Lesson 4

Business Continuity (BC) Policy

When you fail to plan, you are planning to fail

ST2610

Security Policy & Incident Management (SPIM)

All Nets services restored after temporary outage islandwide

ST VIDEOS

Controversial Malaysian rapper Namewee reveals softer side at his Singapore concert

Singapore firms give China couples' baby-making efforts a push

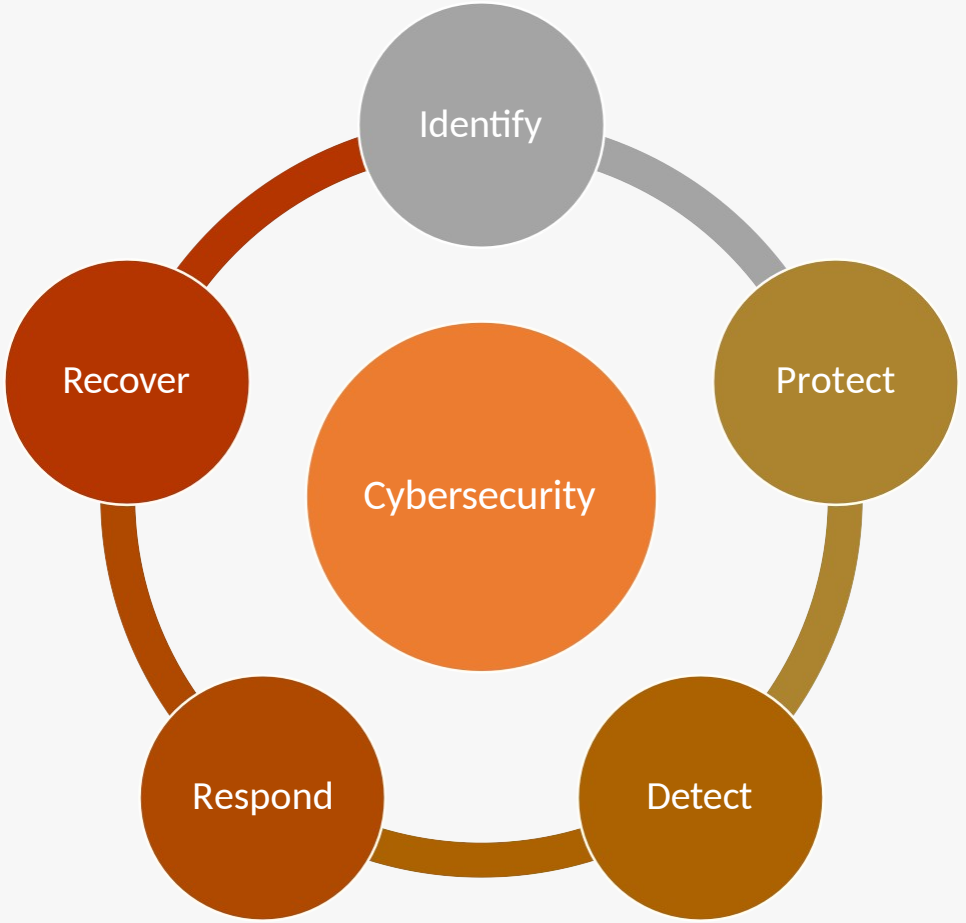
Dr Love on new conquests

North Korea earned over US$200 million from banned exports, and sends arms to Syria, Myanmar...

BC Policy Objectives

in relation to C.I.A.

5 Core Cybersecurity Functions



- Remember your Detection, Response & Recovery Capabilities as well
- In the current threat landscape, we need to plan in scenarios of failure

