It resource contingency planning critical thinking example

Environment, Disaster

INTRODUCTION

Information systems are vital documents in many organizations. Because information system resources are so essential to the operation of an organization and its success, it is crucial that major services provided by these systems operate optimally without excessive interruption. Contingency planning support these necessities by providing the required plans, procedures, and technical parameters that will allow a system to operate and recover quickly and effectively as possible from a disruption.

Contingency planning is unique to each and every system, detailing the preventive measures, recovery strategies, and technical aspects appropriate to the systems information CIA requirements.

Thus an information system contingency planning refers to a coordinated strategy involving plans, procedures, technical necessities and aspects that ensure the recovery of information systems, operations and data after a man-made or natural disaster or catastrophe. It involves among others one or more of the following approaches to restoration of disrupted services.

- Restoration of information systems using alternate requirements
- Conducting some or all of the disrupted services using alternate means or processes for short term periods until the main systems are up and operational.
- Recovery of alternate information systems at alternate locations for long-term disruptions or those that physically impacts the facility.
- Implementing appropriate contingency planning controls based on the information system’s security impacts at the appropriate level.

Incident management processes, business continuity and disaster recovery planning are the fundamental concepts required of any business entity. Incident management is a coordinated practice at the corporate level that is dependent on round the clock reporting line and quick assessment and escalation for severity. A sound and formal protocol and procedure should be adhered to in relation to incident resolution and recovery. This may include 24 hour incident response team and incident communication procedures. In addition, virtual meeting rooms may be designed to bring together all the required personnel with regular status update.

Business continuity planning is best practices tailored by an organization to ensure the delivery of services and resume normal operations after an incident. A plan is required to detail the necessary resources, vital documents and critical conducts and applications necessary to revive disrupted activities to its normal states.

Finally, disaster recovery mechanisms are the mechanisms and procedures that an organization engages in while trying to restore the complete functioning of the technical environment including software and tools for meeting production applications to their previous states. In a case of a data center disaster, critical workload need to be restored at the disaster recovery sites considering minimum disruption of services to guarantee data integrity, availability and confidentiality.

DRBC policy is an influential document that must be availed to all employees and participants in a company. The lack of distribution and awareness of the policy tends to compromise its adherence. It is difficult for employees to adhere to what they do not know. Therefore, the fact that the copy of the policy is found on the company’s network does not guarantee universal knowledge of it. The policy must be published in the company website as well as avail it in all other communication boards and bulletins in the shortest time possible to increase awareness and improve the level of adherence.

Every business requires a contingency plan to coordinate the resumption of activities in times of uncertainties and disasters. Whatever given as the definition of these processes, the ultimate goal is that it serves to restore business operations to normalcy with little impact on the employees, customers and other stakeholders. The ultimate goal is to get the business back to normalcy in the least time possible as an elongated downtime has adverse effects on the business. The problem causing the downtime might be a single computer crashing, or an entire network, power blackout, terrorist attack or natural catastrophes such as floods.

BUSINESS CONTINGENCY/CONTINUITY PLAN

The goal of this paper is to describe a contingency plan that restores business IT resources to normal in the least time possible. A business contingency and recovery plan is a user’s manual that outlines the preparations, responses and undertakings at the time of the disaster, mitigation strategies and adverse effects prevention. The document must be created and tested before the interruption n occurs. Business continuity in this sense refers to disaster recovery. Lost revenue is the driving motivation for business continuity. The reason behind a recovery plan is to fundamentally keep the business revenue coming in and services going out while serving customers.

In order to execute a business contingency and disaster recovery plan, several processes and steps must be followed to develop a comprehensive document that fits to a particular business. This includes;

- Development of a contingency planning policy
- Business impact analysis
- Identification of preventive controls
- Creation of contingency strategies
- Development of contingency plan
- Plan testing and exercise
- Plan maintenance

The processes can be summarized as shown in the diagram 1

CONTINGENCY PLANNING POLICY

A clearly developed and implemented contingency planning policy ensures that personnel fully understands and adheres to it in the execution process. The contingency planning policy document defines the organizations overall contingency objectives and establishes the organizational framework and responsibilities for system contingency planning. The policy must be in lieu with FIPS 199 impact level and contingency control or any other relevant standards that the policy refers to. The development of a contingency/continuity planning policy for a business entity comprises of key policy elements which may include;

- Roles and responsibilities for business recovery and continuity
- Scope of the plan as applicable to common IT platform types such as telecommunication, electronics and hardware, personnel among others.

