INFO6027 S2022:
Information Security Planning

Week 7: Data Protection and Restoration

FANSHAWE

Housekeeping

- Test #2 (15%) is in week 10 (March 15th) during our normal tutorial time
  - If you are part time or studying abroad, **you may request an alternate test time 48 hours in advance**. Test **will use Respondus Monitor**

- Mid term grades have been submitted (either an S or a U)
  - Reminder about peer tutors (FOL, email, live sessions)

In the News…

- https://www.wired.com/story/godaddy-hacked-3-years/
- https://www.npr.org/2023/02/28/1160112051/hackers-steal-sensitive-law-enforcement-data-in-a-breach-of-the-u-s-marshals-ser

Agenda for today - Lesson 7

Data Protection & Restoration

- Containment Issues
- Network Infrastructure
- Backup Strategies
- Backup Technologies
- Location, Location, Location
- Restoration Protocols
- Testing , Planning, Documentation
- Chaos Theory
- Offsite Storage

BCM and BCP

Disaster Recovery Process

Data – what are *they*?

- Distinct **pieces of information** that have been translated into a form that are more convenient to move or process.
- Information converted into binary digital form
- The main content of a transmission unit
- *Digitally-encoded information*
- in science, data are a gathered body of facts and stats
- Data is a collection of facts, such as numbers, words, measurements, observations or even just descriptions of things
- **Data is the plural** of *datum*, a single piece of information
- Symbols or signals that are input, stored, and processed by a computer, for output as usable information.

Where are all the Data? (Are data an asset?)

Where is all the data? Where is it being made/stored?

- Corporate
  - Servers – In house / Branch Office / Hosted (be selective here!)
    - “off-book servers” (issues with backup, failures, IT security, patching, specifications, maintenance, etc)
    - Often unreported – even when you ask!
  - Clients – Desktops / Laptops
  - Portable data – any Personally Identifiable Information (PII) on the local machine?
  - Shared / Partnership
  - Suppliers – Lawyers, Accountants, Contractors
  - Non-Digital / Historical
  - Data Mining suppliers – “Big Data” analytics that draw conclusions through the analysis of data
- Non-Corporate
  - Marketing / Advertising
  - Social Networking
  - Blogs / Customer Forums

Do any of these numbers surprise you?

1.0 Data Containment Issues

Containment Issues

- Corporate Data
  - Moved off network
  - Created off-network
  - Flash drives, PDAs, Chips, Digital Recorders
- Personal Data
  - Facilitate, don't Integrate
  - Segregation
- Contamination

Containment *is "the action of keeping something harmful under control or within limits."*

Contamination *is "the unwanted pollution of something by another substance."*

2.0 Data Protection: Network Infrastructure

Network Infrastructure

- LAN based – how to protect data travelling on LAN connected infrastructure?
- WAN based – how to protect data travelling on WAN connected infrastructure?
- Does public access = need for encryption? Other tools?
- Document Management Systems – hard and soft copies
- VoIP – do we need to protect voice communications across the network from unauthorized access?

- Challenges with network infrastructure?
  - Centralizing traffic
  - Managing the flow of information/data
  - Cost, maintenance, selection, scale, etc.

3.0 Data Backup Strategies

Backup Strategies

- Media / Location Duplication
  - Back up the backup (Difference between backup vs archive?)
  - Diversity - store the back on different media because you never know what equip will be available!
- Storage Availability: Off-line, Near-line, On-line
  - human intervention is the key determinant
- Prioritization (who's data do we backup first?)
  - COD by department
  - Applications and Location
- **Frequency** – Rotations, scheduling
- Replication – expensive and complex, but effective
- System Wide? Strategic? What is FEASIBLE?
- In-source / Outsource

4.0 Data Backup Technologies

Backup Technologies – Media types and options

- Magnetic Tape (reel to reel still being used) – 185TB on one tape (Sony, 2014)
- Disk – (VTL: virtual tape library, D2D: disk to disk)
- Removable media (CD Rom, DVD, USB Drives,
- Server based (Local or SAN)
- Network Based (such as NAS)
- Cloud Based (usually third party but can be hosted locally)
  - MSP (managed services provider) Outsourced / Remote – RBS (remote backup service)
    - Application
    - Server
    - Location
    - Network
- **MTBF of each of these media is relevant!**

5.0 3L's of Data: Location, Location, Location!

