Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Integration of Covid-19 in the Business Contingency Planning of MEGHNA Bank

Rabeya Ahmed

Received: 8 September 2021 Accepted: 4 October 2021 Published: 15 October 2021

Abstract

Abstract- Contingency planning denotes the overall planning preparation for any firm to meet unexpected events at any time to avoid losses from any human-made or natural or technological catastrophe. In the event of Covid-19, contingency planning requirement is a demanding issue. The planning helps to Identify the activities, resources, and procedures needed to carry out the bank's data processing requirements. In the pandemic, Banks need to assign responsibilities to designated personnel and provide guidance for recovering during prolonged periods of interruption to normal operations and ensure co-ordination with other staff who will participate in the contingency.

Index terms— business contingency planning, covid-19, disaster recovery plan.

1 IntegrationofCovid19intheBusinessContingencyPlanningofMEGHNABa

Strictly as per the compliance and regulations of: Introduction ata contingency planning will benefit the bank to maintain the smooth flow of the business. As the bank deals with financial and other sensitive information about clients and remains an excellent value for the bank, proper data management is essential for the bank. Banks need to protect against damage D caused by unforeseen and adverse events affecting information handing out. So the importance of business contingency planning is talked about all over the world. (Wehinger, 2012). Today with the advancement of technology, different online threats have increased manifold. Hacking, data stealing, credit card fraud etc. are widespread. So banks need to keep back up on all the data. Importance can be specified from the view of restoring data, financial loss, and regulatory perspectives.

2 II.

3 Contingency Planning

Contingency planning consists of three part-Incident response, disaster response and Business continuity. Incident Response Plan (ICP) emphasizes on immediate response to any incident. Disaster Recovery plan (DCP) emphasizes on restoring operations at the primary site after the disaster occur. Business Continuity Planning (BCP) facilitates establishment of operations at an alternate site after the disaster.

4 Business Impact Analysis(BIA)

5 Threat attack identification and Prioritization

6 Business Unit Analysis

Attack success scenerio development

7 Potential damage assessment

8 Sub ordinate plan development

9 Incident Response Plan (ICP)

Incident planning

10 Incident detection

11 Incident reaction

Incident Recovery

12 Disaster Recovery plan (DCP)

Plan for distaer recovery First the bank will do a thorough a detail Business Impact Analysis (BIA). The bank will develop a detail questionnaire about what the possible damages may arise, will conduct a workshop to instruct business function and process managers how to complete the BIA. The bank will collect questionnaire from different branches on BIA. The team will arrange continuous follow up system. They will assess potential damage and make themselves prepared for everything.

13 Crisis management

14 Recovery Operation

15 Business Continuity Planning

16 Establish

Here is the diagram of all plans and sub plans of ICP, DCP and BCP.

The BCP team should focus on these issues-? Identify specific applications needs to be processes ? Key personnel involved ? Necessary equipments for the applications of the process ? Necessary suppliers needed for the relocation ? Strategy to address the unprocessed task ? Full details of user manual (Lyons, 2009) First the bank will prepare a management team who will be responsible for handling BCP. Among them a group will be responsible for ICP, DCP and BCP.

This Continuity Planning (CP) team will make the personnel's known to all employees for further query providing their-? Mail address ? Contact info ? Home address ? Office telephone no etc

The CP team will do-? Clear delegation of roles and responsibilities ? Execution of the alert roster and notification of key personnel. ? Clear establishment of priorities. ? Documentation of the disaster ? Inclusion of action steps to mitigate the impact of the disaster on the operations of the organization. ? Inclusion of alternative implementations for the various systems components, should primary versions be unavailable.

III.

17 Policies and Procedures

In their plan, the personnel will follow up their current data processing system regularly-1. The committee will review these areas to examine all these to make them prepared for the Incident Response Plan (ICP)

? Physical computer security strategy such as physical access controls. ? Network security policies (for example, e-mail and Internet policies). ? Data security policies (access control and integrity controls).

