CASE STUDY: Small Organization Business Continuity Plan Creation

By Veo Taylor

Spring 2009

Abstract

Why develop a business continuity plan? Organizations have an inherent responsibility to their members. The executive staff of an organization is there not only to run the organization effectively for stakeholders, but also to protect the members of the organizations and its assets. A business continuity plan is one way to achieve this. Planning ahead is more likely to reduce issues if "something" occurs. Without a BCP, the organization could lose financial earnings as well as the not be able to fulfill its mission.

What is the first step in creating a BCP? Initially, a project team must be established. A project manager will be needed to control the project itself; people (personnel) will be needed on the team to get the project moving forward.

Who should be on the BCP project team? The plan will need to have senior level management commitment, i.e. CEO, CIO, and COO. Representatives from IT, HR, and (physical) facilities management are keys to the project. These are essential infrastructure pillars to the plan. Senior member representation of other areas will be needed to cover the functional areas of the plan.

How much time should the BCP take? To get the BCP created is approximately a 3 to 4 month process. Key infrastructure personnel will spend about 20 to 40 hours per week on the BCP during this initial period; personnel from the other areas will spend about 8 to 16 hours per week on the BCP. Once the plan is completed, a few hours per quarter is all that will be needed to maintain/update the BCP.

What are some BCP creation obstacles?

<u>Commitment</u> : Sr. level organizational support is key; without this support, the project will fail.

<u>Time</u> : Time has to be made for this project as well as for already existing projects.

<u>Budget</u>: The project needs proper funding.

<u>Personnel</u>: Staff members are needed to work on this project.

What is the goal of the BCP? The goal of the BCP is to develop a plan to ensure that recovery from a major incident is as expeditious as possible. The company shall practice due diligence and be prepared as much as possible in the event of a disruption in the normal business activities of the company. The BCP will greatly assist any company with any unforeseen events. But organizations must get started with the BCP creation and make it part of their normal business practices. When new business programs are developed, BCP impact for those programs must be assessed. Having the BCP firmly embedded into the fabric of the enterprise will be great for business and give stakeholders more confidence in the company's business practices moving forward.

Table of Contents

Prelude

Business Continuity Planning (BCP) is a rigorous and well-informed organizational methodology for developing a step-by-step guideline defining how the organization will recover from a disaster or extended disruption. It is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. In plain language, BCP is working out how to stay in business in the event of disaster. BCP is very necessary today given terror threats, increased climate volatility, etc.

It prepares companies and organizations to maintain business technology during a catastrophe. A Business Continuity Plan ensures the required infrastructure solutions are in place and defines procedures for recovering in the event of a disruption of business processes. Through a BCP, a business can return to normal operational status within an acceptable and reasonable timeframe. Given today's overwhelming reliance on computers and technology, IT restoration is a crucial factor for every business. [1]

Through the use of a fictitious company, this case study will illustrate *how to create a BCP*. It will document in detail key steps to follow for BCP creation: management commitment, BCP project personnel, employee training, physical security, due diligence via risk analyses and assessments, logical security, backing up critical data, and other tasks. This case study will be very useful to small companies which have yet to implement a BCP or to organizations needing to improve their standing BCP's.

Introduction

The company that will be the focus of this case study is **Blue Viceroy Health Data**. It provides a structure for gathering electronic health information and accessing the expertise of the Blue Viceroy team to ensure the information is confidential, unaltered, and available. The information includes demographic information collected from an individual, which identifies the individual or can be used to identify the individual. The company has 100 employees and is located in Chicago with all of its employees living within the Chicago-land area. It has five business departments plus its executive board of directors. Its main base of customers includes pharmacists, physicians, patients, educational institutions, day care establishments, government agencies, and insurance companies.

Planning the Organizational Strategy

Initializing the BCP Project

The incoming (ISM) Information Security Manager is given an out-dated emergency plan with a list of names to contact in-case there is some type of emergency within the company and list of now out-dated and unused systems. However, there is nothing formally written in terms of disaster recovery and business continuity. IT has its data backup, but that is no substitute for a fully implemented BCP. Therefore, he makes it a priority to instantiate a proper Business Continuity Plan that's more appropriate for Blue Viceroy Health Data.

Senior Management Meeting Preparation

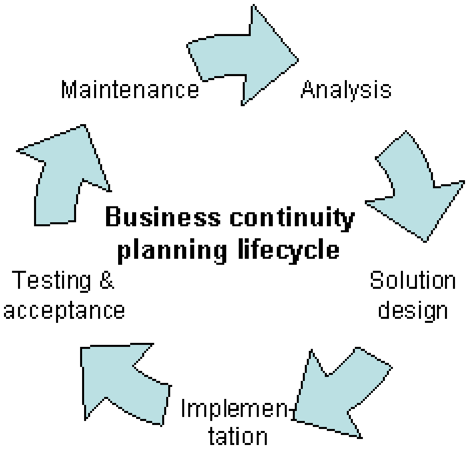
He appoints his Senior Engineer to lead this effort as the Project Manager. The Sr. Engineer's education and work experience qualifies him for the task at hand. The qualifications for PM are as follows:

- Managing small or medium scale IT software and database development projects which included analysis, design, coding, unit testing, quality assurance, implementation, infrastructure and security tasks, as well as system maintenance work
- Developing and managing project plans and resources using project management software, such as Microsoft Project
- Defining and managing project Cost, Scope, Schedule, and Quality including developing project budgets, scope statements, project schedules, and quality standards
- Performing Risk Identification including the development of a Risk Assessment
- Developing and executing project communication plans
- Monitoring and controlling risks
- Managing project execution and control
- Experience with managing projects in the healthcare information field

The (PM) project manager's first assignment is to identify key personnel from each department of the company that will be able to provide valuable input to the plan. This information is necessary as the ISM prepares to take this issue to the company leadership for its backing. Without the support of Senior Management, the ISM's BCP initiative will surely fall short. Key areas of focus are IT, HR, and building management. Input from these three areas is critical, so proper and effective representation is first and foremost. Even though the project manager has focused on certain personnel from the core areas, the senior manager from each area eventually chooses its representative for the BCP. These core representatives do have equal input with the BCP. Eventually, the plan needs to reflect the important business needs of each department.

