International Journal of Engineering Science Invention Research & Development; Vol. I Issue X April 2015
www.ijesird.com e-ISSN: 2349-6185

A FRAMEWORK - BUSINESS CONTINUITY PLANNING FOR SECURE INFORMATION SYSTEMS

Manoj Nainwal[1], Anurag Awasthi[2]
[1]*Singhaniya University, School of Computer Science,PacheriBari(Junjhunu), Rajasthan, India.*[2] *CEO, CampCorp Consulting,New Shahadara, New Delhi ,India*
Manoj.nainwal13@email.com,Anuraag_awasthi@hotmail.com

Abstract: **The more your business relies on its IT systems, the more you need to consider how unexpected disruptions might affect your business. As a part of Business Continuity Management the Business Continuity Planning improves your business' ability to react to such disruptions. It describes how you will restart your operations in order to meet your business-critical requirements. These disruptions could come from many sources, from flood, fire and theft or malicious attacks on your systems, such as viruses or hacking. The aim of a BCP is to enable your business to restore business-critical systems and infrastructure as soon as possible after a 'disaster' event takes place. The plan should connect and focus on all systems used within the business, not just IT, as well as facilities and resources for staff.**

Organizations constantly evolve and recovery strategies must evolve with them. This means you need to monitor your BCP and make changes to it as and when necessary. For example: Business processes change and people join, transfer and leave organizations on a regular basis. Plans should be updated to reflect changes in recovery teams. New IT systems are introduced to support business activities. As these may be essential to your business, before you implement them you should consider your ability to recover them following a systems failure.

There are real business benefits to be gained from having a BCP. In some industries, eg financial services, regulators stipulate that organizations have sufficient continuity and security controls. Failure to have such controls - and have them tested - could result in heavy fines. If you have a BCP to show to potential customers, this may help you win - and retain - business. Having a BCP demonstrates to insurers that you are proactively managing risks to your business - and may help reduce your insurance premiums.

This research paper explains the importance of business continuity plans to the success of your business, and various considerations to have an effective and fault-proof business continuity planning to minimize the threat, and subsequent damage and ensuring business continuity. The paper suggests a catalogue for organizations wishing to identify and manage IT risks to their business.

Keywords: **Information Security, Business Continuity Management, Business Continuity Planning**

I. INTRODUCTION

Effective security of the information, which is an essential resource for all businesses today as a key to growth and success, can help you control and secure information from malicious changes or from unauthorized disclosure. Earlier the security of business IT systems has never been so important. But with the advancement in internet technology businesses rely more and more on IT to support their activities, and this makes them increasingly vulnerable to threats from hackers, viruses. As more and more data and information is transferred through internet and the impact of a security breach may be far greater than you would expect, you need to ensure that the information held on your IT systems is secure.

According to the Information Security Breaches Survey (ISBS) businesses of different sizes tend to exhibit different security profiles. Dependence on IT systems remains high, at similar levels to those seen two years ago - only one in six small companies would be able to continue their businesses without IT. Financial services, telecommunications and energy companies are most concerned about corruption of records since their turnover is largely dependent on electronic records. Availability is a significant concern to most sectors, though not-for-profit organizations are least concerned about outages. [6]

Information also needs to be protected if you share it with other organizations as the loss of sensitive or critical information may not only damage your reputation but also affect your competitiveness. For many businesses, the internet

has replaced traditional paper-based ways of exchanging information. It can be sent and received faster, more frequently and in greater volume.

However, the internet brings its own security issues which businesses must consider. Some of the threats posed by hackers on the internet include:

- gaining access to sensitive data such as employee records, price lists, catalogues and valuable intellectual property, and then altering, destroying or copying them
- altering your website to damage your reputation or direct your customers to another site
- gaining access to financial information about your business, employees or your customers for the purposes of fraud [1]

