ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Nguyen Cao Tri	**Student ID**	Gcs16241
Class	FA20-GCC0801-1623	**Assessor name**	Le Huynh Quoc Bao

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

❒ Summative Feedback:	❒ Resubmission Feedback:

Grade:	Assessor Signature:	Date:
Signature & Date:		

Contents

P5 Discuss risk assessment procedures.

IT security risk:

Information technology risk, **IT risk**, **IT-related risk**, or **cyber risk** is any risk related to information technology. While information has long been appreciated as a valuable and important asset, the rise of the knowledge economy and the Digital Revolution has led to organizations becoming increasingly dependent on information, information processing and especially IT. Various events or incidents that compromise IT in some way can therefore cause adverse impacts on the organization's business processes or mission, ranging from inconsequential to catastrophic in scale.

IT risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

Risk assessment:

Cyber risk assessments are defined as risks assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

Risk assessments are used to identify, estimate and prioritize risks to organizational operations and assets resulting from the operation and use of information systems.

To begin risk assessment, take the following steps:

Identify asset

In information security, computer security and network security, an **asset** is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

The first step is to identify assets to evaluate and determine the scope of the assessment. This will allow you to prioritize which assets to assess. You may not want to perform an assessment on every building, employee, electronic data, trade secret, vehicle, and piece of office equipment. Remember, not all assets have the same value.

You need to work with business users and management to create a list of all valuable assets. For each asset, gather the following information where applicable:

- Software
- Hardware
- Data

- Interface
- End-users
- Support personal
- Purpose
- Criticality
- Functional requirements
- IT security policies
- IT security architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security controls
- Environmental security

Identify Threats

A cyber threat is any vulnerability that could be exploited to breach security to cause harm or steal data from your organization. While hackers, malware, and other IT security risks leap to mind, there are many other threats

- **Natural disasters:** Floods, hurricanes, earthquakes, lightning and fire can destroy as mh as any cyber attacker. You can not only lose data but servers too. When deciding between on premise and cloud-based servers, think about the chance of natural disasters.
- **System failure:** Are your most critical systems running on high-quality equipment? Do they have good support?
- **Human error**: Are your S3 buckets holding sensitive information properly configured? Does your organization have proper education around malware, phishing and social engineering? Anyone can accidentally click a malware link or enter their credentials into a phishing scam. You need to have strong IT security controls including regular data backups, password managers, etc.

- **Adversarial threats**: third party vendors, insiders, trusted insiders, privileged insiders, established hacker collectives, ad hoc groups, corporate espionage, suppliers, nation-states

Some common threats that affect every organization include:

- Unauthorized access: both from attackers, malware, employee error
- Misuse of information by authorized users: typically an insider threat where data is altered, deleted or used without approval
- Data leaks: Personally identifiable information (PII) and other sensitive data, by attackers or via poor configuration of cloud services
- Loss of data: organization loses or accidentally deleted data as part of poor backup or replication
- Service disruption: loss of revenue or reputational damage due to downtime

After you've identified the threats facing your organization, you'll need to assess their impact.

Explain the risk assessment procedure

Assessments should be done by a competent person or team of individuals who have a good working knowledge of the situation being studied. Include either on the team or as sources of information, the supervisors and workers who work with the process under review as these individuals are the most familiar with the operation.

In general, to do an assessment, you should:

Determine the likelihood of harm, such as an injury or illness occurring, and its severity.

- Consider normal operational situations as well as non-standard events such as maintenance, shutdowns, power outages, emergencies, extreme weather, etc.
- Review all available health and safety information about the hazard such as Safety Data Sheet (SDS), manufacturers literature, information from reputable organizations, results of testing, workplace inspection reports, records of workplace incidents (accidents), including information about the type and frequency of the occurrence, illnesses, injuries, near misses, etc.
- Understand the minimum legislated requirements for your jurisdiction.

Identify actions necessary to eliminate the hazard, or control the risk using the hierarchy of risk control methods.

Evaluate to confirm if the hazard has been eliminated or if the risk is appropriately controlled.

Monitor to make sure the control continues to be effective.

Keep any documents or records that may be necessary. Documentation may include detailing the process used to assess the risk, outlining any evaluations, or detailing how conclusions were made.