Kickoff Meeting

The ISM shows the Executive staff what he currently has as a BCP, the out-dated emergency plan. He then gives a very eloquent soliloquy on why it's necessary and just plain good business practice to have a formal BCP. Since we're dealing with patient data, HIPAA compliance makes it necessary. At this point, if the company is subjected to an audit, it will fail and be primed for legal discipline. He points out what a good BCP will illustrate with the following diagram:



2

Figure 1. Business Continuity Life Cycle.

The ISM lets them know that this is not just a one-time "deal". This is an on-going process that needs to be tested and maintained, and moreover, as the business grows and changes, more analysis will need to be done so that the plan will continue to reflect current business functions.

Executive staff realizes that it puts forth a huge amount of effort into the function and growth of the business but lacks in the maintenance and support of a formal BCP. The ISM has just saved the company from some serious harm with this initiative. The Exec-staff fully supports the ISM and the new BCP project.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to improve the efficiency and effectiveness of the health care system by encouraging the development of a health information system, through the establishment of standards and requirements for the electronic transmission of certain health information. Any health care provider, health plan, hospital, health insurer, and health care clearinghouse that electronically maintains or transmits any electronic protected health information (EPHI) must comply with HIPAA regulations. [4]

The HIPAA Security Standards provide a structure for covered entities (health plans, clearinghouses, or covered health care providers) to develop and implement policies and procedures to guard against and react to security incidents. The Security Rule provides a flexible, scalable and technology neutral framework to allow all covered entities to comply in a manner that is consistent with the unique circumstances of their size and environment.

To understand the requirements of the Security Rule, it is helpful to be familiar with the basic concepts that comprise the security standards and implementation specifications. Each Security Rule *standard* is a requirement: a covered entity must comply with all of the standards of the Security Rule with respect to the EPHI it creates, transmits or maintains.

Many of the standards contain *implementation specifications*. An implementation specification is a more detailed description of the method or approach covered entities can use to meet a particular standard. Implementation specifications are either *required or addressable.* Regardless of whether a standard includes one or more implementation specifications, covered entities must comply with each standard. Where there is no implementation specification for a particular standard, such as the “Workstation Use” and “Person or Entity Authentication” standards, compliance with the standard itself is required.

- A **required** implementation specification is similar to a standard, in that a covered entity must comply with it. For example, all covered entities including small providers must conduct a “Risk Analysis” in accordance with Section 164.308(a)(1) of the Security Rule.

- For **addressable** implementation specifications, covered entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in the covered entity’s environment. After performing the assessment, a covered entity decides if it will implement the addressable implementation specification; implement an equivalent alternative measure that allows the entity to comply with the standard; or not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment. Covered entities are required to document these assessments and all decisions. For example, all covered entities including small providers must determine whether “Encryption and Decryption” is reasonable and appropriate for their environment in accordance with Section 164.312(a)(1) of the Security Rule.

- Factors that determine what is “reasonable” and “appropriate” include cost, size, technical infrastructure and resources. While cost is one factor entities must consider in determining whether to implement a particular security measure, some appropriate measure must be implemented. An addressable implementation specification is not optional, and the potential cost of implementing a particular security measure does not free covered entities from meeting the requirements identified in the rule. [12]

Table 1 illustrates HIPAA regulation requirements:

Table 1: HIPAA Regulation Defined Contingency Plan

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation
ADMINISTRATIVE SAFEGUARDS		
164.308(a)(7)(i)	Contingency Plan	-
164.308(a)(7)(ii)(A)	Data Backup Plan	Required
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Required
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Required
164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable
PHYSICAL SAFEGUARDS		
164.310(a)(1)	Facility Access Controls	-
164.310(a)(2)(i)	Contingency Operations	Addressable
164.310(d)(1)	Device and Media Controls	-
164.310(d)(2)(iv)	Data Backup and Storage	Addressable
TECHNICAL SAFEGUARDS		
164.312(a)(1)	Access Control	-
164.312(a)(2)(ii)	Emergency Access Procedure	Required

6

Project Team Formation

The ISM informs the executive staff of whom he's chosen to manage this project. The PM gives the executive staff a list of persons from each area of the company he feels that will be able to provide good input to the BCP. Approval for use / availability of proposed personnel must be given by the department heads and if necessary, the executive staff. But first representation from the key areas (IT, HR, Bldg-Mgt) must be finalized. Personnel from these areas will make up the core of the BCP. The ISM along with the executive staff has these roles filled. Representation from other areas of the company will be included as the need arises during the development of the BCP. Even though the functions of these areas are part of the business, they are not deemed critical to base-functioning of the business; pertaining to the BCP, these are lower priority areas. Finalizing those roles is not necessary at this point in the BCP process, but Mgmt in those areas need to keep in mind that their service to the BCP will be coming so it should start now in finalizing its representation.

