IMPACT: International Journal of Research in Engineering & Technology
ISSN(P): 2347-4599; ISSN(E): 2321-8843
Vol. 7, Issue 7, Jul 2019, 1-10

IMPLEMENTING DATA SECURITY AND DISASTER RECOVERY IN IT COMPANIES THROUGH A PROCESS BASED PRACTICAL APPROACH

Sanjivesaxena & Ritumunjal

Research Scholar, Jagan Institute of Management Studies, New Delhi, India

Received: 19 Jun 2019 **Accepted:** 01 Jul 2019 **Published:** 08 Jul 2019

ABSTRACT

The advancements in information technology have generated data which needsto be protected so that the business can survive. This is due to the fact that data has generated an innate need for protection, security and the estimations pertaining to the loss arising out of data breach. This paper is thus an attempt to design, develop and implement a practical approach for the data security and disaster recovery plan for the organization. The genesis of the paper goes to the industry experience of the author of having implemented data security and disaster recovery processes in IT companies. The methodology followed is a structured approach starting with the macro level operations of the processes and gradually moving down to the micro level controls of the organizational processes for data security and disaster recovery. The limitation of the paper is the fact on the restriction of the page size and this has resulted in covering the essential components of the plan. The contribution of the paper is that it provides a practical approach for implementation. By customizing the parameters and developing the appropriate means and mechanism for the identification of the crucial assets a more sound and robust data security and disaster recovery plan can be developed and maintained.

KEYWORDS: *Business Continuity, Data Security, Disaster Recovery*

INTRODUCTION

The advancements in Information and Communications technologies has brought significant change in the means and mechanism of performing day to day operations. For example, today, we seek the services of google navigator to reach our desired destination based on the traffic conditions and other impediments. On the other hand, ecommerce websites keep us informing about the new sales campaign or the various discount offers that are applicable. All this indicates that data has carved a niche amongst the world. In fact, no matter in which industry we work or whatever decision we have to make we need data [1]. Data on its own has no value but generates a much larger (generallymonetary) value when it is processed. In other words, it produces information [2]. It is this information which must be protected, made secure and anall-round effort are required to protect the secure andprotect the data which is generated and has large potential commercial returns.

However, despite several attempts to protect data, disasters do happen. For example, data may be leaked to competitors and is thus likely to be exploited which may endanger the survival of business operations. Or, a malicious virus slowly ingresses its way into the system and 'eats' vital data there by putting the entire business at a grave risk [3]. In other words, there is an urgent need for ensuring data security and of ensuring recovery from the disaster.

Today organizations are spending heavily to ensure that data issecure, it's privacy is maintained and above all processes are in place to recover from the disaster which may be camouflaged in the form of a natural disaster [4] [5]. Thus, IT companies are invariably including the aspects of data security and data privacy and on disaster recovery as a post-operative measure should the data be breached anyhow.

Related Work

The previous sections highlighted the need and importance of having data security and privacy plan as well as the need for a disaster recovery process in place. However, implementing the plan and processes is a difficult and cumbersome task [6][7]. This is due to several issues and challenges which needs to be taken into consideration before the implementation process can commence. The challenges include various aspects such as adoption of data strategy which will serve the business objectives; a strong coherent data management strategy for identifying, classifying, organizing, deploying the crucial data protection processes which form the sub set of disaster recovery processes of an organization. The business world isdynamic hence issues and challenges are bound to increase. The majorchallenges of data protection and disaster recovery includes the disproportionate planning for disaster management and data security practices between top down and bottom up approaches; the lack of coordination and co-operation amongst various strata of the organization and above all the absence of a long term vision for dealing with the issues and challenges of data which is dynamic and high complex [9].The other issues which generate complexity and challenges are related to the implementation of well-developed system of processes, supportof the executive management and the regular monitoring of the implemented system.

OBJECTIVE OF THE PAPER

This paper is developed to provide a concrete practical approach tothe process of implementing and developing a data security and disaster recovery system for an Information technology company. Though the target company is Information Technology Company yet it can be customised to develop the system for any other type of industry or company which is not into Information technology.

