Business Contingency Planning: A Road Map to Protect Company from Unforeseen Threats

Ankur Kumar Shrivastava, Nitisha Payal, Abhinav Kumar, Amod Tiwari

Abstract: - Unforeseen threats never knock the door before their arrival; they just arrived and destroy everything that comes in the path. Establishing a secure business is not just about supply and demand. It is about the prevention and protection measures that you can put in place against cyber-crime, the consequences of an electronic attack, natural disaster, acts of terrorism and other events that would have a negative impact on your organization. In this paper our major focus on creating an effective and globally accepted business contingency plan, which is applicable on almost all type of business and their processes to handle any crises and smooth operation of their critical functions. This paper also focuses on need of BIA and discusses all the key aspect of BIA model for analysing the impact of an unforeseen threat over a business critical function. In this paper we also try to provide a complete overview of existing business contingency and risk assessment model.

Keywords: - BCM (Business Continuity Management), BCP (Business Continuity Plan), BIA (Business Impact Analysis), DRP (Disaster Recovery Plan), Risk Rating, RTP (Risk treatment plan).

I. INTRODUCTION

Consider a scenario of centralized data centre building of an email server which may be demolish due to any one of these scenario, i.e. consequences of an electronic attack, natural disaster, acts of terrorism. In this situation what are the major disruption to a business organization:

- Company will lose all the critical data related to their business.
- Costumer's personal information will be lost permanently.
- Costumer's and users are not able to access their email account or other web services.
- Company loses the confidence of their Bank, Financial Institute and stakeholders.
- Company loses the organizational assets.

Thus business contingency plan play a vital role to reduce the impact of any unforeseen threat and respond quickly to recover the business from disruption to their normal operating routine.

So business contingency ensure that your company can continue doing business even when its normal facilities or place of business is unavailable. A contingency plan is the process of developing advance arrangements and procedure that help any organization to respond to an unforeseen event that could occur by chance or unforeseen threats. It is a framework or preventive action used by an organization to overcome with the negative impact of any failure or disruption in operations.

A business contingency plan may use variety of resource including working procedure, an alternate operational area, a third-party agreement, or shifting resources.

A. Business Contingency planning is important to answer:

- What would you do tomorrow if your building were on fire today?
- What would your market competitors do?
- What would your shareholders and bank do?
- What are the risk rating criteria?
- What is your risk treatment plan?
- What is your expected down time to recover?

B. Some threats usually covered in contingency plan are:

- Crisis Management
- Continuity Plan
- Asset Security
- Mismanagement
- Reorganization

C. Some Standard related to Business Contingency is:

- BS25999
- ISO270025

II. MODEL & METHODOLOGIES

There are various business contingency planning models and methodologies. Most of the models include the following phases of the business contingency planning:

- Understanding Your Business
- Business Contingency Strategies
- Development and Implementation of Contingency Plan and Solutions
- Building and Embedding a Contingency Culture
- Exercising, Maintenance and Audit

Fig.1. Generic Model of BCP

Manuscript received on August 25, 2012

Ankur Kumar Shrivastava, CMJ University, Shillong, Meghalaya,India.
Nitisha Payal, Department of Computer Science MIET, Meerut, India.
Abhinav Kumar, Mahindra SSG, Mumbai, India,
Amod Tiwari, Department of Computer Science PSIT, Kanpur, India.

This emphasis on the importance of:

- Understand business contingency need and the necessity for establishing policy and objectives for business continuity.
- Implementation and operation of controls for ensuring an organization's global business continuity risks.
- Monitoring and reviewing the performance of business contingency plan.
- Continual improvement based on business contingency objectives, measurements.

III. RISK ASSESSMENT MODEL

There are various risk models. For creating effective business contingency plan we focus on the following phases of the risk:

- Technical Risk.
- Economical Risk
- Social Risk
- Risk associated with People

Fig. 2. Risk Assessment Model

This emphasis on the importance of:

- Understanding technical risk like IT system break down and Industrial Accident.
- Analysing economical risk such as government crisis and utility failure.
- Understand the impact of social risk such as terrorism, labour strikes, off-site product tampering.
- Monitoring and reviewing the people so that on-site product tampering, malicious acts and organizational failure can be identified on time.