Location Issues and considerations

- Which files are the right files? How do you determine this?
- Remote storage location – how large a facility? What equipment/resources can it support?
  - Do you need ALL your data?
- Site-to-Site replication a challenge based on location?
  - ex. US to CAN? Cross border? Check out the "***USA PATRIOT" Act (2001)***
- Networking Considerations:
  - Private / Wan ; Internet / VPN
  - Internal
  - MSP (Remote Backup Service)
- Environmental considerations:
  - Security – Physical / Logical / political unrest / natural disasters / weather etc.
  - Heat (data centers don't like heat)
  - Moisture (data centers don't like moisture)
  - EMR (data centers don't like EMR/EMI ex. High voltage cables)

6.0 Restoration Protocols

- Restoral Protocols
  - MTTR – Mean Time to Repair
    - Media Limitations – ex. how much can you store on it?
    - Network Limitations – how fast can it send your data (QoS)?
    - Platform Readiness – compatibility/currency of your platforms/applications.
      - "**Ripple effect**" of a small technological change can make restoration a challenge!
  - Reverse Prioritize
    - COD by department
    - Application
    - Location
  - Target Location Viability
  - Document Version Management
  - Mobile Re-Distribution

7.0 Testing, Planning, and Documentation

- The 5 “W”s and How
- Simulation – **high fidelity test** of if this is going to work
- Spares
  - Hardware
  - Software
- Document Policies and Procedures, then
- Educate, Train & Enforce those policies

8.0 Chaos Theory

Source: https://scienceonblog.wordpress.com/2017/04/13/chaos-theory-in-jurassic-park/

Chaos Theory

- Mathematically, all systems are dynamic, fluctuation is natural
- Human Factor – **73% of all network / data loss error**
  - "I'm only Human", "Everybody makes mistakes"
  - Robust systems can survive longer and withstand more
- If it *can* break, it probably will at the worst possible time…
- "Things are going well…" **Complacency an issue**!
  - Assume something is going to go wrong – because it will. Therefore – Failure is NOT Random
  - **Expect it**: Not if – WHEN - Why FUD works!
- Plan to Fail if you Plan to Succeed
  - Ask the question: What if?….
  - What is our Worst Case Scenario…

9.0 Off Site Storage – CRITICALLY IMPORTANT

When a facility is lost or inaccessible, all items inside are no longer available.

What will you need in off site storage if you have to **recover** from scratch?

- Does PC backup media need to be **stored off-site**?
- Critical, documents and materials must be available in an off-site location, accessible by appropriate individuals or teams during a disaster or exercise.
- **Consider HARD COPIES**
- Communicate the **plan** and the **location**!
  - Key personnel must know where off-site storage items are located and to where items will be shipped (Hot-site, Incident Command Center or remain in off-site storage?)

Let’s finish our discussion on

Business Continuity Management (BCM)

FANSHAWE

BCM (picking up from last week…)

- Extract from ISO27002:2005 Code of Practice
- Reasons Why Business Operations Must Continue
- BCM Program
- Extracts from ISO 22301

- What is the difference between BCM and BCP? Is there a difference?
  - Business Continuity Management (BCM) is a **structure** (or a framework) for **maintenance and management** of the BCP.

1.0 BCM – extract from ISO 27002:2005

14.1.1 Including information security in the business continuity management process

(Extract from ISO27002:2005 Code of Practice).

Control

A managed ***process*** should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

Implementation guidance:

The process should bring together the following key elements of business continuity management:

a) understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritisation of critical business processes (see 14.1.2);

b) identifying all the assets involved in critical business processes (see 7.1.1);

c) understanding the impact which interruptions caused by information security incidents are likely to have on the business - including incidents causing **smaller impact**, as well as **serious incidents** that could threaten the viability of the organization – and **establishing the business objectives** of information processing facilities;

d) considering the purchase of suitable **insurance** which may form part of the overall business continuity process, as well as being part of operational **risk management**;

e) identifying and considering the implementation of additional preventive and mitigating controls;

f) **identifying** sufficient financial, organizational, technical, and environmental **resources** to address the identified information security requirements;

g) ensuring the **safety of personnel** and the **protection of information processing facilities** and **organizational property**;

2.0 Reasons Why Business Operations Must Continue

Why is it so important the business operations continue?

- To collect money from customers (receivable).
- To maintain a service.
- To pay accounts (payable).
- To maintain market presence.
- To meet business obligations.
- To protect the company brand name.

BCM Program

Like BCP, BCM is a program, not a project.

- **Program**: a portfolio comprised of multiple projects that are managed and coordinated as one unit with the objective of achieving outcomes and benefits for the organization.
- **Project**: a temporary entity established to deliver specific (often tangible) outputs in line with predefined time, cost and quality constraints.

