INFO6027
Information Security Planning

Week 4

FANSHAWE

HOUSEKEEPING… ☺

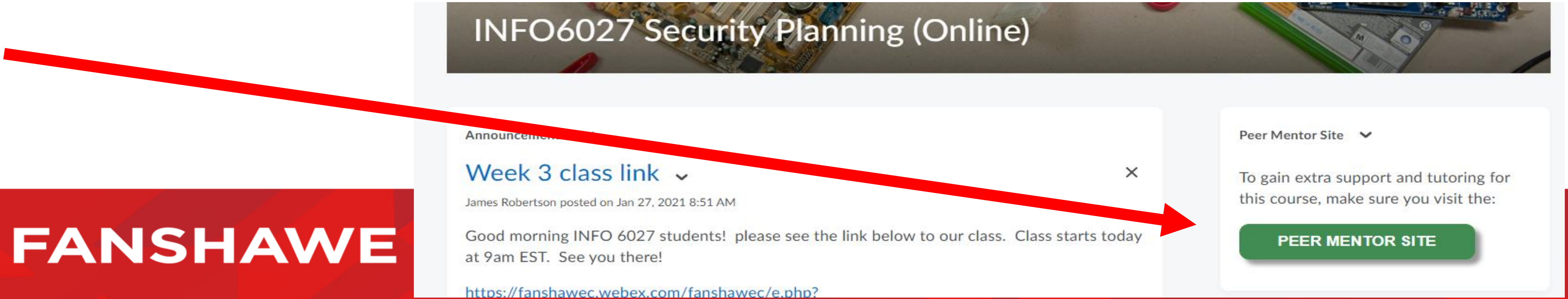
- Questions from last week? What do you think of assignment #1 so far?

- **Test 1** is Wednesday February 08 at 12:00 noon
  - Alternate test times are available to part-time students. Part-time students need to email me with their test times (preferably on Friday but we can discuss)
  - Test will cover the first four weeks textbook, tutorial, and assignments
  - May use a variety of questions. Ex. **Short/long answer**, multiple choice, true/false, fill-in-the-blanks, matching, etc.
    - Be strategic with your time during the test ☺
  - Uses **Respondus Lockdown Browser**, but is not Respondus Monitor
  - Test is NOT open book. No resources are permitted.
  - Make sure you have reliable internet and power (hard-wired is best)
  - **I mark each test manually**, so ignore any auto-graded marks at the end of the test.
- We will continue with week 6 lesson after the exam.

Peer Tutors

- The Peer Tutoring site is running, you will find scheduled sessions that you can attend but you can post a question at any time and the peer tutor will answer next time they are available. Please do not expect an instant response as everyone has many other commitments, which is why time management is so important - do not leave things to the last minute!

- I suggest you log into the site and take a look: ISM/NSA Peer Mentor Site (22S)
- This resource is for you so please make use of it.
  - Dedicated times for live chat, direct and private email correspondence, and it’s FREE!
  - Week 6 progress reports. If unsatisfactory you might consider PM’s as a resource for you.



INFO6027 Security Planning (Online)

Announcements

Week 3 class link

James Robertson posted on Jan 27, 2021 8:51 AM

Good morning INFO 6027 students! please see the link below to our class. Class starts today at 9am EST. See you there!

https://fanshawec.webex.com/fanshawec/e.php?

Peer Mentor Site

To gain extra support and tutoring for this course, make sure you visit the:

PEER MENTOR SITE

In the News

- Please check out:

- https://www.bloomberg.com/news/articles/2023-02-01/crypto-thefts-soared-to-record-3-8-billion-last-year-on-north-korea-hacks?srnd=technology-vp

- https://www.nist.gov/ This site has a wealth of information

- https://www.wired.com/category/security/

- https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

https://memegenerator.net/instance/61410383/drago-rocky-iv-that-man-is-like-a-piece-of-iron
https://www.britannica.com/biography/Jeff-Bezos

Agenda for this tutorial

Today we will be discussing

- Corporate and Security Governance
- **Incident** Management
  - ✓Types of Incidents, Incident Classification
  - ✓Incident Response
  - ✓Security Incident management Process
    - ✓Incident Response Teams (ex. CSIRT)
- Reminders and Test Review Exercise

Finishing off our discussion on BIA and decision-making

Determine Mission/Business Processes and Recovery Criticality

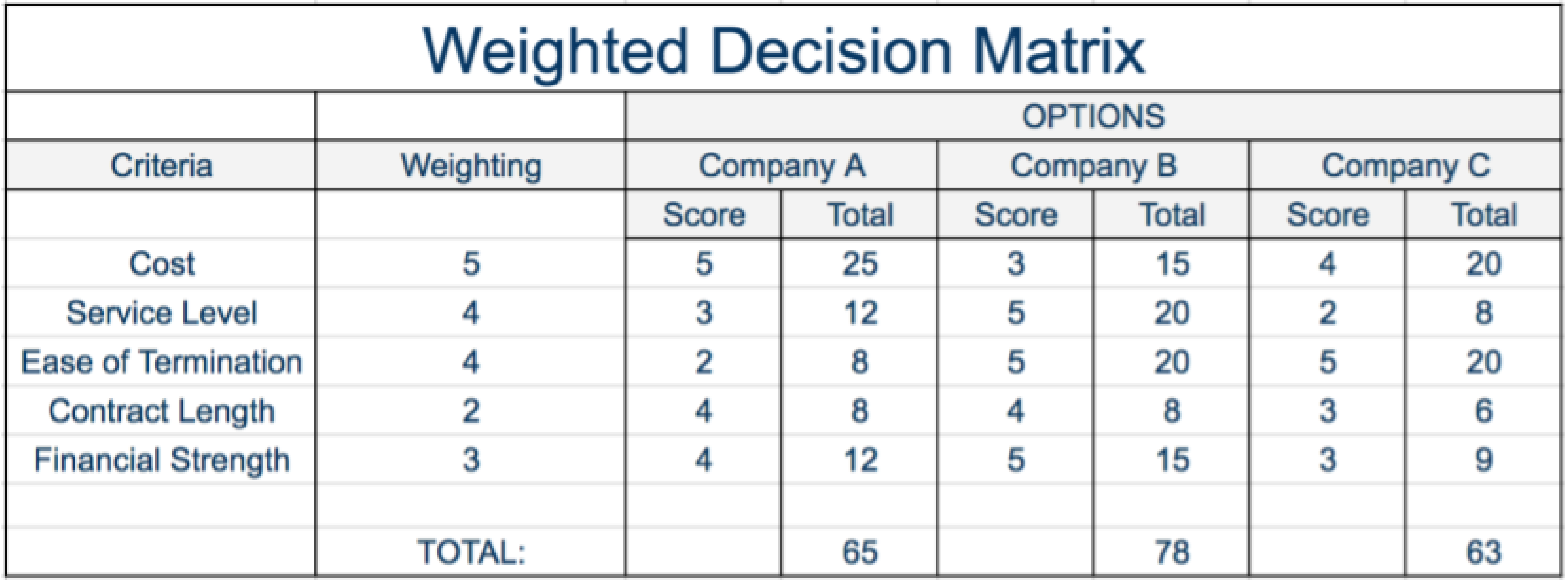
- The first major BIA task is to analyze and prioritize the organization’s **business processes** based on their relationship to the organization’s **mission**
  - Are business processes an “asset” to be protected?
- Each business department, unit, or division must be evaluated to determine **how important** its functions are to the organization as a whole
  - Ex. Is the IT department more important than the HR dept? Or payroll? Or custodial?
- The term “**mission/business process**” is used frequently throughout the textbook
  - Essentially describing a task performed by an organization (or organizational subunit) in support of the overall organization’s mission
- Avoid “**turf wars**” and focus on the selection of ***core business functions*** necessary for operations to continue