When doing an assessment, also take into account:

- The methods and procedures used in the processing, use, handling or storage of the substance, etc.
- The actual and the potential exposure of workers (e.g., how many workers may be exposed, what that exposure is/will be, and how often they will be exposed).
- The measures and procedures necessary to control such exposure by means of engineering controls, work practices, and hygiene practices and facilities.
- The duration and frequency of the task (how long and how often a task is done).
- The location where the task is done.
- The machinery, tools, materials, etc. that are used in the operation and how they are used (e.g., the physical state of a chemical, or lifting heavy loads for a distance).
- Any possible interactions with other activities in the area and if the task could affect others (e.g., cleaners, visitors, etc.).
- The lifecycle of the product, process or service (e.g., design, construction, uses, decommissioning).
- The education and training the workers have received.
- How a person would react in a particular situation (e.g., what would be the most common reaction by a person if the machine failed or malfunctioned).
- It is important to remember that the assessment must take into account not only the current state of the workplace but any potential situations as well.
- By determining the level of risk associated with the hazard, the employer, and the health and safety committee (where appropriate), can decide whether a control program is required and to what level.

P6. Explain data protection processes and regulations as applicable to an organization.

Data protection

Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Data protection is also known as data privacy or information privacy.

Data protection should always be applied to all forms of data, whether it be personal or corporate. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.

The context of data protection varies and the methods and extent also vary for each; there is data protection on the personal level, that of business or public entities, and that of data so highly classified that it should never fall into the hands of others aside from its owners — or in other words, top secret.

Explain data protection process with relations to organization

For many companies, data is something we take for granted as being safe and sound, stored away on computers and difficult to access. If you work with data from your customers, hold sensitive information from your industry or even just keep your employees' information on your company server or cloud, then data protection should be one of your big priorities.

The important of data protection

Firstly, the purpose of personal data protection isn't to just protect person's data, but to protect the fundamental rights and freedoms of persons that are related to that data. Whilst protecting personal data it is possible to ensure that persons' rights and freedoms aren't being violated. For example, incorrect processing of personal data, might bring about a situation where a person is overlooked for a job opportunity or, even worse, loses current job.

Secondly, not complying with the personal data protection regulations can lead to even harsher situations, where it's possible to extract all the money from a person's bank account or even cause a life-threatening situation by manipulating health information.

Thirdly, data protection regulations are necessary for ensuring and fair and consumer friendly commerce and provision of services. Personal data protection regulations cause a situation, where, for example, personal data can't be sold freely which means that people have a greater control over who makes them offers and what kind of offers they make.

If personal data is leaked, it can cause companies significant damage to their reputation and also bring along penalties, which is why it's important to comply with the person data protection regulations.

To ensure that personal data is secure, it's important to know what data is being processed, why it's being processed and on what grounds. In addition, it's important to identify which safety and security measures are in use. All of this is possible through a thorough data protection audit, which identifies the data flow and whether the data protection regulations are being followed. The audit can be carried out

by answering a set of specific questions that have been prepared for that purpose. The results will give a clear overview of the procedures and possible data leaks, which can then be stopped.

P7. Design and implement a security policy for an organisation.

Security Policy

A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.

A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well.

Elements of an information security policy

Purpose

Institutions create information security policies for a variety of reasons:

To establish a general approach to information security

To detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications.

To protect the reputation of the company with respect to its ethical and legal responsibilities

To observe the rights of the customers. Providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective

Scope

An information security policy should address all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties in a given organization, without exception.

Information security objectives

An organization that strives to compose a working information security policy needs to have well-defined objectives concerning security and strategy. Management must agree on these objectives: any existing disagreements in this context may render the whole project dysfunctional.

The most important thing that a security professional should remember is that his knowledge of the security management practices would allow him to incorporate them into the documents he is entrusted to draft. That is a guarantee for completeness, quality and workability.

Simplification of policy language is one thing that may smooth away the differences and guarantee consensus among management staff. Ambiguous expressions are to be avoided, and authors should take care to use the correct meaning of terms or common words. For instance, “musts” express negotiability, whereas “should” denote a certain level of discretion. I

Ideally, the policy’s writing must be brief and to the point. Redundant wording makes documents long-winded or even illegible, and having too many extraneous details may make it difficult to achieve full compliance.

How management views IT security is one of the first steps when a person intends to enforce new rules in this department. A security professional should make sure that the information security policy is considered to be as important as other policies enacted within the corporation. In cases where an organization has a very large structure, policies may differ and therefore be segregated in order to define the dealings in the intended subset of this organization.