Types of Threats | some

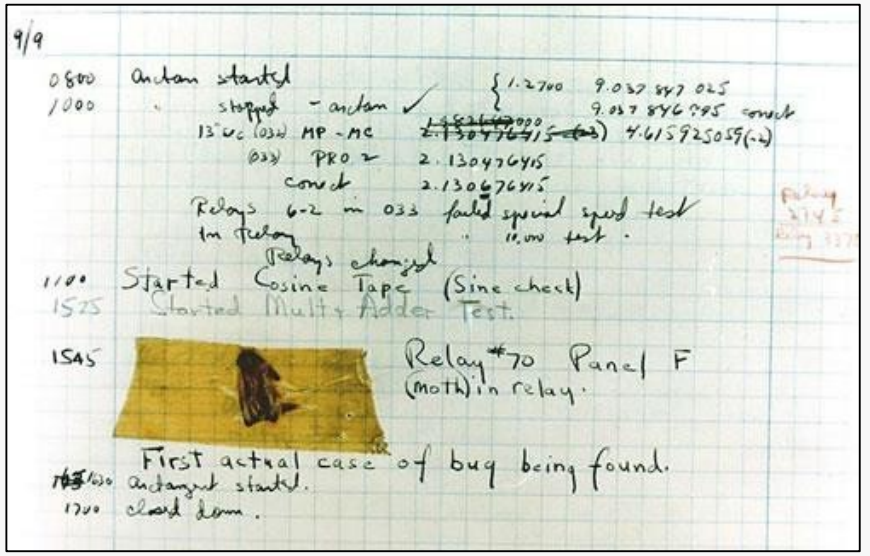
e.g.

- Logical
  - Hacking, Unauthorised use of applications, Malware
- Communications
  - Communication infiltration, Misrouting, DoS attacks
- Technical Failures
  - Network host, Storage, Gateways, Communication lines, Firewall, Power environment, System software
- Human Error
  - Operators, Application programmers, Maintenance staff, Users, Security administrators
- Physical
  - Theft, Willful damage, Terrorism, Fire/Arson, Water damage, Natural disaster, Staff shortage

Types of Disasters | some

e.g.

- Natural Disasters
  - Storm, Earthquake, Flood, Animal Bite Cable, etc.
- Man-Made
  - War
  - Criminal Intent e.g. Sabotage
  - Accidental (P-E-B-K-A-C)
  - Cyber Attack / Malware
- System Failure



Cyber Resiliency

- "Cyber Resilience is the organisation' **capability to withstand negative impacts** due to **known**, **predictable**, **unknown**, **unpredictable**, **uncertain** and **unexpected** threats from activities in cyberspace."

Information Security Forum (ISF)

- The **inability to eliminate** the unknown unknowns in cyberspace is why the focus on cyber resilience is so important.

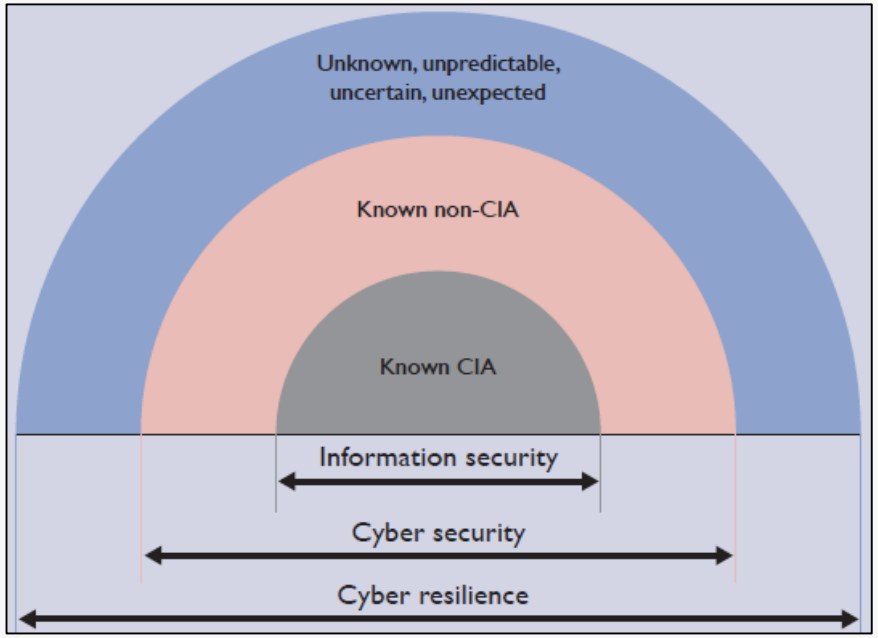
"There are known knowns, there are things we known we know. We also know there are known unknowns, that is to say we know there are something we do not know. But there is also unknown unknowns – the ones we don't know we don't know."