Determine Mission/Business Processes and Recovery Criticality

- A **weighted analysis table** can be useful in determining which business functions are most critical to the organization
  - Identify the categories ***that matter most*** to the organization
  - **What are some sample categories?**
    - **Ex. When you bought a car or planned a trip, which categories had more weight?**

- A useful tool in identifying and collecting information about business functions is a **BIA questionnaire (sample)**
  - Can be used to allow functional managers to enter:
    - Information about their functions
    - Impacts the functions have on the business (and other functions)
    - Dependencies that exist for the function from specific resources and outside service providers

Example of a Weighted Analysis Table



Weighted Decision Matrix

		OPTIONS					
Criteria	Weighting	Company A		Company B		Company C	
		Score	Total	Score	Total	Score	Total
Cost	5	5	25	3	15	4	20
Service Level	4	3	12	5	20	2	8
Ease of Termination	4	2	8	5	20	5	20
Contract Length	2	4	8	4	8	3	6
Financial Strength	3	4	12	5	15	3	9
	TOTAL:		65		78		63

https://expertprogrammanagement.com/2017/09/decision-matrix-analysis/

The Impact of Downtime on a Business (aka Recovery Criticality)

FANSHAWE

NIST Business Process and Recovery Criticality

Link: file:///C:/Users/James/Downloads/32482.pdf

Key Downtime Metrics:

Maximum Tolerable Downtime (MTD)

- total amount of time the system owner is willing to accept for a mission/business process outage or disruption
  - Ex. “We can only have these systems down for 4 hours per month before negatively affecting operations”

Recovery time objective (RTO) – also called MAD (maximum allowable downtime).

- Refers to the period of time within which systems, applications, or functions must be recovered after an outage.
  - Ex. “We can only be down for 3 hours after an incident before negatively affecting operations”

Recovery point objective (RPO)

- point in time, prior to a disruption or system outage, to which mission/business process data can be recovered after an outage. Basically “**the point where we can get back to**”.
  - Ex. “After an incident, we should only have to reload no more than 6 hours of data or processing to restore operations to current status after the most recent data backup is restored.”

NIST Business Process and Recovery Criticality (continued)

- **Work Recovery Time (WRT)** - amount of effort that is necessary to get the business function operational AFTER the technology element is recovered
  - *Second half of the MTD works with RTO to equal MTD (**MTD = RTO+WRT**)*
  - Can be added to the RTO to determine the realistic amount of elapsed time before a business function is back in useful service
- Total time needed to place the business function back in service?
- **(RTO) must be shorter than the MTD** (RTO < MTD**)**
- Must balance the cost of system inoperability against the cost of recovery
- **The higher the criticality, the shorter the MTD is likely to be**

Identify Resource Requirements

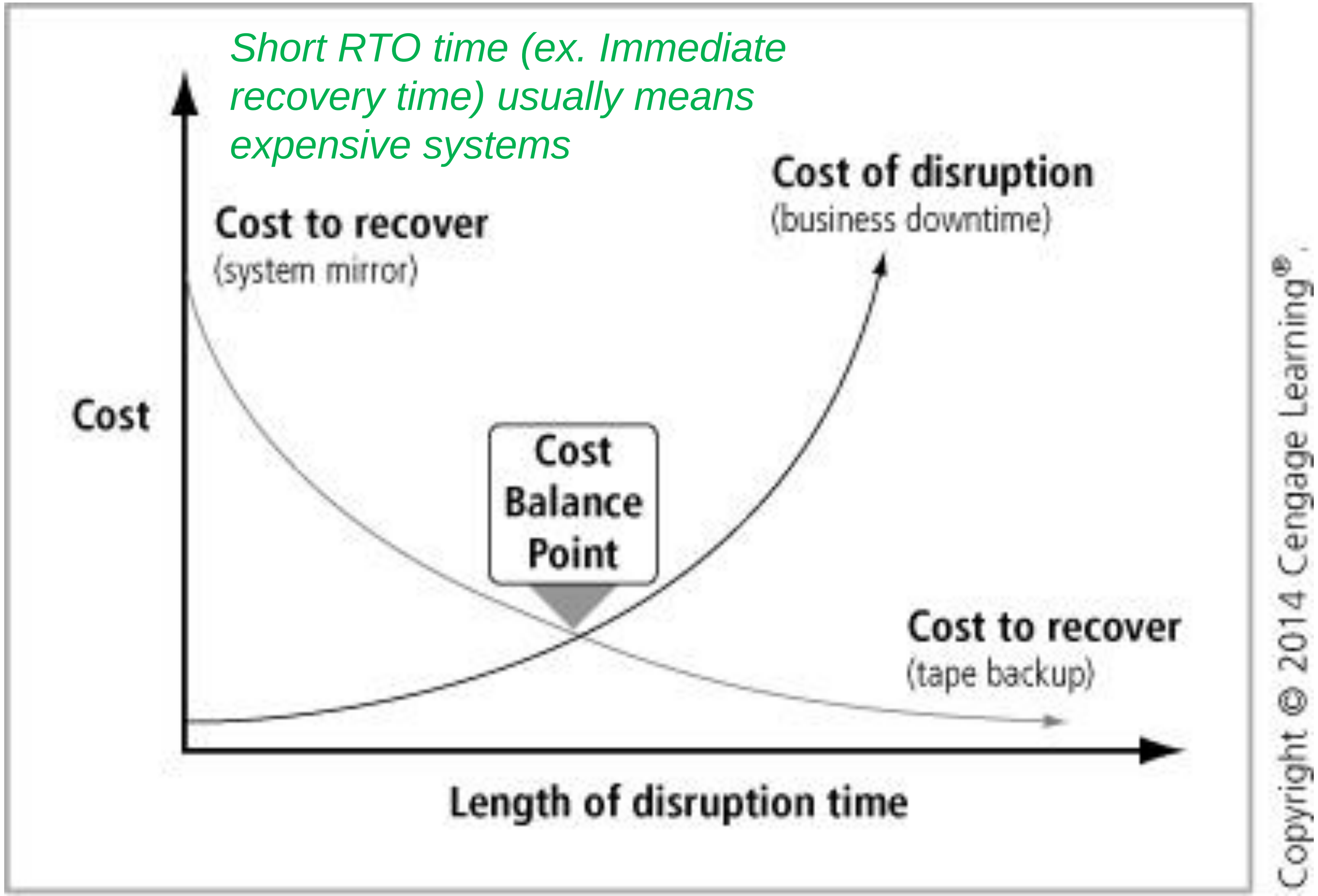
- Once the organization has created a prioritized list of mission/business processes, it can determine what resources would be needed to recover those processes and the assets associated with those processes
- Some processes are resource intensive (use a lot of resources)
  - Example: IT functions, payroll,
- An easy method for organizing this information is to put it into a **resource/component table**:

Mission/Business Process	Required Resource Component	Additional Resource Details	Description
Provide customer support	Helpdesk ticket management software	Server and database	X number of techs need simultaneous access…

Cost balancing

Note:

the longer the disruption, the more impact on/cost to the organization and it's operations



Short RTO time (ex. Immediate recovery time) usually means expensive systems

Copyright © 2014 Cengage Learning®.