Setting the Project Schedule

The PM is planning for this project to be approximately 4 months long. Personnel representatives of the BCP core areas will be spending the most time on the BCP, (50 – 100)% of their work week. Representatives from the other areas shall spend up to 40% of their work week on the BCP. With approximation of plan creation time given and the team members in place, a project start date for the PM remains; that date shall be 4/1/2009. Figure 2 schedules the BCP with the all of the departments of the company plus building services:

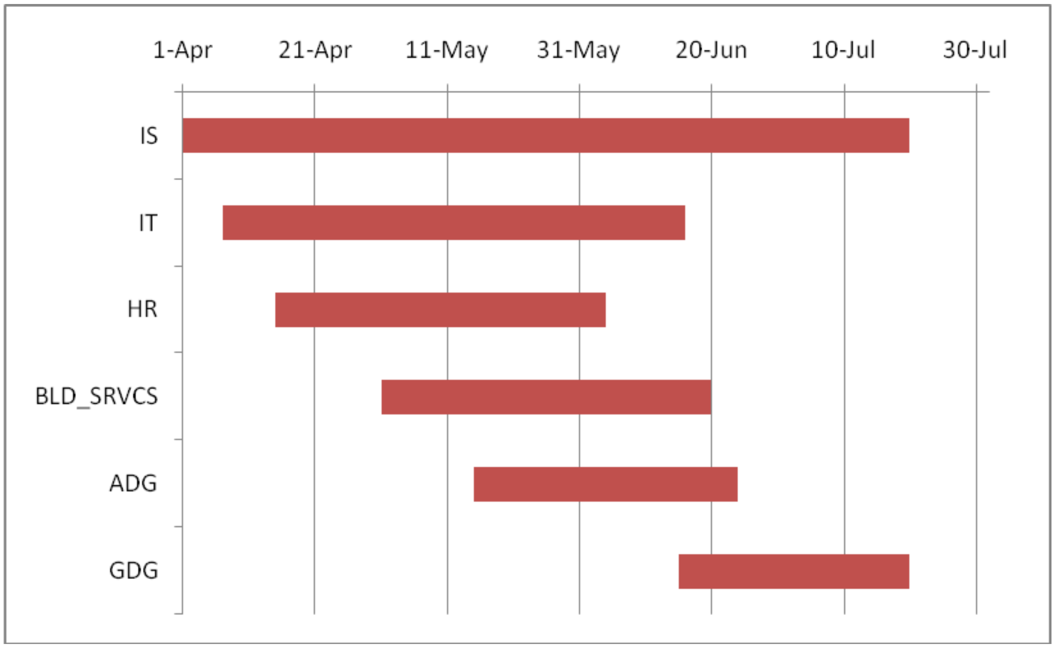


Figure2. Gantt Chart of BCP Creation Schedule

Business Impact Analysis

Definition

It is the task of identifying, developing, acquiring, documenting, and testing procedures and resources that will ensure continuity of a firm's key operations in the event of an accident, disaster, emergency, and/or threat. It involves (1) risk mitigation planning (reducing possibility of the occurrence of adverse events), and (2) business recovery planning (ensuring continued operation in the aftermath of a disaster). [3]

Business impact analysis (BIA) is an essential component of an organization's business continuance plan; it includes an exploratory component to reveal any vulnerabilities, and a planning component to develop strategies for minimizing risk. The result of analysis is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes. As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence. [5]

Questionnaire

The next task is to prepare a Business Impact Analysis (BIA) Questionnaire: The BIA is intended to help understand the degree of potential loss (and other undesirable effects) which could occur. This will cover not just direct financial loss, but many other issues, such as loss of customer confidence, reputation damage, regulatory effects, and so on. The project team should prepare a BIA questionnaire, introduction memo, and questionnaire instructions to gather the following information from the business operations to be surveyed:

- Financial impacts to the organization resulting from each business operation’s

inability to conduct operations for a prolonged period of time.

- Operational impacts relating to each business operation.
- Extraordinary expenses involved in continuing operations after a disruption.
- Current state of preparedness to resume business operations.
- Seasonal Impacts relating to each business operation.
- Technology requirements for resumption and recovery.
- Other special resumption and recovery resources.
- Information Systems support for resumption of time-sensitive operations. [8]

In performing [BIA] assessments, questionnaires are very helpful to facilitate the information gathering process. The questionnaires provide key questions related to common security-related processes to help one determine where potential vulnerabilities might exist. Questionnaires should not be interpreted as a complete list of questions because every company is different. The questionnaires include questions based on best practice standards such as the ISO 17799, industry best practices, and past experience. [7]

The purpose of these questionnaires is to provide guidance for [BIA] practitioners and help in facilitating conversations and meetings with clients when performing a [BIA] assessment. They will not only provide relevant information for the [BIA] assessment, but also spark conversation about other business processes, other initiatives, and security issues that are relevant to the assessment. They should be tailored for a given company based on the company's specific business processes. [7]

Data Collection

The following questionnaire is comprised from various checklists from Reference #7 as it's made applicable to Blue Viceroy:

GENERAL BUSINESS INFORMATION

1. What are the business drivers for the security assessment and what are you expecting from it?

Blue Viceroy Response:

Laws such as Health Insurance Portability and Accountability act requiring security assessment and good business practices are drivers for the assessment. Expectations are BCP preparedness and positive confidence from our customer base.

2. Describe what the company does.

Blue Viceroy Response:

The company provides a structure for gathering electronic health information or health care payment from physicians, hospitals, clinics, and long-term care facilities. The Blue Viceroy team uses its expertise to ensure the information is confidential, unaltered, and available so that the information is easily learned and understood to help individual in any way possible as well as using the information to identify the individual upon life termination.

3. What are your mission-critical operations and what are the supporting technologies?

Blue Viceroy Response:

Transferring patient data on demand and processing payments are mission-critical operations. High speed internet access, VPN, and data encryption are supporting technologies.

4. Describe any future business initiatives that may be impacted by technology (e.g., increasing number of employees, adding locations, and introducing a new service or product).

Blue Viceroy Response:

Increasing in number of employees, increase in number of resource / workstations, plans of buying additional servers and adding additional location.

5. Do you have any regulatory requirements that govern your business and if so, what steps have been taken to achieve compliance?

Blue Viceroy Response:

HIPAA - HIPPA is applicable to Blue Viceroy. HIPAA a complex regulation that was developed to address growing concerns about electronic access to and use of private health information.