Donald Rumsfeld, Former US Secretary of Defense (Feb 2002)

Cyber Resiliency

Beyond Cybersecurity / Risk Management

- **Risk management** focuses on achieving security through management and control of **known risks**
- Rapid evolution of opportunities and risks in cyberspace is outpacing this approach and it no longer provides the protection required for an organisation to succeed
- Organisations must extend risk management to include risk resiliency
  - Enable organisations to manage, response and withstand the impact of activity in cyberspace

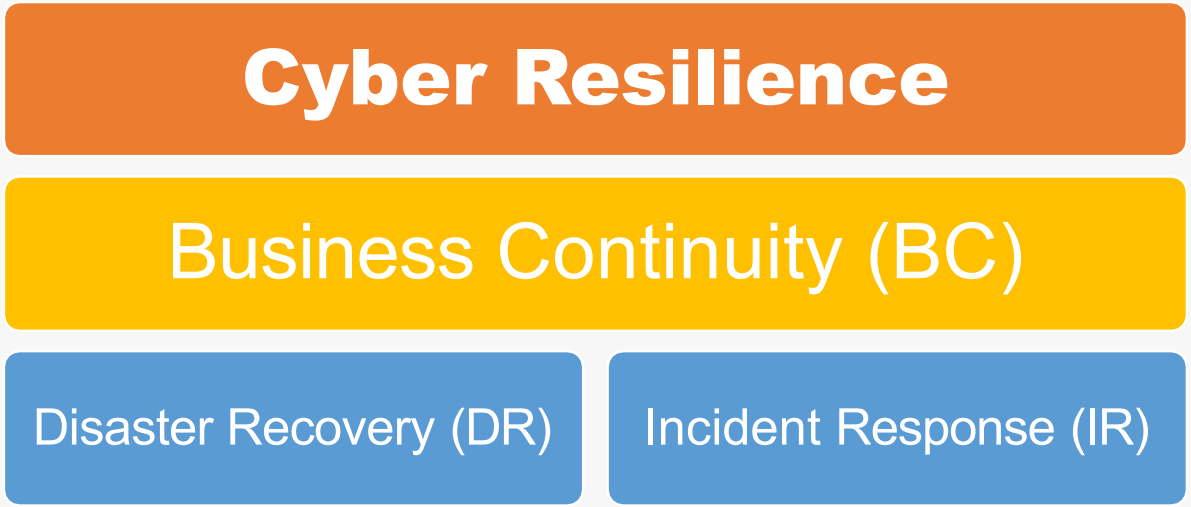


Cyber Resiliency

Multipronged Response Needed

- Cyber resilience requires recognition that organisations must prepare now to deal with severe impacts from cyber threats that cannot be predicted or prevented
- Cyber resilience requires very high levels of partnering and collaboration, including –
  - External collaboration
    - e.g. ISPs, intelligence agencies, industry groups, security analysts, customers, supply chains, etc.
  - Internal collaboration
- Cyber resilience requires that organisations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences of the incidents
  - Good governance
  - Nimble IT and information security responses
  - Up-to-date and well-tested public relations policies with key issues decided in advance
  - Crisis preparedness
  - Human relations responses
  - Investigative and forensic capability
  - Ability to share information
  - Legal responses

3 Policies / Plan / Components of Cyber Resiliency



– Cyber resiliency is a relatively new concept in today's world where we assume we are already compromised, or **not totally protected** against cyber attacks without becoming operationally inefficient, and in such a scenario, how do we **continue to be able to operate**, **whilst trying to fix** the downed or compromised systems, or neutralise the attack.

Resilience v. BC

- Resilience
  - Resilience is the capability of an organisation to continue its Minimum BC Objective (MBCO), if not immediately then very quickly, when it has suffered a disaster or crisis.
  - The ability of an organisation to absorb the impact due to a risk occurrence and to continue
    to operate in such a way as to achieve its MBCO.
  - The ability of an organsiation to resist being affected by an incident.
- MBCO
  - The minimum level of service and/or products that is acceptable to the organisation to achieve its business objectives during an incident, emergency or disaster.
  - Set by the Executive Management of the organisation and can be influenced, dictated and/or change by current regulatory requirements or industry practices.
  - The management specification of what this level should be from a policy/'top down' perspective.