Longer RTO means using a less expensive recovery systems

Cost of Downtime (COD)

Amazon lost 99M in 63 minutes (2018)

- The all-in cost of a general (overall) or specific (process) outage as measured in operational currency (dollars) over a specific unit of time (usually hours) e.g: “A total IT outage will cost $10,000 per hour”
- The COD calculation is most effective when all operational costs, lost profit and lost opportunity costs are captured and presented as a total number representing the loss to the organization or the business/process affected. THIS IS HARD TO DO!
  - Will require input from senior management:
    - Operations – idle facility costs
    - Human Resources – idle worker costs
    - Finance – lost profit or non-allocated incurred costs
    - Sales / Marketing – lost opportunity for future or existing revenues (relates to brand/reputation as well)

Rating your Recovery Time Objectives (RTO’s)

As you collect your impact data, you'll also need to begin determining the **recovery time objectives**. You may choose to create **a rating system** so you can quickly determine recovery time objectives.

- **Category 1**: Mission-Critical -- 0--12 hours
- **Category 2**: Vital -- 13--24 hours
- **Category 3**: Important -- 1--3 days
- **Category 4**: Minor -- more than 3 days

Smaller companies tend to have longer MTDs. For example, do you need to be back in two hours or will next business day be ok?

(**Hint:** It's within the BIA where you have to begin making these kinds of assessments).

Return on Investment (ROI)

ROI can be a challenge to calculate. <u>WHY?</u>

- Essentially means
  - “if I spend this much (the <u>*investment*</u>), I can make/save this much (the <u>*return*</u>)”
- ROI can be estimated as the money saved if the COD is not incurred less the cost of the avoidance (or mitigation ratio)
  - E.g.: ROI on buying a new $2,000 firewall would be $8,000 should the firewall prevent the affected COD of $10,000 for one hour of a calculated IT outage.
- ROI is commonly used as a management decision support tool when considering investments, budgets and financing business operations. Many managers have never considered or don’t understand the cost significance of their dependence on the continuous operation of IT assets that support organizational objectives or operations.
- Can be used as an <u>*effective security dept. financing positioning tool*</u> to assist senior management in understanding the value in investing in InfoSec resources.

Corporate and Security Governance

Corporate Governance

- Part of a robust InfoSec program (ISMS) is to ensure InfoSec is mapped to the business’s drivers, ***legal and regulatory requirements***, and threat profile.
  - *Requires upper management involvement*

“Information security governance is all of the tools, personnel and business processes that ensure that security is carried out to meet an organization's specific needs.”

- Governance is the formal means by which senior management **discharges its responsibilities** which include delivering value and the need to manage risk in all its forms.

Popular Areas of InfoSec Governance

- Organizational Structure
- Policy
- Risk Management
- Performance Measurement
- Reporting (Auditing)
- Regulatory Compliance
- Strategic Planning
- Roles and Responsibilities

The Governance Environment

Governance takes place in the organizational environment that is determined by existing conditions and circumstances that include:

- Federal and state/provincial laws, directives, and guidelines
- Industry regulations and governance practices
- Organization mission and strategies (mission, vision, and strategic plans)
- Organization ethics, culture, and values
- Organization risk tolerance
- Organization locations and management approach to locations
  - centralised or decentralised
- Organization policies, standards, processes, and procedures
- Organization roles and responsibilities
- Organization plans and reporting
- Organization monitoring for compliance (Auditing)

The 5 Governance Domains

The domains in the IT governance framework are:

1. **IT Strategic planning and alignment** — the forethought and capabilities necessary to deliver organisational value.
2. **Value delivery** — generating the benefits promised on time and within budget.
3. **IT Risk management** — a continuous process that starts with identification of risk (threats and vulnerabilities) and their impact on assets, mitigation of the risk by countermeasures, and the formal acceptance of the residual risk by management.
4. **IT Resource management** — deploying the right capabilities (people, facilities, hardware, software, etc.) to satisfy organisational needs.
5. **IT Performance measurement** — providing feedback the organisation needs to stay on track or take timely corrective measures.

The Principles of Governance

- Clear expectations
- Clear values
- Explicit policies and standards
- Strong communication
- Clear strategy
- Proactive change management
- Timely and accurate disclosures
- Independent review and continuous improvement

- Responsible and clear handling of operations
  - Competent organizational structure
  - Clearly defined roles and responsibilities
  - Orderly processes and procedures
  - Effective use of technology
  - Responsible asset management

Security Governance Activities

Enterprise security governance activities involve the **development, institutionalization, assessment and improvement** of an organization's enterprise risk management (ERM) and security policies.

Governance of enterprise security includes determining how various business units, personnel, executives and staff should **work together** to **protect** an organization's **digital assets**, ensure **data loss** prevention and protect the organisation's **public reputation**.

Enterprise security governance activities should be consistent with the organization's compliance requirements, **culture** and management policies. The development and sustainment of enterprise security governance often involves conducting threat, vulnerability and risk analyses tests that are specific to the company's industry.

https://www.entrepreneur.com/article/249293

Enterprise Security Governance (CISO perspective)

Enterprise security governance is a *company's* ***strategy*** *for* ***reducing the risk*** of unauthorized access to information technology systems and data. A CISO’s responsibilities must include **convincing executives to take an active role** in security governance.

“60% of those surveyed did not get regular reports about security risks or participate in security governance”

http://searchsecurity.techtarget.com/tip/CISO-responsibilities-Commit-senior-management-to-security-governance

Enterprise **Security** Governance

Enterprise security governance is a company's strategy for reducing the chance that physical assets owned by the company can be stolen or damaged.

In this context, governance of enterprise security **includes physical barriers**, locks, fencing and fire response systems as well as lighting, intrusion detection systems, alarms and cameras. **(CPTED, anyone?)**

- Also requires an intentional focus on future risks from new technologies and human threats.
  - E.g.: Surveillance Drones have become prevalent in just a few years? They are inexpensive and easy to operate. What relevance is becoming apparent? (now we also have to look up!)
  - **Another example could be the trend towards working from home, working when you want to, etc.**

Drivers for Implementing Corporate Governance

- **Business Requirements**
  - ISO27001
  - PCI DSS (Payment Card Industry – Data Security Standards)
  - Business Continuity
- **Regulatory Requirements**
  - PIPEDA – Canadian Privacy Act
  - SOX – Sarbanes Oxley Act (Corporations accounting activities - ex. Enron Scandal)
  - HIPAA – Health Insurance Portability and Accountability Act (1996)
  - GDPR (2018)
- **Various Frameworks & Standards**
  - ISO 27001 - security
  - ISO 38500 - IT governance
  - BS10012 - Data Privacy
  - ISO 22301 or BS 25999 – Business Continuity
  - GDPR (2018) – handling digital information linked to a person

Incident Management

What is incident management?

Incident management refers to the generic **process** followed by organizations when managing a wide variety of incidents. Regardless of the unique attributes of different types of incidents, fundamentally, the same high level processes can be followed to deal with them, involving steps to:

1. Identify what happened and determine the implications
2. Limit the effects of the incident and then eliminate its cause
3. Recover from the incident and resume normal business operation
4. Review the incident to help prevent recurrence.

ISO 27035 - Information security incident management

Incidents are bound to happen since preventive controls may not be totally reliable, effective, or **comprehensive**.

- Managing incidents effectively involves detective and corrective controls designed to:
  - minimize adverse impacts,
  - gather forensic evidence (where applicable) and
  - ‘learn the lessons’ in terms of prompting improvements to the ISMS.