A **BCM Program** requires you to:

- Understand your organisation
- Work out a strategy
- Draw up documented plans
- Test, maintain and review

Business Continuity Mgmnt System (from ISO 22301:2019)

Developed from BS2599-2 (iso standard is available here)

Emphasizes the importance of:

- understanding the organization's needs and the necessity for establishing business continuity policies and objectives;
- operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions;
- monitoring and reviewing the performance and effectiveness of the BCMS;
- continual improvement based on qualitative and quantitative measures.

Business Continuity Standards from ISO 22301

A BCMS, like any other management system, includes the following components:

- a policy;
- competent people with defined responsibilities;
- management processes relating to:
  - policy;
  - planning;
  - implementation and operation;
  - performance assessment;
  - management review;
  - continual improvement;
- documented information supporting operational control and enabling performance evaluation.

BCM Steps

BCM – Key Phases

- Collect the information you need to start the BCM program. What kind of information do you need?
  - Recognition
  - Classification
  - Application (Methodology)
  - Documentation
  - Corporate Politics
  - Budget Approvals
  - Governance and oversight
- **Results in a Business Continuity Plan >** Plans should result in policies & training
- Repeat the cycle for **continuous improvement**

ALE: Defining Some Important BCM Terms

- Departmental Responsibility
- Methodology/process
- Assessment
- Redundancy
- Diversity
- Establishing ROI
- Budget Allocation
- Corporate COD vs. ICT COD
- OpEx vs CapEx

GREAT resource for this can be found here

Business Continuity Planning (BCP)

FANSHAWE

Review: What is BCP

- Business Continuity Planning (BCP) involves devising a plan that guards against business disruption in case of unforeseen events.

- BCP is a **process** that defines the **procedures** employed to ensure timely and orderly resumption of an organization's business cycle through its ability to **execute plans** with minimal or no interruption to time-sensitive business or service operations.

- The objectives of business continuity planning include
  - minimizing interruptions to the business's ability to provide its products and/or services,
  - minimizing financial loss, and
  - being able to resume critical operations within a specified time after a disaster.

Reason for BCP/DRP

- What comes first to a business? Data or people?
  - The primary reason for all BCP and DRP planning is the preservation of human life.
  - Almost everything else can be replaced.
  - Data can be rebuilt, replaced or recreated. A person cannot.
- After people come the data.

Humanlytics: People before the data

Investment in BCP

- Time spent on BCP can mean the difference between business survival or failure if disaster strikes. A fire, a flood, a hard drive failure or data theft - any or all of these could put your business out of commission.

- **Taking the time** to do some contingency / recovery planning will help ensure that your business is able to resume operations in the shortest possible time.

- This can be difficult in a business world where “time is money”. How do you convince your upper management that a BCMS and BCPs are worth doing?

Image credit: https://www.inc.com/gordon-tredgold/if-time-is-money-are-you-spending-yours-wisely.html

BCP - Procedures

- The detailed information about **how** to implement response and recovery actions.
- These should include at least:
  - health and safety
  - welfare
  - security of facilities and information
  - invocation and implementation of alternative resources
  - resumption of business processes or activities
  - internal and external communication including media handling.

BCP - Risks?

1. Determine what the main risks are to the business.
2. What is the (most **likely**) potential problem? data theft? hacking? flooding? earthquake? Other?

Working out what types of disasters that are most likely to happen will focus the business contingency plan and not waste time and money preparing for something that's very **unlikely** to happen.

BCP - Communications System

- Who would be responsible for notifying each employee?
- Who will be responsible for communicating with the public and how (press releases, signs in the windows, radio announcements etc.)
- Are phone (cell & land lines) and email contact lists up to date?
- Do the people responsible for contacting others have access to lists in the event that all the technology fails sooner or later and usually at the most inconvenient time?

How BCP Helps: Protecting Business Data

- Business data is one of your most valuable assets.
- If it was stolen or destroyed, **would your business be able to quickly get up and running again** or even carry on at all?

