ASSIGNMENT 3
ISEC3800

Pod 7 – Courtney Hagen, Jessey Harlow, Zach Slaunwhite

Table of Contents

Assignment 3

Introduction

The purpose of this document is to demonstrate the creation and testing of our Business Continuity and Disaster Recovery plans.

Task 1 – Business Continuity Plan

Business Continuity Plan Information

Company Name	**Nova Scotia Community College**
Business Continuity Manager	Courtney Hagen
Contact Information	W0263284@nscc.ca
Alternate Manager	Zach Slaunwhite
Contact Information	W0414242@nscc.ca
Business Continuity Plan Location	G7 – Winter 2020\Documents\ISEC3800 – Advanced Security Analysis and Implementation\Assignment 3

Revision List

Revision Number	Details	Revised By	Revision Date
R001	Initial revision	Courtney Hagen	March 29th, 2020

Vital Information

Business License Number	**0920-9780-4524-7542**
GST Number	5393-5219-7428-1790
Insurance Policy Number	11421407
Critical Paper Records Location	A001
Back-Up Computer Records Location	G7 – Winter 2020\Documents\ISEC3800 – Advanced Security Analysis and Implementation\Assignment 3

Associated Policies, Documents, and Procedures

All policies and procedures are located at the following link:
https://www.nscc.ca/about_nscc/policies_procedures/index.asp

Staff Contact Numbers

Name	Title	Phone	Alternate Phone
Courtney Hagen	Student	9025555555	9025555556
Zach Slaunwhite	Student	9025555557	9025555558
Jessey Harlow	Student	9025555559	9025555560

Emergency Contact List

Name	Title	Phone	Alternative Phone
Nova Scotia Power	Customer Service Line	1-800-428-6230	
Armour Electric Ltd.	Electrician	902-225-7274	
Marie Dootkas Insurance	Insurance	123-123-1234	
Emergency	Emergency Call	911	
Police	Local RCMP	321-321-4321	
Water Cleanup Inc	Industrial water removal	132-333-1234	
Waste B-Gone	Industrial material removal and cleanup	775-238-4456	
Fire Department	Fire department	345-676-3375	
Internet Security Inc.	Internet security contractors	000-000-0000	

Supplier Contact List

Company	Phone
Graybar Canada	9024438311

Critical Software

Name	Function	Location
Firewall Extraordinaire	Filter user traffic	Each computer on the network
Citrix Receiver	Software distribution	Each computer on the network

Critical systems

Name	Function	Location

Switching Backbone	Networking	Comms Closets throughout the school
Primary Domain Controller	Domain Functionality	Toll
Secondary Domain Controllers	Domain Functionality	Each campus, in main floor server room
Backup Servers	Data storage	Toll
Brightspace Servers	Student services	IT campus main floor server room
WSUS Server	Windows updates	Ivany campus main server room
Printing Servers	Printer connectivity	Each campus, in main server room
Nscc.ca Hosting Servers		Ivany campus, server room
SDC Functionality	Student data center sandbox environment	Main floor, attached to d316

Backups

Full backups are done at the end of each day, and differential backups are done every 35 minutes throughout the day. Important containers are kept for 6 years, where less important data is only kept for 6 months, and employee data, if important, is expected to be self-backed up. All backups are sent to toll at 2am.

Action Plan

1) If there is a power outage, revert all IT infrastructure to backup power/generator.
2) If there is a power outage or any critical system is nonfunctional, revert to off-site backups.
3) Verify if remote access is functional in the event the location cannot be accessed. Check email for when it is once again safe to return. Do not return unless it is safe to do so.
4) Prioritize regaining functionality based on company impact.

Task 2 – Disaster Recovery Plan

Revision List

Revision Number	Details	Revised By	Revision Date
R001	Initial revision	Courtney Hagen	April 2nd, 2020

Risk Management Table

Potential Disaster	Probability Rating	Impact Rating	Brief Description of Potential Consequences & Remedial Actions
Hurricane	3	3	Power outages for possible days or weeks. Permanent damage to infrastructure and surrounding area., Service delays, business delays
Earthquake	4	3	Infrastructure damage to building and surrounding area, Service delays, business delays
Flood	3	2	Building Infrastructure damage, equipment damage, Service delays, business delays
Structure Collapse	3	1	Critical structural damage, Service delays, business delays
Fire	2	2	Structural damage, Service delays, business delays
Power loss	1	5	Service delays, business delays
Data Breach	2	3	Information leaks, potential lawsuit.
Network Attack	2	3	Service and business delays.
Robbery/Theft	1	5	Replacement of items.