Information security incidents commonly involve the exploitation of previously unrecognised and/or uncontrolled vulnerabilities, hence **vulnerability management**

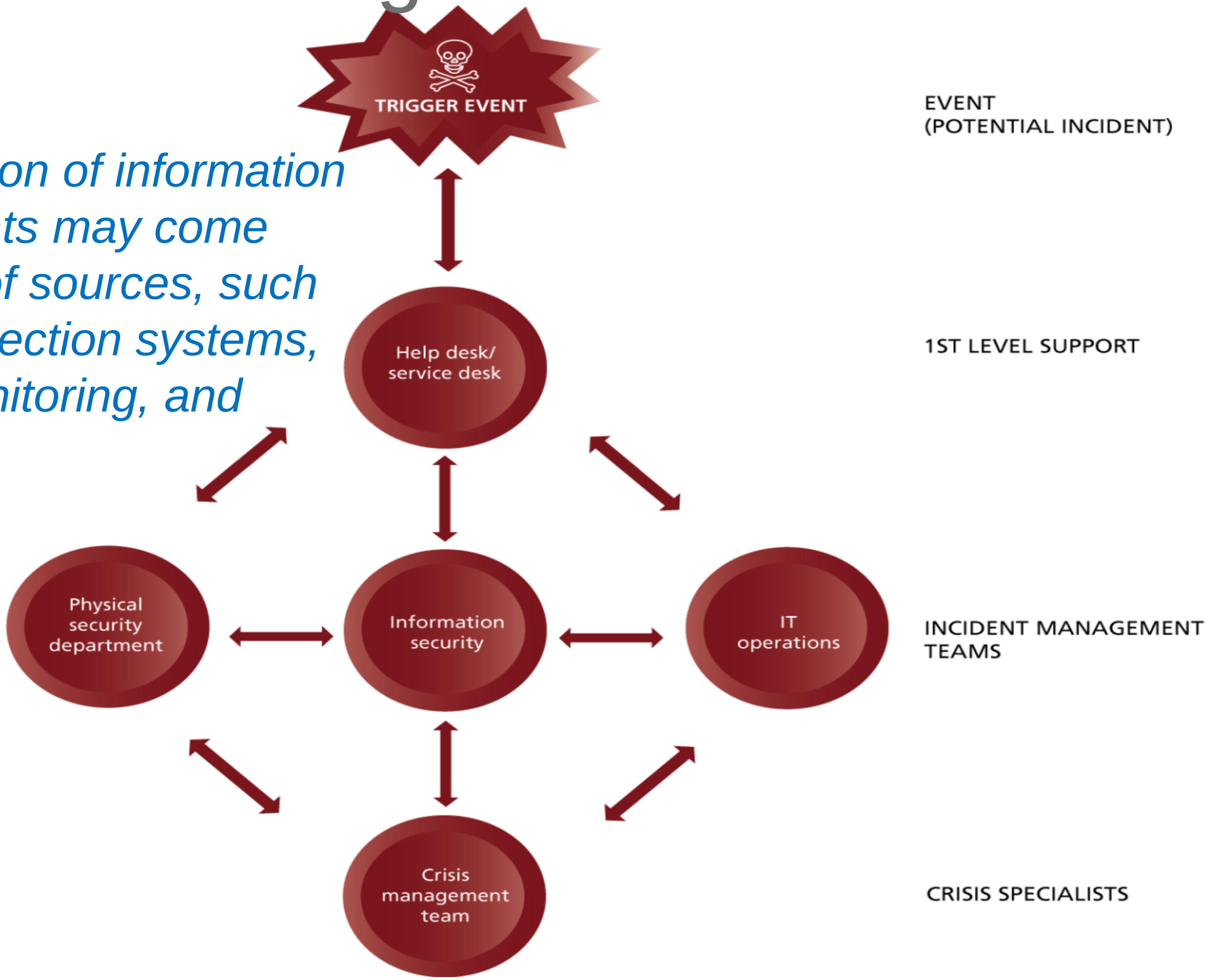
The standard covers the **processes** for managing information security **events, incidents and vulnerabilities**. The standard expands on the information security incident management section of ISO/IEC 27002.

https://www.iso27001security.com/html/27035.html

What is incident management ?

- In order to deal with this process an organizational <u>structure of teams must be established</u>.
- Efficient <u>interaction between these teams is vital</u> in effectively resolving incidents.

Note: Notification of information security incidents may come from a variety of sources, such as intrusion detection systems, IT systems monitoring, and customers



*Nc
Nc
in
in
a
as
sy
m
cu*

Detecting Incidents

Incidents may be detected by users or administration staff…

- Staff should be encouraged **AND TRAINED** to make reports of system malfunctions or anomalous behaviors

…or Automated tools

- System integrity verification tools
- Log analysis tools
- Network and host intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)

The Need for Incident Management

- The key reasons why organisations need an **information security incident management** capability include:
  - Increasing frequency and impact of information security incidents
  - Limitations of conventional information security controls
  - Mounting pressure to meet legal and regulatory requirements.

- Despite the widespread improvement in information security controls, information security incidents **continue to occur**, often **causing significant business disruption and serious business impact**.
  - **WHY?**

Events and Incidents

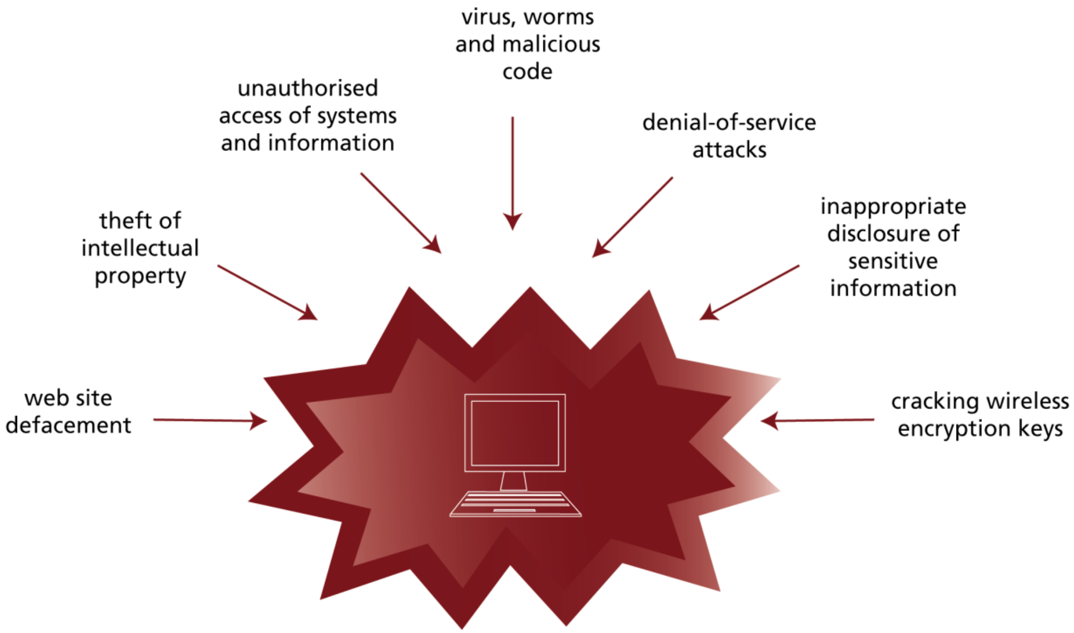
- A security ***event*** is an observable occurrence in a system or network.
  - user connecting to a file share,
  - a user sending electronic mail,
  - a firewall blocking a connection attempt, etc.

