International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

IT Infrastructure Business Contingency Plan

Anshuman Awasthi

Director –IT Infrastructure Engineering, Restoration Hardware

Abstract: ***Business Continuity planning is the one of the core function for an organization Disaster Recovery and Incident Management plan. If an organization wants to save itself from heavy losses that may occur due to a disaster or a critical process failure it is essential to have a robust and working Business continuity plan (BCP). Risk Management is a critical function for an organization when it comes to BCP. Risk Management has two critical parts; the first one is creating a Risk Register and second is drafting the responses for the documented risk factors.***

Keywords: Business Continuity Planning, Risk Management, Risk Mitigation, IT Infrastructure Risk Factors

1. Discussion

This article explains how to create a Risk Register and draft Risk Responses for Business Continuity Planning for an organization.

2. Methods

Business Continuity Planning, Risk Management

3. Results/Conclusion

To formulate a BCP it is mandatory to start documenting risk factors that may affect the business directly or indirectly and prepare a risk response. It is better to assign severity to each risk factor to prioritize our work and channel our resources and efforts on the critical factors first followed by medium and low.

Emergencies can come in many forms: physical perils such as floods, fires, or earthquakes; work accidents; walkouts, or it can be other problems like labor scarcity; absence of utilities like electricity or lack of required supplies; or deliberate acts of sabotage or terrorism. Any emergency that happens suddenly disrupts the routine of daily activities, jeopardizes the economic position or organization's reputation, and demands urgent attention should be considered as a crisis. In a few cases, emergencies may provide a sign of warnings for a few days in advance. Emergencies can come unexpectedly—varying in level of impact and degree. Disasters are referred to as catastrophic events or Large-scale or emergencies are referred to as. Loss of assets and reputation can occur if we do not work on Business Continuity Planning (BCP). By being prepared for expected emergencies, an organization is better suited to deal with unexpected and unforeseeable emergencies.

Significant business disruption can come unexpectedly, and plans for a disorder can vary depending on a type of disruption. As an interruption can go suddenly, drills, rules, and policies, and for organization business operations need to be created and prepared for each department by the board members to avoid frustrations.

Organization incident response pre-incident planning should have one goal: to minimize the adverse effects of a disaster. This goal can be completed through a program created to evaluate the vulnerability, risk of potential emergencies, and threats, and a strategy needs to be designed to mitigate any risk involved.

The strategy can be implemented through the development of an organization incident response pre-incident planning. This plan explains the actions that we should take to create an incident response plan. This method outlines responsibilities before, during, and after a disaster and provides responsibility for implementing the actions. It is not practical to adopt a single emergency plan for all the organizations and situations; all companies are different, having varied concerns and available resources.

A company should start with below general practices that can be adapted universally; the use of a single, generic emergency plan could result in situations where the resources necessary to implement a required action are not available. There are nine essential elements of emergency preparedness planning:

- Identify the planning team
- Perform Business Impact Analysis
- Conducting resource and capability assessments
- Analyzing and assessing the risk
- Developing the organization incident response plan
- Identify the potential targets
- Conduct training
- Conduct drills and exercises
- Conducting vulnerability and risk assessments

C-level officers' and managers' responsibilities start with taking necessary approvals, planning the budget, and then eventually create a process that can allow the rest of the organization to develop and implement necessary steps as per the plan. Once we start on the planning, you're we need to analyze each delivery unit to understand what all systems will needs protections and what should be the priority levels. To determine Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), we need to understand what all systems are performing critical functions. Management needs to oversee the overall process to know how the higher levels of DR solutions can be translated to gather the budget requirements and find the real protection statistics required for each type of critical system.

4. Protecting Your Critical Data

Data ownership needs to be understood across different geographies is as the definition of critical data may be different for different types of business. For some of the organization's customers, financial data needs to be protected, while for pharmaceutical companies, they want to secure their intellectual property and their trade secrets. Law firms may consider privileged information or their client data of utmost importance.

To properly secure high-worth data and high-risk data, risk management solutions need to flexible enough to create our definitions as per the business requirements for sensitive data and then be able to categorize, discover, and control it throughout the enterprise.

Critical Data must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. For a retail organization, the most sensitive information is personal information.

Personal information is identifiable information is data that can be traced to an individual and should be protected during the complete transaction. It can be a piece of medical information, biometric data, medical information, personally identifiable financial information like credit card numbers, transaction records, and unique identifiers such as Social Security numbers or passport. Risk is involved with not only the identity theft crimes but also the information that needs to stay private or personal data getting into the wrong hands. The critical data needs to be encrypted both in transit and at rest.

An organizations IT security department need to map critical data across all local area network completely, third-party applications, cloud repositories like office 365, but new regulations also require us to illustrate the business policies for any data stored locally or in the cloud and archived longer than necessary.