? Contingency and disaster recovery plans and tests. 1. Establish Proactive and reactive strategies-Proactive strategies are for incident response plan where steps should be taken before the incident occurs. Reactive strategies will be done after any disaster occurs. In proactive strategy the officers need to determine the damage the attack may cause, determine the vulnerabilities, weakness and needs to take steps to minimize the vulnerabilities and weaknesses. 2. Testing-The team should continuously test their effectiveness of taken methods. 3. The Incidence Response team-This team will develop incident handling guidelines with the necessary software to handle the incident. They will create training and awareness activities to solve those.

For Disaster Response Plan (DCP) ? The Personnel will rush to the spot ? Apply sophisticated Engineering technology to detect the threat ? Retrieve all the attacked data to the alternative server ? Try to assure clients if anyone knows about the mischief ? Create prefixed support system for managing the crisis ? Conduct recovery operation with the latest technology

Here their tasks will be divided in three stages-1. Assess the damage-Where damage has been done needs to assess swiftly.

18 Determine the cause of the damage-what resources

have been under attack need to judge here. 3. Repair the damage-As early as possible the damages needs to be repaired.

IV.

19 Business Continuity Planning

The Bank Head office will take rigorous training programs to educate the employees about the possible threat, creating awareness, making them up to date with the latest technology. MEGHNA bank will use state of an art electronic vaulting system to safeguard their data as it is the quickest recovery solution. (Bronner, 1997). This vaulting system allows a bank to maintain duplicate data and systems at a recovery site. Remote shadowing and mirroring, two technological components of electronic vaulting which allow a bank to replicate information as they are created just after any transaction and transmit that information at real time basis via high speed fiber optic circuits to a remote site. As this information are stored and protected at a remote site, these data can be readily available if any disruption occurs. Remote mirroring provides nonstop accessibility of mission significant information. This shadowing and remote mirroring technique is quite popular in tech-savvy organizations for safeguarding the data.

V.

20 Hypothetical Incident Scenario

On 27th January 2014, officers of MEGHNA Bank, Maryland branch noticed something wrong in their computer while starting work on the day's morning. They found many new files on their computer and they cannot open their software of the bank. His happened to every computer of the bank. Meanwhile, the customers were gathering around the bank for transactions. To make the plan activated the contingency planning team needs to notify all the team leaders and inform them of the event's details and necessary relocation. Upon notification from the contingency plan coordinator, branch managers are to notify their respective officers. The team revealed that the branch server was hacked and attacked by Trojan virus, all data has been gone. There was no other than the option of recovering data from an electronic vault. They retrieved data and IT experts rushed to the bank and fixed all the computers for the operation. The team took almost two hours and thirty minutes to resolve the crisis. There were no significant losses due to their rapid action, but there were some losses and customer dissatisfaction a little bit. But their expert BCP team handled the issue smartly and continuously follows up on the matter.

21 VI.

22 Covid-19 Plan and Economic Impact in the Security Breaches

The shutdown of the economy and restrictions imposed due to Covid-19 on the social movement forced the economic activities to operate on a limited scale. This unprecedented event can have a substantial impact on economic growth and prosperity. The unemployment rate has skyrocketed, and businesses were forced to shut down due to a liquidity crisis (Ahamed, 2021). Banks deal with customers frequently which forced the bank employees to have the most exposures. The economic impact due to stress in liquidity and capital can make the situation worsen. (Abodunrin, Oloye, and Adesola, 2020). Officers are to be informed of all applicable information and prepared to respond and relocate if necessary. Here, if there causes IT disruption, there will be problems reporting the problem to the CP team and the concerned department will ask the help desk for the solution. The CP team will retrieve data from the electronic vault of the bank. Thus they will maintain BCP Covid-19 protocol and continuous follow-up will be there. The same process applies if there causes any telephone system failure or branch disaster. If any major disaster attacks head office, then the BCP team may sometimes take help from the legal department and the outside IT specialist to resolve the issue. As they have an electronic vaulting system, there is less tension about the possible threat.

