# m

*by* L T

**Submission date:** 04-Jun-2021 11:03AM (UTC-0400)
**Submission ID:** 1600430326
**File name:** contigency_strategies.edited.docx (211.69K)
**Word count:** 2851
**Character count:** 16101

# Developing Contingency Strategies for Information Systems

Name

Institution

Course

Instructor

Date

**Developing Contingency Strategies for Information Systems**

**BIA**

Every company is subjected to risks that can occur for different reasons, whether natural or manmade. Therefore, conducting business impact analysis is essential in realizing and examining the company roles then aligns the information technology suitably with the organization. The objective of performing BIA for Lopes manufacturing is to help forecast what might come to happen from the disturbance that affects the company procedures and systems. When Lopes Manufacturing recognizes these results, they can create the proper approaches for company recovery from the risks that might happen on their way and reduce the dangers to the organization. The examination will concentrate on both the financial and process effects that can interrupt the company.

Performing BIA has significant advantages and possible outcomes to Lopes Manufacturing because it reduces the dangers by preparing ahead and arranging the processes when the tragedy happens. Therefore, by preparing the probable catastrophes, the company can stop itself from failing due to bad losses when the disaster occurs. Furthermore, poor planning results in haphazard and incompetent recovery situations (Fernando, 2017). Nevertheless, proper planning will make Lopes Manufacturing have confidence when implementing the plans to counter the catastrophe. The company enhancement is achieved through the plan providing s testing space for recovery as well as recognizing augmented costs and loss of income from disruptions. This will improve the processes and security of the company system.

| **Threat** | **Impact** | **Recovery** |
|---|---|---|

| | | |
|---|---|---|
| Damage to client's data | Can lead to significant costs to safeguard the customers and losing them | Apologizing to clients, reimbursing and securing the database |
| Damage of workers data | Increases employee turnover probable lawsuits | Ask for forgiveness to workers, reimbursements and auspicious safeguarded records. |
| Leakage of company information | Punishments, consequences and reduction in customers | Improved protection of the company processes |
| DHCP server becoming disconnected | Stoppage of operations | Restoration of server |
| AD severed becoming disconnected | Stoppage of operations | Renewal of server |
| The web server is disconnected | Operations stopped and business losses | Refurbishment of the server |
| Corporate solutions not functioning | Harm in production and discontented clients | No other part of restoring the cooperate solutions |
| Operating system not functioning | Harm in production and discontented clients | No other part of restoring the operating system |
| Mobile phones | Reduction in clients | recuperate laptop and implement strict rules |
| Loss of data in laptops | Reduction in clients | Wipe/recuperate laptop and implement strict rules |

| | | |
|---|---|---|
| desktop | Reduction in customers | Recover desktop and implement strict security |
| printers | Probable data breaks | Reduces access from various hardware on the network |
| routers | Harm in production and discontented clients | Substitute a router and reinstate data from backup |
| Antivirus not functioning | Provides a chance for breaches | Troubleshoot, replace or have a backup protection |

