www.thebci.org/Canada

How BCM Practices Help Build Organizational Resilience

Des O'Callaghan, FBCI

DRIE Toronto Symposium – September 7, 2018




Overview

- Definitions
- Evolution
- OR Relationship with BC
- BC Lifecycle
- Other involved disciplines
- Examples of collaborative activities

Definitions

- The mental ability to recover quickly from depression, illness or misfortune.
- The physical property of material that can resume its shape after being stretched or deformed; elasticity.
- The positive ability of a system or company to adapt itself to the consequences of a catastrophic failure caused by power outage, fire, bomb or similar (particularly IT systems)

Alternative definition

Crowds panic as flooding threatens Ireland...

The evolution of resilience

- Recognition that we are concerned not just with “traditional” emergency response and business recovery
- Considering continuity through a risk lens
  - mitigation, protection and prevention, as well as recovery
- Resilience is an attribute across the spectrum of planning:
  - An aspect of business as usual
  - A consideration in mitigation and prevention – by design
  - A factor in awareness and preparedness
  - A measure of success in the return to normal, or better state

The advance of resilience thinking

- In recent years resilience has received increased attention as an important aspect of how organizations function, due to:
  - Greater awareness of risks in operating environments
  - More frequent and severe disruptive events
  - Increased interdependencies between organizations
  - Higher global impacts from singular disruptions
- Improved horizon scanning and risk awareness allows more focus on mitigation strategies and protective measures

Resilience Characteristics

- Resilience is not an outcome from one discipline
- Grows from the convergence of many disciplines
  - Each is necessary, none is sufficient
- Resilience is relative term; there is no absolute condition
- We can be more or less resilient – the effort is to **improve**
- Resilience is relevant to how an organization functions, before, during and after any disruption

Relationship with business continuity

- Business Continuity and organizational resilience are not the same thing, but share much common ground
- Business Continuity provides principles and practices that are essential contributors for any organization seeking to develop and enhance its reliance capabilities
- Therefore business continuity is key to achieving organizational resilience

The BCM Lifecycle: *improving organizational resilience*

Six Professional Practices (PP)

Management Practices

PP1	Policy & Programme Management
PP2	Embedding Business Continuity

Technical Practices

PP3	Analysis
PP4	Design
PP5	Implementation
PP6	Validation

Other disciplines - importance

- Business Continuity is at the heart of organizational resilience, but alone is not sufficient. Collaboration is needed
- As resilience should permeate an entire organization, contributions from a variety of key areas must converge
- Let's discuss some of the more relevant other areas, with examples of specific activities requiring collaborative effort….

Risk Management

- Engagement with Risk in an organization is essential to ensure programs aimed at building resilience are correctly focused
- Risk and threat analysis is a pre-requisite for developing appropriate strategies

Risk Management Activities

- Engagement with Risk in an organization is essential to ensure programs aimed at building resilience are correctly focused
- Risk and threat analysis is a pre-requisite for developing appropriate strategies

- Risk and Threat Assessment (TRA) considers uncertainty, identification of specific risks, the probability of threats becoming realized and the impacts of adverse events when they occur
  - Probability and impact are combined to produce a "score" or ranking
- If the organization has already conducted a TRA, the BC professional can exploit the analysis and identify specific risk mitigation strategies that are in place, or could be implemented to improve resilience.
- When no assessment has already been performed, BC can take the lead on identifying and analyzing relevant risks using available resources, such as BCI's Horizon Scans and other research

Human Resources / Health & Safety

- Staff are a critical resource for any organization
- Safety and wellbeing support personal resilience
- HR has a role to play in different ways
  - During business as usual
  - During disruptions and incident responses

HR / Health & Safety Activities

- Staff are a critical resource for any organization
- Safety and wellbeing support personal resilience
- HR has a role to play during business as usual and during disruptions and incident responses
- Examples of HR activities contributing to resilience are:
  - Employee Assistance Programs
  - Managing employee personal information with security and privacy
  - Ensuring the continuity of employee payroll and expense reimbursement
  - Providing flexibility in policy areas (relocation, extended working hours, etc.)
  - Providing cross-training opportunities to diversify skills
  - Awareness programmes to promote continuity and resilience thinking
  - Regular fire safety drills – (may sometimes be combined with BC exercises)
  - Regular workplace inspections by competent staff / authorities
  - Identification and management of any hazardous materials
  - Quality controls on air and water supply
  - Prompt repair or replacement of any broken equipment, or furniture
  - Effective and tested alarm systems and fire suppression equipment
  - Placement of sufficient first aid supplies, defibrillators and like equipment

Information & Communications Technology

- Technology is the lifeblood of most organizations
- IT involves many specialist skills (e.g. cyber)
- IT is an area ripe for resilient design
- Responsibility for technology disaster recovery

ICT Activities

- Technology is the lifeblood of most organizations
- IT involves many specialist skills (e.g. cyber)
- IT is an area ripe for resilient design
- Responsibility for technology disaster recovery