- A security ***incident*** is a violation or imminent threat to computer security policies, acceptable use policies or standards (i.e.: denial of service, malicious code, unauthorized access, inappropriate uses etc. ***Involves an "unplanned interruption" of IT services. Implies some level of harm or unwanted outcome.***

What is an **information security** incident?

- People interpret and define the term ‘information security incident’ differently. Some variations of the term used include:
  - incident
  - security incident
  - information security incident
  - computer security incident.

  The term can be defined as:



virus, worms and malicious code

unauthorised access of systems and information

denial-of-service attacks

theft of intellectual property

inappropriate disclosure of sensitive information

web site defacement

cracking wireless encryption keys

“an event (or chain of events) that compromises the confidentiality, integrity or availability of business information.”

https://www.citicus.com/sites/default/files/citicus_one_risk_glossary.pdf

Incident Response

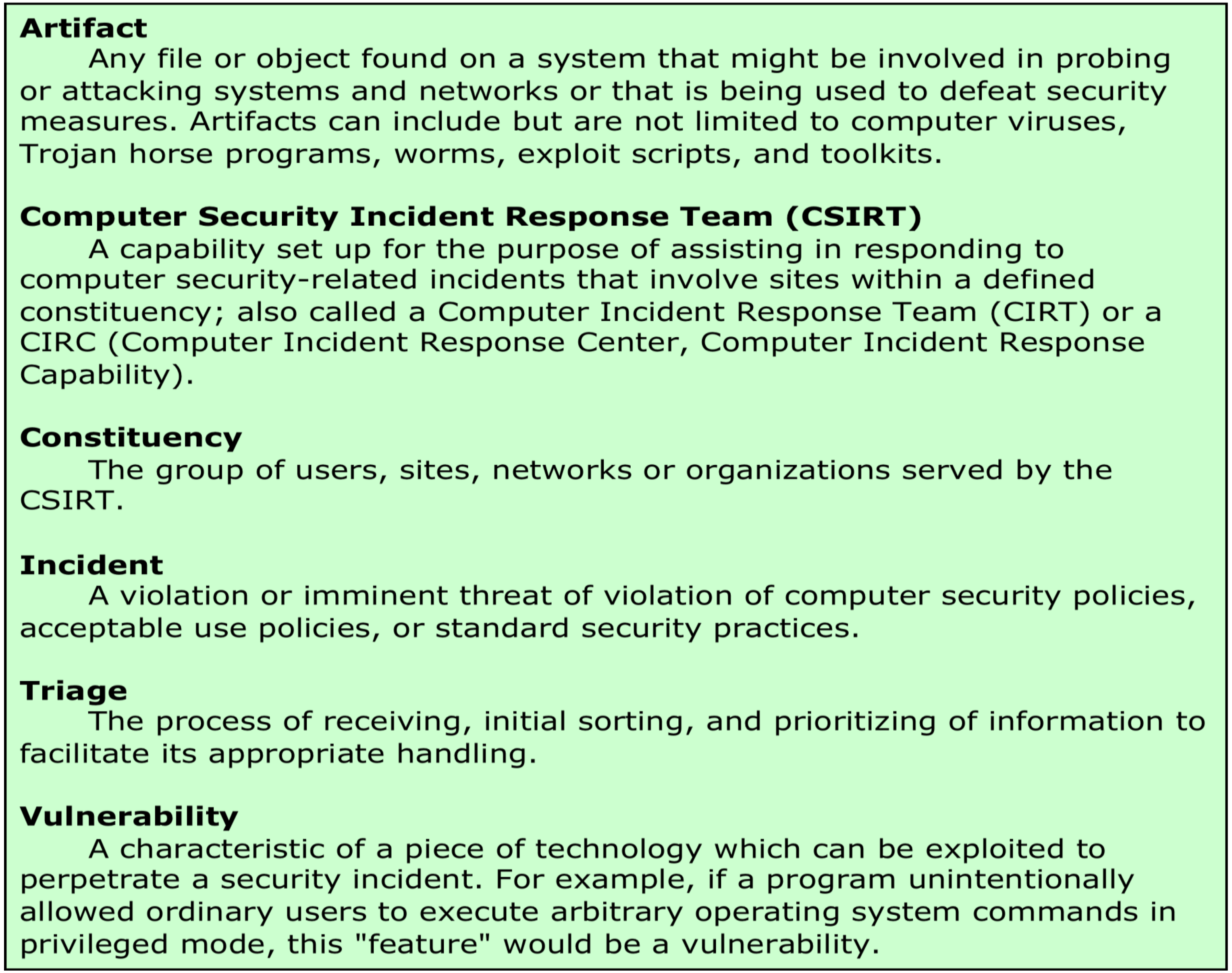
Security Incident **Response**

- Response procedures to incidents are an essential control for most organizations
  - **Procedures** need to reflect possible consequences of an incident on the organization and allow for a suitable response
  - Developing procedures in advance can help avoid panic.
  - **Why do we need procedures? Isn't training enough?**

- **What are some benefits of having incident response capability?**
  - Systematic incident response
  - Quicker recovery to minimize loss, theft, disruption of service
  - Use information gained during incident handling to better prepare for future incidents
  - Dealing properly with legal issues that may arise during incidents

Table 17.2

Key terms related to computer security incident response.



Artifact

Any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Computer Security Incident Response Team (CSIRT)

A capability set up for the purpose of assisting in responding to computer security-related incidents that involve sites within a defined constituency; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Constituency

The group of users, sites, networks or organizations served by the CSIRT.

Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Triage

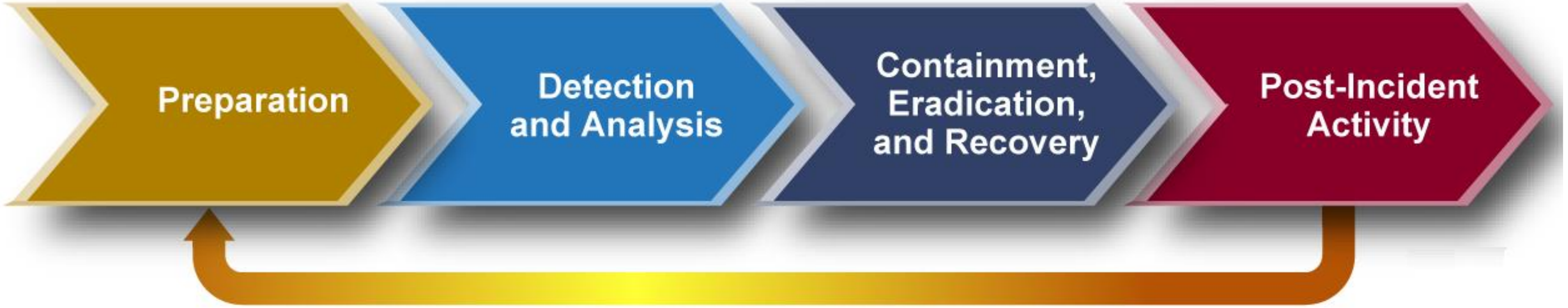
The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.

Vulnerability

A characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program unintentionally allowed ordinary users to execute arbitrary operating system commands in privileged mode, this "feature" would be a vulnerability.

