Unit 6 Disaster Response

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**January 17, 2023**

**Part 1**

The following is a step-by-step process divided into categories for an associated it department as part of an action plan for incident response. It is important that personnel uphold the criteria of this action plan during a possible event in order to mitigate further damage done by malicious actors. Bolstering organization by following this plan can be paramount to the success of the organization.

Preliminary characteristics:

Before a potential vulnerability is exploited by a malicious actor it is important for a business to gather a few identifying and clarifying points of information. First and foremost, the business must establish a proper maximum tolerable downtime (University of Rochester, 2018). This maximum tolerance will downtime determines the maximum amount of time that a system is able to cease function without causing substantial damage to a business. The maximum tolerable downtime for this organization must be recorded before an incident occurs.

A second point to establish well determining business continuity plans would be that of the recovery point objective. Recovery point objectives serve as a maximum time the business is targeting while solving a potential crisis (University of Rochester, 2018). It is additionally important that this recovery point objective does not exceed the maximum tolerable downtime.

The third and final promote preliminary objective would be establishing a recovery time objective. Your recovery time objective is a basic unit in which a business is planning the recovery of a system (University of Rochester, 2018). This gives the organization a decent benchmark to gather additional statistics and evaluate loss potentials.

Steps for Action as outlined by the Systems Security Certified Practitioner Official Study Guide (Second Edition) (Wills, 2019):

1. Determine if an Incident has occurred
   1. Analyze the precursors and indicators.
   2. Look for correlating information.
   3. Perform research perspective to the anticipated event.
   4. When the handler believes an incident has occurred, began thorough documentation and evidence gathering.
2. Far tries handling the incident based on relevant factors such as functional and information impact, and recoverability.
3. Report the incident to internal executives, and external stakeholders.
   1. Ensure documentation and presentation includes relevant information on Recovery Point Objectives, the Recovery Time Objective, and Maximum Tolerable Downtime.
4. Acquire and secure documentation and evidence.
5. Contain the incident.
6. Eradicate the incident.
   1. Identify and mitigate all vulnerabilities that were exploited.
   2. Remove malware that may be installed materials that may be contaminated, and unnecessary components.
   3. Perform containment procedures on all affected hosts. Repeat section 1, 5, and 6 for all affected hosts.
7. Recover from the incident.
   1. Return affected hosts to become operational ready.
   2. Confirm that affected hosts are operating nominally.
   3. Implement additional monitoring technology to look for future related activity.
8. Create a report upon a follow up distant from the event.
9. Hosted meeting for relevant personnel to document lessons learned, and discuss behavioral changes.

Concluding Procedures:

Once the investigation and action portion of the incident response has been successfully completed organizational tools must be employed in order to develop a clearer understanding of what happened and why. During this procedure old document is to be organized within secure our confines that establish a trajectory on how to mitigate such an attack in the future. Security teams working with incident response are to brief an organizational executive in order to ensure that all information recorded is accurate to the best extent possible.

**Part 2**

**Investigate and identify a ranking of disaster types.**

There are many ways to categorize disaster risks within a business. Although a combination of ranking types may be suitable for a business to maintain effective operation, there are a few ways to ensure a business is properly preparing for risks at the beginning steps of operation. One central way would be to use a risk index. In this risk matrix, risks are scored on two categories. The first category is the impact ranging from low to high (University of Michigan, n.d.). This determines each risk factors impact on a business, be it monetary, temporal, or otherwise impactful. The second category risks are scored on would be the likelihood. This ranges from unlikely to highly likely, and sees how often a risk might manifest itself throughout the course of the business’s activities. Using this matrix may give business strategists a good idea on how risks might not only manifest themselves, but also present themselves to the business in question. This will also help associated business strategists to develop actionable plans regarding these risk factors. In doing so, a business is further secured from potential risk factors while also taking steps to mitigate unnecessary behaviors for risks that may potentially become impossible as time develops. This will further strategize resources the businesses have to deploy against such risk factors.

A risk index matrix may work well when combined with additional resources. Sample, the National risk index for natural hazards provides a free ranking for natural disasters well explored by area (The Federal Emergency Management Agency, 2024). It ensures that natural disasters that may be more common to an area of operations within a business’s structure are ranked accordingly to natural disasters that may be uncommon or impossible given that area. This is a useful tool to understand and utilize when planning business disaster scenarios.

