

report

by Nn Nn

Submission date: 09-Mar-2020 02:46PM (UTC-0500)

Submission ID: 1272473992

File name: Olnofrmation_system.doc (72K)

Word count: 2314

Character count: 13561

Information System

Student Name:

Institutional Affiliation:

Date:

DEVELOPING CONTINGENCY STRATEGIES FOR INFORMATION SYSTEM**Business Impact Analysis (BIA) for IT Infrastructure**

The objective of conducting the BIA will be to identify the potential threats to the organization's IT infrastructure, quantify how much the identified threats will cost the organization and prioritize on the recovery plans. Concerning the identification of the potential threats to the organization's IT infrastructure, after breaking down the IT operations into diverse discrete processes, the risks associated with every process are identified. The risk assessment involves the listing of each potential threat, which can disrupt one or multiple information system functions (Singh & Joshi, 2018). In addition, it entails the assessment of the relative probability of every threat. The external threats are mostly the more definite such as man-made, as well as large-scale disasters, for instance, floods, earthquakes, and even protracted power outages.

On the other hand, internal risks entail inadvertent data corruption, failed software patches, and failing hardware. Some threats, such as disgruntled employees, together with hackers, can be either internal or external. Assessment of risks uncovers probable disruption risks, which are, in most cases, overlooked.

Regarding cost assessment, it offers an objective look on the manner in which a threat would cost, on the side of sales, clients, or reputation, in case it actually occurs. Each of the costs is expressed in real dollars. The losses may be a result of disruptive communication with existing, as well as prospective clients. They may also be lost sales because of the hacking of the ordering webpage. Identification of the potential costs of the threats makes their danger quite real. Besides, it puts within perspective any budget needed for the implementation of continuity plans (Whitman, Mattord & Green, 2014).

Most importantly, the BIA offers an objective procedure of assessing the functions that do or do not require comprehensive recovery plans and to plan their respective mitigation, as well as recovery plans. In that respect, it paints a roadmap for formulating the other parts of the BCP (Business Continuity Plan). Upon identifying the vital business processes, the prospective threats to each, along with the approximated cost of the threats, the priorities get to be clear. In the absence of a BIA, creating the other parts of the BCP would simply be at random or best-guess.

List of Threats and Impact

² Business Function or else Process	Business Impact Factor	Recovery Time Objective	IT Systems or Apps Infrastructure Impacts
¹ Accounting & finance support: Accts receivable, Accts payable, etc.	Severe	Within the hour	File server, Application ,Accounting, payroll management, point of sales, logistics, electronic payments
¹ e-Commerce website for online customer purchases and scheduling 24x7x365	Medium- Severe	Within the hour	Point of Sales system, Web Server
Payroll also human resources for employees	Medium- Severe	Within the hour	File server, , benefits management, records,

			personnel
2 DNS – for internal also external IP communication	Medium- Severe	Within an hour	Interoperability among servers, workstations,&web

² Internal and external voice communications with customers within real-time	Medium	Within the day	Minimal impact inside the infrastructure.
Internal & external e-mail communications with clients via forwarding messaging	Medium	Within an hour	Minimal impact on the infrastructure or ¹ Medium effect on the interoperability within internal depts.
Internet connectivity for e-mail	Medium	Within an hour	¹ Email server, interop among clients & servers
Self-service site for customer accessibility to personal account information	Medium	¹ Within the day	Point of Sales system, Web Server

INCIDENT RESPONSE PLAN (IRP)

Timely, as well as thorough action of managing cyber incidents' impact is a vital element of the reply process. Basically, the response is set to limit the possible damage through making certain that actions are not only fit known but also corresponding well. The occurrence reply objectives include:

- Protecting the well-being of the company's community.
- Protecting the integrity, availability, and confidentiality of the company systems, data, and networks.
- Assisting the company personnel to recover business process following a network otherwise computer security incidents.
- Offering a consistent reply strategy to the network as well as system threats which set the company data as well as classification at risk.
- Developing and activating a communications program, inclusive of original incident reporting together with continuous communications as essential.
- Addressing cyber-related lawful concerns.
- Coordinating efforts through other external teams that deal with computer incident response.
- Minimizing the company's reputation risk by sending a notification to the responsible company personnel about the cyber incident.
- Incidents which may also turn out to be high profile events and the implementation of timely, as well as, appropriate corrective actions (Whitman, Mattord & Green, 2014).

