existing Process
    - Outsource

Business Impact Analysis

- CTFITD(cont'd)
  - **Implementation**
    - Strategy
    - Divide and conquer
    - Divest
  - **Testing**
    - Modeling
    - Historical data
    - Simulation
  - **Duration**
    - Devaluation curve
    - Generational adaptation / evolution
    - Environmental adaptation / evolution
    - Asset Replacement / Migration / Divestiture

Business Impact Analysis

- Disaster Avoidance
  - Always cheaper and less disruptive
- Disaster Recovery
  - Always more costly, critical
- Both?
  - DRP when DAP is not 100%
    - What is the ratio between Avoidance and Recovery?
  - Examine and compare to the InfoSec budget….
- Track details to prove the analysis.
  - BIA Template Worksheet

SampleBIA Template Worksheet

Name							INFO6027		Specific Details:							
ID				Date:			EXERCISE 1		Make, Model, Serial Number:							
									Configuration:							
Business Impact Analysis																
Risk ID	Threat	Asset Affected	Risk Description	Risk Type	Probability (High/Medium/Low)	Risk Impact (High/Medium/Low)	Primary Effect-(Cost of Downtime)	Trigger (Initial Cause)	Avoidance Plan	DAP to DRP Ratio (% avoided)	Incident Management Required	DR Process	Risk Owner	Status	Ranking	

- The BIA template is a generic form so it may not exactly fit your needs but you must complete as much as possible. When using the BIA template it may be necessary to extend the table by adding further rows / columns.
- The titles in bold relate to the BIA column headings and indicate the entries which (in most circumstances) should appear in those columns.
- **Threat:** indicate – system failure, theft, AOG, hack etc.
- **Probability:** risk type – risk to input, risk to output, risk from business tools, human risks, natural events, technological risks, terrorism, cyber terrorism.
- **Risk Impact: Low:** Continue to Function
- **Medium:** Function Impaired
- **High:** Not Functioning
- **Trigger –** if there is consistency consider addressing the trigger
- **Primary Effect:** Indicate – cost, scope schedule or quality.
- **Avoidance Plan:** Accept**,** Avoid, Transfer, Mitigate.
- **Incident Management:** Indicate – None, Contain, Eradicate, Recover.
- **DR Process:** Indicate – Replace Infrastructure, Retrain People, Recover Data.
- **Status:** Active, Future, Past.
- **Rank** – 1,2,3 – based on analyses criteria (cost, downtime, etc.)

Summary and Reminders

Summary:

- Risks, Threat, Vulnerabilities, Assets
- SWOT
- Risk Assessments
- BIA

Reminders

- **Assignment #1** (worth 10% of your grade) will be released this week
  - due in Week 3
- **Discussion Forum** posts for this week due by week 4
- **Next week** we will be discussing ITSM, ISO standards, Security Controls, and Policy