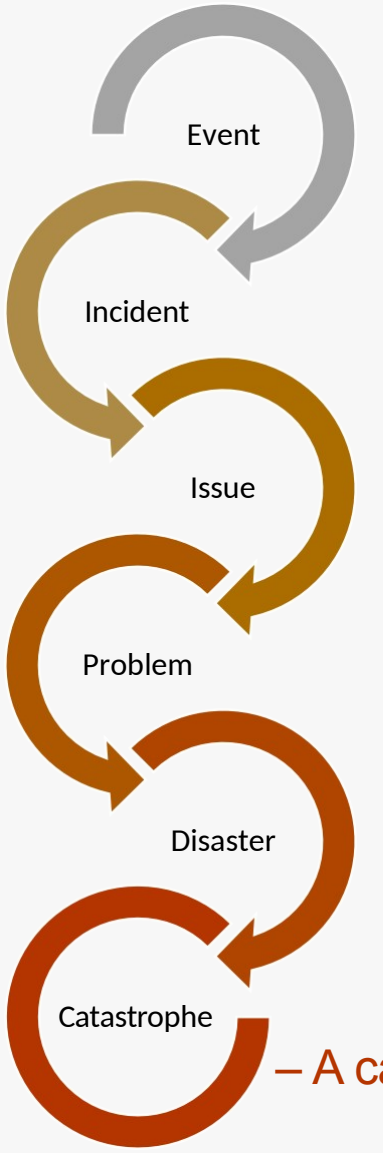
BC

- The capability of the organisation to **continue delivery** of products or services at acceptable **predefined levels** following a disruptive incident.

  ISO 22301:2012 – Business Continuity Management Systems (BCMS)

- Other Definitions
  - Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-determined level.
  - A comprehensive managed effort tor prioritise key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organisational response to the challenges that surface during and after a crisis.
  - The capability to provide continuous key services to customers and business partners at an expected level regardless of the circumstances.

Event/Crisis Level/Severity



Crisis is a situation where organisations shift from routine to non-routine operations. Management is required to divert a proportion of their attention, time, energy and resources away from normal operations to managing this event.

- Events and/or incidents, after checking, may turn out to be "non-issues" and life goes on i.e. ticket closed
- An incident or issue may be resolved easily without escalation or leading to a problem or disaster
- A problem could be declared a disaster if e.g. it fails to be resolved or meet certain requirements within a stated time limit e.g. 36 hours.
- As an event escalate, additional resources and authorisation will be deployed
  - A case of near-total operations shutdown

If all event/incident is a disaster, nothing is.

Crisis/Event Levels

- Event
  - Occurrence or change of a particular set of circumstances.
  - e.g. An event is pre-announced large-scale activity that would lead to a disaster. The stakeholders are made aware by a set of announcements or early indicators. These events could potentially cause disruption to businesses due to closure of premises and access routes, increase security restrictions and inconvenience of customers.
    e.g. APEC meetings, the Olympics, WTO meetings, etc.
- Incident
  - Occurrence by chance or due to a combination of unforeseen circumstances, which, if not handled in an appropriate manner, can escalate into a disaster.
- Disaster
  - A sudden, unplanned calamitous event that causes great damage or serious loss to an organisation, resulting in an organisation failing to provide Critical Business Functions (CBFs) for some pre-determined minimum period of time.

- Balancing the No. of Crisis/Event Levels
  - Too Many – Cognitive overload in determining Crisis/Event Level v. managing the incident
  - Too Little – Inappropriate level of response to a perceived incident

Crisis/Event Level Escalation

- 3 Determining Factors of Crisis/Event Level
  - Business Functions (BFs) and/or Assets Affected
  - Time – How long can the business stand the pain?
  - Resources Needed
- Hence, Criteria for Crisis/Event Level Escalation
  - Criticality of and Impact to the Business Function and Asset e.g. Systems & Application
  - Pre-defined Time to Fix
  - Resources and/or Authorisation Required to Fix

If all BFs and/or Assets are critical, nothing is.

BC Policy Strategy

- Identifies potential impacts to BFs and/or Assets
- Create a framework for resilience and response capabilities
- Safeguard interests of key stakeholders

BC Planning (BCP)

- The process of developing prior arrangements and procedures that enable an organisation to respond to an event in such a manner that CBFs can continue within planned levels of disruption.
- Domains Addressed
  - **Continuation** of CBFs and critical processes when a high severity cevent destroys business services and/or data processing capabilities
  - **Preparation**, **Testing** & **Maintenance** of specific actions to recover to normal processing
- Objectives
  - The end results of BCP is the BC Plan.
  - Create a document, test, and update the plan that will:
    - Allow timely recovery of CBFs
    - Minimise loss
    - Meet legal, regulatory and contractual (e.g. Service Level Agreements (SLAs)) requirements

If a disaster has rendered the business unusable for continued operations, there must be a plan to allow the business to continue to function.

