Information Security Updates

Newsletter for General Users

Issue 4 - **Business Continuity Management**

Related Article

Disaster Recovery: Protecting Campus Data against the Inevitable

South Carolina's Coastal Carolina University uses technology to strengthen its IT infrastructure against weather emergencies. The backup system encompasses various appliances that protect the institution's entire IT infrastructure. At the heart of the system is an on-site data protection unit (DPU), which allows the university to protect local data (files, folders, and all user data) on its own servers, desktops, and laptops.

(http://campustechnology.com/articles/2010/07/29/disaster-recovery-protecting-campus-data-against-the-inevitable.aspx.)

Standard Update

BCM Legislations, Regulations and Standards

When designing, developing and implementing BCM, legal and regulation compliance issue is an important factor to be considered by their management. In Hong Kong, various regulators, such as the Hong Kong Monetary Authority and the Office of the Government Chief Information Officer, have issued a set of BCM related legislations, regulations and standards. Other countries also have certain BCM related laws and regulations enforced by respective government bodies.

(http://www.thebci.org/LRSGVersion4.pdf.)

I. Background

As a holistic process to identify potential threats to an organisation and the impacts that those threats might cause to operations, Business Continuity Management (BCM) provides a framework for building organisational resilience with the capability for an effective response to safeguard key stakeholders' interests, reputation and value-creating activities.

Industry Story

Highlights from the Gartner Business Continuity Management Summit

BCM is an established part of the preparations for the possible threats posed to organisations, whether from internal systems failures or external emergencies such as extreme weather, terrorism, or infectious disease.

In a BCM summit by Gartner, 71 per cent of respondents claim that BCM is regarded as important by senior management in their organisation in 2010. This may reflect increased awareness of the importance of BCM following the high-profile disruptions experienced across in the UK in 2010, such as the extreme winter weather.

See the article:
(http://www.managers.org.uk/sites/default/files/u217/Disruption_Resilience_2010.pdf)

Why Universities need Business Continuity Management

In today's universities, IT has become an essential component in various operational processes including financial accounting, communication, academic research and teaching. Such intensive reliance on IT demands high levels of system resilience and effective contingency plans for possible system outages. With BCM, universities would be able to recover critical operations during various disruptions including system outage.

BCM will be especially important if a university relies on IT processes under the following circumstances:

- Student registration and administration process are highly automated via web portals;
- Traditional paper-based information, such as staff/student records, academic research papers, sensitive financial data, are being digitalised;
- External IT vendors are employed to provide services on critical IT processes; and
- Certain information resources or processes are consolidated and shared among multiple universities, for example shared IT service centres.

Reference:
http://www.bs25999.com/2009/12/bs25999-bcms-summary/
http://www.thebcicertificate.org/pdf/GPG_2010_Edited_Highlights.pdf
KPMG Publication - Business Continuity Management

Statistical Report

Symantec sees opportunity as world is awash in data

Surveys point to a 400% rise in data growth over the next four years. What is of critical significance to industry is that over the next few years, IT budgets are projected to grow only 20% and administration staff is likely to increase only 10% as against the data growth of 400%. The changing scenario caused by data growth will lead to increased storage, administration and back-up window costs, besides making disaster recovery more expensive.

(http://economictimes.indiatimes.com/infotech/software/Symantec-sees-opportunity-as-world-is-awash-in-data/articleshow/6261756.cms)

Related Article

Professional Practices for Business Continuity Practitioners

BCM identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and value creating activities. The primary objective is to allow the Executive to continue to manage business operations under adverse conditions, by the introduction of appropriate resilience strategies, recovery objectives, business continuity, operational risk management considerations and crisis management plans.