6. Have you had any security incidents? If not, how do you know?

Blue Viceroy Response:

Yes, Sensitive document containing patient information was found in trash bins. Related incidents - Indianapolis TV station WTHR inspected nearly 300 trash bins and found nearly 2,400 patient records, including pill bottles customer refill lists and prescription labels. Most of the bins belonged to Walgreens Co., CVS Corp. The station said its investigation began after a grandmother from Bloomington, IN, was robbed at her front door by a thief authorities said found her address in a CVS trash bin. Thus all patient information including hard copy is stored in protected data center.

7. With what security issues are you concerned (e.g., confidentiality of information, availability of systems, integrity of data, and compromise of sensitive information) ?

Blue Viceroy Response:

The threat of patient information being stolen and used in some scam or ID theft is one issue of concern. Making sure patient data maintains its integrity is another.

ORGANIZATIONAL INFORMATION

8. How many employees do you have? Break down into business units and locations if information is available.

Blue Viceroy Response:

100 people work within this company

All work in the Chicago location

20 IT, 20 HR, 20 American Data Group, 20 Global Data Group, 10 IS, 5 Execs

9. Can you provide a high-level view of the organizational structure?

Blue Viceroy Response:

BV-Executive Staff

/ \

ADG GDG HR IT IS

10. What are the high-level roles and responsibilities in the IT staff?

Blue Viceroy Response:

Functionality of the server and backup server, network operations and equipment,

11. Who is responsible for information security?

Blue Viceroy Response:

IS Group

12. Is there an IT audit function that examines information security?

Blue Viceroy Response:

The IS group internally audits itself in preparation for regular audits by HIPAA.

13. Is information security a separate item on the budget?

Blue Viceroy Response:

Yes

GENERAL INFORMATION TECHNOLOGY

14. Describe your current environment.

- Number of:
    - Servers by location
    - Desktops by location
    - Other systems by location
- What operating systems (and versions) are you running?
    - What network operating system (and versions) are you running?
    - Critical applications

Blue Viceroy Response:

2 locations, 2 servers per location

100 PCs in main location,

Contract with HP/best buy for 50 leased PCs in case of disaster

Windows XP for desktop PCs, Win2k3 for Network OS

15. Do you have a process for ensuring that security patches are applied to systems on a timely basis?

Blue Viceroy Response:

Patches are done weekly along with weekly scans to make sure patches have been applied

16. Do you have standards for hardware and software? Are there standard builds that are used for computers?

Blue Viceroy Response:

2+ GHz processor HP PCs, Win2k3 Server software

Ethernet LAN Architecture, 802.11g WRLS standard

17. Is there an asset management process in place?

Blue Viceroy Response:

Yes, they are accounted in inventory, tagged and assigned to personnel.

Upon termination, they are immediately seized and logged.

18. Describe your remote access environment.

    - How many remote access users do you have?
    - What percentage are home users and how many travel?
    - How are the users obtaining remote access —e.g., virtual private network (VPN), dial-up
    - What resources are users accessing remotely?
    - Do third parties remotely access your systems?
    - What technology is being used for remote access?

- Are there any planned changes for remote access?

Blue Viceroy Response:

- How many remote access users do you have? (IT staff and executives) 20 persons
- What percentage are home users and how many travel? No home users, 5 travel
- How are the users obtaining remote access — VPN
- What resources are users accessing remotely? Servers, routers, databases
- Do third parties remotely access your systems? No
- What technology is being used for remote access? Cisco Secure VPN

19. Do you have any business-to-business (B2B) partner arrangements?

Blue Viceroy Response: No

20. Do you engage in any electronic commerce activities and offer products and services over the Internet?

Blue Viceroy Response: No

21. Do you outsource any of your business functions?

Blue Viceroy Response: No

SECURITY

22. Do you have any security policies in place and are they readily accessible by employees?

Blue Viceroy Response:

Yes, Blue Viceroy has full set of security policies namely - Access Authorization policy, Information Access Management Standard policy, Access Control and Validation Risk Analysis policy, Facility Security Plan policy, Facility Access Control policy, Acceptable Usage policy, Workstation Security Standard policy , Risk Management policy, Disaster recovery policy, data classification polices and finally HIPAA Security policies and procedures which are issued (hard copy) whenever a new staff is appointed and the staff is required to attend security awareness seminar and complete a quiz before joining the organization. Also the security policies are updated every 6 months (hard copy is issued) and all polices are accessible to employees any time via company's intranet.

23. Do you have security policies for the following at a minimum?

- Acceptable use
- Data classification
- Data retention
- User ID administration
- Obtaining initial access
- Termination of access
- Periodic review of user access lists
- Backup and recovery
- Incident handling
- Business continuity and disaster recovery
- Change management
- Physical security

Blue Viceroy Response:

Yes Blue Viceroy has security policies that cover all minimum requirements as mentioned in the previous answer. The security policies are available as PDF files and are accessible any time via company's intranet.

24. Are there any programs that promote security awareness?

Blue Viceroy Response:

New employees have mandatory security awareness as a part of their orientation program. Every time a security policy is updated or changed there is security awareness seminar that is mandatory for the employees which can be general open to all the employees or it can be based on specific department.

25. Does someone own the responsibility of updating security policies as the business changes? If so, how are the changes communicated?

Blue Viceroy Response:

The external audit team updates the security policies along with chef information security officer and board of directors. Every time a security policy is updated or changed there is security awareness seminar that is mandatory for the employees which can be general open to all the employees or it can be based on specific department.

26. Describe your security architecture.

Firewall Intrusion detection/prevention Anti-virus Other security architecture — e.g., proxy servers, vulnerability management

Blue Viceroy Response:

IDS is in place for data traffic monitoring; all servers are patched and up to date, anti-virus is up to date, IS team has trained and certified staff members, disaster recovery in place, backup data center is up to date and secure, physical security is monitored and switched firewalls.

27. What security-related logs are enabled — e.g., system-specific logs, firewall logs — and are they reviewed on a regular basis?