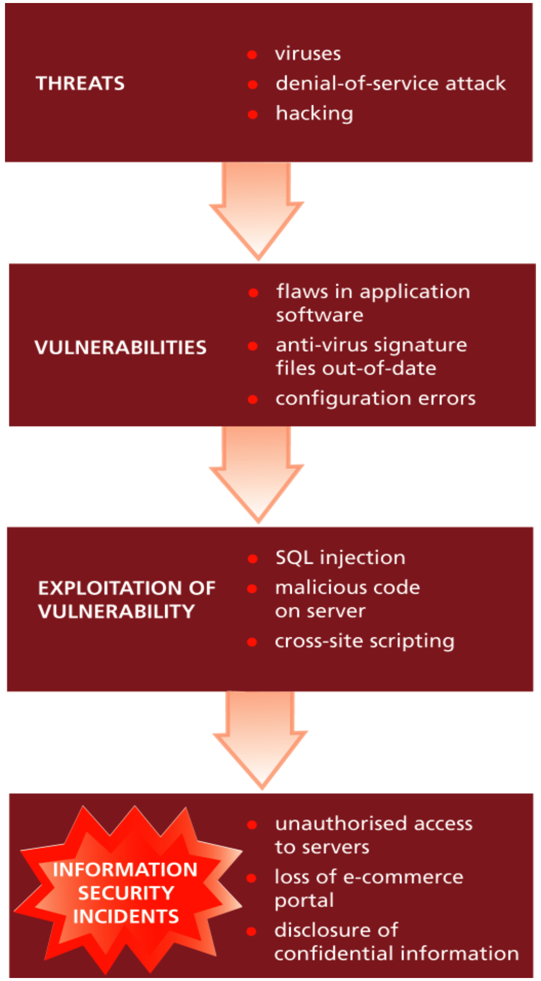
Incident Response

- Organisation should have an incident response **policy** and supporting **processes**:



Limitations of conventional security controls

- Organisations are subject to a range of factors which increase the likelihood of serious information security incidents occurring. These include the:
  - evolution of threats (eg due to new variants of worms and viruses)
  - increase in vulnerabilities (eg due to flawed software)
  - failure of technical security controls (eg due to errors in installation).



THREATS
- viruses
- denial-of-service attack
- hacking

VULNERABILITIES
- flaws in application software
- anti-virus signature files out-of-date
- configuration errors

EXPLOITATION OF VULNERABILITY
- SQL injection
- malicious code on server
- cross-site scripting

INFORMATION SECURITY INCIDENTS
- unauthorised access to servers
- loss of e-commerce portal
- disclosure of confidential information

Legal and Regulatory Drivers

- **An increase in legal and regulatory pressure** and focus on compliance have become drivers for organisations to improve their information security incident management capability.
- Examples of legislation and regulation that have implications for information security incident management include the:

  - PIPEDA, Personal Information Protection and Electronic Documents Act
  - US Federal Information Security Management Act (FISMA)
  - California Security Breach Information Act (SB-1386)
  - US Health Insurance Portability and Accountability Act (HIPAA)
  - International Convergence of Capital Measurement and Capital Standards (Basel II).
  - PCI DSS, Payment Card Industry Data Security Standard

Types of incidents

- Managing information security incidents is a **complex** undertaking
- Organizations experience a wide range of incidents that can affect the smooth operation of critical business processes and result in significant business impact.
- *Incidents can occur in many different parts of the organisation* and include:

  - **operational incidents** (eg failure of production systems)
  - **environmental incidents** (eg storm damage and flooding)
  - **IT-related incidents** (eg hardware failure or application error)
  - **information security incidents** (eg denial-of-service attacks, enterprise-wide virus infections and misuse of computer equipment).

Triage Function – What does it mean to “triage”?

Goal:

- Ensure that all information destined for the incident handling service is channeled through a single focal point
- Commonly achieved by advertising the triage function as the single point of contact for the whole incident handling service

Responds to incoming information by:

- Requesting additional information in order to categorize the incident
- Notifying the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability
- Identifies the incident as either new or part of an ongoing incident and passes this information on to the incident handling response function

Incident Response Capability

Establishing an incident response capability requires commitment of resources and should include the following actions:

- ✓Creating an incident response policy and plan
- ✓Developing procedures for performing incident handling and reporting
- ✓Setting guidelines for communicating with outside parties regarding incidents
- ✓Selecting a team structure and staffing model
- ✓Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- ✓Determining what services the incident response team should provide
- ✓Staffing and training the incident response team.

Common Attack Vectors

Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

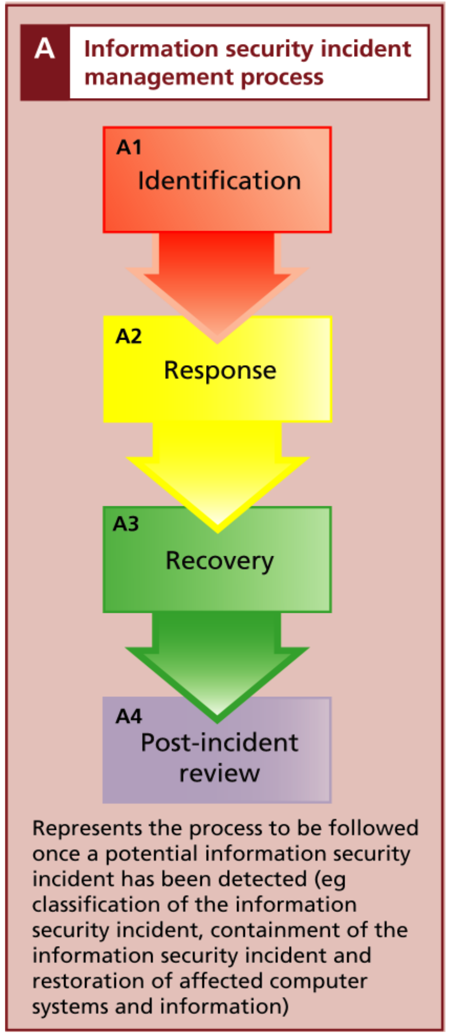
- **External/Removable Media:** An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- **Web:** An attack executed from a website or web-based application.
- **Email:** An attack executed via an email message or attachment.
- **Improper Usage:** Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- **Other:** An attack that does not fit into any of the other categories.

Incident Management in **Information Security**

FANSHAWE

What is information security incident management?

- Information security incident management is similar to the generic incident management process, but with **specific activities that are unique to information security incidents**, such as, analysing log files and conducting root-cause analysis.
- The information security incident management process typically commences following the detection of an event referred to as the ***trigger event***.



Represents the process to be followed once a potential information security incident has been detected (eg classification of the information security incident, containment of the information security incident and restoration of affected computer systems and information)

Key components of an information security incident management capability

- There are five key components which need to be addressed to establish an effective information security incident management capability.

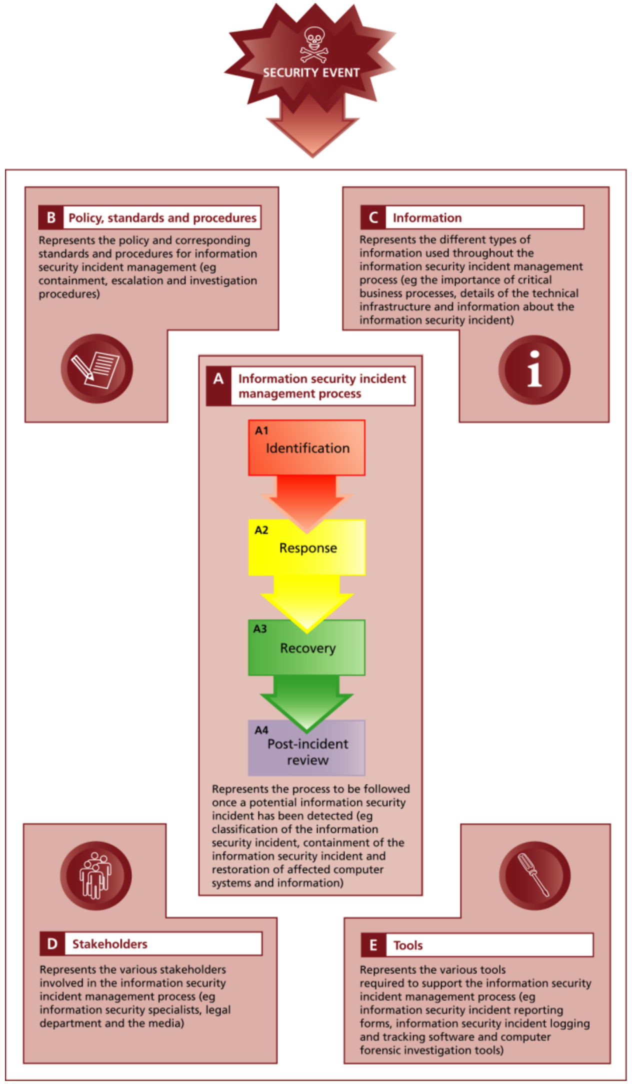
A Information security incident management process