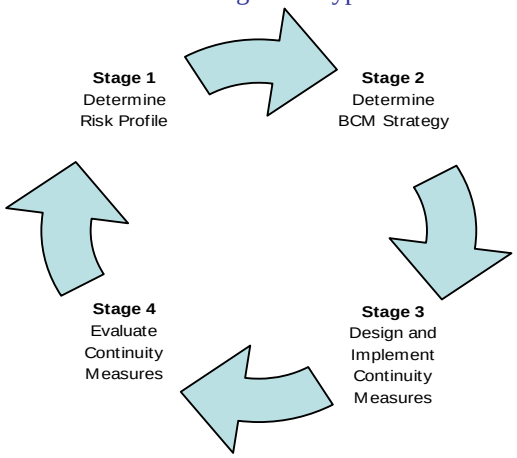
(https://www.drii.org/docs/ppintro.pdf)

II. Management

Facing with increased exposure to new risks and a decreasing tolerance for disruptions to their operations, universities may find it prudent to evaluate their ability to respond to crisis and mitigate possible future risks.

BCM Lifecycle

BCM Lifecycle is a series of good practices for universities to implement business continuity management. There are four stages in a typical BCM lifecycle.



Stage 1 – Determine Risk Profile

To start the BCM Lifecycle, universities' management shall understand its organisation by reviewing what its objectives are, how it works functionally and the constraints of the environment where it operates. Several tools and methodologies can be used to understand the organisation and determine the risk profile.

- **Business Impact Analysis (BIA)**
  BIA evaluates the impact over time of a disruption to an organisation's ability to operate.
- **Continuity Requirements Analysis (CRA)**
  CRA estimates the resources, facilities and external services that each activity will require at both resumption and return to "business as usual" after a disruption.
- **Risk Assessment**
  Risk assessment estimates the likelihood and impact on specific functions based on threats to known vulnerabilities.

Stage 2 – Determine Business Continuity Management Strategy

After determining the risk profiles (i.e. vulnerability, threat and impact) of universities' key resources and activities based on BIA, CRA or risk assessment outcome, management shall develop corresponding BCM strategies in response to the assessed risk profile of each key resource or activity. The most commonly applied BCM strategies are listed below:

- **Risk Acceptance**
  Universities may adopt a "do nothing" BCM strategy if the risk level is low and can be acceptable within universities' risk appetite.

References:
http://www.bs25999.com/2009/12/bs25999-bcms-summary/
http://www.thebcicertificate.org/pdf/GPG_2010_Edited_Highlights.pdf

II. Management (cont'd)

- **Risk Transfer**
  In the event of loss, universities may choose a risk transfer strategy that can transfer the economic damage to external insurance providers for financial compensation. However, such strategy does not provide protection against a loss of reputation.
- **Risk Mitigation**
  Universities may implement a set of internal controls and actions plans to reduce the possibilities or impact of a vulnerability being exploited.
- **Risk Avoidance**
  When the risk is significant, in terms of either the probability or the impact of threats, the most effective strategy is to bypass / replace the original high risk activities or resources.

Upon completion of Stage 1 and Stage 2, management shall also determine the priorities based on assessed risk profiles and BCM strategies.

Stage 3 – Design and Implement Continuity Measures
The third stage of the BCM Lifecycle is to develop and implement a BCM response that realise agreed strategies through the process of developing a set of Business Continuity Plans (BCP). The following steps should be included:

1. Design
Universities should determine the people, processes and technologies that meet the minimum availability of key resources and the maximum time frame within which the key activities must be resumed.

The following major elements should be defined:
- Crisis Management Team members and reporting hierarchy;
- Staff resources and skills for implementing continuity measures;
- Backup operation premises;
- Secondary telecommunication architecture; and
- Data restoration techniques and equipments for backup operation premises.