Blue Viceroy Response:

Install log monitoring software. Monitoring networks means regularly checking (at least) three event logs and other application logs on each machine. This can lead to hours each day spent watching logs Enable extended logging for your IIS web/FTP server and move the location of your log files. Security logs are enabled namely audit logs, firewall logs, IDS logs which are reviewed every morning by information security team.

BUSINESS PROCESS–RELATED QUESTIONS

28. Significant *business processes and supporting technologies*

    - Describe how the business process works.

- What are the critical roles in the process and are there backups in the event that key individuals are not present?
- What technology supports this business process?
- Who is responsible for managing the supporting technology?
- If the supporting technology was unavailable and this business process could not occur, what are the impacts related to revenue, legal or regulatory concerns, and reputation damage?
- What is the tolerable downtime?
- Are there any manual or other workarounds that can be done while the technology is unavailable? For how long can the workaround be done?
- What critical data is generated as a result of this process and where does it reside?

Blue Viceroy Response:

- Patient data is updated and provided to insurance companies, hospitals, doctors' offices, pharmacies, and patients themselves.
- Data retrieval, and distribution → must be done correctly & confidentiality maintained at each process point
- Windows Access Database
- IT team manages the supporting technology.
- There would be an impact because there would be a delay in normal business processes. Backup processes would have to be activated. This could be done in a timely manner. No legal, regulatory, or reputation concerns as long as we are running within tolerable downtime.
- Two hours is tolerable downtime.
- Hardcopy processing can be done via the backup facility. This can be done for as long as it takes to get the technology back online.
- Medical record information updates are received and records distributed; all handled at the backup facility.

29. Determine whether your Information Asset is mission critical by answering the following questions.

If my Information Asset is unavailable for any amount of time…	YES	NO
▪ Is the physical safety of the public or the company's employees jeopardized?		x
▪ Is the company's ability to provide adequate power for customers impacted?		x
▪ Is the company unable to meet its legal or regulatory requirements?	x	
▪ Will it significantly affect the customer confidence level?		x
▪ Will it be detrimental to the company's public image?		x
▪ Are the functions of a critical facility compromised		x
▪ Will a significant amount of revenue be lost?		x
▪ Will the downtime incur serious extraordinary expenses?		x

If you answered YES to any of the above questions, your Information Asset is most likely mission critical.

WORKAROUND PROCESS

30. Is there a documented "workaround" process available for your Information Asset? (Consider alternatives such as manual tracking, telephone or fax machine usage.)

Blue Viceroy Response: Physical and digital copies of data are kept at another location for backup to keep the business going if any event occurred ceasing functionality at the main facility.

31. *Integration with other departments.*
    - Dependencies between departments
    - System integration and determination of single points of failure
    - Transmission of information

Blue Viceroy Response: N/A, Departments have mutually exclusive functions

32. *Past security incidents (questions for each incident).*

- What was the nature of the security incident?
- How soon did you become aware of the incident? Did you find out because of a documented process or by accident (e.g., happened to be talking to somebody)?
- What was the reaction?
- What was the impact of the incident?
- What has been done to prevent such incidents from happening in the future?

Blue Viceroy Response: Yes, there was a past security incident. Discarded, non-shredded documents containing some patient data were found in a company dumpster. We became aware of it within 30 minutes of its occurrence during a random office sweep. The impact was minimal since the dumpster was still in-house. We put policies in place and made employees well aware of the seriousness of this incident pertaining to personal medical data.

SECURITY-RELATED QUESTIONS

33. *User ID administration: What is your role in users gaining access to systems — e.g., approval authority?*

Blue Viceroy Response:

To authenticate an Administration a user ID and password are required. Application Servers uses these credentials to perform authentication against a pre-defined user registry. SSL is used for encryption of all requests and responses, including the client's user ID and password, and for authentication of the server. The user ID with administration rights are given device read write role while other users are only given device read only role.

34. *Employee termination.*

    - What do you do if an employee reporting to you is terminated?
    - What are you accountable for?
    - Is there a documented process for terminations that you follow?

Blue Viceroy Response:

Upon termination the employee user ID is disabled and the employee email account is deleted immediately the next day after termination. Also the physical access security card and keys are handed over on the day of termination. The employee access to data center is restricted and terminating payroll. The termination process is well documented and is included in policy.

35. *Data retention and classification.*

- Are you aware of any policies related to data classification or data retention?
- Do you specify retention or classification requirements for data you are responsible for?

Blue Viceroy Response:

Yes, we are aware of policies related to data retention.

Yes, retention requirements for data are specified.

36. *Backup and recovery.*

- For data that you own, do you specify any backup requirements for that data?
- In the event of a disaster, what data would need to be restored for you to become operational?
- Is that data readily available?

Blue Viceroy Response:

Yes, the patient information is mirrored in remote server in a remote location. In event of disaster, privileged users and administrators have secured VPN connection to the backup server which has the copy or backup of original data.

Yes, once authenticated the data is readily available.

37. *Incident handling.*

- Do you know what to do in the event of a security incident?
- To whom would you report an incident?
- Are you aware of any documented procedures for incident handling?

Blue Viceroy Response:

Yes, it is reported immediately to Information security team.

Yes, the procedures are well documented and are available as a part of the security policies.

38. *Acceptable use of IT resources.*

- Is there documented Acceptable User policy?
- Has HR or management ever discussed what is considered acceptable use of IT resources?

Blue Viceroy Response:

Yes, Blue Viceroy has list of Acceptable User Policy which is included in list of company's security policies.

Yes, the acceptable user policy is written and documented based on management's discussion and is reviewed every 6 months for consistency.

39. *Physical security.*

- What physical security measures are in place for the areas of the facility you access?
- Do you have any sensitive information in your desk or office and if so, how is it secured?
- Do you practice a "clean desk" policy when you leave the office?
- Do you use screensavers on your computer?
- Do you shred sensitive documents before throwing them away?

Blue Viceroy Response:

Physical security is in place, Blue Viceroy has surveillance camera both inside and outside data center where patient information is stored.

