Business Continuity Management & Cloud Security

CA – BIA - BCP

By Dean xxxxxxxx

B0009xxxxxxxxxx

Department of Informatics
School of Informatics and Engineering
Technological University xxxxxxxxx
xxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxx
Application Security
Mark xxxxxx

10/11/2019

Plagiarism Declaration

TECHNOLOGICAL UNIVERISTY OF xxxxxxxxxxxxxxx
DEPARTMENT OF INFORMATICS
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
LECTURER: MARK xxxxxxxxx

DECLARATION ON PLAGIARISM

I declare that the work I/We am (are) submitting for assessment by the Institute examiner(s) is entirely my (our) own work, except where the author or source has been duly referenced and attributed.

I confirm that this material has not been previously submitted for a degree or any other qualification at xxxxxxxor any other institution. I further confirm that I have read and understood the Institute policy on plagiarism in assignments and examinations (3AS08.doc) and that I am not, so far as I am aware, in breach of any of these regulations.

Signed: Dean xxxxxxxxxxx

Date: 10/11/2019

Table of Contents

Company Profile

Company Name: ReliaQuest

Field: CyberSecurity

Staff Numbers: 200-500

Office Locations:

Tampa, Florida, USA

Las Vegas, Nevada, USA

Salt Lake City, Utah, USA

Dublin, Ireland

London, UK

Office Location Information:

Tampa: Corporate Headquarters and Security Operations Center

Las Vegas: Security Operations Center

Salt Lake City: CyberSecurity Technology Center

Dublin: Security Operations Center

London: Business Office

Specific Process for Incidents

This plan will contain the information needed in the majority of incidents, which would include information needed in response to incidents such as fire's, water leakage and cyber-attacks. Each incident requires its own individual response and level of response

General Procedures for Incidents

In General procedures change depended on severity level of the incident, it is always recommended to gage the level of severity, after each step is taking as situations can develop into deeper stations than originally anticipated

Maintenance of Systems

Maintenance of response systems are important to deal with possible failures, the maintenance process includes but is not limited to, checking that fire extinguishers are maintained, checking that

insurance coverage is up to date, to confirming that all contracts are signed and updated with the necessary information regarding data storage and offsite backup countries

Business Continuation Plan

Purpose

The purpose of the plan is to build a set out plan that can be used by the response team in the event of an emergency or incident that may interpret daily operations of the company

Scope

Office location that is at risk and specified in this Business Continuation Plan

Reliaquest Dublin, Ireland Security Operations center

Recovery Objectives

Recovery Time Objective

Length of time services can be off line before having impact on the company

Since once the main operations of Dublin office is as a Security Operations Center “SOC” means that this is critical service to provide to clients. If the Security Operations Center is to go offline it could potentially mean that the Client systems are vulnerable. The Length of time depends is dependent on how wide-spread the issues halting the operations are and what effects they have on the system

Recovery Point Objective

The Maximum amount of time the business can tolerate being offline before major impact

Since once the main operations of Dublin office is as a Security Operations Center “SOC” means that this is critical service to provide to clients. If the Operations Center goes offline for a long period client may be forced to use another service provider. Meaning a finical lose for Reliaquest and a possible loss of clients to competitors who provide similar services, for this reason the maximum amount of time that the company can last while is less than 2 days, after a 2 day period a client could be forced to go to a revival to maintain security of their business

Recovery Team

Service / Role / Contact

These are the members of the response team, their roles and contacts

Name	Role	Location	Contact
Jane Doe	Data Recovery	Blanchardstown	087 326 4345
John Doe	Network Maintenance	Dundalk	087 326 4345
Jane Smith	Security Maintenance	Navan	087 326 4345
John Smith	Power Management	Dublin City Center	087 326 4345
John Doe Smith	Building Security	Rush	087 326 4345
Jane Smith Doe	Finance	Drogheda	087 326 4345
Jane Doe Smith	Maintain Contact	Blackrock	087 326 4345
John Smith Doe	Situation Monitoring	Kildare	087 326 4345

Responsibilities

This list includes the members of the response team and their individual responsibilities

Name	Responsibilities
Jane Doe	Recovery of lost data
John Doe	Maintenance of network Infrastructure
Jane Smith	Maintenance of network security systems
John Smith	Maintaining power for the Security Operations Center
John Doe Smith	Maintaining Security for the building
Jane Smith Doe	Maintaining Finance for receiving and sending payments
Jane Doe Smith	Maintaining Contact with client with updates
John Smith Doe	Monitoring of current situation and changes

Dependencies

This list includes the member's and requirements for the members of this team to be successful