BC Plan

- Comprises clearly defined and documented procedures and information for use when a disaster occurs.
- Guide organisations to reduce, respond, recover, resume, restore and return (i.e. the 6Rs) to fully recovery.
- Covers **key personnel** (include both business and IT personnel), **resources**, **services** and **actions** required to ensure CBFs can continue within planned levels of disruption.
- An **ongoing process** (CBFs may evolve, not a project with a beginning and an end) **supported by senior management** and **funded** to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing and maintenance.

BC Plan | Scope

- Used to be just the data centre
- Now includes:
  - All aspects of an organisation
  - Networks, Power, Personnel
  - Distributed operations
  - … and more …

BC Management (BCM) & Lifecycle

ISO/IEC 22301 BCMS

– A Continuous Interlocked Process
i.e. BCM is not an event

ISO/IEC 27001's BCM

Business Continuity Institute Good Practice Guidelines 2013

BCM

- An **organisation-wide** discipline and a **holistic management** process that identifies potential impacts to an organisation and the impacts to business operations that those threats, if realised, might cause.
- Provides a **framework** for building **organisational resilience** with the capability for an effective response that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities.

5 BCP Phases

1. Project Management & Initiation
2. Business Impact Analysis (BIA)
3. Recovery Strategies
4. Plan, Design & Development
5. Testing, Maintenance, Awareness, Training

5 BCP Phases

1. Project Management & Initiation

- Get Management Support
- Establish Team (Functional, Technical, BC Coordinator)
- Create Work Plan (Scope, Goals, Methods, Timeline)
- Establish Needs (Risk Analysis)
- Initial Report to Management
- Obtain Management Approval to Proceed

5 BCP Phases

2. Business Impact Analysis (BIA)

- Goal
  - Obtain formal agreement with senior management on the MBCO, Maximum Tolerable Downtime (MTD) a.k.a. Maximum Allowable Outage (MAO) for each time-critical business function i.e. CBFs
- Quantifies loss due to business outage (financial, extra cost of recovery, embarrassment, etc.)
- Does not estimate the probability of the kinds of incidents, only quantifies the consequences

5 BCP Phases

2. Business Impact Analysis (BIA) Phases

- Choose information gathering methods (surveys, interviews, software tools)
- Select interviewees
- Customise questionnaire
- Analyse information
- Identify time-critical business functions i.e. CBFs
- Assignment of MBCO and MTD
- Rank CBFs by MBCO and MTDs
- Report recovery options
- Obtain management approval

5 BCP Phases

2. Business Impact Analysis (BIA) – Classification of Systems

- To examine and prioritise functions and systems to be recovered or replicated.
- CBFs
  - Business activities and processes that must not be disrupted such that they impact the ability of the organisation to achieve its MBCO.
  - Must be restored in the event of a disruption to ensure the ability to protect the organisation's assets, meet organisational needs, and satisfy regulations.
  - Other Definition
    - "Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organisation."
    - "Key business processes are those processes essential to delivery of outputs and achievement of business objectives."
    - "Vital functions without with an organisation will either nor survive or will lose the capability to effectively achieve its critical objectives."

Remember: If all Business Functions and/or Assets are critical, nothing is.