The methodology that is followed is a two-step process. One part takes into consideration the development of an information management system deals with data security and data privacy system the other part takes into consideration the disaster recovery and prevention system. At the same time the methodology takes into consideration the other aspects such as project criticality parameters, risk management parameters and assessing the impact it has on the recovery measures.

The Implementation Process

The organizational Setup

In order to commence the implementation process, the most crucial aspect is the formation of an information security cell of an organization which is headed by the information security officer. This is the most crucial step as it fixes the responsibility and establishes the centralized controlling authority for the management of data security and privacy issues as well as leads the way for the development of disaster recovery processes.

The Information Security Officer then is Required to Develop the Team While Fixing the Responsibility of the Team Members. Figure 1 Illustrates a Team Structure Which May be Used

Figure 1: Depiction of Information Security Department in an Organization

Team Structure

The information security officer is the main person responsible for the management of information security management system. The information security officer is required to lead various security officer sand is a part of the overall security forum. The security officers are responsible for dealing with the day to day security aspects of the organization's information processing infrastructure and updates the information security officer on the status of the information system.

Moving down further under the security officers there are several other sub teams which form the core functions of information security management system. They are

- Disaster Prevention and recovery team (DPART). This team is responsible for handling all the incidents and carrying out recovery procedures when the disaster happens.
- Information security operations team. This team is responsible for maintaining and overlooking the security aspects of the organization during the normal business-related day to day operations through intra, extranet and other form of networking. They are also responsible formaintaining the confidentiality and integrity of the information system
- Information security administration team. This team is responsible for maintain the security in administrative functions of the organization such as defining security guidelines, reviewing security policies, administrative controls to be deployed in the information security management system and taking disciplinary actions when there is abreach of information security which impacts the business objectives
- Network and communication team. This team is responsible for ensuring the availability of the necessary resources required in the day to day operations of the organizations information security managementsystem.

- Technical support team. This team is responsible for providing the technical support and necessary help to the concerned information security team and other personnel's for carrying out business related operations and functions of the organization.
- Help Desk team. This team is responsible for providing the necessary help and redirecting distress calls to the respective departments at of an incident.

Responsibilities

Once the basic organizational structure is complete the next task moves onto the process of defining the roles and responsibilities without which information security management system will notfunction.

This Section Takes into Consideration Some of the Basic Roles and Responsibilities of Key Persons in the Organization

- Top Management. The top management is responsible for providing necessary support, co-operation, development, implementation and maintenance of information security management system in the organization. The management support must be visible to the staff members and must be ardently followed by top management otherwise the information security management system will not function properly in the organization.
- Information security officer. The information security officer is responsible for collection, protection and authorizing access to the organizations data. In particular, the information security officer is responsible for approving the access to the various resources which are under the business operations and under the directions of top management. The information security officer is also responsible for estimating the value of the asset in terms of monetary loss and other aspects as communicated to his from time to time. He is also requiredto regularly monitor an review the classification and authorized as well as unauthorized access to the identified assets.
- Security Officers. They are the officers who are responsible for the safety and integrity of the data which is under their operations and custody. They are responsible for implementing the controls as specified by the organizational policies from time to time. They are also responsible for implementation of controls applicable to the assets.
- Other staff members of the organization. The main responsibilities of the staff members include prevention of disclosure of sensitive and confidential information of the organization. In addition, they are also responsible for ensuring that only authorized persons are accessing the information and that any attempt to distortion, deletion and mismanagement of the information is reported to security officers

Organizational Security Management System

Once the roles and responsibilities are defined the next crucial tasks is the definition of the various policies for information security management system.

The design, development and implementation of the information system are guided by means of policies. These policies form thedirection and flow of the system implementation process. Accordingly,the polices are also classified on the basis of their applicability.