Information security is considered as safeguarding three main objectives:

- Confidentiality: Data and information assets must be confined to people who have authorized access and not disclosed to others
- Integrity: Keeping the data intact, complete and accurate, and IT systems operational
- Availability: An objective indicating that information or system is at disposal of authorized users when needed.

Donn Parker, one of the pioneers in the field of IT security, expanded this threefold paradigm by suggesting additional objectives: “authenticity” and “utility”.

Authorization and access control policy

Typically, a security policy has a hierarchical pattern. Junior staff is usually required not to share the little amount of information they have unless explicitly authorized. Conversely, a senior manager may have enough authority to make a decision about what data can be shared and with whom, which means that they are not tied down by the same information security policy terms. This means that the information security policy should address every basic position in the organization with specifications that will clarify their authorization.

Policy refinement takes place at the same time as defining the administrative control or authority people in the organization have. Essentially, it is a hierarchy-based delegation of control in which one may have authority over his own work, a project manager has authority over project files belonging to a group he is appointed to and the system administrator has authority solely over system files.

A user may have the need-to-know for a particular type of information. Therefore, data must have enough granularity to allow the appropriate authorized access and no more. This is all about finding the

delicate balance between permitting access to those who need to use the data as part of their job and denying such to unauthorized entities.

Access to the company's network and servers should be via unique logins that require authentication in the form of either passwords, biometrics, ID cards or tokens etc. Monitoring on all systems must be implemented to record login attempts (both successful ones and failures) and the exact date and time of logon and logoff.

As the IT security program matures, the policy may need updating. While doing so will not necessarily guarantee an improvement in security, it is nevertheless a sensible recommendation.

Classification of data

Data can have different values. Gradations in the value index may impose separation and specific handling regimes/procedures for each kind. An information classification system will therefore help with the protection of data that has a significant importance for the organization and leave out insignificant information that would otherwise overburden the organization's resources.

A data classification policy may arrange the entire set of information as follows:

- High Risk class: Data protected by state and federal legislation (the Data Protection Act, HIPAA, FERPA) as well as financial, payroll and personnel (privacy requirements) are included here
- Confidential Class: The data in this class does not enjoy the privilege of being protected by law, but the data owner judges that it should be protected against unauthorized disclosure
- Public class: This information can be freely distributed

Data owners should determine both the data classification and the exact measures a data custodian needs to take to preserve the integrity in accordance to that level.

Data support and operations

In this part, we could find clauses that stipulate:

- The regulation of general system mechanisms responsible for data protection
- The data backup
- Movement of data

Security awareness sessions

Sharing IT security policies with staff is a critical step. Making them read and acknowledge a document does not necessarily mean that they are familiar with and understand the new policies. On the other hand, a training session would engage employees and ensure they understand the procedures and mechanisms in place to protect the data.

Such an awareness training session should touch on a broad scope of vital topics: how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of IT systems, correct usage social networking and so on. A small test at the end is perhaps a good idea.

Responsibilities, rights and duties of personnel

Things to consider in this area generally focus on the responsibility of persons appointed to carry out the implementation, education, incident response, user access reviews and periodic updates of an information security policy.

Prevention of theft, information know-how and industrial secrets that could benefit competitors are among the most cited reasons as to why a business may want to employ an information security policy to defend its digital assets and intellectual rights.

References to relevant legislation

There are a number of different pieces of legislation which will or may affect the organization's security procedures. For example, in the UK, a list of relevant legislation would include:

- The Computer Misuse Act (1990)
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)

Other items that an information security policy may include

An information security policy may also include a number of different items. These include, but are not limited to: virus protection procedure, intrusion detection procedure, incident response, remote work procedure, technical guidelines, audit, employee requirements, consequences for non-compliance, disciplinary actions, terminated employees, physical security of IT, references to supporting documents and more.

Conclusion

Authorization and access control policy is the most important element and must have while create policy

Because it relates directly with data hierarchy inside organization, by that organization can be clear which information a particular company position can access.

Steps to design a policy

Identify need

Policies can be developed:

- In anticipation of need (e.g. child protection policies should be in place once an organization starts to work with children or young people).
- In response to need (e.g. a policy position on a government strategy may be developed in response to a consultation paper).