Name	Role	Location	Requirements
Jane Doe	Data Loss	Dublin	Data recovery software and equipment
John Doe	Infrastructure	Dublin	Backup Hardware and cabling
Jane Smith	Security	Dublin	Security Systems and staff
John Smith	Power	Dublin	Generators and Fuel
Jane Smith Doe	Client Side	Dublin	Communications software and hardware

Expected Response Time

This list contains the average response time for the response team after initial contact, if they are no currently present at the office location

Name	Time To Respond
Jane Doe	45 Minutes
John Doe	2 hours
Jane Smith	1 hour
John Smith	15 Minutes

John Doe Smith	30 Minutes
Jane Smith Doe	1 Hour 45 Minutes
Jane Doe Smith	25 Minutes
John Smith Doe	1 Hour 30 Minutes

Recovery Strategy

Initial Recovery

Upon Initial incident, the response procedure is to contact all those who are on the response team and to get the response team the materials needed to begin the response to the incident

Overall recovery Strategy

The main strategy in the recovery process is to get the business critical systems online as quick as possible, these being client essential systems and operations such as remote logging and security operations monitoring. Then for this will be to get the client contacts back online, this way to maintain receiving payments and sending invoices to clients. After this the next will be bringing normal systems online for the rest of the staff to re-start day to day operations

Recovery Scenarios

In the best situation a full recovery would be perfect, but due to the nature of common situations things can take a delayed for a long time, so for purpose of the recovery process it is important to bring back the needed steps piece by piece so the most focus can be given to each part in each step. The recovery process should start at the most client needed critical systems, which would include communications and power followed a secure connection to the client systems

Return to operations

A full return to standard operations can be achieved when the office is ready and all client systems can be configured and monitored from the either Original or new Security Operations Center. The client services should be the number one priority when returning to normal operations, after client services are available and can be provided for, then all other operations can start to return as needed, starting from most critical to least critical

Plan Activation

These are the incidents in which this plan will be put into effect and beginning procedures to getting the company from the emergency situations back to a full operational state

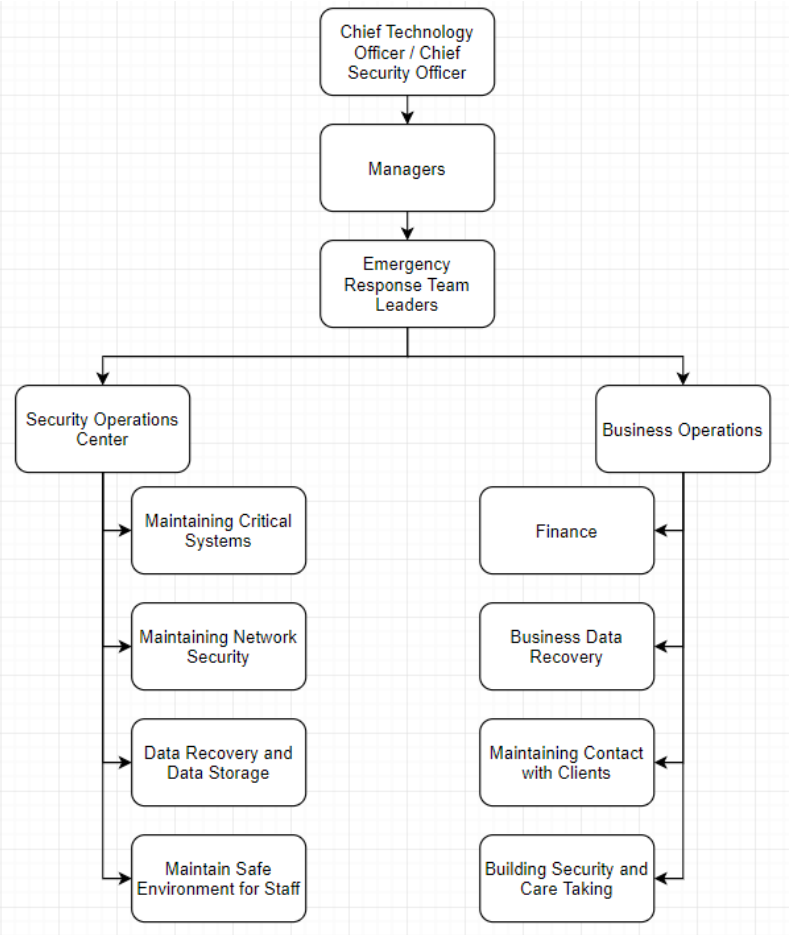
Emergency Alert

An emergency Alert would be an external source such as Law Enforcement, Government announcement that the SOC needs to shut down due to staff safety, when this type of alert is announced a full continuation plan is put into effect to insure that the company can function on trough the emergency, which may or may not be limited to Viral Infection, Terror Attack or weather event that can causes damage and injuries to the SOC and staff.