5 BCP Phases

2. Business Impact Analysis (BIA) – Classification of BFs & Systems

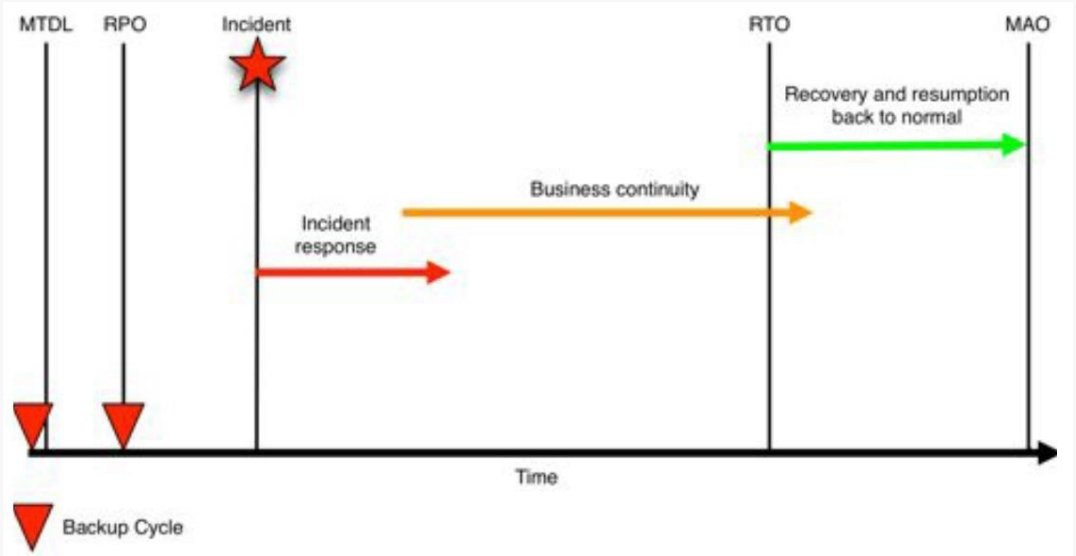
- Systems Classification Levels
  - Critical – Absolutely must be in place for any business process to continue at all
  - Essential – Must be in place to support day-to-day operations
  - Necessary – Contribute to the smooth operations and comfortable working conditions of employees
  - Improve working conditions and help to enhance the organisation's performance

Remember: If all Business Functions and/or Assets are critical, nothing is.

5 BCP Phases

2. Business Impact Analysis (BIA) Terminologies v. Recovery Objectives

- BIA
  - MTD / MAO
  - Recovery Time Objective (RTO) / Maximum Allowable Downtime (MAD)
- Continuity Requirements Analysis
  - MBCO
  - Maximum Tolerable Data Loss (MTDL)
  - Recovery Point Objective (RPO)



5 BCP Phases

2. Business Impact Analysis (BIA) Terminologies (cont'd)

- MTD
  - The maximum period of time that a given business process can be inoperative before the organisation's survival is at risk.
- MAO
  - The time frame during which a recovery must become effective before an outage compromises the ability of an organsiation to achieve its business objectives and/or survival.
  - The maximum period of time that an organisation can tolerate the disruption of a CBFs,
    before the achievement of objectives is adversely affected.
- MAD
  - The absolute maximum time that the system can be unavailable without direct or indirect
    ramifications to the organisation.

5 BCP Phases

2. Business Impact Analysis (BIA) Terminologies (cont'd)

- RTO
  - The maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organisation.
  - The maximum agreed time for the resumption of the CBFs.
  - Comprised of 2 components:
    1. The time before a disaster is declared.
    2. The time to perform tasks (documented in the BC Plan or DR Plan) to the point of business resumption.
  - Other Definition
    - "The period of time within which systems, applications or functions must be recovered after a disruption has occurred. e.g. CBFs must be restored within 4 hours upon occurrence of a disaster."
    - "Target time set for resumption of product, service or activity delivery after an incident."
    - "The period of time within which systems, applications, or functions must be recovered after an outage (e.g. 1 business day). RTOs are often used as the basis of the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation."
    - "The period of time required to fully re-establish adequate resource requirements to recover a critical
      activity, process, function, or other capability, to a required minimum operational level."

5 BCP Phases

2. Business Impact Analysis (BIA) Terminologies (cont'd)

- RPO
  - The point of time to which systems and data must be recovered after a disaster has occurred.
    - e.g. Data should be restored up till the start of the day.
  - Includes the amount of data needed to be reconstructed after the functions or systems have been recovered.
  - Other Definition
    - "The capability at a pre-disruption point in time to which systems and data must be recovered after
      an outage (e.g. to end of previous day's processing)."
  - Often used as the basis for the development of backup strategies.
  - Determinant of the amount of data that may need to be recreated after the functions or systems have been recovered.

5 BCP Phases

3. Recovery Strategies

- The conceptual summary of recovery processes that must be carried out between the occurrence of a disaster and the time when normal operations are restored. It is the alternate processing or interim ability to process data and continue providing critical service whilst a full recovery of the primary site is underway.
- A system for identifying available resources to enable timely and unimpeded access to resources needed to prevent, mitigate, prepare for, respond to or recover from an incident.