The organization needs to constantly assess its activities, responsibilities and the external environment in order to identify the need for policies and procedures. (More on what policies you need to develop).

Identify who will take lead responsibility

Delegate responsibility to an individual, working group, sub-committee or staff members, according to the expertise required. (More on the management committee's role in policy development).

Gather information

Do you have any legal responsibilities in this area? Is your understanding accurate and up to date? Have other organizations tackled the same issue? Are there existing templates or examples that you could draw on? Where will you go for guidance?

Draft policy

Ensure that the wording and length or complexity of the policy are appropriate to those who will be expected to implement it.

Consult with appropriate stakeholders

Policies are most effective if those affected are consulted are supportive and have the opportunity to consider and discuss the potential implications of the policy. Depending on whether you are developing policies to govern the internal working of the organisation or external policy positions, you may wish to consult, for example:

- Supporters
- Staff and volunteers
- Management Committee members
- Service users or beneficiaries.

Finalize / approve policy

Who will approve the policy? Is this a strategic issue that should be approved by the Management Committee or is the Committee confident that this can be dealt with effectively by staff? Bear in mind

that, ultimately, the Management Committee is responsible for all policies and procedures within the organization.

Consider whether procedures are required

Procedures are more likely to be required to support internal policies. Consider whether there is a need for clear guidance regarding how the policy will be implemented and by whom. (E.g. a policy regarding receiving complaints will require a set of procedures detailing how complaints will be handled). Who will

be responsible for developing these procedures? When will this be done? What will be the processes for consultation, approval and implementation?

Implement

How will the policy be communicated and to whom? Is training required to support the implementation among staff and volunteers? Should the organisation produce a press release (for external policy positions)?

Monitor, review, revise

What monitoring and reporting systems are in place to ensure that the policy is implemented and to assess usage and responses? On what basis and when will the policy be reviewed and revised

Example of security policies

Information is a critical company asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss, or m issue can be costly, if not illegal. The intent of this Security policy is to protect the information assets of the organization.

In addition, in this policy. the main objective followed by [COMPANY NAME], is to establish and maintain adequate and effective security measures for users. to ensure that the confidemiality, integrity and operational availability of information is not compromised.

Sensitive information must therefore be protected from unauthorized disclosure, modification, access use, destruction or delay in service.

PURPOSE

The purpose of this policy is to safeguard information belonging to [COMPANY NAME] within a secure environment.

This policy informs [COMPANY NAME] staff and other persons authorized to use [COMPANY NAME] facilities of the principles governing the retention, use and disposal of information

SCOPE

This policy applies to all employees of [COMPANY HAME] who use computer systems or work with documents or information that concerns customers, suppliers or any other partner lor whom the organization has collared information in the normal course of its business

GOALS AND OBJECTIVES FOLLOWED

The goals and objectives followed of this policy are:

- Protect information from unamortized access or m issue
- Ensure the confidentiality of information;
- Maintain the integrity of information;
- Maintain the availability of information systems and information Jar service delivery,
- Comply with regulatory. contractual and legal requirements
- Maintain physical, logical, environmental and communications security; Dispose of information in an appropriate and secure manner when it is no longer in use

AUTHORIZED USERS OF INFORMATION SYSTEMS

All users of [COMPANY NAME]'s information systems must be formally authorized by the company's [SPECIFY] department. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

Authorized users shall take necessary precautions to protect the [COMPANY NAME} information in their personal possession Confidential, personal or private information must not be copied or transported without consideration of the permission of the owner of the information; the risks associated with loss or falling into the wrong hands; how the information will be secured during transport to its destination.

ACCEPTABLE USE OF INFORMATION SYSTEMS

User accounts on the company's computer systems must only be used for the company's business and must not be used for personal activities during working hours.

During breaks or meal time, limited personal use is perm it ted, but use must be legal. honest and decent while considering the rights and sensitivities of others.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PGs or workstations, unless they have received specific authorization from the employees! manager and ’or the company IT designee. Users shall not download unauthorized software from the Internet onto their PCs.

Unauthorized use of the system may constitute a violation of the law, theft and may be punishable by law. Therefore, unauthorized use of the company’s computer system and facilities may constitute for civil or criminal prosecution.