**Incidence Response Plan**

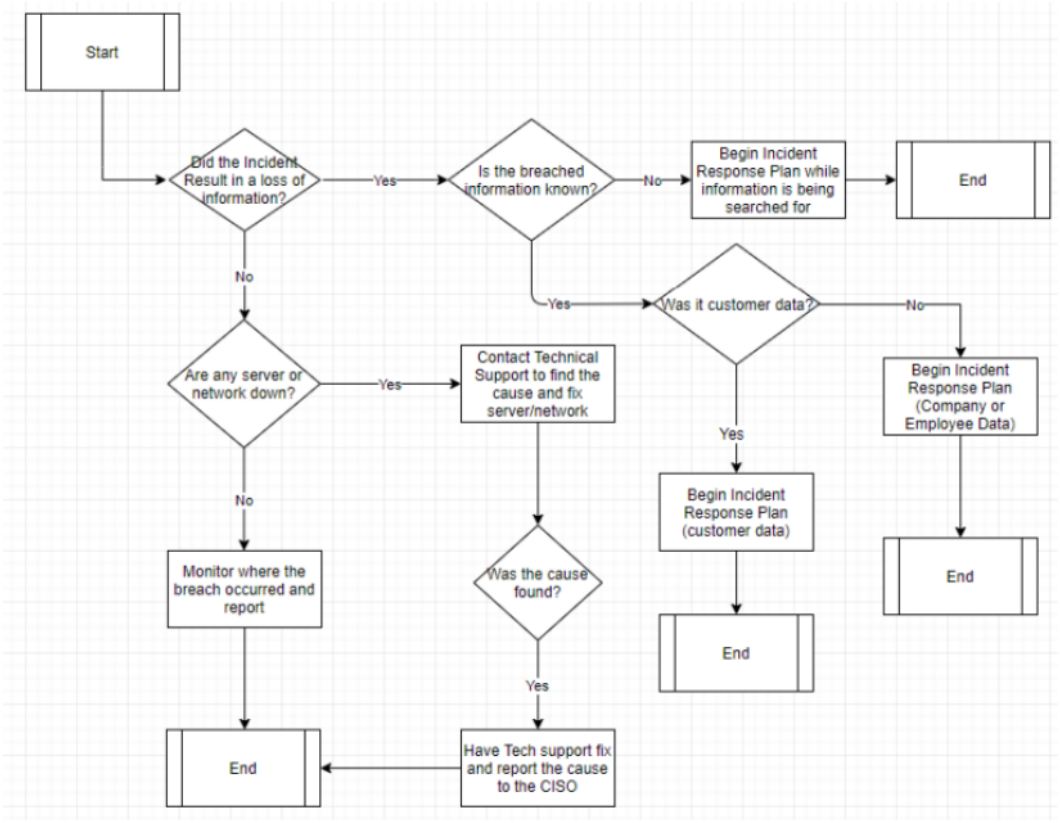
IRP plays a critical role in Lopes Manufacturing because it ensures that the information technology team can handle data loss and cybercrime challenges. Alsmadi (2019) defined IRP as the set of directions to assist the information technology team in identifying, reacting to and recuperate from the network security occurrences. Therefore, this IRP will provide the activities that will be considered when an incident happens in Lopes Manufacturing, explain the parts and tasks, reporting strategies, workflow diagram, and the phases of incident management and increase measures.

Different tasks will be performed by various parties in the IRP to ensure an effective plan. For instance, leaders will play a crucial role in the incidence response tasks because they can control their teams. Similarly, through the team leader, the group members can maintain their roles and be determined on the assigned work. This will help in the reduction of damages and provide a hasty recovery. Also, another role is the Lopes Manufacturing investigator, who will gather and examine data to obtain the cause of the incident. Thompson (2018) insisted that

the investigator is essential in the company because they instruct other security examiners and recover. Also, another vital party is the documentation and timeline team that will be accountable for documenting all the activities conducted in IRP; for example, they will start from the examination process to detection and regaining. Therefore, through the documentation team, Lopes Manufacturing will obtain the time frame for every step. Also, the communication team is essential in performing the messaging across the company. Finally, is the human resource and the legal group is responsible for assisting and directing the company of any legal situations and the significances that may arise from the type of incidence that happened.

Reporting directives are important in the IRP because the response plan will be initiated as soon as the incidence is reported. Therefore, it will result in hasty recovery when reported fast, hence reducing the reparations to Lopes Manufacturing. Lopes has developed an incident reporting tool that will facilitate reporting because all security teams access the tool. Therefore, the tool will request the specific incidence that happened, the individual who identified the event; the challenge recognized, and the required team.