- Predefined
- Recovery strategies based on MBCO and MTD
- Driven by Business Requirements
- Different Technical Strategies
- Careful Cost-Benefit Analysis
- Metrics & Decision Trees
- Management Approved

5 BCP Phases

3. Recovery Strategies (cont'd)

- Strategies should address recovery of:
  - Business Functions & Operations
  - Facilities & Supplies
  - Network
  - Data
  - Users

5 BCP Phases

3. Recovery Strategies – Technical Recovery Strategies

- Scope e.g.
  - Data Centre, Networks, Telecommunications
- Methods e.g.
  - Subscription Services
    - Hot – Fully Equipped
    - Warm – Partially Equipped
    - Cold – Empty Data Centre
    - Mirror – Full Redundancy
    - Mobile – Trailer Full of Computers
  - Internal Provided Backups – Companies with multiple data processing centres may create internal excess capacity
  - Mutual Aid Agreements – I'll help you, if you'll help me!
  - Service Bureaus – Shared facilities
    - Empty Shell – Involves 2 or more organisations that buy or lease a building and remodel it into a computer site, but without computer equipment
    - Recovery Operations Centre – A completely equipped site – Very costly and typically shared amongst many companies
  - Redundant Processing Centres – Expensive!
- Data e.g. considerations
  - How much Data can you Lose?
  - Backups of Data & Applications
  - How Fast Can Data be Recovered?
  - Off-Site v. On-Site Storage of Media
  - Security of Off-site Backup Media
  - Types of Backups (Full, Incremental, Differential, etc.)
- Business & Operations Considerations e.g.
  - Fast incident response
  - Reduction of risk
  - Reduction of loss of profit
  - Compliance with laws, regulations and contractual agreements (e.g. Service Level Agreements (SLAs)

5 BCP Phases

4. Plan, Design and Development

- Detailed Plan for Recovery
  - Business and Service Recovery Plans
  - Maintenance, Awareness and Training Planning
- Plan Phases | Sample
  - Initial Disaster Response
  - Resume CBFs / Critical Operations
  - Resume Non-Critical BFs / Operations
  - Restoration (Return to Primary Site)
  - Interaction with External Groups
    - e.g. Emergency Responders, Customers and Media

- Recall: Multipronged Approach Needed for Cyber Resiliency

5 BCP Phases

5. Testing, Maintenance, Awareness, Training

- Testing
  - Until it's tested, you do not have a plan
  - Types of Testing
    - Checklist
    - Structured Walkthrough
    - Simulation
    - Parallel
    - Full-Interruption
- Maintenance
  - Fix problem found in tests
  - Implement change management
  - Audit and address audit findings
  - Annual review of plan
  - Build plan into organisation
- Awareness
- Training
  - On-going training
  - Part of standard on-boarding
  - Part of corporate culture

Importance of Testing the BC Plan

- To make sure the plan works
- Personnel involved may change
- Environment (Assets, Systems, Services, Regulations, Contractual Agreements) may change | e.g.
  - New business department or product-line
  - New software or IT services e.g. Cloud and BYOD
  - New building, equipment, production system
  - Contractors and Sub-Contractors
  - M&A
  - Public Listing Status

ISO 22301 BCMS

Extract

1. Scope & Applicability

   This section defines the scope of the standard, making clear that it describes generic best practice that should be tailored to the organisation implementing it.

2. Terms & Definitions

   This section describe the terminology and definitions used within the body of the standard.

3. Overview of BCM

   A short overview is the subject of the standard. It is not meant to be a beginners guide but describe the overall processes, its relationship with risk management and reasons for an organisation to implement along with the benefits.

4. BCM Policy

   Central to the implementation of BC is having a clear, unambiguous and appropriate resourced policy.

5. BCM Programme Management

   Programme management is at the heart of the whole BCM process and the standard defines on approach.

ISO 22301 BCMS

Extract (cont'd)

6. Understanding the Organisation

   In order to apply appropriate BC strategies and tactics the organisation has to be fully understood, its critical activities, resources, duties, obligations, threats, risks and overall risk appetite.

7. Determining BCM Strategies

   Once the organisation is thoroughly understood the overall BC strategies can be defined that are appropriate.

8. Developing and Implement a BCM Response

   The tactical means by which BC is delivered. These include incident management structures, incident
   management and BCPs.

9. Exercising, Maintenance, Audit and Self-Assessment of the BCM Culture

   Without testing the BCM response an organisation cannot be certain that they will meet their requirements. Exercise, maintenance and review processes will enable the BC capability to continue the meet the organisations goals.

10. Embedding BCM into the Organisations Culture

    Business continuity should not exist in a vacuum but become part of the way that the organisation is managed.

Information Security Continuity in BCM

ISO/IEC 27002

Remember: All C.I.A. are Important!