ACCESS CONTROL

The fundamental element of this security policy is the control of access to critical information resources that require protection against unauthorized disclosure or modification

Access control refers to the permissions assigned to persons or system s that are authorized to access specific resources Access controls exist at different layers of the system, including the network. Access control is implemented by username and password. At the application and database level, other access control methods can be implemented to further restrict access.

Finally, application and database systems can limit the number of applications and databases available to users based on their job requirements.

NORMAL USER IDENTIFICATION

All users must have a unique username and password to access the systems. The user's password must remain confidential and under no circumstances should it be shared with management and supervisory staff and*or any other employees. Also, all users must comply with the following rules regarding password creation and maintenance:

Password must not be found in any English or foreign dictionary. This means, do not use a common noun, worm, verb, adverb or adj. These can be easily cracked using standard "hacking tools";

Passwords should not be displayed on or near computer terminals or be ensily accessible in the terminal area:

- Password must be changed every [NUMBER] days
- User accounts will be frozen after[NUMBER] of days of failed logon attempts
- Logon IDs and passwords will be suspended after[NUMBER] of days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be locked for access by unauthorized users. Copying, reading, deleting or mod4ying a password file on any computer system is prohibited.

- Users will not be allowed as a System Administrator. Users who need this level of access to production systems must request a Special Access account.
- Employee Logon IDs mid passwords will be denominated as soon as possible if the employee is terminated fired, suspended, placed on leave or otherwise leaves the employment of the company office.

Employees who forgot their password must call the IT department to get a new password assigned to their account The employee must identify himself or herself by (e g. employee numbers to the IT department

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems

CONFIDENTIALITY OF INFORMATION

Any information or documents that are not to be made public are designated as "Confidential Information". This information is invaluable to the company and therefore, all employees who. in the course of their duties, handle this type of information are expected to behave as follows

All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have a business need-to-know."

All electronic confidential information should be protected via firewalls, encryption and passwords.

Employees should clear their desks of any confidential information before going home at the end of the day

Employees should refrain from leaving confidential information visible on their computer monitors when they leave their workstations.

All confidential information, whether contained on written documents or electronically, should be marked as "confidential."

All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)

Employees should refrain from discussing confidential information i n public places,

Employees should avoid using e-mail to transmit it contain sensitive or controversial information.

Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver's license numbers) unless it is integral to the business transaction and restrict access on a “need-to-know’ basis.

Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

SECURITY OP INFORMATION

Information stored on computer systems must be regularly backed-up so that it can be resto red if or when necessary. All care and responsibility must be taken in the destruction of sensitive information Electronic information relating to customers, administrative and commercial information must be disposed of in a secure manner.

Sensitive or confidential paper documents must be placed in the shredding bins or destroyed in the manner indicated to you by your department head.

USER RESPONSIBILITIES

Any security system relies on the users of the system to follow the procedures necessary for upholding security policies. Users are required to reopen any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

Employees are therefore expected to:

Complies with security procedures and policies;

Protects their user ID and passwords;

Inform the [SPECIFY] department of any security questions, issues, problems or concerns;

Assists the [SPECIFY] department in solvi ng security problems!

Ensures that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery;

Be aware of the vulnerabilities of remote access and their obligation to repon intrusions, misuse or abuse to the [SPECIFY] department

Be aware of their obligations in the event that they store secure, transmit and dispose of vital information concerning the activities or operations of the company, customers, banners or strategic information on the company’s product and services

MONITORING OF THE COMPUTER SYSTEM

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network.

Howe ver. users of the systems should be aware that the company may monitor usage. including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files on messages to the extent necessary to ensure that the Internet and other electronic communications are being used i compliance with the law and with company policy.

SYSTEM ADMINISTRATOR

System administrators, network administrators and security administrators will have access to the host systems, routers, hubs and firewalls necessary to perform their tasks.

All system administrator passwords will be deleted immediately after an employee who has access to these passwords has been terminated, dismissed or otherwise left the company's employment,

MANAGERS DUTY

Supervisors Managers shall immediately and directly contact the company manager to change in employee status that requires terminating or modifying employee logon access privileges.

EMPLOYEE AGREEMENT ON SECURITY POLICY

I acknowledge that I have received a copy of the [COMPANY NAME] Security policy. I have read and understand the policy. I understand that, I'll violate the policy. I may be subject to disciplinary action, including termination. I further understand that I will contact my supervisor if I have any questions about any aspect of the policy.

P8 List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.