- Resource requirements
- Training requirements
- Exercise and training essentials
- Plan maintenance schedule
- Backup and storage media

A business contingency/continuity plan cannot be created by a single individual in an organization. As such a team should be mandated with the creation of a plan. While small businesses may require the efforts of a few individuals, large organizations will require the involvement of individuals from various departments to provide the needed portions. One group may be responsible for the technical/computer portion while another team handles the personnel. The plan should also outline the personnel in charge of making decisions. Like any other practice, a business contingency/continuity plan outlines the managerial hierarchy from the top down to the bottom. A clear outline should be drafted to indicate the person or team responsible for a certain task or level of engagement to eliminate collision of duties. Likewise, the plan should be specific to outline the recovery steps that should be executed first as well as the personnel with the required information. The logic and order of steps depends on the nature of the business and the disaster or interruption faced. A considerable note is that the plan should not be too dogmatic that it lacks the flexibility for implementation. It should have room for common sense such that it can be implemented without the presence of person or the team that created it. Likewise, it should be legible, understandable and easy to interpret by even the lay workers who are not tech-savvy. Plans that exclusively require techies to implement in most instances fail up to the expectation.

BUSINESS IMPACT ANALYSIS

Business impact analysis is the main driver in the implementation of a contingency plan. Conducting a business impact analysis is fundamental in CP controls according to NIST SP 800-53. It enables the information resources contingency plan coordinator to evaluate and characterize the system components, supported mission processes and their interdependencies. BIA seeks to develop a correlation between the system critical business processes and the services offered and based on that information evaluate the consequences of the disruption. A successful BIA informs the ISCP coordinator of the contingency planning requirements and priorities. BIA is carried out at the initiation phase of the system development life cycle in case of information system resources. The results from the BIA are appropriately incorporated into the analysis and strategy development efforts for the business DRP, COOP, and BCP.

A complete and successful business impact analysis incorporates the following three fundamental elements;

Determination of business processes and recovery functions critically to evaluate the business processes supported by the IT resources and their impacts upon disruption. An estimated downtime is also evaluated in this stage to determine the maximum time the business can tolerate while the IT resources are down. According to FIPS 199 impacts should be analyzed in terms of confidentiality, integrity and availability and categorization of information systems placed either as low impact, moderate impact or high impact as per the CIA objectives.

Identification of the resource requirements to explicitly determine the exact resources required to resume the business to normalcy. The resources may include equipments, software, data files, system components and vital records.

Finally, the identification of recovery priorities for IT resources forms the last feature of an effective BIO. This is based upon the results of the previous activities and system resources. Priority levels are established to sequence recovery activities and resources. Information resources recovery priorities are a function of business process criticality, disruption impacts and tolerable downtime.

PREVENTIVE CONTROLS

In some instances, outage impacts identified in the BIA process are better mitigated by employment of preventive measures. This is meant to deter, detect and minimize IT resource impacts. Where feasible and cost effective, preventive methods are more preferable to actions that may be essential for recovery. Some of the feasible preventive controls applicable to IT resources include;

- Appropriate UPS systems to provide power backup to all business system components

- Gasoline/diesel powered generators to provide long term power back ups

- Air conditioning systems to safeguard failure of certain components such as compressors

- Water sensors in computer room ceiling and floors
- Fire suppression systems
- Heat-resistant and water-proof storage containers for backup media and important electronic records
- Security controls such as cryptographic key management and encryption methods
- Regular scheduled backups and storage of offsite and onsite backup media
- Emergency master system shutdowns

CONTINGENCY STRATEGIES

Contingency strategy implementation in a business is essential for the mitigation of risk arising from the use of information technology resources. Contingency strategies include set of security controls implemented in accordance with federal or state standards and laws. For instance, NIST SP 800-53 standard covers the set of controls that mitigate risks associated with backup, recovery, contingency planning, testing and ongoing updating and maintenance.

