Business Continuity with a Forensic Focus

David C. Shields

University of Maryland University College

Table of Contents

Abstract 4
Analyze the Assets 5
How Risky is this Business? 7
Protect it! 12
Did it Work? 15
Conclusion 17
Bibliography 18

Table of Tables

Table 1: Qualitative Analysis Example 9

Table 2: Quantitative Attributes..... 10

Table 3: BIA Matrix for ABC Retailers 10

Table 4: Forensic BIA Matrix Example..... 11

Abstract

Every enterprise should be prepared for a disaster regardless of geographical location, political climate or any other factors perceived to curtail it. Natural disasters such as floods, earthquakes and power loss as well as human factors may not be avoidable but their damage can be minimized. A business continuity program (BCP) can be an invaluable resource in light of a disaster, especially if staff is trained and the program is tested. Unfortunately, many BCPs do not include provisions for recovering from a cyber-attack. Enterprises must understand what items should be protected, what kind of fallout might be experienced if these items are not protected, as well as the importance of determining what parties are responsible for what assets in the event of a disaster. This document is intended to illustrate how to assess, implement, and test a BCP that aids in securing assets in the event of a disaster including a cyber-attack while also giving much needed attention to the importance of digital forensics in a plan.

Keywords: *business continuity plans, disaster recovery, recover from cyber-attacks*.

Business Continuity with a Forensic Focus

The world can be a dangerous place. Natural disasters such as earthquakes, tornadoes, and hurricanes can strike with little notice and do intense damage. In an enterprise, there is always the potential that an insider can damage company property either intentionally or unintentionally – especially if the information is stored on a digital medium such as a computer. Worse yet, when computers are involved, there is always the potential for a malicious cyber-attack from the inside or the outside. Enterprises the world over have learned to prepare for the worst by implementing a business continuity program (BCP) to prepare the organization for when disaster strikes. Any downtime as a result of a disaster or cyber-attack has the potential to cause considerable financial damage to a company so it is important for an organization to answer such questions as “What needs to be protected and Why?”, “What could happen if it is not protected?”, “Who is responsible for protecting it?”. All of these concerns can be used to generate a business continuity plan for an organization. This document is intended to illustrate how to assess, implement, and test a BCP that aids in securing assets in the event of a disaster including a cyber-attack.

Analyze the Assets

The first question that any organization desiring to create a Business Continuity Plan (BCP) must ask is “What needs to be protected?” This question can honestly be one of the most difficult and challenging questions to answer and can also take the greatest amount of time and resources to answer. In fact, the answer to that question is likely to be completely different from one company to another and even different when comparing multiple companies in a particular business sector like energy or aerospace (Caballero, 2009).

Each organization has its own critical items to protect and each item may require a different level of protection depending on how valuable it is to the company's operations. For instance, in an oil company the most critical assets could be well logs, seismic data for various geographical locations, or records of current land leases or any combination of these. The organization must ask 'What could my competitor do with my leaseholder records?' or 'How much would it cost my company if our competitor got access to our well logs?' or even 'What if a hacktivist attacked my network and wiped out all the seismic data we have?' Depending on the answer to these questions, a company may choose different methods to try and secure this data.

Once the organization has at least some understanding of the importance of their data, it would be wise to determine who actually is in charge of controlling this data. In many instances, a company is likely to control their hardware and software internally and is likely to have a team or at least a designated staff member or two who can be considered responsible for a particular system (Swanson, Bowen, Wohl Phillips, Gallup, & Lynes, 2010). However, it is more common for an entire department or group to be considered responsible for a series of systems so that each member of the department is not individually accountable for a large number of systems. Alternatively, a smaller organization or one with specialized software in place may have a Service Level Agreement (SLA) that places a majority of the responsibility on a third party for data protection.

Once the organization has analyzed the items it needs to protect, has at least a basic idea of the criticality of an interruption, and has some responsibility matrix, the groundwork has been laid for BCP. But the BCP is not even ready to begin implementation yet. Before the plan is designed, a risk analysis needs to be completed in order to show the viability of the solution to the leadership of the company (Balaouras, 2009).

How Risky is this Business?