Yes, we practice clean disk policy which is listed in the company security policies (workstation security standard policy).

No, we don't employee screen savers computer monitor is turned off when an employee leaves his/her desk.

Yes, Blue Viceroy does shred redundant sensitive documents and stores copies of patient information in a secure data center.

Risk Assessment

Information Security Risk assessment is an on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. The risk assessment will help each agency determine the acceptable level of risk and the resulting security requirements for each system. The agency must then Devise, implement and monitor a set of security measures to address the level of identified risk. [11]

The objective of a risk assessment is to balance the safeguards identified in the *risk* (i.e. probability) of failing to meet your business objectives. The most you can lose is your *exposure*. In the context of a typical commercial enterprise, your exposure would be measured in terms of regulatory penalties and financial loss.

- for a given exposure, the removal of safeguards will increase the risk of loss (i.e. make the situation "risky"). The addition of too many safeguards could, on the other hand, render the security system OTT ("over-the-top"). The objective is to achieve a proper balance of safeguards, resulting in a well "managed" security system.

- given a well balanced system, any increase in exposure will result in a "risky" situation, while a reduction in exposure will render the security system OTT. [10]

The following is an assessment data of Blue Viceroy laid-out in the format of a table. The information within this table is to be commuted to a three dimensional representation known as a risk assessment cube. This cube will give one a visual representation of the assessment, one that is easier to comprehend. The cube will be based upon the last three columns of the data table. The illustration of the cube was originally referenced but then modified to fit Blue Viceroy's specific risk assessment data.

Table 2: **Assessment Data**

Segment	**Threats/ Event Examples**	**Severity of Loss**	**Duration of Impact**	**Probability of An Incident**
A	Civil lawsuit, retaliation or vengeance brought by employee for discrimination or harassment.	High	Isolated	Rare

B	Hardcopy / Electronic Fraud or extortion	Low	Isolated	Rare
C	I.T personnel do not have complete understanding of HIPPA regulations	High	Extended	Rare
D	Backups unreliable and other mission-critical systems	High	Extended	Rare
E	Non sophisticated hacker or DoS attacks	Low/Medium	Isolated	Rare
F	Malware & spam, possession of unlicensed software.	Low	Extended	Rare
G	Technology Obsolescence databases or other mission critical systems.	Low	Extended	Rare
H	Disruptive or destructive malware (Trojan, worm or Virus)	Medium/High	Isolated	Common

Recommended Controls

The selection and implementation of appropriate *security controls* for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [13]

A - All Employees have a mandatory security awareness program which educates the employee about lawsuit pertaining to leakage of patient information

B - The disposal of patient information hardcopy is done carefully using shredders and other latest technique. All employees as made aware of lawsuits in past (thrash can containing patient information)

C - Security awareness and training with more focus of HIPPA.

D - Third party backup services should be used.

E, F - Operating system and all enterprises security tools are patched up to date.

G, H - Update to latest technology on mission critical systems.

Table 3: **Business Impact**

Assets	**Loss of Integrity**	**Loss of Confidentiality**	**Loss of Availability**
Patient Information	High	High	Medium
Internal Documents	Medium	Medium	Low
HR Records	High	High	Medium

Advertising literature	Low	Medium	Low

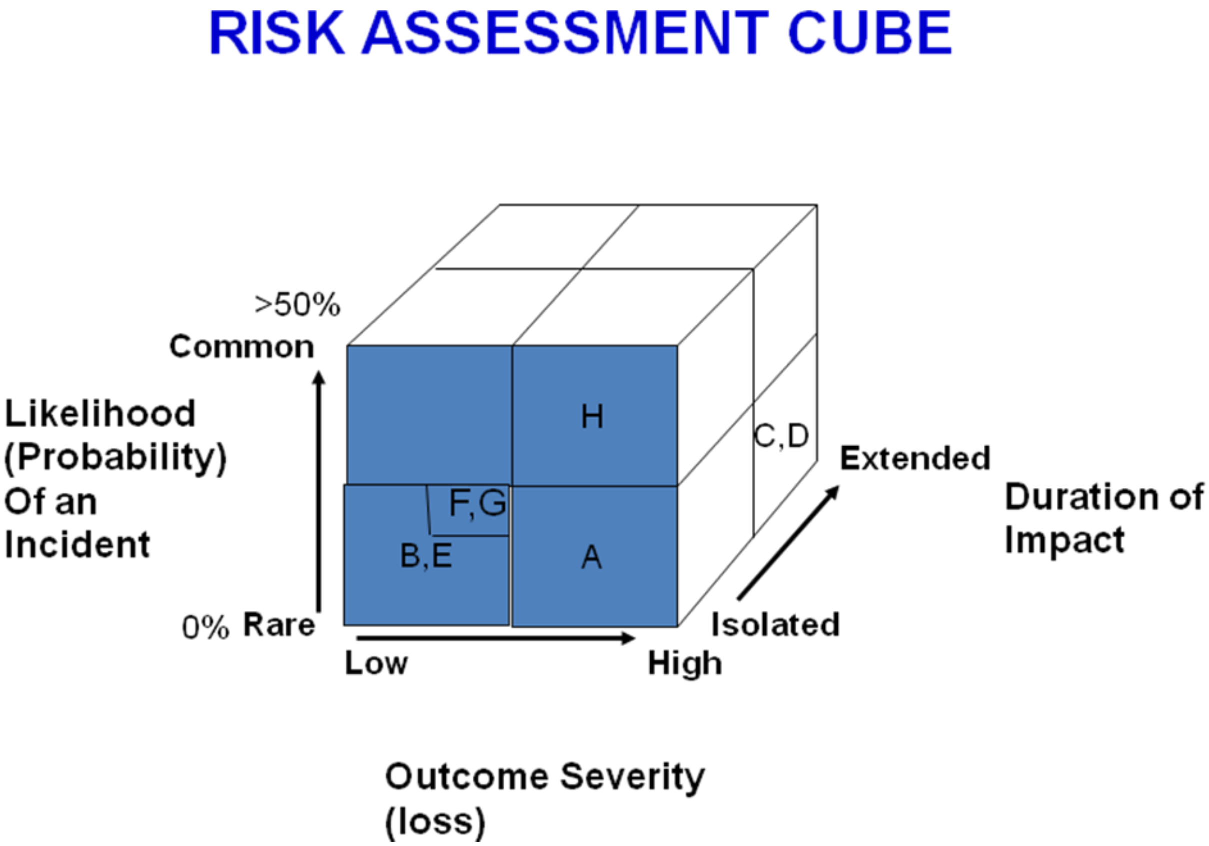


Figure 3. Risk Assessment Cube [9]