- Information security continuity should be embedded in the organisation's BCMS
  - Planning information security continuity
    - The organisation should determine its requirements for information security and the continuity of information security management in adverse situation e.g. during a crisis or disaster.
  - Implementing information security continuity
    - The organisation should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
  - Verify, review and evaluate information security continuity
    - The organisation should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

BC v. DR

- BC
  - The capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

    ISO 22301:2012 – Business Continuity Management Systems (BCMS)
- ICT DR
  - Ability of the ICT **elements** of an organisation to **support its critical business functions** to an **acceptable level** within a **predetermined period of time** following a disruption.

    ISO 27031:2011 – Guidelines for ICT Readiness for Business Continuity
  - Immediate intervention taken by an organisation to minimise further losses brought on by a disaster and to begin the process of recovery, including activities and programmes designed to restore CBFs and return the organisation to an acceptable condition.
- BCP refers to plans about how a business should plan for continuing in case of a disaster. DR refers to how the IT elements should recover in case of a disaster.
- BCP is a plan that allows a business to plan in advance what it needs to do to ensure that its key products and services continue to be delivered at a predefined level in case of a disaster, whilst a DR allows a business to plan what needs to be done immediately after a disaster to recover from the event.

DR Planning (DRP) & DR Plan

- DR Planning
  - Process of developing advanced arrangements and procedure that enable an orgnaisation to respond to a disaster and resume the critical business applications within a predetermined priod of time, minimise the amount of loss, and repair or replace the damaged facilities ASAP.
  - Identifies
    - Actions before, during and after an disaster
    - Disaster Recovery Team
    - Priorities for restoring critical systems and applications
- DR Plan
  - A document that describes how an organisation is to deal with potential disasters that will disrupt IT services.
  - Defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption.
  - Designed to assist in restoring the business process within the stated DR goals.
  - “A clearly defined and documented plan which recovers IT and telecommunications capabilities
    when a disaster does occur. Typically, it covers key personnel, resources, services and actions
    required to be carried out to ensure that IT systems for CBFs can continue within planned levels
    of disruption. For an organisation which relies heavily on IT, the DR Plan is an integral part of its
    BC Plan.”

DRP Phases

1. Critical Applications

   Rank critical applications so an orderly and effective restoration of computer systems is possible.

2. Create DR Team

   Select team members, write job descriptions, describe recovery process in terms of who does what.

3. Site Backup

   A backup site facility including appropriate housing, furniture, computers, and telecommunications. Another valid option is a mutual aid pact where a similar business or branch of same company swap availability when needed.

4. Hardware Backup

   Some vendors provide computers with their site i.e. hot site or Recovery Operations Centre. Some do not provide hardware – i.e. cold site. When not available, make sure plan accommodates compatible hardware e.g. ability to lease computers.

5. System Backup

   Some hot sites provide the OS. If not included in the site plan, make sure copies are available at the backup site.

DRP Phases (cont'd)

6. Application Software Backup

   Make sure copies of critical applications are available at the backup site.

7. Data Backup

   One key strategy in backups is to store copies of data backups away from the business campus, preferably several miles away or at the backup site. Another key is to test the restore function of data backups before a crisis.

8. Supplies

   A modicum inventory of supplies should be at the backup site or be able to be delivered quickly.

9. Documentation i.e. DR Plan

   An adequate set of copies of user and system documentation.

10. Test

    The most important element of an effective DR Plan is to test it before a crisis occurs, and to test it periodically (e.g. once a year).

DRP Audit

- Audit Objective
  - Verify that the DR Plan is adequate for dealing with disasters
- Audit Procedures
  - Evaluate adequacy of backup site(s)' processes and resources
  - Review list of critical systems and applications for completeness and currency
  - Verify that procedures are in place for storing off-site copies of applications and data
  - Check backups and copies currency
  - Verify that documentation, supplies, et.c., are stored in backup site(s)
  - Verify that the Disaster Recovery Team knows its responsibilities
    - Check frequency of testing the DR Plan
- Major DR Controls Concerns
  - Backups
  - DR Team
  - Testing the DR Plan Regularly

BC/DR v. the 5 Core Cybersecurity Functions

- **Identify** your crown jewels i.e. CBFs and critical assets and systems
- **Protect** your crown jewels
- **Detect** cybersecurity events/incidents
- Escalated **Response**
- Escalated **Recovery**