Every organization has a tendency to avoid risk as much as possible when it comes to matters such as financial risks, building and environmental risks, etc. but understanding and mitigating the risk of cyber-attacks is still an emerging field (Blokdijk, 2008). Now that the organization has an idea of the most critical systems in its enclave, it is wise to do a thorough examination of the potential impact of system compromise from natural, human, and cyber-security related incidents. But determining the best way to illustrate the importance of these items may prove somewhat challenging, especially when one attempts to illustrate the potential damage to a company's image and consumer trust if any system is compromised or lost without a potential contingency plan or in the event of customer data loss. Although many methods exist to aid in risk management, one of the most respected and thorough methods are to utilize a business impact analysis.

When performing a business impact analysis or BIA, the organization will use a three step process to determine which assets/departments present the highest risk and calculating the qualitative and quantitative impact of any loss of service (Miora, 2009). In the first step of the BCP process, the organization should have already compiled a list of their most critical assets but this list alone is insufficient for starting a BIA. The organization needs to consider whether or not any of their critical assets or services interdepends upon other assets or services. For example, an accounting department at a major retailer may perform a majority of the accounting work within particular software or system but this system may draw data from other software or systems in order to provide complete financial data.

In this instance, if a cyber-attack were triggered against one of the secondary data sources and causes it to fail, it could potentially damage the entire system – this is known as a critical path. An organization must determine what level of recovery of this system is needed for the business to function in a disaster as well as determine how long the system can potentially be unavailable before other operations are impacted. The speed at which the records of the system can be forensically examined after a breach and the overall complexity of system interactions for digital evidence may cause the system to be considered a higher risk than it would be otherwise. All of these factors are compiled to determine the criticality of this resource (Miora, 2009).

Once criticality of a system is determined, the BIA must then determine the actual financial cost of a disaster or cyber-attack. In the case of the financial system mentioned previously, the retailer may look at the nature of a disruption (such as the damage to the secondary data source), the category of disruption (loss of power, system error, Denial of Service, etc.), the degree or significance of the disruption (corruption of over 5,000 accounts, one or two invalid entries in a report), and lastly the duration of the disruption (minutes, days, etc.). If the retailer determines that the core accounting system is capable of generating $250,000 in revenue per day and the secondary data source is responsible for $50,000 of this revenue and the Denial of Service attack caused the system to be inaccessible for 2 days, the company has lost $100,000. If a digital forensics investigation is necessary to determine the source of loss and to aid in securing the source before operations can resume, the company must accept not only the continued compounding loss for each day the secondary source is unavailable but also the cost of paying for the investigation.

Calculations such as these can be performed across all critical assets to help determine financial impact as illustrated in Table 1.

Qualitative Impact Analysis - ABC Retailers					
Asset	Revenue/Day	Duration (days)	Recovery Cost	Loss	Criticality
Retail Point of Sale	$ 500,000.00	2	$ 40,000.00	$ 1,040,000.00	Critcal
Accounts Payable	$ 100,000.00	4	$ 250,000.00	$ 650,000.00	High
eCommerce site	$ 175,000.00	1	$ 250,000.00	$ 425,000.00	Medium
Fleet Management System	$ 200,000.00	3	$ 50,000.00	$ 650,000.00	High
Warehouse Fulfillment	$ 15,000.00	1	$ 300,000.00	$ 315,000.00	Medium

Table 1: Qualitative Analysis Example

Upon completion of the Qualitative Impact Analysis, the BIA must then calculate the Quantitative Impact a disruption of a particular asset or service may cause (Kirvan, 2009). The qualitative impact is far more challenging as it must depend on several abstract concepts which may prove difficult to determine. Factors to consider include how long the department or company could survive in the event of asset unavailability, criticality of asset to operations, number of users impacted, time to restore functionality and likelihood of attack. The scoring system used to calculate these items is likely scale of 1-10 wherein lower numbers are likely to be less impactful and higher numbers more impactful respectively. When the BCP is being created, it is highly unlikely that the enterprise has actually taken the time to consider these items; therefore, accurate calculation may require considerable research to complete (Miora, 2009).

In the case of the retail accounting system mentioned earlier, the company may determine that it could only survive a matter of two days without serious impacts to operations in the event of an outage.