**Workflow diagram**

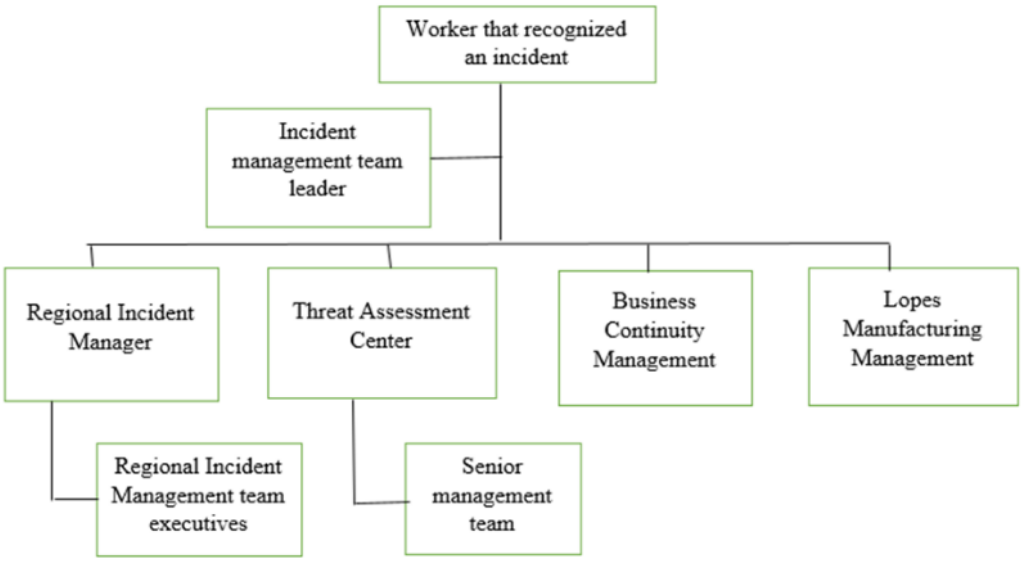



An incidence response plan should integrate all individuals, procedures, and technology that are recognized, verified, and trained to handle a security break. Nevertheless, every stage in the response preparation is critical because they all lead to the stoppage of data and financial losses as well as recovery to the usual procedures of the company. The first step after the required Lopes Manufacturing team has attained the incident is the incidence response tool they will prepare for the event. This will evaluate and classify the safety strategy, complete dangers valuation, and recognize susceptibilities of assets and describe probable events from the smallest to the maximum disparagingly.

The next step is recognizing, which comprises monitoring the company systems to check for irregularities in the Lopes infrastructure to have a security danger. For instance, immediately the event is identified, then all signs will be collected to realize the event's severity and then documentation is done. The team will then move to the next step, which is containment. Thompson (2018) stated that containment is the method of separating the network divisions attacked or at risk. This will help in examining the threat and realizing the solutions that can be used to reduce losses. Also, the next step is to eliminate the threat. After the systems are separated, the threat such as the virus can be eliminated from the network or systems. Through this process, the security team will know how the virus or threat managed to get access to the network, hence providing a chance to add more prevention approaches to stop such threats from reoccurring. Recovery is the next step that requires the team to return the systems to normalcy. Alsmadi (2019) defined recovery as the procedure of returning the affected system to production. This will require the team to test, authorize and check to certify there are no irregularities. Finally, the team will have to learn from the events by conducting more examinations and analyzing the plan to check what may be enhanced in the future.

The escalation process is vital in Lopes Manufacturing, especially in the occurrence of critical events. The first step in the escalation process in Lopes Manufacturing is to recognize the probable event. Therefore, the first worker realizes the event will have to instantly report through the incident reporting tool on the company website. The next step will be for the incident management group to check the reporting tool and evaluate the occurrence. When the sternness of the event requires an incidence response leader, regional event director, risk evaluation centre, corporate steadiness management and all the Lopes Manufacturing directors will be informed on the occurrence.