Specific policies. These are the policies which are applicable organizational wide. Depending on the size of the organization and the information security system to be implemented, the following points form the core aspects of the information security system.

- A management framework is formed which will initiate and controlthe implementation of information security across the Organization.This framework is responsible for providing clear direction andsupport on the matter of dealing with information security and its management. In other words, every information assets will be governed by this framework.
- The security of an information system that is the data generated will be the responsibility of the owner of that system. For eg.the project manager is responsible for the data which is generated by the project from day to day operations as well as form other operations. The project manager may delegate this responsibility to any individual but ultimately the whole responsibility lies with the project manager.
- The following points define the various aspects of managing the information.The various assets and associated security processes for each individual system;
- The responsible person for each asset or security process, and the responsibility documented;
- Authorization levels defined and documented. A management authorization process for new information processing facilities should be established.
- The risks associated with access to various data security and the assets comprising of information system must assessed and appropriate security controls implemented so as to ensure the minimum loss. Foreg. every project manager must estimate the project criticality matrix for each of the project. This criticality matrix provides the risk associated with the project and the assists the project manager in estimating the recovery time (Figure 2)

Project Criticality Plan

Project Name						
Project Code						
Sl. No	Criticality Criterion	Data	Score	Weight in %	Weighted Score	
1	Size of project (Revenue $)	$0.00	0.00	10	0.00	
2	Profitability ($)	$0.00	0.00	10	0.00	
3	Penalty clause in contract (Amount $)	$0.00	0.00	15	0.00	
4	Days left for delivery in working days	1	5	20	20	
5	Resources/ skills availability	Difficulty Level 1	1	10	2	
6	Phase of project	SRS	1	8	1.6	
7	Type of project	offshore	10	4	4	
8	Impact on client business	Low	2	5	2.5	
9	Link dependency	Link Independent	0	8	0	
10	IT Infrastructure dependency	Low	1	5	5	
11	Project Geography	Indian Project	3	2	1.2	Recovery Period
			Total	100	39.30	5 days

Figure 2: Depicting Project Criticality Plan for the Project

Other Policies Which Must be Defined and Documented Include the Aspects Such as

- Access parameter of the information assets and their procedures for handling them.
- Authorized user access, maintenance and they are up gradation Restrictions on the respective security, legal and business liabilities associated for the assets as well as day to day business operations
- Audit and monitoring rights and mechanisms for the various information assets and parameters
- Restrictions on information copying and disclosure and other form of unethical and ethical usage.
- Anti-virus measures and their prevention mechanism on the information assets
- Arrangements for reporting and investigating security incidents and drafting prevention plans

Classification of Organizational Assets

Depending on the business operations of the organization, the various department will identify, classify and protect their information assets including automated files, databases, software's, hardware's and applications that are used in the department.

Generally, the classification in an organization is carried out as Restricted, Internal, Confidential and Public. Further, all the unclassified information is generally assumes the classification as Confidential or Restricted. The following are the general parameters for classifying the assets but to reiterate again, they are dependent on the organizational business operations and the degree of importance attached to the data so generated.

Confidential is the classification of information in which unauthorized disclosure or use is not to the best of the interest of the organization and/or its customers for example new product design details, strategic planning documents, organization personnel data, budget information and other vital data. The loss or leakage of such information may prove to be disastrous for the organization.

Restricted is that classification of information in which the unauthorized disclosure or use will result in damage to the organization. For example, the productrange design documents, company documentation, and other cores aspects of documentation which would prove to be harmful to the organization's business.

Internal is that classification of information that does not need any degree of protection against disclosure within the organization's premises. For example, the operating procedures; policies and standards inter office communications documentation

The public is that classification of information that does not require anydegree of protection within or outside the company.

Further, the collection of information such as data warehouse, data repository, integrated database, dataset, file and any other form of data such as social media will carry the highest form of classification of data. There may be occasions where in if there are two strands of data is accessible at the same time and one is unclassified whereas the other is Confidential then the remaining data is treated as confidential. Further, any access to confidential information must be properly accounted for that is the user must have secured the proper permission from the owner of the information. In the absence of the permission, this will result in a security breach.