2. Implementation
During the implementation phase, universities should consolidate all elements determined in the design phase and formulate them in the BCP. A typical BCP can include (but is not limited to) the following essential information for preparation for and recovery from an incident:
- Overview of the adopted recovery strategy;
- Overview of the BIA / CRA / Risk Assessment results;
- Management structure and composition;
- Management and staff cascade lists and notification procedures;
- Invocation authorities and procedures;
- Detail of recovery teams, members and tasks;
- Definition of recovery requirements and timeframes:
- Number of staff requiring recovery at each timeframe;
- Critical technology (hardware, software);
- Detail of offsite recovery locations and storage facilities, and the retrieval procedures; and
- Details of critical users and suppliers

Related Article

Ensuring business continuity in higher education IT

In education institutions, as in many other types of organization, the influence of IT systems has gradually crept in to all the functions of the organizations. In all academic subject areas and across administrative functions, IT systems now perform a range of essential roles. However, the gradual creep of our dependence on technology has left many institutions unaware of their reliance upon it. As a result, it is easy to neglect the effect that a catastrophic event might have in IT terms.

(http://www.corp.att.com/edu/docs/HEBC.pdf)

Related Article

Ensuring Business Continuity during a Pandemic Outbreak

In the wake of alerts from the World Health Organization (WHO) and President Obama's October 24 declaration of a national H1N1 health emergency, public and private agencies in the U.S. and other countries have been mobilizing their responses to the swine flu outbreak. With 74 countries reporting cases of H1N1 infection as of October, the epidemic is providing a real test of pandemic preparedness at all levels of society.

(http://www.symantec.com/business/resources/articles/article.jsp?aid=20091027_ensuring_business_continuity)

References:
http://www.bs25999.com/2009/12/bs25999-bcms-summary/.
http://www.thebcicertificate.org/pdf/GPG_2010_Edited_Highlights.pdf.

II. Management (cont'd)

Stage 4 – Evaluate Continuity Measures

Before finalising a BCP, adequate tests should be conducted by the university's management and relevant process owners to ensure correctness and applicability of the BCP. Common test approaches include paper test (process owners review BCP), structured walkthrough test (in-depth discussion of BCP procedures) and preparedness test (simulation of an actual incident in specific areas).

After the BCP is finalised and comes into effect, periodic BCP drill and review is a necessary practice within the BCM lifecycle as most organisations, including universities, exist in a dynamic environment and are subject to changes in people, processes, environment, risk, geography and strategy. Implementation of such regular BCP maintenance procedures seeks to ensure that the operational continuance capability accurately reflect the current nature, scale and complexity of the universities, and is understood by all universities' stakeholders and members.

Roles and Responsibilities

The roles and responsibilities per each level of management and user are summarised in the table below.

	Top Management	IT Management	Middle Management (e.g. Department, Process Owner, etc)	General User
Stage 1	• Understand the risk of the university and the need of Business Continuity Management	• Perform risk assessment specific to the IT environment	• Perform risk assessment specific to individual departments • Carry out business impact analysis	• Assist individual departments on risk assessment and business impact analysis
Stage 2	• Determine how the university should treat the existing risks	• Provide advice to top management for addressing IT related risks	• Provide advice to top management for addressing risks identified in individual departments	• Report their concerns of the acceptability of risks in individual departments
Stage 3	• Assign relevant resource • Ensure the BCPs address the risk profile of the university	• Coordinate with individual departments to design and implement BCPs based on risk assessment and BIA results	• Coordinate with IT management to design and implement BCPs based on risk assessment and BIA results	• Understand the continuity measures • Be familiar with relevant BCPs and emergency contact
Stage 4	• Evaluate the BCP based on the BCP tests • Initiate periodic BCP drill and review	• Conduct adequate tests to ensure the correctness and applicability of the IT continuity measures in BCP	• Conduct adequate tests to ensure the correctness and applicability of the operational continuity measures in BCP	• Participate in the BCP tests and provide feedbacks to management

Related Article

Hayward's end just first step for BP

Tony Hayward's resignation as BP's chief executive will go some way to meeting this precondition for recovery. But it will be nowhere near enough on its own.

While Mr Hayward was in many ways an effective leader, he is right to step down. He must bear the ultimate responsibility for what went wrong after the Deepwater Horizon rig blew up on April 20. The explosion revealed many shortcomings, notably Mr Hayward's failure to fix BP's poor safety record. BP's crisis management was also poor. Mr Hayward made unwise statements to the media which appeared to play down the size of the spill.