Damage to Property

In the event of property damage that renders the building unstable then it would be required for the Continuation plan to come into effect as the location will no longer be safe and viable for common operations, at this point it is advised to intact the plan and start the continuation process for getting all systems back online

Recovery Structure



Shutdown Procedures

These are the procedures needed to follow when shutting down the Security Operations Center for movement offsite

1. Contact Clients to let them know of temporary shutdown of services
2. Contact incident response team to be on alert for issues during shutdown
3. Get Off Site location online and ready for Instant transfer
4. Confirm with offsite locations that everything is ready
5. Transfer control to offsite location
6. Prepare backup and transfer of local data
7. Transfer local data to secure backup offsite
8. Shutdown all systems starting from user to backbone finally
9. Move all hard drives to secure storage and systems to agreed storage

Offsite Data Storage:

This is the details regarding the company chosen to host our data off site if there is an emergency that means the main office location has become compromised and unusable in some form

Name of Company:	Iron Mountain
Main Contact:	David Hynes
Phone Number:	1800 732 673
Email Address:	CustomerResolutions@ironmountain.co.uk
Street Address:	Iron Mountain, Damastown Rise, Damastone
City:	Dublin 15
Website:	https://www.ironmountain.ie/

Iron Mountain can provide full storage of a secondary backup and systems offsite in their offices in Dublin. The location was chosen for the following reasons after an inspection from both our security team and incident response team

Distance from Office:	28 Minutes via M50
Backup Allowance:	Weekly and Monthly backups of data are allowed by the company under current contract
Site Security:	The location contains multiple forms of modern security systems, as well as physical security protecting that data stored at each location
Pricing:	Iron Mountain came in under budget with a price meeting all our expectations
Site Safety	The Site contains multiple features such as Fire Suppression systems, water detectors, heating and ventilation

Data to be stored at this Location:

Below is the data to be stored at this location

To Be Stored	**Includes**
Client Data “Sales”	Contact Details, Current and Passed Contracts
Client Data	Software, Recorded Storage Tapes,
Business Document’s	Essential Documents, Receipts, contracts
Legal Documents	Copies of Legal documentation and Leases
Insurance Documents	Documents Regarding Insurances
Assets Listings	Complete Company Asset Listing
Architectural Documents	Floor plans, Architectural documents
Vendor Documents	Contracts, Receipts, sales invoices

The location is accessible 24 hours a day to have information either transferred digitally or manual stored information, at current the company’s contract is set to have 10 weeks of full support at the location in the event of an emergency.

Communications

This section looks at the planning presets for the event of a failure of communications; both of the chosen services have agreed to an allowance of up to 10,000 terabytes of data within our chosen budget range, the service has no time frame only the allowance of 10,000 terabytes, more can be requested as needed.

Low Level

This would include temporary issues in the local region

Service	Company	Contact	Contact Number
Cellular Internet Service	3 Ireland	Josephine Rogan	+353 01 33 256

High Level

This would include longer term issues such as area long term cable damage

Service	Company	Contact	Contact Number
Satellite Internet	BigBlu	Stephen James	+353 01 85 131

Temporary Offices

If needed in the time of the building becoming unusable there are offsite offices available for critical services. All other employees non-critical can work from home during this period,

Location	Lease Period	Contact	Contact Number
We Work, 2 Dublin Landings, North Dock, Dublin	1 month	Alex Jones	01 903 9302

The location is available for 1 month of time for critical staff; all other staff for the period will be asked to work from home and remote into the office.

The office location allows access to the following items

- Phones
- Computer Systems
- Internet Connections
- Self-Sustainable Power
- Business Supplies
- Desks and equipment's
- On site cooking facilities

Property Protection

After the location is shut down and moved offsite onsite security is required to protect the offices from damage

Company Name	Contact	Contact
CG Security	Joe Smith	+353 86 952 2254

CG Security is the on call security company for location; this company can supply mobile security camera systems for the location, they can also supply up to 20 security guards on rotation to provide physical security on the site premises for the period of shutdown and transfer.

In an emergency situation during shutdown procedures the security manager is the go to contact for the location, they deal with all current situations such as fire and medical concerns.