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

Testing Plan

The table below is a template to follow when testing this plan. Copy the template and get a signature for each test passed for records.

Test	Acceptable Outcome	Signature
Test Environment Run through	Test environment operates with full functionality it is trying to replicate.	
Full Simulation Test (Test shut off with actual equipment and actual site	Less than one-hour downtime of any one system occurs.	

backups to verify functionality. Do this on down time in case of any impact.)		
Specific Systems Test (Shut down specific systems to simulate their failure)	Less than one-hour downtime on tested system.	
Powerless Test (test power backup)	Systems able to continue with less than 30 mins down time.	

Action Plan

Risk	Hurricane
Risk Level	Medium
Recovery Time Objective	24 Hours
Business Functions Affected	School database, access to authentication for locally hosted applications like Brightspace, accepting payment.
Potential Impact	Power outages for possible days or weeks. Permanent damage to infrastructure.
Action	- Assess for infrastructure damage. If any is present, make an insurance claim. Order any required replacement equipment. - If there is a resulting power outage, call NS Power to determine how long it will last.
Resource Requirements	Cellular device and/or landline, generator.

Risk	Earthquake
Risk Level	Low
Recovery Time Objective	Less than 24 hours
Business Functions Affected	School database, access to authentication for locally hosted applications like Brightspace, accepting payment.
Potential Impact	Power outages for possible days or weeks. Permanent damage to infrastructure.
Action	- Identify what critical equipment can be repaired within 6 hours. If it cannot be repaired, order a replacement. Any non-critical equipment prioritize repair and only replace if necessary. - Assess for infrastructure damage. If any is present, make an insurance claim. - If there is a resulting power outage, call NS Power to determine how long it will last.
Resource Requirements	Cellular device and/or landline, generator.

Risk	Flood
Risk Level	Low

Recovery Time Objective	48 Hours
Business Functions Affected	School database, access to authentication for locally hosted applications like Brightspace, accepting payment.
Potential Impact	Permanent loss of systems due to water damage.
Action	- Move all unaffected equipment to unaffected site. - Determine level of damage to affected equipment. Call for replacements and make insurance claims on irreparable infrastructure. - If there is resulting electrical issues, contact the electrician listed on the emergency contact list.
Resource Requirements	Cellular device and/or landline, generator

Risk	Structure Collapse
Risk Level	Low
Recovery Time Objective	7 Days
Business Functions Affected	School database, access to authentication for locally hosted applications like Brightspace, accepting payment.
Potential Impact	Permanent loss of systems, temporary loss of systems, loss of on-site backups.
Action	- Check email updates to find out when or if you can return to the campus - Upon return, establish what needs to be replaced and make an insurance claim.
Resource Requirements	Internet access, mobile/landline, generator

Risk	Fire
Risk Level	Low
Recovery Time Objective	48 Hours
Business Functions Affected	School database, access to authentication for locally hosted applications like Brightspace, accepting payment.
Potential Impact	Access to the section of the building being limited, loss of all campus functionality for the first 48 hours, expensive cleanup and building costs.
Action	- Evacuation - Call fire department to put out fire

	- Meet to discuss what needs to be done to make the school usable for students and staff
	- Repair damaged area
Resource Requirements	Faculty, fire department, clean up contractors, inspectors, builders.
Staff Requirements	Faculty for discussions on how to handle the situation.

Risk	Power loss
Risk Level	High
Recovery Time Objective	Immediately
Business Functions Affected	No functions affected, because of generator.
Potential Impact	No impact
Action	No actions need to be taken; preventative actions have already been taken with installing a generator.
Resource Requirements	Generator
Staff Requirements	None

Risk	Structure Collapse
Risk Level	Low
Recovery Time Objective	14 Days
Business Functions Affected	Anything
Potential Impact	Loss of access to the building during reconstruction, and assessment of damage and stability.
Action	- Evacuate
	- Search and rescue for any missing people
	- Structural assessment
	- Building clean up
	- Structural Rebuilding
	- Safety inspections
	- Resuming of regular business and activities
Resource Requirements	Faculty for emergency plans, search and rescue personnel, people to assess damage, clean up crew, construction engineers and workers, safety inspectors.
Staff Requirements	Faculty to discuss contingency plans, and help with initial emergency plans.