5. Normal Data Protection

It is essential to be compliant with new regulations and protect data as per new rules, and this process is about asking straight, but challenging questions. Trust is something that an organization needs to work hard to create with its customers, partners, or vendors and, once the trust is lost, it is challenging to regain. Implementation of the right technologies, along with proactive data management policies, makes it much simpler to comply with new rules and sustain the necessary trust. IT security teams often have to work to manage data that was usually stored in silo geographic locations. Today, due to heavy use of multi-cloud hybrid environments and virtualization have moved security team’s effort in a multi-dimensional landscape with an increasingly large amount of data in "borderless" data stores.

An effectivity strategy is to work on five fundamental principles to protect its sensitive Data

1) TAKE STOCK. Know what personal information we have in our files and on your computers.
2) SCALE DOWN. Keep only what we need for our business.
3) LOCK IT. Protect the information that we want to keep. (Access control, Local Area Network segmentation, data is protected behind firewall)
4) PITCH IT. Proper disposal of what we no longer need.
5) PLAN AHEAD. We have a documented plan to respond to security incidents.

6. Disruption Data Protection

Many organizations keep the disaster recovery process only in the documentation phase. Often organization makes incomplete attempts for disaster recovery like just copying the data to a remote location. In a few scenarios, business decides to use the mirroring process of their storage area network (SAN) vendor. These incomplete options are not good enough to provide the complete DR model. The job of implementing a full DR model is too complicated for many data and storage protection solutions, so IT system admins settles on executing partial solutions.

In case an organization needs to run its operations during a disaster, it needs a complete DR solution that works across different layers and supports several business functions. It needs to implement practices that will help them recover full IT business operations after a disaster - primarily from their customer's perspective.

An IT team needs to understand that data mirroring is an essential requirement of Business continuity planning. If we back up mission-critical information off-site, that can work as a good insurance policy for the business. In the event of a disaster or a critical system failure, accessing the critical data to run business transactions will be among IT's first tasks to bring business applications back online. However, those off-site data storage do not replace or automate or the other critical jobs IT system admins must perform so that enterprises can resume IT business operations. Instead, Data Center staff is forced to take on the intricate manual work of installing operating systems, rebuilding servers and applications; configuring networking, assigning storage volumes, and making sure things start correctly and in the correct order.

If we need to ensure the full restoration of business applications and services, we need to implement a complete DR solution; ABC home furnishing has adopted the service-oriented data protection model. Service-oriented data protection requires thinking about each IT service and what it contains.

The service-oriented data protection model ensures that data is safe to its original content and is replicated along with the unique permissions at the disaster recovery site. File and block-level security ensure that unauthorized users cannot access data even if the system is compromised in case of a disaster.

The organization’s business continuity plan should be in line with regulations, is tested at least annually, and is documented in your policies and procedures. The company has to ensure that all vendors involved in disaster recovery operations adhere to information security and related certification and standards.

7. Ethical Use of Data

Potter Stewart, associate justice of the U.S. Supreme Court, once said, "Ethics is knowing the difference between what you have the right to do and what is right to do."

Technology is moving faster than the implementation of new laws and policies that are done to keep up with this change. The owners of data, usually, will sit outside our organization. To protect the interests of the company and the attention of the data owners, we need to focus on data governance. Data stewards have to be the trusted custodians of the data. The company needs to ensure that they have policies in place that benefit not only the corporate welfare but also the interests of customers and partners or face reputational risk and potential loss of business.

Ethics matter to our customers and our partners. Providing transparency to our data governance policies and the appropriate mechanisms for data owners to truly govern their data at points of interaction and engagement is critical. Blur the lines between your back-office and front office, and even extend to the interactive edge for comprehensive data governance across all data owners. We know that if we do not address ethical use of data in your governance policies and procedures, there are unintended consequences that may not harm you, but positively can affect or harm your customers and partners.

The organization should document a recovery plan to follow in case of a disaster that authorizes only relevant users to access data even in case of an emergency. It is essential to develop a pre-planned document so that we do not compromise on any policy to bring up an online system post-disaster.

Security measures like the use of a secure password, laptop encryption, and use of mobile management, employee education, and training help ensure the ethical use of data in case of a disaster.

References

[1] The Definitive Handbook of Business Continuity Management
[2] Corporate Risk Management-By Tony Merna
[3] https://strategiccfo.com/
[4] https://www.fosterfuelsmissioncritical.com
[5] https://www.tandfonline.com/doi/pdf/10.1080/21693277.2014.882804
[6] https://disastersafety.org
[7] https://www.business.qld.gov.au
[8] https://www.aferm.org/erm_feed/the-business-impact-of-trump-tariffs/
[9] https://www.nyu.edu
[10] http://www.emergency-response-planning.com
[11] https://searchdisasterrecovery.techtarget.com
[12] https://www.healthdatamanagement.com/news/the-role-of-ethics-in-data-governance
[13] https://www.ijsr.net/archive/v9i3/SR20312083156.pdf (DOI: 10.21275/SR20312083156)

Author Profile

Anshuman Awasthi, Director, Infrastructure Engineering at Restoration Hardware, responsible for IT Infrastructure Management and New Implementations. Member of Forbes Technology Council.