Insurance

Insurance coverage in the event of emergency

Coverage	Contact Name	Phone	Limits	Effect from
Staff	Joan Donald	+353 85 12 135	€150,000,000	Aug-1-2020 – 1yr
Systems	Joan Donald	+353 85 12 135	€150,000,000	Aug-1-2020 – 1yr
Client	Joan Donald	+353 85 12 135	€150,000,000	Aug-1-2020 – 1yr
Office	Joan Donald	+353 85 12 135	€150,000,000	Aug-1-2020 – 1yr

The insurance policies will be stored in the secure document housing with the chosen provider, the data stored will be information pertaining to the insurance coverage of staff, computer systems, client site loses and office specific issues such as replacement of office equipment.

Cyber Attack

Contacts in case of a Cyber Attack on the location

Coverage	Contact Name	Phone	Company
Staff	Connor Smith	Ext 5941	ReliaQuest
Legal	Jane Doegal	Ext 0569	ReliaQuest
Law Enforcement	Sgt Stephen Moe	+353 01 254 12	An Garda Siochana Cyber Team
Incident Response	Alexander Gray	+353 01 652 25	Secure Insiders

These contacts are the people to be contacted in order in event that is a cyber incident such as a cyber-attack on the location, these are only to be contacted in the event that a cyber-attack happens and is confirmed by the designated response team

Sitemaps needed for Incident

These are all the documents required

- Utility Contacts
- Maps of Area
- Building Blueprints
- Maps of Electrical cables
- Maps of Water Pipes
- Maps of Gas Lines
- Local Emergency Contacts
- Designated Escape Routes
- Locations of Fire Suppression Systems
- Maps of High-Value item locations

Event training

Walk-Through Drill

A walk through drill will would involve the appropriate staff and senior management having a building walk through, having a the members of the response team, showing the managers all the locations for emergency points, emergency systems and also how the appointed staff should act and responded any of the situations for each department

Functional drills

A functional drill will be to test the issues regarding functionally of backing up files, moving files from the office to the storage location. The functionality drills also include testing of fire suppression systems, emergency contact systems as well as needed emergency security response as needed

Evacuation Drills

Running an evacuation drill is a drill to test the response time of security staff and employees to leave the building, these drill best tests a response to a building based issue, such as a fire or damage for the location.

Full-scale Exercises

A full scale operation involving multiple different areas of response, to gage the response time and skill of the teams in response to an emergency situation, such as fire, damage to property or possible even a terror attack, each level or exercises are depended on different scenarios that are run such as a Fire, Terror Attack, or Water leak.

Business Impact Analysis

Software Issues

Software Failures

Failures of the software system could lead to clients getting attacked; this could mean that there could be a finical loss to both the client and the company

- Finical Loss
- Claim by client against company's cyber insurance

Theft of Proprietary Code

Theft of GreyMater source code or custom scripts could allow a rival company being able to configure a system similar to ours and potential remove business from us. It could also potentially mean that there may be security vulnerabilities found by hackers who may not report them to us

- Loss of Software
- Loss of Market Standing
- Loss of Clients
- Security Vulnerabilities

Software Vulnerabilities

If there are potential security vulnerabilities found in the software then a client system could become at risk of exploitation. Causing loss to both our company financially and a loss of critical data to our clients

- Loss of Clients
- Finical Loss
- Possibilities of exploitation

Network Failures

If there are potential network failures our Security Operations Center would become unusable and we would not be able to provide an effective service to our clients, while the network is offline. This could in turn put our clients system at risk during the outage

- Loss of Service to Clients
- Loss of Clients
- Finical Loss

Expiration of Licenses

If software license go out of date on our system it is not an immediate failure, of systems. Software will not be updated during the time of critical updates for security of systems such as VMware or Windows systems

- Loss of features
- Inability to use certain systems

Cyber Attack

If there is a Cyber Attack on the company, it is possible that multiple systems of importance may become compromised, if this happens a large majority of the security operations center maybe effect or be offline and have an inability to be used.

- Loss of ability to provide service to clients
- Loss of ability to monitor security
- Possibility of private credential / information leakage
- Impact on company image if leak went public

Property

Fire

If there is a fire is possible there could be a loss of systems, documentation, the location may become unusable for a long period of time. This can cause a finical loss to the company and an inability to support clients from that location. A Fire could also lead to the loss of equipment and software to damages which would cause an inability to provide service to clients, a fire could also affect the business side of operations

- Finical Loss
- Inability to deliver services
- Loss of offices
- Loss of data
- Loss of systems
- Inability to provide services
- Injury to employees

Water

If there is water damage the location this could mean that the location could be closed for multiple days depending on the severity of water damage, the levels can go from simple spillage to a pipe bursting, at the level of pip bursting it is possible there could be a sever loss of equipment and

hardware causing an inability to provide services to clients. Water leaks could also affect the business side of operations