- Duplication of resources in multiple locations or instances
- High availability strategies and solutions
- Remote storage of data
- Diversity, or redundancy, of resources (especially power and telecom)
  - Can easily make use of multiple service providers
- Threat monitoring and early warning recognition are examples of common ground between business continuity and cyber security
- Cyber response principles and protocols are likely to be similar
  - May involve the same response structure, teams and specialists
- Cyber intelligence should be represented in any BC / Crisis team
- Adoption of a standard, such as ISO 27001

Facilities Management / Security

- Functions may be combined, or a service provided by a landlord to multiple tenants
- Buildings remain a vital resource for most organizations and important for business continuity
- Physical facilities require varying levels of protection
- Facility protection and access control, are well-established risk mitigation strategies, to guard against intrusion
- Appropriate emergency procedures contribute to resilience by ensuring fast and effective response when threats materialize

Facilities / Security Activities

- Buildings remain a vital resource for most organizations and important for business continuity
- Physical facilities require varying levels of protection
- Facility protection/access control, are well-established risk mitigation strategies, to guard against intrusion
- Appropriate emergency procedures contribute to resilience by ensuring fast and effective response when threats materialize
- Access controls – to prevent unwanted intrusion (can be multi-level)
- HVAC should be well maintained, with redundancy and peak capacity
- Power supply should be robust and highly available
- Standard operating procedures in place to handle emergencies
- Fire safety and evacuation drills
- 24/7 security coverage
- Emergency procedures to handle such incidents as bomb threats, workplace violence, criminal acts on premises, etc.
- Strong liaison with civil authorities – Police, Fire, Ambulance

Supply Chain Management

- Most organizations have critical third party dependencies
  - Providers of technology / telecommunications services, utilities
  - Vendors and suppliers of products, materials and other services
  - Outsource partners
- Where there are dependencies, the resilience capabilities of those other organizations become part of our own resilience
- Diligence is required to assess third party capabilities
- Typically this will involve the organization's Procurement function, perhaps also Legal (for contract issues)

Supply Chain Management Activities

- Most organizations have critical third party dependencies
- Where there are dependencies, the resilience capabilities of those other organizations become part of our own resilience
- Diligence is required to assess third party capabilities
- Typically this will involve the organization's Procurement function, perhaps also Legal (contracts)

- Contracting with more than one provider for critical products/services; selecting suppliers with multiple outlets
- Ensuring there are enforceable business continuity capability provisions built into contracts and service level agreements
  - Obtaining and reviewing attestations as to their capabilities
- Involving third parties in Business Continuity exercises

Crisis Management

- Most incidents are handled and resolved with structured and well-rehearsed response procedures
- Some can escalate in seriousness and become crises, due to:
  - Magnitude / severity
  - Duration – prolonged impact
  - Escalation of impact – because of duration, or cascading effects
- A capability to go from standard response to a higher level of incident management is a measure of a resilient organization

Crisis Management Activities

- Most incidents are handled and resolved with structured and well-rehearsed response procedures
- Some can escalate in seriousness and become crises, due to Magnitude / severity, duration, prolonged impact
- A capability to go from standard response to a higher level of incident management is a measure of a resilient organization

- Crises require the involvement of multiple departments
- It is imperative to have a crisis team formed in advance, with rehearsed roles and responsibilities
- A Crisis Management Team will typically include senior staff who have decision-making skills and authority
- Most, or all corporate functions should be represented in the team:
  - Communications, HR, Legal, Finance, ICT, etc.
- Regular rehearsals will build resilience in both the individual team members and in the overall organizational response to disruptions

Change Management

- "Organizational resilience is the ability of an organization to absorb and adapt in a **changing** environment…"
- Risk and uncertainty abound. It is imperative to be aware of all changes that can affect operations and impact resilience
  - Change in the organization's context – e.g. regulation
  - Change in the organizational structure – e.g. mergers and acquisitions
  - Other changes to lines of business / organizational functions
  - Change in the technological environment
  - Change in the risk landscape, or risk appetite
- The ability to identify changes is itself a step towards resilience
- Mechanisms must be in place to identify and communicate change

Change Management Activities

- "Organizational resilience is the ability of an organization to absorb and adapt in a **changing** environment…"
- Risk and uncertainty abound. Imperative to be aware of changes that can affect operations and impact resilience
- The ability to identify changes is itself a step towards resilience
- Mechanisms must be in place to identify and communicate change

- Identify the types of changes that could impact resilience
  - e.g. regulatory, organizational, technological, etc.
- Embed a protocol to ensure that change, whether anticipated or unexpected, is quickly communicated to interested parties
- Make resilience and business continuity mandatory sign-off criteria for changes to be approved
  - Most important in IT. Changes should not proceed without sign-off
- Ensure there are mechanisms to identify changes of external origin
  - Such as through horizon scanning – business continuity may take the lead on some of this

Thank you

Questions