- If your data are so important to your business, how are you going to protect those data?
- Against ransomware, data breaches/leaks, trade secrets,

- This is where your BCP plays a major role…

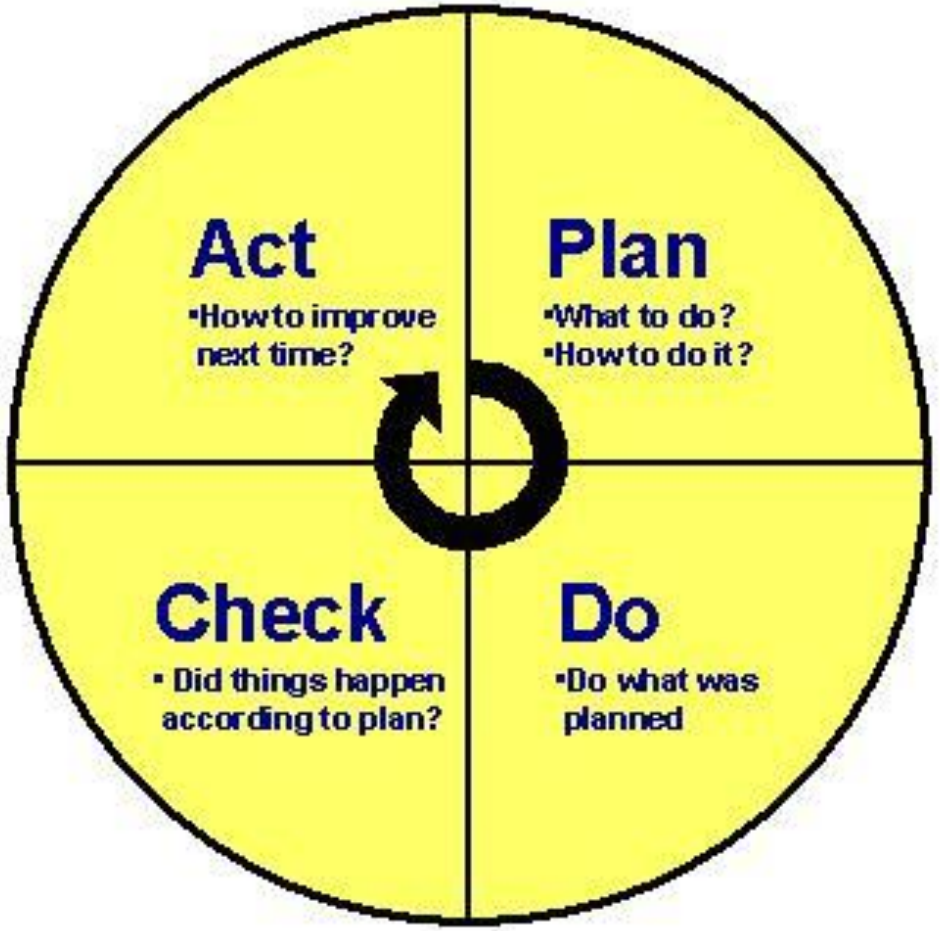
BCP - Insurance?

- Transfer or Accept the risk?
- Besides obvious physical disasters such as fire, flooding or wind damage, consider the damage that could result from theft, for instance. And then there's the potential liability factor if the business is engaged in activities that might open it up to lawsuits.

BCP Policy

- In addition to making the commitment to BCM and resourcing the program, the planning stage should also include:
  - The development of a policy.
  - The policy should be concise and include statements setting out:
    - scope
    - commitment and intent
    - summary objectives for minimising impact, providing continuity to customers and protecting stakeholders.
- Where practicable, write the policy so that it can be read by **any interested party** (for example, avoid “legalese” or industry jargon where possible)
- Employees are key to embedding BCM as part of the organisation’s culture

Remember P.D.C.A.?



Plan Do Check Act

- The PDCA cycle **is used in business process management** for the control and continuous improvement (CI) of processes and products.

It can be summarized as:

- **Plan** what you need to do to achieve the objective (which can include defining the objective)
- **Do** what you planned
- **Check** that what you have done achieves what you had planned for it to achieve, and identify any gaps or shortfalls
- **Act** on the findings of the check phase to address the gaps.

The BCMS Life Cycle

(From ISO 22301)

BCMS Lifecycle is older model than PDCA, but the two share many similarities

BCMS (from ISO 22031:2019)

The BCMS is designed to ensure that **the plan is fit for purpose**.

- It does this by:
  - understanding and analysing the business recovery requirements, so that the impact resulting from an incident or interruption is properly understood and balanced across the organisation.
  - identifying and planning the resources that would be required in the worst possible situation, and ensuring that they would be available
  - creating a documented plan that is based upon valid assumptions, delivers the required recovery outcomes and is properly understood, or ‘owned’, by those that are likely to need to use it
  - testing the plan, resources and people involved so that everything remains up to date, capabilities are tested and the best level of assurance can be given as to the fitness for purpose of the plan.