If the calculation is based off the qualitative analysis, the accounting system may be considered a high criticality asset and its unavailability would impact approximately 20 users. The system could take approximately 4 days to restore in the event of damage or attack but it is relatively unlikely to be attacked. The quantitative analysis scores would be calculated as outlined below:

Asset Attribute	Score
Survivability	8 – Major – Only 2 days to survive
Financial Criticality (from Qualitative Analysis)	6 – High - $250,000 revenue per day
User Impact	5 – Medium – 20 users impacted
Restoration Time	7 – High – 4 days to recover
Likelihood of Attack	1 – Very Low – System is well protected and difficult to access externally.

Table 2: Quantitative Attributes

In order for the BIA Quantitative Impact to be an effective measurement of the company's risks, it is important for the values of each asset to be analyzed using the same scoring system. The completed scores for each item can be added to a cumulative matrix which will allow the leadership of the company to quickly and clearly determine the risk to any of these assets or systems. The BIA matrix for ABC Retailers may look similar to the one illustrated in Table 3.

Asset	Survivability	Financial Criticality	User Impact	Restoration Time	Likelihood of Attack	Risk Score	Ranking
Accounting System	8	6	5	7	1	**5.4**	Medium
Retail Point of Sale	9	10	10	4	4	**7.4**	High
Accounts Payable	7	5	5	9	4	**6**	High
eCommerce Site	7	6	8	2	8	**6.2**	High
Fleet Management	8	5	8	4	2	**5.4**	Medium
Warehouse Fulfillment	9	4	8	3	2	**5.2**	Medium
Employee HR System	4	7	8	6	4	**5.8**	Medium
Enterprise Email	5	5	5	7	3	**5**	Medium
Vendor CRM	7	2	2	1	1	**2.6**	Very Low

Table 3: BIA Matrix for ABC Retailers

Once the three steps of the business impact analysis have been completed, the business should have a wonderful framework for understanding the risks to their assets. A business analyst could then present the data to upper management to illustrate the areas of highest risk from both a qualitative and quantitative perspective. However, the forensic risk of the organization's assets is still somewhat difficult to quantify with the given information. The system may require more time to forensically examine due to its operational state (virtual or physical), system complexity or legal requirements. As a result, this study proposes that a forensic qualitative analysis also be performed using the categories of: Analysis Time, Potential for Data Corruption, Complexity of forensic analysis, and Legal Impact. Table 4 illustrates this theory using the same assets as observed earlier for ABC Retailers but with a forensic focus.

Asset	Analysis Time	Potential for Data Corruption	Complexity of Forensic Analysis	Legal Impact	Risk Score	Ranking
Accounting System	10	9	8	8	**8.75**	Very High
Retail Point of Sale	10	9	9	7	**8.75**	Very High
Accounts Payable	6	6	4	4	**5**	Medium
eCommerce Site	9	10	7	8	**8.5**	Very High
Fleet Management	2	5	2	4	**3.25**	Low
Warehouse Fulfillment	4	6	1	1	**3**	Low
Employee HR System	8	7	7	9	**7.75**	High
Enterprise Email	8	9	7	4	**7**	High
Vendor CRM	3	6	8	7	**6**	Medium

Table 4: Forensic BIA Matrix Example

As evidence d by the data in the Forensic BIA analysis, the assets may be at a higher risk from a forensic standpoint than from a standard risk standpoint. The leadership of the company must be made aware of the potential negative impact on business continuity if forensic capabilities are not also part of the proposed BCP. Now the organization will finally have a more complete idea of what is at risk and the impact a disaster or cyber-attack may have on their business.

The Business Continuity Program (BCP) can finally be made and the organization can implement changes to aid in protecting critical assets (Balaouras, 2009).

Protect it!

The implementation of a BCP is highly unlikely to be a rapid process but it is most certainly a vital one. For each system or asset, the company must determine what protective measures they wish to employ as well as consider any steps that are needed to maintain the protection measures. It is important to strike a balance between the cost of protecting assets and the actual risk to the asset. While it is certainly true that a disaster or attack against an accounting system has a rather high potential of damage, this should be balanced against the potentiality of an attack. In essence, it is not sensible to spend $1M dollars on a state-of-the art security appliance to protect the accounting system if the amount of protection already in place makes it a very difficult target to reach.

As discussed earlier in this document, risks are not just technical in nature they may include natural risks such as tornado or fire, environmental risks such as power loss, insider threats (both intentional and unintentional), and cyber-attacks. In the case of natural risks, the organization should have tornado/fire evacuation plans in place that will guarantee safety of the building inhabitants and perform drills to confirm organizational readiness (Kabay & Kelley, 2009). The type of natural threats may vary by geographic location and local stability so it is important that the natural disaster portions of the BCP are varied accordingly.