B Policy, standards and procedures

C Information

D Stakeholders

E Tools



B Policy, standards and procedures: Represents the policy and corresponding standards and procedures for information security incident management (eg containment, escalation and investigation procedures)

C Information: Represents the different types of information used throughout the information security incident management process (eg the importance of critical business processes, details of the technical infrastructure and information about the information security incident)

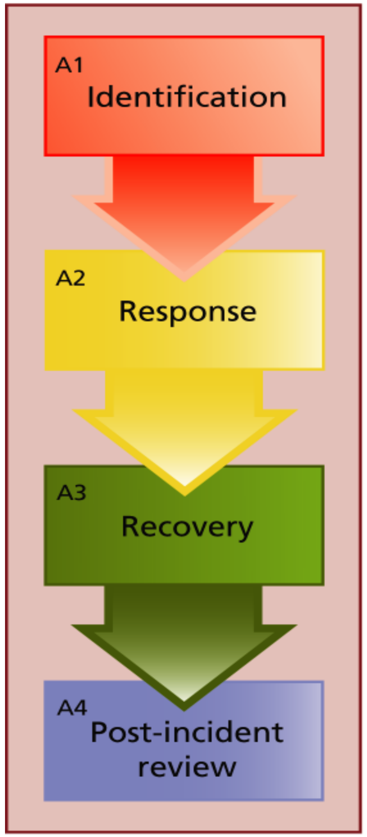
A Information security incident management process: Represents the process to be followed once a potential information security incident has been detected (eg classification of the information security incident, containment of the information security incident and restoration of affected computer systems and information)

D Stakeholders: Represents the various stakeholders involved in the information security incident management process (eg information security specialists, legal department and the media)

E Tools: Represents the various tools required to support the information security incident management process (eg information security incident reporting forms, information security incident logging and tracking software and computer forensic investigation tools)

The information security incident management process

- The information security incident management process is the main component in the information security incident management capability.



Typically involves determining if an event is actually an information security incident, performing an assessment of the impact on the business, and categorisation/ classification of the information security incident.

Includes activities such as the mobilising of information security specialists, containment of the information security incident, escalation to other parties and elimination of the cause of the information security incident.

Typically involves restoration and testing of affected computer systems, applications and data in order to resume normal business operations.

Includes activities such as review of the information security incident management process, root cause analysis and forensic investigation of the information security incident plus the production of a post-incident report for top-level management.

The information security incident management process

Identification

- The Identification stage is typically triggered following the detection of a potential information security incident.
- The primary objective of the Identification stage is to **determine whether an information security incident has occurred**.
- A wide variety of information is gathered and assessed (often referred to as **triage**) to:
  - understand the type of information security incident that has occurred (eg defacement of a web site)
  - determine the actual and potential impact to the organisation (eg major impact to production systems)
  - identify and prioritise the necessary incident management activities (eg mobilise the information security incident management team).

The information security incident management process

Response

- The Response stage is triggered following the positive identification of an information security incident (eg virus infection across the network or unauthorised access to server).
- The Response stage involves various internal (eg IT, HR, legal) and external (eg the media, law enforcement agencies) stakeholders in order to help resolve the information security incident.
- Containment is a critical activity and is a method of **isolating the area affected by the information security incident to prevent further damage** to the infrastructure and the organisation.
- Eliminating the cause of an information security incident typically involves a combination of disabling the **threat** (eg removing the method of access used by an attacker) and fixing **vulnerabilities** exploited by an attacker.

The information security incident management process

Recovery

- The start of the Recovery stage typically coincides with the end of the Response stage.
- The Recovery stage primarily involves the steps required to **resume normal business operations** (i.e. return the computer systems, applications and data to their state prior to the information security incident).
- The Recovery stage typically includes the individuals responsible for maintaining the infrastructure (e.g. system administrators, network engineers, IT operations personnel) who perform many of the required recovery tasks, such as regaining network connectivity, rebuilding systems and applications, and restoring data.
- Once all systems, applications and data affected by the information security incident have been restored and normal business operations have resumed the information security incident can be **closed**.

The information security incident management process

Post Incident review

- The Post-incident review stage follows the recovery from and closure of an information security incident. It can consist of a range of activities to:
  - support **follow-up action** (eg performing forensic investigations to support legal action)
  - help the organisation **understand more** about the information security incident (eg performing a root-cause analysis)
  - **identify areas for improvement** in both the information security incident management process (eg better communication required) and the information security arrangements (eg more event log information required).
- Post incident review provides a valuable opportunity for organisations to **learn lessons about the strengths and weaknesses of their information security** arrangements and therefore, make necessary improvements.

Computer Security Incident Response Team (CSIRT)

For large and medium-sized organizations, a computer security incident response team (CSIRT) is responsible for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

CSIRTs are responsible for:

- **Rapidly detecting incidents**
- **Minimizing loss and destruction**
- **Mitigating the weaknesses that were exploited**
- **Restoring computing services**

Information Security Incident Response Team

Central Incident Response Team.

- Single incident response team handles incidents throughout the organization. Effective for small organizations and those with minimal geographic diversity in terms of computing resources.

Distributed Incident Response Teams.

- The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. Effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility).
- Teams should be part of a single coordinated entity so that the incident response process is consistent across the organization and information is shared among teams.

Coordinating Team.

- An incident response team provides advice to other teams without having authority over those teams—e.g. a department wide team may assist individual agencies' teams.

Information Security Incident Response Team

Staffing models:

Employees.

The organization performs all of its incident response work, with limited technical and administrative support from contractors.

Partially Outsourced.

The organization outsources portions of its incident response work.

Generally organisations outsource 24-hours-a-day, 7-days-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite Managed Security Services Provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization’s incident response team.

Fully Outsourced.

The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organisation needs a full-time, onsite incident response team but does not have enough available, qualified employees.

Information Security Incident Response Team

Structure

- An incident response team should be available for anyone who discovers or suspects that an incident involving the organization has occurred.
- One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident.
- The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services.
- Success depends on the participation and cooperation of individuals throughout the organization..

Benefits of Having an Incident Response Team

Help personnel recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services.

Information gathered during the incident can be used to be better prepared for future incidents and will assist in providing stronger protection for systems and data

Allows the organization to deal properly with legal issues that may arise during incidents

Incident Classification

Although all security incidents must be reported and responded to, not every security incident will require corrective action.

Some security incidents will require an immediate attempt at resolution, while others may require an acknowledgement that the incident has occurred.