Specific Asset Protection Policies

Once the criterion for the classification is taken up, the next stage is the protection policies for the specific assets. The following points summarize the points of consideration

An inventory register is maintained for the assets the assets which are important for the security of the organization. This register is required to be updated at frequent intervals and further, the classification of the important assets is changed due to changing dynamics. For example, figure 2, pertaining to project criticality matrix changes as and when the project nears the completion stage.

All the information that is generated from the classified data is appropriately labelled and accounted for. For example, any change in the project commercials, is appropriately documented and accounted for.

Any information in the form of magnetic media and having classified as the status is labelled with appropriate classification. This will enable media to be stored to the same level of security afforded to its computer counterpart.

In a similar manner access procedures and processes are appropriately defined, documented and managed according to the requirements of the organization.

Personal Security

Policies are required to be defined for personal for the purpose of introducing security responsibilities and awareness arising from day to day operations resulting in information processing activities. The following points depict the information security measures that are applicable to personal working in the organization.

The managers including the human resource managers and the project managers must ensure the relevant security roles and responsibilities of the employee. This includes background and referral checks and other applicable measures while the applicable security controls pertaining to the projects are briefly communicated and accounted for by the project manager to the employee. Further, confidentiality and non disclosure agreement must be signed by the employee. Also, employee must be trained in the matters pertaining to security issues and any incident pertaining to the security of the assets and the data generated through these assets.

Physical and Environment Security

As the domain of security and information management is large, correspondingly the physical and environment security too is accounted for. The following points of consideration are covered in this section

The critical, secure and sensitive business information processing units such server, databases, legal documents, financial information and the like are to be installed and commissioned in secure areas where the entry is restricted to authorized personals only. The secure access controls must be in accordance with the defined policies as approved by the management of the organization.

The perimeter of the building must be secure and its access must be properly accounted for. Other aspects such as safe and proper disposure of electronic waste and the prevention of leakage of data and its unauthorized usage; storage of hazardous elements at safe and isolated location and the like

A Business Continuity and Disaster Recovery Planning

The previous sections covered one aspect of the data security and data privacy. This included the implementation of the various aspects of the information management system. However, the next stage includes the business continuity planning and disaster recovery processes in the case when disaster does materialize. Figure 2 provides the glimpse of the recovery process of a project on the basis of the criticality and the time needed to recover the project based on the

critical parameters.

This section discusses the disaster recovery and business continuity aspects of data security and privacy.

In order to implement a disaster management plan, the first task is to define the word disaster from the organizational perspectives and in accordance with the business objectives. Generally, the words disaster is defined as a mishap, a calamity or an incident that causes heavy losses which may be in the form of monetary or other aspect such as loss of customer, market standing and any other form which is crucial for the survival of the business. the example of the disaster may be in the formof Floods, Earthquake, Fire, Virus attack, Server crash, Datacorruption, Arson, Terrorist attack, Hacking, Network failure and thelike.

Further, the severity of the disaster is estimated based on the preset parameters such as (figure 2) phase of the project, the type of the project, penalty clause, profitability and the revenue that is to be incurred from the project and any other parameters. Hence it becomes imperative to have the business continuity plan in place in order to ensure the

- Safety of personnel and equipment
- The risk or the impact of the risk can be minimized
- Business is able to recover from the disaster in minimum amount of disruption
- Confusion and uncertainty is minimum when the disaster happens

Business Continuity Plan or Disaster Recovery Plan

For an organization, Business continuity plan is prepared at 2 levels. One is prepared at the organizational level while the other is prepared at the particular component of the business operations such as project. Figure 2 is an example of level 2 where in a project is taken into consideration and has an element of risk. On the other hand the level 1or the organizational business continuity plan includes the general and specific precautions and activities which are to be taken care to minimize the risk and the path that must be taken into consideration sothat the business is able to recover from the disaster in a minimum amount of time when a disaster occurs.