Without power, most organizations cannot do business. The importance of power supply and consumption increases drastically as the amount of technology used by a facility increases.

For instance, a smaller office building may only have computer workstations and printers but an enterprise data center may house an exponentially large number of servers, and computer systems. In these starkly different structures, the importance of power is vastly different. Although the small office building may wish to have battery backups or Uninterruptable Power Supply (UPS) units, the loss of power would only cause a mild disruption. However, in a data center, the loss of power could have cataclysmic results both locally and across the enterprise. If the enterprise has a large enough need for power, they should consider the use of redundant power distribution systems such as generators to produce power in the event of loss (Caballero, 2009). Furthermore, the BCP should include measures for testing the use of backup generators for reliability and continuity purposes.

Protecting against the potential risks of insider threats within the enterprise is a far more complex undertaking than the previous items. Computer security and data loss prevention is not a one-size-fits-all discipline. However, the organization should be aware of the various systems requiring protection at this point in the BCP process and there are several common sense techniques to protect these systems. Any critical information system in the enterprise should be kept in a physically secure location with limited access. The data kept within the system should be backed up regularly and the backup media could potentially be stored in an offsite location while ensuring that technical staff is trained in the proper backup procedures (Valacich & Schneider, 2010).

Any technological assets should include some sort of authentication and access control to prevent unauthorized use which usually takes the form of a user name and password.

Some organizations, including the US Government, require the use of a smart card for three-factor authentication (Defense Security Service, 2006). The level of authority a person has on an information system can be controlled in a central system so that it is protected and auditable.

All information systems need to be properly patched to insure that the system is compliant with the latest security posture from the vendor. However, the patches should be tested in a small supply of machines to ensure that the changes do not cause the system to become unstable or incompatible with other systems. It is also important that patches be applied to computers during non-peak hours or scheduled patch cycles to prevent disruption of normal operations (Cole, 2009). The BCP should include patch cycle time frames as well as illustrate the patch testing process and any measures for the rollback of a patch should it cause damage to the infrastructure.

Regardless of the integrity of the data backup policy, system security policy, and all applicable system controls, the users themselves are the most critical protection measures for systems. The organization should create mandatory user education documents and even computer based training if possible to make users aware of their role in the BCP. The training should be conducted at least once per year and updated however frequently as is necessary with supplemental training added when needed. Users who are responsible for more specific pieces of the business continuity process (such as high level systems administrators or those responsible for coordinating fire drills, power drills, etc.) should be given additional training beyond the mandatory training so that they are fully aware of their responsibilities and agree to the authority they are given.

In the case of forensic functionality, the BCP should include a thorough explanation of the various security tools built into the company network (IDS, firewalls, data storage, etc.).

If critical data is stored in both physical and virtual locations, the BCP should provide direction to the forensics team reflecting this. If the company decides to utilize a warm or hot disaster recovery site, the forensics portion of the BCP needs to reflect the location of these sites and instructions for accessing the data it contains. It would also be wise for the BCP to reflect live testing of DR sites and how quickly a forensics team was able to access a particular piece of data. Once all pieces of the BCP have been completed, the organization is prepared. The final step is testing of the BCP at accurate intervals.

Did it Work?

Even the best BCP ever created will be considered useless if it is not tested and updated accordingly. In the course of a two year time frame, the company should conduct several tests to determine their readiness for disaster and these items should be included in the BCP and the dates these were last tested should be included. The organization's testing schedule may vary depending on need and criticality but there are a few general guidelines for testing.

The natural disaster portion of the plan should be tested as frequently as is relevant. Fire drills should at least be conducted every 6 months or in the event of any major change to the plan. It is also prudent to perform tornado/hurricane/earthquake drills every six months and if these events fall into a seasonal pattern (i.e. tornado season is generally March thru June) it would be wise to drill near the beginning of the season and at a point in time outside of the season.

Testing the power failover mechanisms may vary depending on the scope of the power needs of a facility. In the aforementioned example of a small office with no servers and only basic computer systems, it may not be necessary to test power generators at all.