Ranking Security Incidents

RANKING	The security incident is……
High	An immediate threat to a production environment, or any classified (non-public) information
Medium	Not immediate threat to a production environment, but it may become one if it is not resolved
Low	More of an inconvenience or an event determined as suspicious activity. Further monitoring is required, but a resolution is not needed at present

Examples of Security Incident Rankings:

HIGH	MEDIUM	LOW
Malicious code (virus, worm, Trojan, etc.)	Unauthorized network scans (internal)	Unauthorized network scans (external)
Unauthorized external access	Unauthorized internal access	Multiple failed logon attempts
Production environment down	Unauthorized use of network or security tools	Attempted access by suspended account
Perimeter security breach	Unauthorized file stores	Access by dormant accounts
	Downgraded performance	
	Tampering with log files	
	System or network access changes	

Documenting Incidents

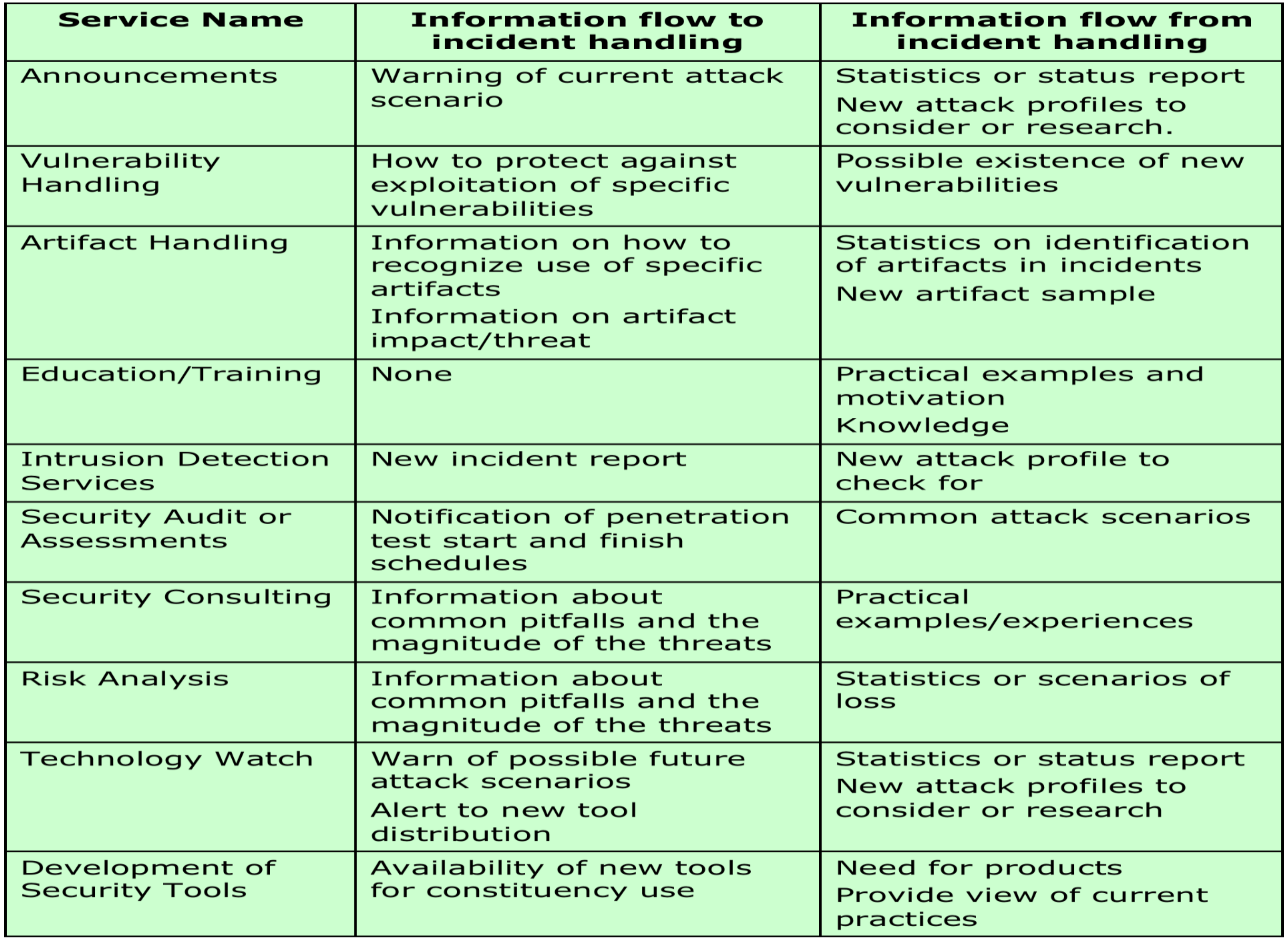
Documentation should be done **immediately** following a response to an incident

- Identify **what vulnerability** led to its occurrence.
- How this might be addressed to **prevent** the incident in the future.
- Details of the incident and the **response taken**.
- **Impact** on the organization’s systems and their risk profile.

- Why “immediately”? Why not after a couple of days when things settle down?

Table 17.3

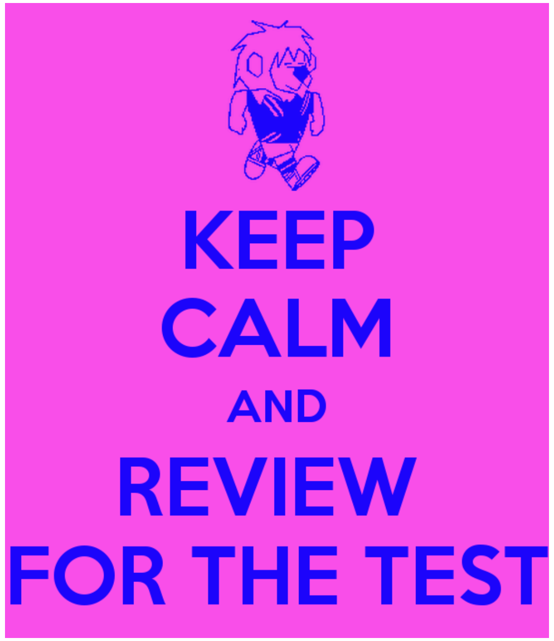
Examples of Possible Information Flow to and from the Incident Handling Service



Service Name	Information flow to incident handling	Information flow from incident handling
Announcements	Warning of current attack scenario	Statistics or status report New attack profiles to consider or research.
Vulnerability Handling	How to protect against exploitation of specific vulnerabilities	Possible existence of new vulnerabilities
Artifact Handling	Information on how to recognize use of specific artifacts Information on artifact impact/threat	Statistics on identification of artifacts in incidents New artifact sample
Education/Training	None	Practical examples and motivation Knowledge
Intrusion Detection Services	New incident report	New attack profile to check for
Security Audit or Assessments	Notification of penetration test start and finish schedules	Common attack scenarios
Security Consulting	Information about common pitfalls and the magnitude of the threats	Practical examples/experiences
Risk Analysis	Information about common pitfalls and the magnitude of the threats	Statistics or scenarios of loss
Technology Watch	Warn of possible future attack scenarios Alert to new tool distribution	Statistics or status report New attack profiles to consider or research
Development of Security Tools	Availability of new tools for constituency use	Need for products Provide view of current practices

Ready for Quiz Review?

https://forms.gle/FCTHyyvPMWtCHYcTA



© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
search ID: rman10110
"You have to *study* for tests,
dummy — you can't just put
a memory stick in your ear!"