Business Continuity vs. Disaster Recovery

- Business Continuity Planning: Ensures the continuity of critical business functions.

- Disaster Recovery Planning: Provides procedures for response, backup and restoration when the organisation suffers a loss of IT and physical facilities.

Disaster Recovery Plans

(finishing off from last week)

FANSHAWE

Review: What is a Disaster Recovery Plan?

- A Disaster Recovery Plan (DRP) covers the **recovery of ICT systems** in the event of a major disruption or disaster.
- The DRP provides the capability to **identify and process** (or recover) essential business applications
  - Even if they are not operating at 100% efficiency. ☺
- The DRP provides the ability to return to normal operations within a **reasonable amount of time**.

Review: What Disaster?

- A technological disaster such as having all your business data wiped out.
- A fire, floods or earthquake, or other natural disaster.
- The death of the business owner or other key personnel.
- **A Disaster is anything that can limit your ability to continue business operations.**

Scenario-based DRPs

Will my response be the same in for all disasters?

- major site or premises incidents
- denial of access/service
- information and communications system failures
- supply chain failures
- pandemic flu
- loss of human resource

DRP Methods

- DRP Methodology
  - Defined Recovery Processes for:
    - **Infrastructure (what do/could we need to replace)**
    - **People (who do we need to retrain)**
    - **Data (what do we need to recover)**
  - Phased Approach
    - Notification / Activation Phase
      - Responsibility – decision to activate
      - Restrictions – conditions,
      - Rules – succession, guidelines, documentation
    - Recovery Phase – regain control
    - Reconstitution Phase – repair and resume

A thorough DRP includes other documents!

- Incident Management
  - Containment
  - Eradication
  - Recovery
- Damage Assessment
  - **COD / ROI**, Time-line, Outsource
- Documentation
  - Inclusion – which documents are included?
  - Improvement – documenting what we've learned and what we need to change
  - Implementation – documenting the steps to putting the policies, people, processes, and systems in place so that the plan can be **executed quickly.**

Post Disaster – What comes after a disaster?

Think of this as **Disaster Aftermath University**. Let's go to school and learn!

Things like:

- What Did We Learn from this Incident / Disaster?
- Will apply to Tests and Simulations as well
- If not planned – then add it
- W5 (Who, What , Where, When, Why, How)
- What worked (Expected and **Unexpected!**)
- Check the Ratios – Avoided? Recovered? (SWOT)
- Make the changes in the BCP (BIA, DAP, DRP)

- What about the people?
  - Who's involvement was essential (and why?)

https://www.tvdsb.ca/en/parents/adult-and-continuing-education.aspx

Put it all together

- Test the plan to see if it really works. **What are the different ways to test?**
- Have both printed and electronic versions of the DRPs ***available and accessible***.
- Some of the things that a plan may include are:
  - communication plan – ex. Who is your media contact? Do you have updated contact lists?
  - data protection measures and operational essentials
  - business's evacuation plan – ex. where will you people assemble? Weather issues?
  - information about emergency kits, insurance policies, and other key information
    - Banking information, building floor plans for emergency services, etc.
  - And whatever else is necessary for business resumption – **Can you think of anything else you might need?**

BCM Goals vs. ICT Roles & Responsibilities

- Goal: The organization needs to survive
- Get everyone to buy in. Be ready for the “This can’t happen to us” arguments
- What can we do to prevent/avoid, and if not, then recover?
- Disaster Recovery is not JUST an “IT thing” or just a “management problem”
  - Company wide responsibility –and cost!
- OK – so we saved the data (yay!) – so…. now what?

Other Types of Plans

- Contingency.
  - Back-up plan
  - What how & when if normal means not available?
  - Establish operation profiles.
- End user recovery.
  - Recovery is not just limited to servers.
- Emergency response.
  - Fire Brigade, Medical, Police
- Crisis management.
  - Psychological help.
  - Contacting family members of victims.
  - Media relations.
  - Stress management.

References and Reminders

- Keep up the Discussion Forum Posts!
- Assignment #2 is due after reading week
- Test #2 (15%) is in academic week 10 at 0900hrs EST (our normal tutorial time)
  - If you are part time **or** studying abroad, you may request an alternate test time. Please email me as early as possible so that I have time to set this up.

References

- Management of Information Security – M Whitman and H Mattord
- Computer Security Principles & Practices, 3rd Edition - William Stallings, Pearson - Prentice Hall
- ISO27000 series of Standards
- ISO22300 series of Standards

Thank you for being here!! ☺