However, in the case of a large enterprise data center, it would be wise to test the power failover quarterly if possible or yearly at a bare minimum. Obviously, the size and scope of datacenter operations may prohibit a 100% test of the entire system at once but if the power can be broken out to different sections of the datacenter, these could be tested every quarter. Despite the potential setbacks, it would be wise to do a complete power failover test every two years (Miora, 2009).

It is impossible to set a universal precedent for data backups as this will vary by system and company but there are some generally accepted guidelines for backups. Due to their durability and low cost, many organizations still use DLT tapes for data backups. DLT tapes can be managed as a single tape drive or may be part of a large scale, automated tape library which orchestrates the backup of data (Valacich & Schneider, 2010). A full data backup should be performed monthly if possible with weekly delta backups and daily or even hourly differential backups to fill the gaps. The BCP should include monthly tests of effective backups as well as yearly tests of the backup process to confirm that a full data set can be obtained in the event of a disaster. The patching cycle should be scheduled in a similar fashion to ensure that data backups are available prior to installing patches.

User awareness training for the general populace should be tested yearly or semi-annually depending on the nature of the data they are working on. If possible the BCP team should do stress tests of user knowledge such as testing social engineering techniques for system access, physical security processes, and other tests at seemingly random intervals throughout the year. If it becomes apparent that user knowledge is lagging in any particular area, the organization may consider updating the mandatory training to account for these findings (Rudolph, 2009).

Establishing testing guidelines for forensic analysis in the BCP may prove a tricky undertaking. Most organizations would prefer to believe that they will never need to conduct digital investigations but this is simply not the case. It would be wise if the BCP included yearly or biyearly testing of forensic processes to determine how much downtime an incident might cause and the challenges of returning to full functionality.

The most critical aspect to understand about a Business Continuity Plan is that it is not a static document that is to be created then kept on a shelf for observation. The BCP is, by all respects, a 'living' document which must be constantly tested and improved in order to remain relevant to the business. The schedules used to test its effectiveness can be changed as long as the plan reflects the change and it remains relevant.

Conclusion

Businesses must be prepared for disaster at any given time. Regardless of whether business operations are hampered by natural disasters, environmental issues, insider threats from their user base or cyber threats from external attackers, they must be prepared to respond. The best way to respond to these threats is to create a business continuity program (BCP) which addresses specific measures the organization intends to take to prevent disruption of service. A company must have completed a business impact analysis (BIA) to use as a guideline for the potential risks and their impact on the company before they can justify the importance of protecting individual assets within the BCP. This document has illustrated how to assess business needs, determine risk and impact, implement a BCP and protect the critical assets via testing methods. No single structure is applicable to all businesses but those presented here can certainly be used to begin the process of securing a business from disaster.

Bibliography

Balaouras, S. (2009). *Businesses Take BC Planning More Seriously.* Cambridge: Forrester Research.

Blokdijk, G. (2008). *IT Risk Management Guide.* Brisbane: Emereo Pty LTD.

Caballero, A. (2009). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. In J. R. Vacca, *Computer and Information Security Handbook* (pp. 225-258). Burlington: Elsevier.

Cole, E. (2009). Information System Security Management. In E. Cole, *Network Security Bible.* Indianapolis: Wiley.

Defense Security Service. (2006). *DoD 5220.22-M.* Defense Security Service, Department of Defense. Washington D.C.: Uniited States Department of Defense. Retrieved from US Department of Defense - Defense Security Service.

Kabay, M. E., & Kelley, S. (2009). Developing Security Policies. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 66.1-66.15). Hoboken: John Wiley and Sons.

Kirvan, P. (2009, July 15). *Using a business impact analysis (BIA) template: A free BIA template and guide*. Retrieved November 23, 2013, from TechTarget: SearchDisasterRecovery: http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-analysis-BIA-template-A-free-BIA-template-and-guide

Miora, M. (2009). Business Continuity Planning. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 58.1-58.36). Hoboken: John Wiley and Sons.

Rudolph, K. (2009). Implementing a Security Awareness Program. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 2* (pp. 49.1-49.43). Hoboken: John Wiley and Sons Publishing Inc.

Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. L. (2010). *Contingency Planning Guide for Federal Information Systems.* National Institute of Standards and Technology, U.S. Department of Commerice. Gaithersburg: NIST.

Valacich, J., & Schneider, C. (2010). *Information Systems Today: Managing in the Digital World.* Upper Saddle River: Prentice Hall.