BACKUP

In the business case, backup and recovery methods are dictated by the business type, which subsequently determine the method and strategy of risks and BIA criteria. A wide variety of recovery approaches apply to different business types. For instance, banking institutions that has evident over time that backup facilities have routinely failed due to unexplained causes. A probe on the causes of the failure needs to be conclusively determined at the item processing facility and relevant software and hardware installed. Backups at the data center and at the item processing facilities are performed on a weekly basis for critical data files, configurations and software programs. Considering the fact that the banking facility has a number of processing sites and each of these facilities act as others processing sites, a complete failure on the affected facility will impact on the back up exercise of its dependent thereby affecting the operations.

The storage mechanisms and backup methods will be dependent on the type of business operation. Businesses dealing with customer details such as banks, insurance companies, and health facilities have no option but to backup their data offsite. This is because compromise of such data will lead to enormous consequences on the side of the business and the clients. Commercial data storage and backup facilities can be obtained on contracted terms from vendor companies. They are designed to archive media and protect the data it holds in environmentally safe locations. Selection of offsite storage facilities is determined by numerous factors including; geographical are, accessibility, security, environmental conditions and cost.

PLAN TESTING AND TRAINING

An information resource contingency plan should be kept in a condition of readiness at all times. A readiness state imply the development of contingency plan, training of personnel to fulfill their roles and responsibilities outlined in the plan, testing systems, system components and other IT resources to ensure operability in the specified environment and constant updating and maintenance of the plan to ensure compliance. These procedures are contained in NIST SP 800-84 Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities. Prior to implementation stage, test, training and exercise activities should be conducted as well as during the maintenance and operation phase. NIST-800-84 is an important information database containing planning, implementation and testing procedures for information systems.

TESTING

Testing is a crucial procedure for a viable contingency plan. Through testing, plan inefficiencies are singled out and addressed through a change or update of one or more inefficient parts of the system.

A test plan designed to examine the selected items against explicit test objectives is needed for a testing procedure. Test plans should include a time frame for each test and test participants. Other parameters include scope, scenario and logistics that mimic the worse case scenario or an incident most likely to occur. In the present case scenario, the test period include a 24-month procedure conducted to test affirm the tolerance of its information systems.

TRAINING

The training process will familiarize personnel with the plan responsibilities and roles to be undertaken to yield desired objectives. The banks recovery personnel will be taken through a course that touch on;

- Purpose of the plan
- Team coordination and communication skills
- Reporting procedures

- Security requirements

- Team specific processes such as activation and notification, recovery and reconstitution

- Personnel responsibilities

EXERCISES

Functional exercises allow personnel to test their operational emergencies through a simulated operational environment. The process is more realistic because it deploys equipment designed to exercise roles and responsibilities of a specific team. The functional exercises in a banking facility will involve communication of system breakdown, emergency notifications, transfer of processing to alternate sites and system equipment setup. The extent of functional exercise differs in respect to anticipated level of attack. It varies from specific aspects to a full blown back and recovery.

PLAN MAINTENANCE

The established plan must be maintained and updated continuously to reflect a state of readiness at all times in its procedures, organizational structure and policies. The information system must undergo frequent changes to accommodate shifting business needs. A plan review should be carried out for accuracy and completeness of the plan at a business level frequency any time changes are made to any element of the plan.

For instance in a period of 24 months, the bank’s information system should be tested and updated after every six months to ensure efficiency. Backup and recovery systems must be continuously monitored and updating. The same applies to firewalls, antivirus and cryptographic techniques to incorporate the latest and most effective methods that are in lieu with evolving insecurity and vulnerabilities.

CONCLUSION

The paper has conclusively discussed the planning procedures, possible recovery options and recommended test that make up a comprehensive business contingency/continuity plan. It has made special inference to banking facility as the business under consideration.

REFERENCES

Bace, R. (2009). Vulnerability assessment: Computer Security Handbook . John Wiley & Sons.

Brian Caswell, J. B. (2008). Snort 2. 1 Intrusion Detection, Second Edition. Syngress.

Company, D. P. (1996). Guidelines for Contingency Planning for Information Resources Services Resumption. DIANE Publishing Company.

Mark W. Huber, C. A. (2008). Information Systems: Creating Business Value. Wiley.

Martin J. Wieczorek, U. N. (2002). Business Continuity: It Risk Management for International Corporations. Springer .

Socha, T. M. (2002). Facility Integrated Contingency Planning: For Emergency Response and Planning. iUniverse .

Swanson, M. (2011). Contingency Planning Guide for Federal Information Systems. Dianne Publishing .