Resultant Details of the Risk Assessment

<u>Assumptions:</u>

Blue Viceroy is fully aware of the illustrated risks and understand their impacts to the business should they come to fruition.

Constraints:

Remaining fully compliant with HIPAA standards

Company's Stance on Mitigation:

The company will invest funds into mitigating the risks via opting to implement the recommended security threat controls for all levels of risk.

Mitigation Technology:

Intrusion Detection Systems, Latest PC/Server hardware, Anti-virus software, Multiple dedicated high-speed links to the backup/reserve facility

Technology Acquired/Purchased:

IDS Snort for Windows, HP High-End Integrity Servers with Windows Server 2008, McAfee Anti-Virus Software, Two dedicated high-speed links: One provided by AT&T and the other provided by Comcast.

Table 4: **Mitigation Cost Due to Assessment Data**

Segment	**Mitigation Cost ($)**
A	500
B	200
C	300
D	10000
E	200
F	100
G	50
H	100

Development & Implementation

Emergency Management Team Definition

The Business Continuity Institute defines the emergency management team (EMT) as ‘the group of management staff who command the resources needed to recover the enterprise's operations at the recovery site.’ I prefer to extend that concept to mean the group of executives who manage and control an emergency situation on behalf of the enterprise. In other words, these people are in charge of the destiny of the total enterprise, with all the attendant responsibility. Indeed it can be said that their influence extends beyond their own enterprise and may affect the long term success of a whole industry. It is crucial that they perform well, both as individuals and as a well-matched team. [15]

If a major incident/disaster occurs, the Emergency Management Team (EMT) will be convened and the situation assessed. It will be the responsibility of this team to decide whether or not to implement the Business Continuity Plan. This Business Continuity Plan (BCP) will be activated by the BCP Team Leader, as identified in the plan, when he/she receives instructions from the Operations Manager on the Emergency Management Team (EMT).

When an emergency has been declared by the ERMT, the BCP Team Leader will report directly to the EMT Operations Manager for the duration of the emergency. All ad hoc requests for decisions, assistance with facilities, acquiring outside services, etc. will be directed by the BCP Team Leader to the EMT through the Operations Manager.

It will be the BCP Team Leader’s responsibility to contact all team members or their alternates and ensure that they convene at the Emergency Operations Centre as defined in this plan.

The BCP Team Leader will be responsible for the successful implementation of this plan.[14]

Because of the size of Blue Viceroy as a company, the core of the EMT will be the BCP team since it will be most knowledgeable of the BCP with others to assist as situations demand. But with larger enterprises, the EMT will definitely be a large set of individuals separate of the BCP team.

Disaster Response Triggers

The following situations will set in motion the BCP:

- Power outage
- Communication links being made unavailable.
- Any man-made disaster (fire, bombing, etc).

- Any viral epidemic in the local area.
- Any pending natural disaster, e.g. flooding or other severe weather warnings.

For any BCP situation, the EMT will assess the amount of damage and implement the appropriate response level to get the company back to operational status.

Disaster Recovery

The key objective of a disaster recovery plan is to detail the key activities required to reinstate the critical IT services within the agreed recovery objectives. The most effective start point for any DR plan is the ‘declaration of a disaster’ once an incident has been deemed serious enough that ‘forward fixing’ at the primary location is impractical or is likely to result in an outage expending beyond the maximum tolerable outage.

It is really important why the data centre is destroyed? As far as the DR [process] is concerned the answer is no. The same process and recovery stages will be followed regardless of the cause, fire, flood, terrorist incident, or the proverbial aircraft impact will all result in the partial or total destruction of the data centre.

The only relevant question is what is the impact and can I realistically continue to host services from my primary site or should I invoke and recover/resume the critical services at my secondary site.[16]

Depending on the level of the disruptive cause, Blue Viceroy has correlating response levels. If the disaster is minor or major, the company will be ready to respond to keep critical operations flowing smoothly and securely.

There is a hot-site is located approximately 35 miles outside of metropolitan Chicago.

The hot site location will contain computer terminals, furniture, and communication lines, serving as an operations base until the primary site is made fully operational. With a smaller crew at the hot site, other employees will have to work remotely via secure VPN high-speed connections. But through this site, the company will be fully operational.

Organization of Data Backup

There are primary and secondary servers at the main site. This secondary server is to be used as an immediate primary replacement in case software or hardware upgrades are being done to the primary, primary maintenance work, primary testing, or primary failure. If an event occurs that cripples the operation of the primary location, a secondary (hot) site containing a tertiary server will be used to run company operations and bring the company back online.

The tertiary server will contain all data & software as at the primary & secondary. Regular backups will be done nightly via the secure high-speed dedicated communication links provided by our primary service provider.

There is also a regional Iron Mountain facility containing encrypted data disks. Weekly deliveries of data are sent to this secured facility in case communication links at the primary and secondary locations are totally unavailable. Business processes will still be able to occur, but at a slower rate.

Testing & Maintenance

BCP Exercise Program

Why should we test the BCP? Gaining experience in real crisis situations is difficult and not the best time to learn. Exercises allow us to identify familiar situations based on experiences and take appropriate actions- Habitual Behavior. They give people the frame of reference to perform a certain BCP function critical to your organization. Exercises help you ID the areas that are in most need of BCP plans (can make part of BIA process).