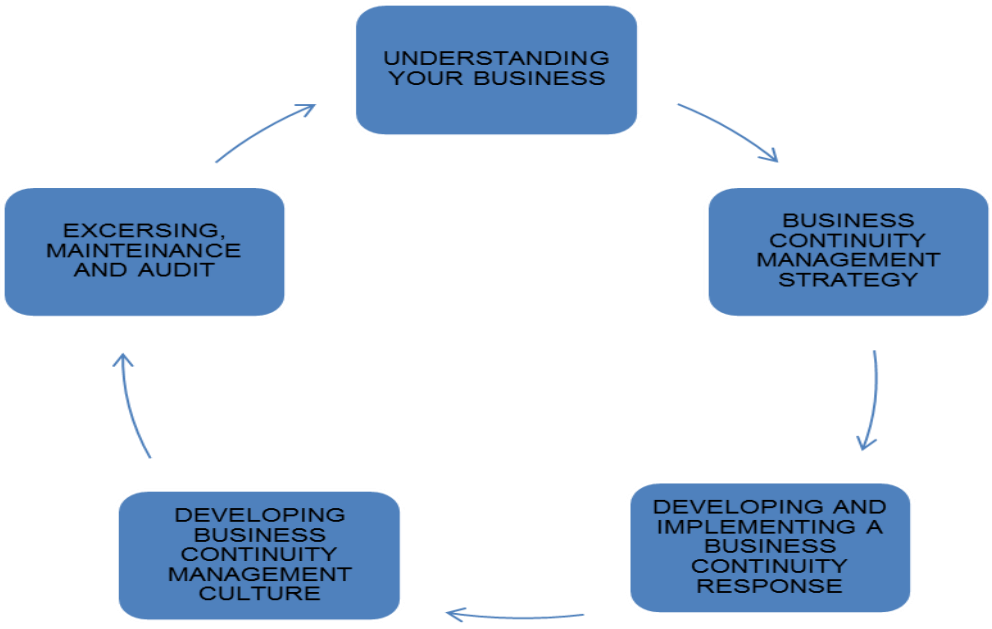
II. IMPORTANCE OF BUSINESS CONTINUITY PLAN

When a 'disaster' event takes place your business should have capability to restore critical systems and infrastructure as soon as possible. Your business should have such application which can recover all systems used within the business, not just IT, as well as facilities and resources for staff.

Business continuity is a process which is developed to handle systems failure. It is a management concern, not something that should just be considered by the IT department. If your IT systems fail or are unavailable, it is likely to have a significant impact on your whole business. Therefore you should take an active interest in establishing business continuity plans for your IT systems.

III. KEY STEPS IN DEVELOPING BUSINESS CONTINUITY PLAN FOR IT SYSTEMS

The Business Continuity Institute's 'Business Continuity Management Life Cycle' model covers five key stages in developing and maintaining a business continuity plan.



1. **Understanding Business Information System Security Requirements**

This step has the following activities: [11]

1.1 Project initiation and management - Establish a management structure to develop and carry out the plan.

1.2 Risk evaluation and control - With e-commerce, computer viruses might be a major threat - the appropriate defense might be regularly updated anti-virus software.

Risk identification for the system

1.2.1 Assessment of risk for its impact on the system

1.2.2 Risk reduction analysis

1.2.3 Risk mitigation - impact reduction

1.2.4 Contingency plans to handle risk

1.2.5 Business Managers Action Plan

2. **Business Continuity Management Strategies**

2.1 Develop an organizational business continuity strategy, identifying which areas you need to concentrate on. Focus on the critical operating requirements of the business, as identified above.

2.2 Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for your e-commerce website goes down, you need a specific strategy for resuming operations.

3. **Developing and Implementing a Business Continuity Response**

3.1 Emergency response and operations - establish a crisis management process to respond to incidents. Find out about crisis management on the Continuity Central website.

3.2 Develop and implement a business continuity plan. This describes specifically how you will deal with incidents. Focus on the priorities of your overall business continuity strategy.

3.3 Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

4. **Developing a Business Continuity Management Culture**

4.1 Awareness and training plans - ensure all staff are aware of the importance of business continuity and can operate effectively following an incident.

4.2 Review the effectiveness of awareness training periodically. Identify any further training needed.

5. **Exercising, Maintenance and Audit**

5.1 Test the business continuity plans. Test any technical aspects - for example if you plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.

5.2 Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.