This section covers the level 1 plan of the business continuity or disaster recovery.

Implementation of Business Continuity Plan

The implementation of the business continuity takes place in a similar manner as covered for the implementation of information security management process. The following are the key activities of the Business continuity plan.

Formation of Disaster Prevention Taskforce. This is the first stage wherein the structure is formulated there by setting a clear cut direction for the implementation activities of the disaster recovery plan. This also includes the aspects

such as selection and recruitment of team members, defining their responsibilities, generating awareness of the employees and selection of floor marshals and training them about the various aspects of the plan, reviewing the plan with respect to the changing dynamics.

Identification of threats. This is the most important step in the business continuity management. This includes defining the measures and means for the identification of threats and vulnerabilities which are likely to impact the business continuity. In addition members are trained to classify the threats on the basis of the likely impact and the changing business dynamics.

Impact analysis. The next part of the business continuity planning is the analysis of the likely impact on the basis of the identified threat and vulnerabilities. This will assist the management in the development of the actions which are to be taken care off during the disaster.

Communication. This is another aspect which is taken into consideration as it deals with he means and mechanisms involved in the communication of the disaster without generating any sort of phobia or in security during the time of disaster

Info structure management. This is another aspect which is a part of the disaster management plan. The members are trained to account for the various info structure of the organization and how toaccounted.

Other aspects which form the part of the disaster plan includes evacuation procedure, training of the employee, alternative site arrangements and the logistics and transportation issues which must be taken care off.

LIMITATIONS AND FUTURE SCOPE

This paper addressed the practical steps required for implementing aprocess based approach to the data security and disaster recovery in an organization. The limitation that came up during the development of the paper is in the form of the constraints on the scope of the paper in terms of the page size. Also, the generic aspect is covered in this paper.

The future scope lies in the fact that the parameters for other types of industry can be customized as per the needs of the organization and thus the customized plan can be developed for the industry in which the organization operates.

CONCLUSIONS

Information security and disaster recovery are an important component for an organization. Any breach of data security puts the survival of the business at stake. Only a comprehensive process based approach with active support of the management will ensure that processes are put in place which will generate some confidence in the data security mechanism.

This paper has provided a practical approach to the implementation of data security and disaster recovery processes. Further, by developing an integrated software based on the practical aspects covered above a robust data security process can be implemented in reality.

REFERENCES

1. *"What is data, and why is it important?" (2018), https://www.import.io/post/what-is-dataand-why-is-it-important/, accessed on 1st March, 2019*
2. *"Data vs. Information" (2011), https://www.diffen.com/difference/Data_vs_Information,accessed on 1st March, 2019*
3. *"Hire Intelligence" (2018), https://www.hire-intelligence.co.uk/blog/disaster-recoveryimportant-businesses/*
4. *" Why it's a top priority to have a disaster recovery plan" (2018),https://www.velocitynetwork.net/blog/why-its-a-top-priority-to-have-a-disaster-recoveryplan/*
5. *"Disaster Recovery and Business Continuity: Putting Your Plan in Place"(2019),https://www.datacenterknowledge.com/open-source/growth-ocp-data-center-gearsales-outpaces-expectations*
6. *"Why is Big Data security so difficult?" (2017), https://jaxenter.com/big-data-securitydifficult-134920.html*
7. *"Understanding Five Key Challenges to Security, Compliance, and IT Ops" (2016),*
8. *https://www.tripwire.com/state-of-security/security-data-protection/understanding-fivekey- challenges-to-security-compliance-and-it-ops/*
9. *"What's your data strategy" (2017), https://hbr.org/2017/05/whats-your-data-strategy*
10. *"Issues and Challenges in Disaster Risk Management in Malaysia: From the Perspective ofAgencies: (2017),https://www.researchgate.net/publication/320076793_Issues_and_Challenges_in_Disaster*
11. *_Risk_Management_in_Malaysia_From_the_Perspective_of_Agencies*