After evaluating the event on its sternness by the incident response team and finding that the regional event director should be made aware. The team will inform the director and organize with the regions director's executives on the occurrence. Then the next step will be developed based on the outcomes of the event evaluation. For instance, if the event sternness permits, the risk valuation centre will communicate with the selected senior administration to deal with the occurrence. After contacting all the required departments and teams, conclusions will be made if the event can be stated as a catastrophe. Finally, suppose the event is declared a catastrophe, the incidence response manager will update the regional incidence management team of Lopes Manufacturing of available updates immediately. Nonetheless, when the event is not stated as a catastrophe, the event response director will organize with local directors and business employees to restore company processes.




**Disaster Recovery Plan**

The purpose of the disaster recovery plan is to safeguard the information systems. Lopes Manufacturing values their customers and workers and thus is enthusiastic about safeguarding and protecting their information in case of a threat in their systems.

Moreover, the strategy will assist with the regaining of Lopes Manufacturing systems, infrastructure and network in case of an attack. Therefore, the plan will comprise all the exposed regions, including clients, company and employee data.

The disaster recovery team has several procedures that must be followed; however, the incident management team will be accountable for most activities. The Incident Management team plays a vital role in this event because they will examine all the events described and evaluate the dangers involved' sternness. Furthermore, once the sternness has been realized, they will include other parts of the company to guarantee that the right individuals are included in the recognition, communication and determination of the adversity.

Several resources can be required depending on the severity of the catastrophe. Some of the human resources that may be needed comprise the event response leader, risk evaluation centre, regional event director and corporate steadiness administration, and the Lopes Manufacturing administration team.

Training plays a crucial role in disaster recovery because it will enhance the operation procedure. Therefore, Lopes Manufacturing is focused on training all workers on how they can detect a threat and how to use the reporting tool. Similarly, the incidence response team will also be trained on suitable security skills, risk evaluation and disaster recovery to make proper evaluations of occurrences.

Monitoring is essential in the incidence management plan. Therefore, table exercises will be filled quarterly to certify that the event response preparation and disaster recovery plan are updated and consider the outlook of all probable dangers that can affect Lopes Manufacturing. Besides, testing will be performed every month and shifting the cyber and security access points to enhance the protection of company information.

Lopes Manufacturing will plan the maintenance time accordingly to avoid interfering with the company operations. Therefore, the maintenance schedule will always start from 9 PM to 5 AM on weekends. This is essential because there are always no customers or employees using the system.

**Business Continuity Plan**

Lopes Manufacturing will use a friendly site. Rezaei Soufi et al. (2019) stated that a warm site is a form of capability in the company to recover their technology infrastructure when their main data centre is offline. Therefore, the site will have several preinstalled server hardware as well as numerous data centre spaces. Furthermore, the warm site always has almost all the information technology devices available in the primary data centre including the hardware and software. Since the warm site provides a fortified data centre with no customer data, the company will create customer data and install more devices on the warm site when the threat has occurred at the primary site.

Warm sites will help Lopes Manufacturing in justifying the effects of incidences. Similarly, the strategy is critical in the business continuity for Lopes because it allows the company to continue operating when the unplanned event occurs and stops more data losses. Decides, the information concerning the site is integrated into the company disaster recovery

plan. Moreover, Lopes Manufacturing has a comparatively short recovery time objective because of the critical operations they perform. Therefore, the strategy will help them because it needs less setup than the cold site.

The warm site strategy will be used when the catastrophe occurs in Lopes Manufacturing. Therefore, the servers will be set earlier without the database. Niemimaa et al. (2019) defined a server as the computer, program, or equipment devoted to handling network resources. Therefore, the servers serve other computers referred to as clients to deliver functionality. Similarly, the company will sustain and maintain the backup services that have a network connection to Lopes Manufacturing situations. to guarantee there will be a reduction in data loss; the company will perform data synchronization at night. Nonetheless, the warm site will not operate on the same level as the production centre because it has fewer working capacity.