Business continuity

Business continuity is the advance planning and preparation undertaken to ensure that an organization will have the capability to operate its critical business functions during emergency events. Events can include natural disasters, a business crisis, pandemic, workplace violence, or any event that results in a disruption of your business operation. It is important to remember that you should plan and prepare not only for events that will stop functions completely but for those that also have the potential to adversely impact services or functions.

What Does Business Continuity Include?

BC covers the planning and preparation needed to ensure an organization will have the capability to perform its critical business functions during emergency events. It identifies, plans for, and/or creates:

- How to communicate with customers, vendors and other third parties to ensure you are providing good information and support.
- How to ensure services or products can still be provided to customers.
- The order and timing required to restore business processes.
- How to support employees during an emergency event?
- The required technology to support the business functions (disaster recovery – or DR – will implement recovery solutions for technology).
- Workaround processes to use when technology is not available.
- Where and how to relocate people and processes in the event business locations are impacted or not available.
- The teams and organization that will be necessary to manage emergency events.
- Business process dependencies (what, or who does each business process rely upon in order to do their work).
- Regular exercises to validate that plans and actions meet requirements and will be functional in an actual event.
- Ensure staffing levels will be adequate during an event for both external and internal needs.
- Documentation of the steps and actions to take during an event to accomplish the items above.

The Anatomy of a BCM Program

At MHA, we divide up the Business Continuity Management (BCM) program into four key dimensions:

- Program Administration
- Crisis Management
- Business Recovery
- IT Disaster Recovery

We believe that when these four dimensions are operating optimally, individually and in an integrated fashion, the BCM program will have an elevated level of sophistication, maturity, and capability.

Organizations may not be able to work on the four dimensions in parallel and effectively implement the components, but without implementing all areas, an organization will not truly be prepared. Many unexpected issues arise during a crisis event, too many to address ad hoc. If your organization tries to address the unexpected and perform critical actions on the fly during a crisis event, it will not be able to effectively and efficiently perform the tasks required for a successful recovery.

Components of recovery plan

A Communications and Roles Plan

Your disaster recovery plan should outline a chain of communication with updated contact information via multiple methods. It should include a leader's role as well as the responsibility each person is taking on in the disaster recovery plan. Design this aspect of your disaster recovery plan collaboratively to ensure that you have everything covered and the right people assigned to each task.

Disaster: Day 1 isn't the time you want to discover holes in your plan.

An Equipment and Local Plan

Your building is sitting in 10-feet of water. What shape will the equipment be in?

If you know a storm is coming like a major flood warning or hurricane, get that technology off the floor on the first floor and/or away from windows. Plan for how this happens to get it done.

Additionally, part of your equipment plan is ensuring that you have enough laptops, phones, etc. for critical employees who need to continue business operations immediately after the disaster, once their own safety is secured.

Finally, where will employs work? Home? A satellite office? Plan ahead because when you do so you have more options and can save a lot of money. Don't be afraid to get creative.

After Joplin, Missouri tornados wiped out much of the city, a small business made arrangements with a church of which the owner was a member. They were able to continue critical operations from the building at little added cost.

A Data Continuity Plan

Employees need data to continue business operations. Even though some departments can switch to paper forms when data access is limited, they can't make informed decisions or properly care for customers or accounts. Your plan should include how you maintain their access to data in the event of a physical (e.g., hurricane) or virtual (e.g., ransomware) disaster. This involves solutions like data backups and remote access to backup servers.

Checking Backup Systems

Backup is so important to data continuity that it deserves its own section. Check and double-check and re-check those backups to make sure they're working. Know how quickly you can recover data or restore access. As a general rule, your backup should always be off-site, in another city that's not likely to be hit by the same disaster. So if one or the other is hit, you never lose your data. Many large businesses back data up in multiple sites using highly-secure cloud storage solutions.

Not having a proper backup system can cost you. Recently, the city of Atlanta spent $2.6 million dollars to respond to, and recover from, a ransomware attack that demanded over $50,000 for the release of the city data they held hostage. Because they lacked proper backup, they had to deploy emergency efforts and do damage control in the aftermath instead of executing a more cost-effective data recovery plan.

Written Asset Inventory

The days after a physical disaster are hectic. You may experience looting or have to hire a cleanup crew to dump destroyed equipment. It's nearly impossible to get an accurate inventory in those conditions. Yet, you'll need it for insurance claims and recovery. So plan ahead. Create a written inventory of

servers, workstations, furniture, printers, telephones and other equipment with any significant value. Create a spreadsheet that is regularly updated as equipment enters or leaves service.