5.3 Regularly audit the plans - do they meet the needs of your strategy? Act on your findings.

IV. COMPONENTS OF BUSINESS CONTINUITY PLAN

The plan should aim to reduce the risks posed by disruption to your business processes. Measures that may be needed include:

- A back-up and data recovery strategy, including off-site storage.
- The development of a resilient IT infrastructure with redundancies (spare capacity) in case of failure. For example, mirrored central server computers sited in different locations, each containing the same information, so that if one goes down, the other one is available to ensure continuity of service and alternative storage facilities.

- The elimination of single points of failure, such as a single power supply.
- The introduction of an uninterruptible power supply for your IT systems. This is a battery-powered device that allows your systems to keep running, giving you time to save any data that you may be working on.

Even if such measures are adopted, things can still go wrong. Therefore, the business continuity plan should specify the actions to be taken in order to recover from any unexpected disruptive event, covering:

- people and accommodation
- IT systems and networks
- services such as power and telecommunications
- critical business processes

Methods of recovery might include:

- carrying out activities manually until IT services are resumed
- moving staff at an affected building to another location
- agreeing with another business to use each other's premises in the event of a disaster
- arranging to use IT services and accommodation provided by a specialist third-party standby site

Keep the business continuity plan short and readable. It should not duplicate other sources of information, and any other relevant documents should be referred to. Encourage staff to review the plan before it is formally issued**. [5]**

V. BENEFITS OF BUSINESS CONTINUITY PLAN FOR IT SYSTEMS

The main benefit of business continuity planning is enabling your business to recover quickly from unexpected events that disrupt your IT systems. However, there are other good reasons to have a business continuity plan.

A. Legal requirements

In some industries, it is a regulatory requirement to have a recovery plan in place. For example, financial organizations must have continuity and security controls.

B. Customer reassurance

A business that can demonstrate an effective business continuity plan has a competitive advantage. For example, if you provide services to customers that are dependent upon your IT systems, like an internet service provider, then evidence of a sound plan can be used to win or retain customers. For instance, if your business is a partner in a supply chain, business continuity planning may well need to be an integral part of your quality assurance.

C. Insurance

Effective business continuity management can help businesses demonstrate that they are managing their business risks and so help to secure lower insurance premiums. In addition, drawing up a business continuity plan can help you assess what types of insurance you need the most.

This is because business continuity planning may help to identify potential business risks that you were previously unaware of, but which you recognize that you need to insure against. So, you may decide to opt for lower insurance cover across a broader range of risks - the original risks plus the recently identified ones - in order to remain within your budgeted insurance cost.

VI. CONCLUSION

In Indian perspective we need to have business continuity planning and a framework which is according to the BS ISO/IEC 27001 standards. The most important aspect of any business now a day is its information and information management systems. To comply with standards we need to have information security policies, policy management in a business, asset classification and control, staff training to respond to a security incident, protection of equipment and information, communications and operations management process, access control to information and security and system and planning compliance with the national and international laws.

BIBLIOGRAPHY

1. IT risk management guidance on the Software Engineering Institute website http://www.sei.cmu.edu/risk/
2. Latest security updates for Microsoft software applications on the Microsoft website http://www.microsoft.com/protect/computer/updates/bulletins/default.msp x
3. Cloud computing security guidelines on the Cloud Security Alliance website http://www.cloudsecurityalliance.org/
4. IT disaster recovery information on the National Computing Centre website http://www.ncc.co.uk/article/?articleref=113201
5. Business continuity good practice guidelines on the Business Continuity Institute website http://www.thebci.org/gpg.htm
6. IT disaster preparation and recovery advice on the lasa knowledgebase website http://www.ictknowledgebase.org.uk/disasterpreparationrecovery
7. BS 25999-1:2006 Business Continuity Management Part 1: Code of practice
8. BS 25999-2:2007 Business Continuity Management Part 2: Specification
9. BS 25777:2008 Information and communications technology continuity management - Code of practice
10. "A Guide to Business Continuity Planning" by James C. Barnes
11. “Rethinking Risk Management” by Audrey Dorofee, Christopher Alberts, NDIA Systems Engineering Conference 2009, Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213