What are the benefits of testing? It improves individual performance. It enables people to practice their roles and gain experience in those roles. It familiarizes employees with the Plan, Task Lists and Operating Procedures. It improves organizational coordination, communications, and the probability of success when responding to a real emergency. Exercising improves the organization's system for managing emergencies. It improves organizational command, control and communications, and reveals gaps in resources and weakness of plans. It yields validations of capabilities before an actual disaster happens and shares key lessons and best practices across the company.

An Exercise Program: The foundation and organizational support for designing, developing, conducting, and evaluating an exercise. The exercise planning process is based on a group of planning activities that result in successful exercises. [17]

For Blue Viceroy, there will be an annual full scale exercise to test the total viability of the current BCP, impacting all departments and business processes; modifications or improvements will be made where necessary. There will be quarterly minor exercises performed by the IS and IT departments.

BCP Maintenance Management

An effective BCP program requires consistent management, maintenance, testing and updates and is not intended as a one-year stand-alone document. Due to the changing nature of operations, technology, risks, infrastructure and the skill sets necessary to maintain operations, a program for keeping the BCP and related programs up to date is crucial. Industry best practices state that business continuity planning should include regular updates to the BCP based on changes in business processes, audit recommendations, and lessons learned from testing. The BCP (and affiliated programs) must stay in step with the business and technical environments to ensure that all information, training, awareness, management and strategies are up to date with the ever-changing topography of operations, best practices and compliance.

All business decisions should include BCP considerations as changes to the environment, operations, personnel or mission of the institution requires updates to the BCP to effectively include any change to scope, execution, infrastructure and operations in the recovery/continuity strategy. To stay effective, and responsive to the myriad of changing requirements and solutions, a system of management and a culture of enterprise-wide maintenance (for all compliance and regulatory programs, not just BCP) are necessary. The culmination of the recurring Maintenance Program establishes a mutually developed methodology of management, education, maintenance and support for the BCP.

The purpose of the recurring Maintenance Program is to create a culture based upon a formalized set of policies and procedures that guarantees effective prevention, detection and response capabilities within the institution. An effective program is never static. The BCP should grow and evolve with the institution through a formalized process of re-evaluation, testing, risk assessments, mitigation efforts, training and maintenance to ensure the information within is accurate and reflects the current infrastructure, operations, roles and functions of the institution.[18]

With the passage of time, all companies change. So too a BCP must change to stay relevant to the company. The following are types of changes that shall be reflected in Blue Viceroy's BCP:

- Changes in personnel
- Changes to important vendors/suppliers and their contact details
- Changes to business functions within departments
- Changes in company mission statement

<u>Conclusion</u>

Business Continuity Planning is the ongoing process of managing risks to the smooth running of organizations or processes within an organization. It includes looking for potential problems or weaknesses and preparing a strategy, in advance, for dealing with these events.

You should carry out Business Continuity Planning because it will help you prepare for, prevent, respond to, and recover from disruptions. Having a continuity plan will help a business to

> manage the turmoil of a disaster, keep [transacting], and instill confidence in your employees, [stakeholders], customers and suppliers.
>
> If you have a disaster your employees will still expect to be paid, your [stakeholders] and customers expect continuity of service, and you still have to pay on finance agreements. Business continuity planning ensures your business can ride the storm and maintain an acceptable level of service. [19]

Through the use of a case study, this paper illustrates the major processes that a small company would have to put into effect to generate a BCP. Since every company is different, this paper provides an overall template of how a small company should begin its BCP creation process.

References

1) Retrieved February 9, 2009, Web site: http://www.technologyexecutivesclub.com/Articles/bizcontinuity/ensuring.php

2) Figure 1 -- Retrieved March 9, 2009, Web site: http:// www.fr-tech.net/bcp-dr.phpen

3) Retrieved March 11, 2009, Web site: http://www.businessdictionary.com/definition/business-continuity-planning-BCP.html

4) Legal Issues in Information Security/HIPAA – Gary Bannister

5) Retrieved March 16, 2009, Web site: http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci820947,00.html#

6) Table 1 -- Retrieved March 16, 2009, Web site: www.supremusgroup.com/hipaa_compliance/Security_Contingency_Planning.htm

7) Kairab, Sudhanshu (2005). *A Practical Guide to Security Assessments*. Boca Raton, Florida: CRC Press LLC.

8) The AnyKeyNow Group. (2002). *Business Continuity Planning*. John Williamson.

9) Figure 3 -- Retrieved April 7, 2009, Web site: http://www.iso27001security.com/html/faq.html

10) Retrieved April 20, 2009, Web site: http://www.gammassl.co.uk/inforisk/index.html

11) Retrieved April 20, 2009, Web site: http://www.mass.gov/?pageID=itdsubtopic&L=3&L0=Home&L1=Networks+%26+Security&L2=Security+Risk+Assessment&sid=Aitd

12) Retrieved April 20, 2009, Web site:
http://www.cms.hhs.gov/SecurityStandard/

13) Retrieved April 20, 2009, Web site:
http://csrc.nist.gov/publications/PubsDrafts.html

14) Canadian Government. (2000). *Canadian Centre for Emergency Preparedness* (1 ed.)

15) Retrieved April 27, 2009, Web site:
http://www.continuitycentral.com/feature0171.htm

16) Retrieved April 27, 2009, Web site:
http://www.continuitycentral.com/feature0524.htm

17) Retrieved April 30, 2009, Web site:
http://www.cpaccarolinas.org/Symposium07/07Presentations/PresentationWS2-Zino_ExerciseBrief.pdf

18) Retrieved April 27, 2009, Web site:
http://goheit.lyrishq.net/media/files/HEIT_BCP_SOW.pdf

19) Retrieved May 1, 2009, Web site:
http://www.123bcp.com/