IV. PROPOSED MODEL

In this approach we are proposing a 7-stage model for contingency planning which can focus on all the major area of contingency plan and help organizations to nurture their business growth according to their set goals or objectives.

Fig. 3. Proposed Model

Stage- 1 Business Contingency Policy and Scope:

- Provide advice in understanding and interpretation of both part of BS 25999, i.e. project plan and corporate security.
- Determine the business contingency scope.
- Developing business contingency document.

Stage- 2 Understanding the Organization:

- Conducting analysis of current organization environment and business contingency plan status, i.e. business contingency strategy, business contingency plan and post review report for exercise.
- Identification of key processes, activities and services.
- Define Timeline.
- Kick off meeting.

Stage- 3 Data Acquisition:

- Perform interviews.
- Gather information.
- Existing IT systems and application.
- Network architecture diagram.
- Existing policy and procedures.
- Previous risk assessment and audit report.
- Gap assessment.

Stage- 4 Business Impact Analyses:

- Identify activities and services that support IT key product and services.
- Identify impact result from disruptions.
- Establish the maximum tolerable period for disruptions.
- Set activity priority.
- Set recovery time period for resumption of critical IT activities.

Stage- 5 Risk Assessments:

- Technical vulnerability assessment.
- IT process vulnerability assessment.
- Business process vulnerability assessment.
- Physical security control evaluation.
- Risk assessment and determination.
- Identification of existing control.
- Identification of planned control

Stage- 6 Developing and Maintaining Business Contingency plan:

- Developing crisis management plan.
- Developing business contingency plan.
- Developing resource recovery plan.

Stage- 7 Exploring Monitoring and Reviewing Business contingency Plan:

- Exercising and maintaining business contingency plan.
- Identification of business contingency plan Improvement.
- Preparation of Business contingency plan certification i.e. BS 25999.

V. BUSINESS IMPACT ANALYSIS

One of the primary duties of a Security Professional in an organization is to ensure that their information system and data can survive even in case of a disaster. In order to achieve this, these professionals identify critical information systems, tasks and processes and also define the priority of one over another so as to identify, which order these processes must be recovered after the disaster. A key requirement to identify such critical functions of organization is to conduct an effective Business Impact Analysis. Like BC planning, there are various methods for conducting BIA. The Most elementary step to conduct BIA is shown below:

Fig. 4. Key Aspect of BIA

A BIA is conducted to find the―maximum tolerable outage‖ [3] for each & every business process of an organization. It tells an organization, for each of its business process, the maximum time duration the organization can tolerate being without the process before its absence makes a significant impact on the business. After performing a Business Impact Analysis, the next vital step in a business continuity planning is to use the information that is collected in BIA as an input for selecting the strategy to recover critical business processes. But before selecting the strategy, one should recognize the preventive controls that exist in the organization. These controls can save money as well as effort while pursuing BCP strategy.

Different types of preventive controls include:

- Information Security Control
- Environmental Security
- Physical Security
- Disaster Recovery Plans
- Awareness Program

VI. CONCLUSIONS

It is evident that there is growing awareness of Business Contingency Plan and its management in current business environment but the only problem is the lack of understanding about what a Business Contingency Plan program is and what it can imply. Another important thing is that there is lack of resources for implementing business contingency plan program. It is mainly due to inadequate manpower designated for such a key area. People are having misconception regarding a Business Contingency Plan and a DRP. So there is a need to increase awareness and branding in business contingency plan to make it more effective. We must remember that "*A journey of a thousand miles begins with a single step*" and we probably are already a few miles on the road

REFRENCES

1. Security fundamentals by Peltier, Thomas R.; Peltier, Justin; Blackley, John.
2. Survey by Deloitte (Deloitte Touche Tohmatsu India Private Limited (DTTIPL)) in association with The Business Continuity Institute, UK ('The BCI').
3. http://www.businesslink.gov.uk/bdotg/action/layer. [11th June, 2012, 11:30am].
4. http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999.
5. http://www.businessdictionary.com/definition/business-continuity-planning-BCP.html.
6. http://www.contingency-planning-disaster-recovery-guide.co.uk/.
7. http://www.bplans.com/ask-bplans/648/how-do-i-write-a-contingency-plan.
8. http://smallbusiness.chron.com/business-contingency-plan-1081.html.
9. http://www.drj.com/new2dr/w3_006.htm.
10. http://www.wikihow.com/Create-a-Business-Continuity-Plan.