The pandemic should be considered as a disaster and included in the business continuity and disaster recovery planning. Maintaining social distancing and working from home using the highly secured software should be in effect. The pandemic also triggered security risk like data breaches, credit card hacking etc. Customer's usage of online activities soared and hackers took the opportunity to gather information using the vulnerable security system. (Montz, 2020).

23 VII.

24 Ethical Concerns of the Plan

Organizations need to understand the privacy, security, and legal implications of storing data. (Klosek, 2005). Ethics training for the employees is the main issue. As employees are the main performer of the bank, they need to be more ethical because unethical employees can bring disaster to the bank. They can malpractice to reap personal benefit through wrong data. So the bank should train ethics to their employees. The bank should seriously provide ethics training to their employee, not just window dressing. (Childers, 2005). Harm may arise from the online transfer of the data. Anyone could easily monitor any unencrypted data.

Consumers' data is another point of ethics. Usually, bank stores huge data of customers. These data may be essential to different ad firms or similar firms. They can push banks to sell customer data in exchange for monetary benefits. Banks need to practice the highest ethical standard to maintain the privacy of the customers. (Davison, 2007). MEGHNA bank has a concrete code of conduct that gives utmost priority to ethics. They urge their employees to follow their code of conduct strictly.

25 VIII.

26 Conclusion

Bank has sent all these materials to every branch and directed them to follow specific guidelines. After all these steps, the bank is thinking itself well prepared with its contingency plan to meet the unforeseen probable damages and believes it will provide real-time services to the customers. The bank will try its utmost to keep the business regular and try as they don't need to plan. Contingency planning is only for extreme cases where regular operation is disrupted.

	Outsiders as ? Computer security management and coordination policies. crackers or hackers	
	Other documents that contain sensitive Malicious	
	information such as:	Insiders
		such
		as
Human	o Computer BIOS passwords. o Router configuration passwords.	disgruntled
		em-
		ploy-
		ees
	o Access control documents.	
	o Other device management passwords.	
Security	1. The committee will identify assets and vulnerabilities Non malicious Ignorant employees	
Threats		
Natural	to known threats-Here the committee know the information s the main asset of a bank and major fra	
dis-		
aters/Pandemic		
	2. Identify likely attack methods, tools and techniques-	
Source:	Attack can be done from viruses and worms to password and e-mail cracking, denial of service attacl	
(Ben-		
son,		
2000)		

Figure 1:

[Wehinger ()] *Banking in a challenging environment: Business models, ethics and approaches towards risks*, G Wehinger . 2012. OECD Journal.

[Bronner (1997)] *Banking Industry and Disaster Recovery Planning*, R F Bronner . http://www.bankersonline.com/articles/sfpv04n11/sfpv04n11a16.html 1997. June 13. 2014.

[Abodunrin et al. ()] *Coronavirus pandemic and its implication on global economy. International journal of arts, languages and business studies*, O Abodunrin , G Oloye , B Adesola . 2020. p. 4.

[Klosek ()] 'Data privacy and security are a significant part of the outsourcing equation'. J Klosek . *Intellectual Property & Technology Law Journal* 2005. p. .

[Childers ()] *Ethics as a strategy. The Internal Auditor*, D Childers . 2005. p. .

[Davison ()] 'Ethics of business continuity and disaster recovery technolgies: a conceptual orientation'. C B Davison . *International Journal of Computers, Systems and Signals* 2007.

[Lyons ()] A J Lyons . *Contingency Planning: Data Processing*, 2009.

[Ahamed ()] 'Macroeconomic Impact of Covid-19: A case study on Bangladesh'. F Ahamed . *IOSR Journal of Economics and Finance (IOSR-JEF)* 2021. 12 (1) p. 2021.

[Montz ()] 'Risk management: Are there parallels between COVID19 and floods?'. B E Montz . *Journal of Flood Risk Management* 2020. 13 (2) .

[Benson (2000)] *Security Strategies*, C Benson . http://technet.microsoft.com/en-us/library 2000. June 13. 2014.

[Minar ()] 'Tatmadaw' s Crackdown on The Rohingyas: A SWOT Analysis'. S J Minar . *Journal of Social Studies* 2019. 5 (1) p. .