For purposes of achieving the aforementioned goals, the IT department has adopted diverse security ever best practices obtained from standardized occurrence reply procedures like the ones published by NIST (National Institute of Standards & Technology) also Special Publication 800-61 together with additional authorities. The various incident reply process fundamentals which include the company's IRP are such as:

- Preparation: maintaining, as well as, making better incident response capabilities, as well as, prevention of incidents by making certain that networks, systems together with applications are adequately secure.
- Identification: categorizing, characterizing, confirming prioritizing, classifying, in addition to scoping suspected incidents.
- Containment: Minimization of ⁵ loss and theft of the information or else disruption of services.
- Eradication: elimination of the threat.
- Recovery: quick and secure restoration of computing services.
- Post-incident activities: assessment of response to handle future incidents better by utilizing reports ‘the Lessons Learned’, as well as, after-action activities otherwise mitigating weakness to avoid similar incidents occurring within the future (Gibson, 2011).

Incident Response Team (IRT)

In order to prepare appropriately for, as well as address incidents within the organization, it is necessary to form a centralized IRT. The IRT will have the responsibility of reviewing security breaches, in addition to taking the required responsive measures. Within its core, the IRT has to consist of:

- Chief Information Security Officer (CISO): The CISO acts as ³ the incident response manager and oversees, as well as, prioritizes actions in the course of the detection, review and containing of an incident. It is also the responsibility of the CISO to convey the unique requirements about the incidents of elevated severity to the entire organization.

- **Security Analysts:** the CISO operates with support from a security analysts' team, which directly works through the network that has been affected to find out the location, details, and time of the incident. These include the triage analysts as well as forensic analysts. The triage analysts are responsible of filtering out false positive and watching for the potential intrusions. On the other hand, the forensic analysts unearth major artifacts and maintain evidence integrity for purposes of ensuring that the investigation is forensically sound.
- **Threat Researchers:** they complement the security analysts by offering threat intelligence, as well as the context for the incident. In that regard, they constantly comb the internet and identify intelligence, which might have been publicized outwardly. Upon combining such information through the organization's earlier incidents records, they establish and maintain a vibrant internal intelligence database.

Getting Cross-Functional Support

The IRT should not be made to exclusively take up the responsibility for dealing with security threats. Each business representative along with employee has to fully comprehend as well as support the incident response plan so as to make certain that emergency procedures are smoothly implemented. Each department of the organization has distinct responsibilities once an incident occurs:

- **Management:** The buy-in of the management turns out as necessary for the making of resources, staff, funding available, as well as time commitment for the planning also execution of incident response.
- **Human Resources:** the HR has to be contacted once it is discovered that an employee was involved in the emergence of an incident.

- **Audit and Risk Management Specialists:** they assist in developing threat metrics, as well as conducting vulnerability assessments while paying attention to best practices within the organization.
- **General Counsel:** the lawyer makes certain that all evidence obtained maintains its forensic worth in case the organization opts to take legal action. Lawyers can also offer advice concerning liability issues once an incident affects clients, business partners, or the public in general.
- **Public Relations:** they communicate with the team leaders, making certain that an accurate turn of events is transmitted to the diverse stakeholders, as well as the press.

Communications Plan

Communications procedures take place throughout the various phases of the incident response and entail the initial reporting about the incident to the respective authorities, together with the continuous communications with the ones affected. A communications plan turns out as vital while dealing with a cyber incident that has already been confirmed (Mallery, 2015). Good communication plans assist in limiting confusion and increasing responsiveness through the sharing of action plans, getting the organization's stakeholders updated, and ensuring that transparency is maintained throughout the process. A communication plan has to identify the stakeholders, the ones that have the authority of speaking concerning the incident, the channels of communication, and the communication schedule along with the procedures of sending notifications to external organizations that are all involved within the incident directly. Communication plans have the potential of minimizing conflicting messages, as well as focusing efforts. The communication plans should encompass the following elements:

- Identification of the parties that have the authority to speak about incidents to the organization's stakeholders, as well as, the media.
- Clearly set message approval protocols in order to ensure accuracy.
- Identification of the various communications channels to be used for both internal, as well as, external stakeholders, which may include, phone conferences, email, social media. Listservs, blogs, learning management systems, and wikis, among others.
- Planned communications frequency between the internal stakeholders.
- Planned communications frequency with the external stakeholders.
- Procedures for notifying the external organizations also involved within the incident directly.