Visual Inventory

Take pictures of everything. If an insurance company challenges your claims, you need this added proof. You don't have to take individual pictures, but walk around each work area, taking multiple pictures. Visually catalog the magnitude of furniture and equipment in each space.

Vendor, Customer and Services Communications

Be prepared to communicate with vendors, customers, service providers and other partners regarding your recovery efforts. If you do have to shut down for a few days, customers may go elsewhere because they don't realize you're open. Vendors and service providers need to know when to restore power or reschedule deliveries.

How you handle communications may be unique to your business. After Hurricane Harvey, one Houston-area business used targeted Facebook ads to keep customers informed regarding their reopen date. Outlining what types of communications are necessary and how they will take place will help you recover faster.

Steps required in disaster recovery process.

Step 1: Set Clear Recovery Objectives

The primary motive to develop a successful disaster recovery plan is to reduce downtime and the cost of data loss. Set key objectives with RTO (Recovery Time Objective) and RPO (Recovery Point Objective), so that you can build an optimal data recovery plan. These parameters help you decide how quickly you need to take steps to recover the data.

An RTO determines the operational downtime within which the system should have its full recovery. An RPO evaluates the maximum limit for manageable data loss that won't lead to a catastrophic impact on business.

Step 2: Identify Involved Professionals

There should be a clear identification of all the included personnel, including internal and external members. The DRP should have documented information on how and when to contact each member. It should also cover their assigned responsibilities in detail.

Also, having a pre-approved budget for resources (recovery tools and services) will help ease the flow and build a successful disaster recovery plan.

Step 3: Draft a Detailed Documentation on Network Infrastructure

A step-by-step guide on network configurations will help with the execution of the data recovery process. A holistic blueprint of the current network infrastructure ensures proper rebuilding and recovery of the entire system. The detailed documentation increases the chances of successful reconstruction of corrupted network infrastructure.

It's advisable to keep all the documents offline and in a private cloud. Either way, the document should be easy for all personnel to access.

Step 4: Choose Your Data Recovery Technique

There are many types of data recovery solutions, such as hard drive recovery, RAID recovery, tape recovery, optical recovery, and more. Selecting the right one for your organization is critical. To choose one of these solutions, consider the requirements of the organizations – on-premise, outsourced, or cloud-based DRaaS (Disaster recovery as a service).

Each data recovery method has its set of capabilities, making it costly or bringing it within your budget. There are a few factors that affect the cost of recovery solutions – storage capacity, recovery timeline, and configuration complexity.

Step 5: Explicitly Define an Incident Criteria Checklist

Every organization faces temporary outages, but these incidents cannot be used to initiate a disaster recovery procedure. No organization would carry out a recovery procedure for a temporary electricity outage, but if it is due to a natural disaster, then the incident needs to be taken into consideration.

Creating an all-inclusive checklist for identifying a disaster will help the recovery team to execute DRP as quickly as possible.

This checklist will differ for every organization, depending on their goals and budget for data recovery. Even the decision to strictly follow this checklist or not is entirely upon organizations.

Step 6: Document Your Entire Disaster Recovery Procedure

After successful identification of a disaster recovery incident, a documented set of procedures help in carrying out the disaster recovery strategy. The DRP should be in accordance with the already established RTO and RPO standards. Both automated to manual processes included in the plan should be neatly documented for maximum efficiency of the DRP.

It's important that at the end of the disaster recovery procedure, all the recovered data should be in an operational state.

Step 7: Regularly Test Your DRP

Your DRP can fall flat if not tested regularly. A thoroughly tested plan is reliable and has a higher chance of giving effective results. For a functional DRP, all the included steps should be routinely tested.

The entire disaster recovery team should participate in these tests. Playing real-time scenarios of data loss and cyberattacks helps the team to stay ready for the unexpected event.

Step 8: Keep Updating Your Recovery Plan

With the growth of the company, the DRP needs to be updated. If your DRP goes through regular testing, then there are fair chances that you will come across some limitations in your existing plan. Keep eliminating these flaws so that the new changes will be aligned with your company's requirements. Also, with every change in DRP, maintain a log for the same.

REFERENCE