AUTHORS PROFIE

Ankur Kumar Shrivastava: Born in 1981 in Ghazipur distict (Uttar Pradesh). Phone Number +919335092777 & E- Mail Id: ankurshrivastava16@gmail.com. He completed his B.Tech. (Information Technology) from Allahabd Agriculture Institute Deemed University, Allahabad, M.B.A. (Marketing) from Sikkim Manipal University, Sikkim, M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad, and currently pursuing Ph.D (Information Security) from CMJ Shillong, Meghalaya.He had 2 years Industry Experince from Reliance (RIPL,DAKC),Mumbai.He had more than 1 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. Ankur has published his research work in Springer International Conference of Computer Networks and Intelligent Computing in August, 2011, IT-BHU National Conference of Artificial Intelligence in December, 2011 and International Journal of Innovative Technology and Exploring Engineering of Computer Science in August,2012.

His major field of Study Areas are Information Security, Forensic Science, Cryptography, Network Security, Vullnerability Assesment and Penteration Testing, ISO 27001 and Software Engineering.

Nitisha Payal: Born in 1987 in Meerut (Uttar Pradesh). Phone Number +917830630414 and E-mail Id: nitishapayal@gmail.com.She completed her B.Tech. (Computer Science And Engineering) with honors from Uttar Pradesh Technical University and currently pursuing M.Tech. She had 1.5 year Teaching Experience from Meerut Institute of Engineering & Technology, Meerut. Nitisha has published her research work in International Journal of Innovative Technology and Exploring Engineering of Computer Science in August,2012. The major field of Study area are Software Engineering, Software Project management, Oops, ITIM and Operating System.

Abhinav Kumar: Born in 1986 in Ghazipur distict (Uttar Pradesh). Phone Number +919920423488 & E-mail Id: er.abhinavshrivastava@hotmail.com. He completed his B.E. (Computer Science Engineering) from University of Rajasthan, and then attained his M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad. He has more than two years of Industry Experience. Currently he is working with Mahindra SSG as an analyst. He worked with NII Consulting (Mumbai), MG Techno Savvy Pvt. Ltd (Jaipur), and Tryst Technologies Ltd (Jaipur). He has also held a position of a lecturer with Meerut Institute of Technology (Meerut) for four Months. Abhinav has published his research work in Springer International Conference of Computer Networks and Intelligent Computing in August, 2011, IT-BHU National Conference of Artificial Intelligence in December,2011 and International Journal of Innovative Technology and Exploring Engineering of Computer Science in August,2012. He is a certified Lead Auditor for ISO27001, ISO20000, and BS25999. His major fields of work areas are ISMS, BCMS, IT Audit, Risk Assessment, Current State Assessment, Artificial Intelligence and Computer Networks.

Amod Tiwari: Born in 1974 in Kanauj district (UttarPradesh). Phone Number +919415539025 & E-mail Id: amodtiwari@gmail.com.He acquired his Bachelor degree in Mathematics and Science from CSJM Kanpur University Kanpur and master degree in Computer Science and Engineering from Bilaspur Central University, Bilaspur (CG) in India. His Academic excellence shines further with PhD in Computer Science and Engineering from Indian Institute of Technology Kanpur. Working for reputed firm like LML Scooter India Ltd, Kanpur, at senior level more than two years. He has been associated with Indian Institute of Technology Kanpur from 2005 to 2010. He is currently working as Associate professor and Dean Academic and Affairs in PSIT Kanpur. Amod Tiwari has more than 40 Publications in his credit.