- Finical Loss
- Inability to deliver services
- Loss of offices
- Loss of data
- Loss of systems
- Inability to provide services

Structural

If there is a structural issue, such as damage to the building or safety of the buildings structure this could mean a temporary or permanent closure of services from that location, this would result in the company being unable to provide services as original provide

- Damage to property
- Finical loss
- Loss of Services
- Possible loss of client
- Loss of Security Operations Center availability

Power Loss

With a power loss system would go offline meaning that the Security Operations Center will not be able to provide services they were asked to provide by the client, meaning the client could possibly go to another provider, a power outage could also affect the business side of operations

- Loss of service
- Loss of data
- Loss of Security Operations Center availability
- Possible loss of client

Theft

Theft from the office would affect the system that is taken, this could be simple as business side operations computer or this could be a server rack. At different levels each other effect the operations of the company in different ways.

- Loss of Service
- Loss of Data

Weather Phenomenon

A weather Phenomenon could come in different forms, this could come in the form of a mild to heavy snow or a major event such as a tsunami. In both situations operations of the security center may be effected meaning that it will not function as needed for the clients.

- Loss of Security Operations Center availability
- Loss of Service
- Loss of clients during the incident

Terror Attacks

In a potential terror incident it might impact the Security Operations Center; a Terror attack could render the location un-usable this could include impact of staff and potentially inability to provide service to clients

- Loss of Security Operations Center availability
- Loss of Service
- Loss of clients during the incident
- Injury to employees
- Employee Post Traumatic Stress

Issues with Client

Client Compromised

If a client company is compromised then it could cause data destruction, data to be lost or data to be stolen. This could in turn cause a client to go to c competitor to have their data protected, depending on the contractor there could potentially be a financial loss if there is need for reimbursement

- Client data Lost/Stolen/Destroyed
- Loss of Client
- Finical Loss
- Leak of proprietary software sold to clients

Client Closure

If a large client is to close it could cause a backlash on the company in the sense that there is less income from that contract coming to the company, this could mean having to move employees to a part time basis or firing of employees.

- Loss of employees
- Loss of income

Legal Related Issues

If there is a legal related issue, this could include mean the halt of operations at the security operations center meaning the center being unable to provide service to other clients. This could also mean a finical payout

- Loss of clients
- Loss of Security Operations Center availability

Financial Issues

Bank Closure

If there is a bank closure for a period of time then it may become hard for the company to be able to pay staff or payout on needed funds for any contracts.

- Loss of ability to pay employee
- Loss of ability to pay contacts

Failure of Payment Software

If there is an issue with the payment software then the company maybe become unable to pay employees and may lose the ability to pay for license, or outstanding payments

- Loss of ability to pay employee
- Loss of ability to pay contacts

Employee Issues

Insider Threat

There could be the possibility that there maybe an Insider threat in the form of employees who are taking proprietary data to competitors or having the insider threat possibly damage hardware in the office.

- Loss of Proprietary code or software
- Potential leakage of company documents
- Loss of passwords and credentials

Death of Employee

If there is a death of an employee there is a possibilities there could be a loss of critical data, logging credentials and information not wrote up or stored in documents. This could come in at a loss to the clients as there might be client information that is lost, there could also be an issue regarding passwords being lost

- Loss of data
- Loss of password
- Effect on other employees

Employee Terminated

If an employee is terminated there could be issues such as the employee taking proprietary scripts and programs to competitors, they may attempt to damage equipment or hardware, or use their login credentials to pull / modify or delete client data

- Loss of data
- Loss of passwords
- Theft of data
- Document damaged

Medical Issues

If an employee has medical issues within the office there maybe a requirement to have medical services called to the offices, this may require the services of the Security operations Center meaning services to client's maybe halted

- Disruption of service
- Loss of employee

Pandemic

During a pandemic it maybe required by laws and governmental request to have employees work from home, this can cause a reduction in work output, in some cases there maybe some work that can be completed at the location maybe unable to be done from home this would include network management that would require physical cabling at the location

- Reduction in work
- Some work maybe unable to be complete

Terror Attacks

There are possibilities of terror attacks these can affect the company in multiple different ways this could be a terror attack on the client which could affect the company finically, or there could be an attack on the company itself that could cause damage to the location, employee loss and cause delays of services being provided to clients

- Client data Lost/ Destroyed
- Disruption of service
- Premises Damaged
- Security Operations Center Becomes unusable
- Loss of Client
- Loss of employees
- Finical Loss
- Employee medical leave due to injuries
- Employee mental leave due to traumatic stress