(http://www.ft.com/cms/s/0/952ce64c-98e6-11df-9418-00144feab49a.html)

Related Article

Do you need a reality check for IT disaster preparedness?

Almost every business has a business continuity and disaster recovery (BC/DR) plan in regard to overall facilities, operations and personnel affected by a disaster. But what most companies consider disastrous threats are weather-related or earthquakes or potential terrorist attacks. Smaller events, in physical scale, such as malfunctioning software caused by a computer virus or a power outage for an unforeseen amount of time, could end up being just as costly. When a disaster of this nature strikes, a business may realize its BC/DR plan has not kept pace with the ever-changing technological environment, and the need for an adequate IT BC/DR plan suddenly becomes glaringly apparent.

(http://www.sbnonline.com/Local/Article/20418/73/244/Do_you_need_a_reality_check_for_IT_disaster_preparedness.aspx?Category=)

References:
http://www.bs25999.com/2009/12/bs25999-bcms-summary/.
http://www.thebcicertificate.org/pdf/GPG_2010_Edited_Highlights.pdf.

III. General Users

The role of general users in Business Continuity Management is often overlooked. However, adequate user participation in BCM Lifecycle is essential to the success of the continuance of BCM capability of the organisation.

Awareness and Training

General users engaged on business continuity activities should equip themselves with the appropriate training and knowledge. This will include an awareness of the university's operational structure and function, understanding the critical resources required for continuous operations, and participating in regular drill exercise.

Departments should ensure that all staff are aware of the expectations held of them should an emergency arise. This could be achieved through exercises, BCP drills, visits to recovery locations, and HR induction and orientation procedures.

Distribution of Business Continuity Plans

Copies of relevant business continuity plans should be available to members of the individual departments and staff. Emergency contact information should be distributed to all staff.

Testing of Business Continuity Plans

A testing process shall be established to verify that the plan is up to date and match the needs of the departments. Members of each departmental recovery team must be familiar with the plans through the testing process. General users should participate in the tests and exercises of the plans.

Emergency Response and Operations

Each individual department should manage the processes of:

- Emergency drills;
- Emergency warden identification and training;
- Evacuation procedures and post review; and
- Salvage and restoration

All levels of general users shall participate in emergency drills and exercises. Reference and guidelines of details of the above should be made to individual departments.

Conclusion

In summary, an effective BCM is a continual process to identify universities' vulnerabilities, assess risk levels and develop corresponding countermeasures, which requires both the commitment from management and cooperation of general users.

Related Article

Airbus Unit Certified to Business Continuity Management Standard

Mindful of the estimated $5 billion loss attributed to flight cancellations when ash from the Eyjafjallajokull volcano in Iceland closed parts of Europe's skies in April 2010, Airbus has become the first aerospace manufacturing company with certification BS 25999, the Business Continuity Management System standard. BSI Group, the London-based standards developer, performed the audit. The Airbus unit achieving certification is a wing manufacturing site in Broughton, England.

(http://ohsonline.com/articles/2010/07/12/airbus-unit-certified-to-business-continuity-management-standard.aspx?admgarea=news.)

Related Article

Disaster recovery planning takes time, but worth it

"The trend is for the enterprise IT departments to plan to have mission critical systems offsite and to make those redundant through high-speed interconnects between the main facility and the offsite disaster recovery facility," Brack said. "Our disaster recovery facility is in Dallas, five hours away. We've spent years ensuring there is dedicated and sufficient bandwidth so we can have a mirrored system five hours inland that affords those levels of protection."

(http://www.cmio.net/index.php?option=com_articles&view=article&id=23375&division=cmio.)

References:
http://www.bs25999.com/2009/12/bs25999-bcms-summary/.
http://www.thebcicertificate.org/pdf/GPG_2010_Edited_Highlights.pdf.