Risk	Data Breach
Risk Level	Low
Recovery Time Objective	1 Hour
Business Functions Affected	No impact on normal business
Potential Impact	IT will be a little more tied up, figuring out how this happened, and m making sure it doesn't happen again, if students or faculty data has been stolen, they need to be notified.
Action	- Figure out where the data breach was
	- Understand how it happened, construct a plan to make sure it doesn't happen again
	- Notify anyone who may be affected by the data breach and provide information
Resource Requirements	IT department, potentially the police depending on what information has been stolen.
Staff Requirements	IT Department

Risk	Network Attack
Risk Level	Low
Recovery Time Objective	24 Hours
Business Functions Affected	Anyone who requires the network to get work done.
Potential Impact	Normal business may be impacted on the operational side, students can continue work at home.
Action	- Network engineers figure out what happened
	- Work on a solution for getting the network back up
	- Develop a plan to stop this from happening in the future
Resource Requirements	Networking personnel, authorities.
Staff Requirements	IT Department, network engineers.

Risk	Robbery/Theft
Risk Level	High
Recovery Time Objective	1 Hour
Business Functions Affected	None
Potential Impact	Not much, the equipment will be replaced, and the police called.
Action	- Figure out who stole what, either through speaking to witnesses, or checking the cameras.
	- Call the authorities and inform them
	- Call insurance companies responsible for covering theft
	- Replace equipment

Resource Requirements	Security guards, IT department for replacing equipment, authorities
Staff Requirements	Security, IT

Review Plan

This Business Continuity plan will be reviewed semi-annually. Each scenario will be run through in a meeting with the management team to assess for issues. Reference will be made to any previous experience dealing with these risks. Amendments will be made, and revision numbers added to the Revision List.

Task 3 – Practice your BC/DR Plans

Phase 1 – Target: 16 Hours

1. Ensure the safety of students and faculty, evacuating to a safe location
2. Initiate call tree
3. Shutdown power to affected areas (excluding emergency lights)
4. Transport equipment out of affected site to the unaffected site
5. Evaluate damages to equipment
6. Switch over to backup site

Phase 2 – Target: 24 Hours

Identify systems and services that were damaged and prioritize the systems to restore first.

Systems and services damaged - ordered by priority to restore	Reason/Justification
Primary Domain Controller	Backbone for all systems, must be restored prior to other systems
SAN Servers	Important to identify if any files were lost - all data is backed up daily and can take a fair amount of time to restore
Email Server	Email communication during a disaster is essential
Firewall Server	Since the email server is up, protecting from threats becomes crucial
Peoplesoft	For the payroll software to function, it relies on the employee management software
Payroll Software	Paying employee is necessary for the business, however, is typically weeks behind the actual pay dates and is not a high priority compared to other systems
Print Server	During a disaster, printing should be the least of the concerns and there are alternative ways to print without a printing server

Phase 3 – Target: 8 hours

1. Order replacement systems
2. File insurance claims

References

6 Risks You Need to Plan for in Your BCP. (2018, June 21). Retrieved April 2, 2020, from https://www.newpig.com/expertadvice/6-risks-you-need-to-plan-for-in-your-bcp/

Outage Centre. (n.d.). Retrieved April 2, 2020, from https://www.nspower.ca/outages

Welcome to Armour. (n.d.). Retrieved April 2, 2020, from https://armourelectric.ca/?gclid=Cj0KCQjwmpb0BRCBARIsAG7y4zZufI3Vs5qkZXFVXHCBCjmofvwKQ7fW5pklVD92cq_6QJySPlCk3BQaAk4uEALw_wcB

IT Disaster Recovery Planning: A Template. (n.d.). Retrieved April 4, 2020, from https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf

Disaster Recovery Plan Testing in IT. (n.d.). Retrieved April 4, 2020, from https://www.ittoolkit.com/articles/disaster-recovery-testing

Sharrieff, M. (2017, November 21). How to Conduct Testing of a Business Continuity Plan. Retrieved April 4, 2020, from https://smallbusiness.chron.com/conduct-testing-business-continuity-plan-4526.html

IT Disaster Recovery: Imperva. (n.d.). Retrieved April 4, 2020, from https://www.imperva.com/learn/availability/disaster-recovery/