Moreover, information technology takes in the company back up data and other devices required in operation during the incident. Therefore, Lopes Manufacturing can take data from the cloud. For instance, through the use of disaster recovery as a service or the utilization of backups kept on media which was not impacted by the failure of the data centre. Besides, the company needs to recognize the type of data to obtain in the warm site because there is information such as customer data that requires urgency in restoration.

Recovery procedures are critical for the continuity of business operations. Therefore, Lopes Manufacturing will start by examining the most valuable data linked straightforwardly with revenue generation. Nevertheless, in case all systems had failed due to the disaster occurrence. The company will start by bringing servers online. Niemimaa et al. (2019) claimed that servers safeguard the company information by offering a more dependable and securely improved infrastructure. Moreover, recovering the servers first is essential in returning

communication after the disaster because they provide a central place to store company information. Thus one can easily regain files that were accidentally deleted as well as retrieve the past versions of the files.

The next element to be recovered is the database. Databases play a crucial function in Lopes Manufacturing company; therefore, prioritizing its recovery will help a lot. For instance, the database has all the records for the customer's orders and payment history. Also, the database contains employee's information which is highly organized. Retrieving it will help in gaining immediate access to critical information. Moşteanu & Roxana (2020) emphasized that having company data stored in the database allows for the suppleness to provide other software applications as well as company processes which can aid in decreasing costs through the eradication of manual data authentication and recovery. The worst-case scenario will be in the database because when the database is blank, the company cannot continue its operations. Therefore, they will need to take every customer as a new individual until the information is recovered. The final element to be recovered is the operating system and hardware. This will make every employee, customer and staff get back connected. Thus, all people can sign up, get individual training, cancel associations and perform all the maintenance required.

Establishing business operations will require the company to safeguard all the essential hardware and software needed. In the occurrence of a threat, to restore the company functions and security works, the warm site will initiate the process. The different site backups will provide a recovery that will not take more than one day and will permit the company to continue its work while utilizing the backup site.

The worst-case scenario will comprise the database losing all the data, requiring the company to collect new data from customers and employees until they recover the information.

Furthermore, to return to the unique situation will take three months. However, the timeline for the best-case scenario will take nearly a month to investigate the incidence, repair the system and enhance the security to safeguard the incident from happening again.

The company incidence team needs to be ready for the incidence; therefore, workers will be trained on how they can realize the threat and the manner of reporting. This will reduce the damages caused because the earlier the threat is realized and hasty measures taken will reduce the severity of the danger. Furthermore, the incident management team will play a core role in Lopes Manufacturing hence should be trained to evaluate the threat sternness and examine the dangers. The company will also exercise competence and efficacy of their plans through table practices of the threat reaction procedures, threat recovery plan and business continuity to guarantee it is updated.

**References**

Alsmadi, I. (2019). Incident response. In *The NICE Cyber Security Framework* (pp. 331-346). Springer, Cham.

Fernando, M. S. (2017, September). IT disaster recovery system to ensure the business continuity of an organization. In *2017 National Information Technology Conference (NITC)* (pp. 46-48). IEEE.

Moşteanu, D., & Roxana, N. (2020). Management of Disaster and Business Continuity in a Digital World. *International Journal of Management*, *11*(4).

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, *49*, 208-216.

Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, *57*(3), 779-800.

Thompson, E. C. (2018). *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*. Apress.

m

ORIGINALITY REPORT

| 1% | 0% | 0% | 1% |
| --- | --- | --- | --- |
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
| --- | --- | --- |
| 1 | Submitted to Coventry University<br>Student Paper | <1% |
| 2 | Submitted to University of the Highlands and Islands Millennium Institute<br>Student Paper | <1% |

| | | | |
| --- | --- | --- | --- |
| Exclude quotes | On | Exclude matches | Off |
| Exclude bibliography | On | | |