**What are some alternate site considerations?**

Alternate sites are a key way that businesses maintain operation during a disaster. They come in a number of different categories. The first category would be a cold site. This is an alternate location for a business to operate with adequate space and infrastructure for a business to maintain reasonable operation (Commonwealth of Pennsylvania Governor's Office of Administration/Office for Information Technology, 2010). Upon a lease these sites don’t usually come with equipment necessary for a business to function, and it is usually required for the business itself to provide that equipment in the case of a disaster. The second location consideration would be a warm site. These sites usually contain necessary hardware and software resources in order to maintain business operation (Commonwealth of Pennsylvania Governor's Office of Administration/Office for Information Technology, 2010). These sites are usually maintained within operational statuses in order to more adequately accommodate a business given a disaster. Hot sites take this even further to introduce a space appropriately sized for a business that contains hardware, infrastructure, and support staff that work around the clock in order to ensure that a business remains operational despite a disaster (Commonwealth of Pennsylvania Governor's Office of Administration/Office for Information Technology, 2010). This is a relatively costly setup, but can maintain crucial operations regardless of an event that has occurred. A final consideration for an alternate site would be that of a mobile site. Mobile sites are transportable shells that offer specific accommodations that a business may need in order to continue operation (Commonwealth of Pennsylvania Governor's Office of Administration/Office for Information Technology, 2010). These are usually relatively bare bones setups that are not particularly suitable for long term usage.

**Analyze backup solutions and why they are important.**

There are many different ways backup systems may come to a business. One way is external cloud storage. External cloud storage may prove useful in order for an accident-prone site to ensure that their data is backed up in the case of a disaster (University of California Berkeley, 2024). Primarily, this allows an external vendor to further handle the specific operations of the businesses data to ensure that security and maintenance are kept properly despite the primary site having a disaster occur. This however can be relatively costly as well as pose some restrictions on data limits. Should a company be dealing in a vast amount of data, cloud storage may become too cumbersome to have full realization of the potential benefits. An alternative to this would be physical backups. Using physical materials such as hard drives with data cloned onto them can keep a vast amount of data stored in an external site for rent no matter how large the data may be, as long as the hard drives may account for it. Keeping this data in cold storage can be a relatively antiquated way of storage solutions, and not provide particularly fast results. Typically, this option is reserved as a last-case scenario to ensure that data is preserved on a physical location should digital options fail.

# **References**

Commonwealth of Pennsylvania Governor's Office of Administration/Office for Information Technology. (2010, December 20). *Guidelines for Establishing an Alternate Processing Site*. Retrieved from Systems Management Buisness Continuity: https://www.oa.pa.gov/Policies/Documents/opd\_sym004a.pdf

The Federal Emergency Management Agency. (2024, Feburary 17). *National Risk Index for Natural Hazards*. Retrieved from FEMA.gov: https://www.fema.gov/flood-maps/products-tools/national-risk-index

University of California Berkeley. (2024). *Backing Up Your Data*. Retrieved from Berkeley Information Security Office: https://security.berkeley.edu/education-awareness/backing-your-data

University of Michigan. (n.d.). *Table: Risk Assessment Matrix*. Retrieved from University of Michigan Campus Involvement: https://campusinvolvement.umich.edu/content/table-risk-assessment-matrix

University of Rochester. (2018, May 21). *Business Continuity Management Program Development Overview*. Retrieved from Buisness Continuity Management Office: https://tech.rochester.edu/wp-content/uploads/Business-Continuity-Management-Development-Information.pdf

Wills, M. (2019). *SSCP Systems Security Certified Practitioner Official Study Guide*. Retrieved from (ISC)2: https://viewer-ebscohost-com.libauth.purdueglobal.edu/EbscoViewerService/ebook?an=2110465&callbackUrl=https%3a%2f%2fresearch.ebsco.com&db=nlebk&format=EB&profId=eds&lpid=lp\_xi&ppid=&lang=en&location=https%3a%2f%2fresearch-ebsco-com.libauth.purdueglobal.ed