DISASTER RECOVERY PLAN (DRP)

The IRT will work in partnership with the affected department in order to validate and analyze quickly every incident and carry out an initial assessment with the objective of determining the scope of the incident, for instance, which applications, networks or systems have been affected; what or who brought about the incident; as well as the manner in which the incident is taking place (for example, the attack methods or tools that are being use, and the vulnerabilities that are being exploited). The premier analysis has to offer adequate information for the team to be in the position of prioritizing activities like incident containment and a deeper review of the impacts of the incident (Gregory, 2008).

A well-coordinated investigation may be needed upon the confirmation of the incident. The IRT will be expected to identify and assign an individual the role of IRM (Incident Response Manager), who, in most cases, is the CISO. The IRM is set to lead the incident response, operates as the contact point for every issue related to the incident, and has the responsibility of coordinating the data for documentation of investigation, as well as gathering evidence. Within certain cases, local, Federal, or State law enforcement can be involved within the incident investigation.

Containment, Eradication, and Recovery

The objective of the containment procedures is to limit actively the scope, as well as, the magnitude of the emerging attack. Vulnerabilities within a specific computer network can end up being quickly exploited. Containment entails acquiring, preservation, securing, and documentation of evidence. The IRM highly prioritizes on establishing the identity of the attackers and the nature of the vector that they are utilizing to attack the company hosts (Mallery, 2015). Upon obtaining the aforementioned information, the IRM should ask for a physical

disconnection or router block to temporarily prevent the port or IP address from getting connected to the company network. Such a move can cause disruption to other regular traffic, although this disruption is to be maintained at a minimum. The following actions have to be undertaken in the course of the containment phase:

- In respect to the direction of the IRM, the system can be repaired as needed by the local system administrators.
- The CISO should remain available in order to offer consulting support in the cause of the repair process.
- Deployment of the IRT to the site.
- Documentation of the incident details.
- Avoid alteration of the system in any way by observing a low profile so as to prevent tipping off the attacker/
- Utilizing a trusted system binary kit such as Windows, Unix, or Linux for purposes of verifying the system binaries that have not been compromised.

After the containment, it is necessary to carry out eradication. Eradication refers to the procedure of removing malicious accounts, codes, or unauthorized access. It also encompasses the repairing of the vulnerabilities, which might have contributed to the compromise. It is recommended to completely re-install the applications and operating system. After containing and eradicating the incident, recovery can commence (Singh & Joshi, 2018). The recovery enables the affected business processes to recover, as well as, resume operations. The recovery process involves the restoring of data to the system, returning the affected systems to their typical operational state, conforming that the impacted systems function as needed, and in the event it is necessary, put in place monitoring measures to help in looking out for related Post-

Incident Activity in future. Lastly, documentation of cyber incidents, together with the steps taken in their mitigation, is vital. The documentation provides an opportunity for making better the incident response processes, in addition to helping in the identification of recurring issues.

References

- Gibson, D. (2011). *Managing risk in information systems*. Sudbury, Mass: Jones & Bartlett Learning.
- Gregory, P. H. (2008). *IT disaster recovery planning for dummies*. Hoboken, NJ: Wiley Pub.
- Mallery, M. (2015). *Technology disaster response and recovery planning: A LITA guide*. Chicago: ALA TechSource, An imprint of the American Library Association.
- Singh, U. K., & Joshi, C. (2018). Comparative Study of Information Security Risk Assessment Frameworks. *International Journal of Computer Application (IJCA)*, ISSN, 2250-1797.
- Whitman, M. E., Mattord, H. J., & Green, A. (2014). *Principles of incident response and disaster recovery*. Australia: Course Technology Cengage Learning

report

ORIGINALITY REPORT

14%

SIMILARITY INDEX

7%

INTERNET SOURCES

1%

PUBLICATIONS

13%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Colorado Technical University
Online

Student Paper

3%

2

www.coursehero.com

Internet Source

3%

3

Submitted to National American University

Student Paper

2%

4

www.otoriyose-select.com

Internet Source

2%

5

Submitted to Southern New Hampshire
University - Continuing Education

Student Paper

1%

6

Submitted to Laureate Higher Education Group

Student Paper

1%

7

Submitted to University of Hertfordshire

Student Paper

1%

8

pages.nist.gov

Internet Source

<1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography On