Nathan Rickett

BCDR Final Project

Dr. Joni L Jones

ISM 6577

18 October 2024

Situational Analysis

The following risks have been identified:

Financial impact (direct loss of revenue)

- A direct loss of revenue will often incur a hefty burden on an organization. This is because much of the incoming cash flow is used to purchase resources for current project. If that cash flow is affected or interrupted due to a direct loss of revenue, the project could be at risk of cancellation. The company could also see this ripple effect on their sales figures.

Damaged reputation

- Damaged reputation can lead to loss of customer trust, resulting in lower sales and market share. Negative public perception can also negatively affect partnerships and opportunities for establishing new connections. This makes it harder for the company to attract new clients or retain existing ones.

Regulatory and law

- Laws and regulations not only pose a financial risk, but an operational one as well. Failure to comply could mean that the company must permanently alter how the conduct business or pay a hefty penalty. Regulations can often be complex, which requires time and other resources.

Data privacy / security

- Data breaches often expose sensitive customer information, such as PII, credit card information, and passwords, leading to lost revenue from regulatory fees loss of customer trust, and lawsuits. The company may face legal repercussions such as criminal charges.

Project delays long term

- Backlogged projects such as product launches or service enhancements can lead to missed market opportunities, lost revenue, and a potential loss of investor confidence. This affects the company's long-term growth.

Supply chain ripple

- Disruptions in the supply chain can cause delays in product delivery, increased costs, and shortages of critical materials. This ripple effect can hinder operational efficiency, reduce customer satisfaction, and impact overall revenue, as the company struggles to meet demand.

Cybersecurity overhaul costs

- A compromise of data confidentiality or integrity will likely result in an overhaul of cybersecurity, which comes with a significant cost. This can include upgrading systems such as intrusion prevention systems, firewalls, data collection and monitoring tools, and more. It could also mean that that new employees will need to be hired to operate and maintain the new technology, which will incur more costs.

Loss of competitive advantage

- If a company fails to adapt to changing market conditions or technological advancements, it risks losing its competitive edge. This can result in decreased market share, reduced customer loyalty, and an inability to attract new clients, ultimately undermining the company's position in the industry.

Employee moral

- A decline in employee morale due to uncertainty, increased workloads, or a toxic work environment can lead to decreased productivity and higher turnover rates. Low morale can also stifle innovation and collaboration, hindering the company's ability to respond effectively to challenges and maintain operational efficiency.

Business Impact Analysis

The key to a successful business impact analysis is careful consideration when identifying the critical business functions. It is a smart idea to start with a large scope and narrow down the processes that belong to the business function that would have the largest impact, both financially and operationally during a disruption of business operations. While I was able to produce the following list of ideas for business functions and their respective processes, I had to narrow them down into the table below, which only contains only ones that are required for maintaining business operations.

- **Information Technology**: help desk, network administration, system administration, asset management, backups, IT change management.
- **Software Development***:* project management, requirements analysis, system development, code creation, QA, continuous deployment, maintenance & improvement.
- **Human Resources**: employee hiring, employee payment, benefits administration, performance evaluation, training, employee conflict resolution, health & safety
- **Marketing**:
- **Cyber Security:** risk assessment & mitigation, IAM, Security awareness training, Incident response / forensics, Threat detection & investigation / hunting, Security compliance / auditing
- **Data Analytics**: Data collection, Data integration, Data filtering, Data interpretation, Visualization & graphing, Data reporting, Insight analysis
- **Business Relations Management:** relations development, stakeholder identification, Stakeholder conflict resolution, Feedback program, communication strategy development, public affairs
- **Facilities**: general facilities maintenance, Health and safety management, Contract management, Facility security

Business Function	**Required Process**	**Resource Interdependencies**	**Impact on Operations**	**Priority / Classification**	**MTD**	**Financial Impact**	**Legal impact**
Information Technology	*network administration*	IT infrastructure, cyber security	Very High	Critical	1-3 hours	Very High	Low
	System administration	IT infrastructure, cyber security	Very High	Important	3-7 hours	Moderate	Low
	Backups	IT infrastructure, cyber security	Very High	Critical	1-2 hours	Very High	Low

Software Development	*Project Management*	Project management software, communication software	High	Preferrable	2-3 days	Moderate	Low
	Requirements analysis	Stakeholder input, documentation tools	High	Preferrable	2-3 days	Moderate	Medium
	Systems development	UML software, collaboration tools	High	Critical	1-3 days	High	Low
	Code creation	IDE, code base, UML diagrams	High	Critical	1-2 days	High	Medium
	QA	Code base, testing tools	High	Critical	1-2 days	High	Low
	Continuous deployment	Code base, CI/DC tools	Very High	Critical	1-2 hours	Very High	Low
	Maintenance & Improvement	System documentation, stakeholder feedback	Very High	Critical	1-2 days	High	Low
Human Resources	*Employee Hiring*	HR platform, recruitment team	Medium	Important	1-3 weeks	High	Low
	Employee Payment	Payroll system	High	Critical	24 hours	Very High	High
	Benefits Administration	Benefits management system	Medium	Critical	1-3 days	High	High
	Employee Conflict Resolution	HR platform	Medium	Critical	1-2 weeks	Moderate	High
	Health & Safety	Safety equipment, training sources	High	Critical	24 hours	High	High
Cyber Security	*Risk Assessment & Mitigation*	Vulnerability assessment tools, risk management framework	Medium	Important	1-2 weeks	Moderate	Low
	IAM	IT infrastructure	Medium	Critical	1-2 hours	High	High
	Incident Response & Forensics	IT infrastructure, forensic tools	Medium	Critical	1 hour	Very High	High
	Threat Detection & Investigation	IT infrastructure , monitoring systems	Medium	Critical	1-3 hours	Very High	High
Business Relations Management	*relations development*	Stakeholder documentation	Low	Preferable	1-2 days	Moderate	Low
	stakeholder identification	Data analysis tools	Low	Preferable	2-4 days	Low	High
	Stakeholder conflict resolution	Communication tools	Medium	Critical	3-4 hours	High	High
	Feedback program management	Survey tools, data analysis tools	Medium	important	1-3 days	Moderate	High
	public affairs	Communication platform, media relationships	High	important	1-3 days	High	High
Facilities	*Health and safety management*	Training resources, safety equipment	High	Important	24 hours	High	High
	Facility security	Security guards, security systems, security protocols, badging office, IT infrastructure	High	Critical	1 hour	Very High	High

Information Technology: Information technology has become the beating heart of every organization in the modern era. Digital applications have become a necessity to every nearly process that a business uses, and thus must be functional for the business to continue operating.

Software Development: Considering SolveTech Inc. is a medium-sized software development company, it is assumed that their main (or only) source of revenue comes from developing software. This poses the risk of long-term projects being backlogged and will slowly reveal how dependent software development can be on other resources.

Human Resources: HR is responsible for ensuring the safety and well-being of employees. If employees are not in a safe environment, then the company could be held legally liable and could receive damaged reputation. HR is also responsible for effective communication during and after a disaster, as well as many other vital processes such as ensuring employees are paid, maintaining moral, and how to adapt to a new working condition.

Cyber Security: Cyber Security is often overlooked when trying to recover from a disaster or disruption, but it shouldn't be misunderstood. Often companies will say something like "just make it work, I don't care what you have to do." This neglect is the perfect opportunity for an adversary to strike, especially if they already have done so once.

Business Relations Management: Business relations are vital to maintaining a strong connection with key stakeholders following a disruption in operations. This function keeps stakeholders up to date with clear and concise information that will benefit both the organization and those external entities who are affected by the disruption.

Facilities: Many organizations operate within a building or on a campus, and thus will need to continue having certain facilities available to them to keep the business running. Employees who cannot work remotely will not be able to work at all if the facilities they use daily aren't available to them. Natural disasters can make facilities unusable and unsafe for employees, so planning for this is vital.

Risk Assessment

From an IT perspective, the main objective during the risk assessment and mitigation plan development phase is achieving a good balance in each section of the CIA triad (Snedaker 162). To achieve this, we need to identify what our risks are by combining threats, vulnerabilities and their likelihood, and the impact that each one of these vulnerabilities has on business operations.

Threat & Impact Assessment

Threat	**Impact**
Legal disputes from clients over SLA breach	Loss of revenue, damaged relationships
Intellectual property theft	Legal expenses for recovery of theft, loss of competition
Malware attacks	Ransom costs, data destruction, data leaks, loss of trust, recovery costs, operations disruption
Hurricanes	Damaged facilities and equipment, operations disruption, cost of repair due, employee safety
Earthquakes	Damaged facilities and equipment, operations disruption, cost of repair due, employee safety risk
Floods	Damaged facilities and equipment, operations disruption, cost of repair due, employee safety risk
Fires	Damaged facilities and equipment, operations disruption, cost of repair due, employee safety risk, increased insurance costs
Supply chain disruptions	Damaged relationship with suppliers, product release delays, backlogged projects
Insider threats	Proprietary data loss/leak, destruction of company assets, legal consequences, investigation costs
Negative media coverage	Damaged reputation, lower sales
Data breach	Legal fines, data recovery costs, damaged reputation, cost of improving CIA triad efforts
Social engineering attacks	Unauthorized access, sensitive data leaks, stealthy operational disruptions, fraud
Systematic error due to internal communication failure	Timeline delays, employee frustration, unfinished projects, increased operational costs
Internal network/ IT outage	Near total loss of operations, massive loss of revenue
A disruption in employee payment occurs	Limited time for restoration before employee turnover, legal implications and fines, loss of employee trust
Employees are unable to file reports of unsafe working conditions	Legal fines and implications, increased exposure to workplace hazards, loss of employee morale and trust
Code base becomes unavailable	Delays in product development, cost of restoring code base access, potential for total loss of a project
Unauthorized changes were made to the code base	Sensitive data leaks and destruction, malicious code tampering affecting customers
A change pushed recently caused a massive outage in the production environment	Potential for catastrophic production failure resulting in loss of public trust, lost revenue from repairs

Vulnerabilities and Their Likelihood of Exploitation by a Threat

Quantitative likelihood of exploitation is not feasible in this scenario

Risk	Vulnerability	Likelihood	Threats
potential legal disputes and financial losses due to contractual misunderstandings	Lack of careful contract planning or review when creating an SLA contract	Moderate	Contract breach
Unauthorized access leading to breach and financial loss	Lack of security controls or policies involving access management	Very High	Malware attacks, insider threats, social engineering, unauthorized changes to code.
Inability to recover effectively from a cyber incident	No existing strategy for cyber incident response	High	Malware attacks, insider threats, data breach, social engineering.
Malicious software compromising confidentiality, integrity, and availability of IT resources	Weak or missing antivirus	Very High	Malware attacks, insider threats, data breach, internal IT outage
Ineffective recovery from natural disasters	Weak or missing disaster recovery and business continuity planning for natural disasters	Moderate	Hurricanes, Floods, Fires, Earthquakes
Loss / destruction of facilities and equipment	Facilities and equipment that are not well equipped withstand destructive forces, or low mobility.	Moderate	Hurricanes, Floods, Fires, Earthquakes
Potential employee harm & loss of equipment from fires	Lack of fire safety measures	High	Fires
Supply chain disruptions cause operational slowness	Over-reliance on third party suppliers	Moderate	Supply chain disruptions, social engineering attacks
Compromise of CIA triad due to employee security violations	Weak/non-existent employee training program for security	High	Insider threats, social engineering, malware attacks
Reputational damage	Poor public relations management	Low	Negative media coverage
Poor public image because of social media	Deliberate attacks on company social media	Moderate	Negative media coverage
Leaked sensitive information due to confidentiality.	Weak data protection measures (confidentiality)	Very High	Intellectual property theft, data breach, insider threats, social engineering
Compromise of CIA triad due to lack of employee social training	No employee awareness program for social engineering attempts	Very High	Insider threats, social engineering, intellectual property theft
Increased chance of error and employee frustration due to communication	Confusion on employee communication mediums	High	Error due to internal communication failure, unauthorized changes to code, SLA contract breach
Lack of employee operational awareness	Lack of effective communication from the top down	Moderate	Internal communication failure
Inability to recover from loss of availability	Lack of IT infrastructure redundancy	Very High	Malware, insider threats, social engineering, internal IT outage,hurricane, earthquake, flood, fire, code repo unavailable
Employee dissatisfaction and high turnover due to lack of pay	Employee payroll processing relies on access to internal IT infrastructure	Very High	IT outage, disruption in employee payment

Increased chance of workplace accidents from hazards	Employee reporting mechanisms rely on access to internal IT infrastructure	Very High	IT outage, employees can't file for unsafe work conditions
Error in code base versions causes project slowness and confusion	Version control processes are not clearly defined including access restrictions	Very High	Intellectual property theft, unauthorized changes to code, changes to prod cause issues
Inability to recover vital company software	Code base does not have a backup	Very High	IT outage, code repo unavailable
Undetected flaws enter the production environment causing issues	QA testing does not follow a systematic process for identifying flaws	Very High	Malware attacks, insider threats, production outage

Risk Mitigation Strategies

Now that our risk assessment is complete, we can choose how we want to mitigate them. Susan Snedaker says in her book *Business Continuity and Disaster Recovery Planning for IT Professionals* that there are four main approaches to mitigating risks: avoidance, acceptance, reduction, and transference.

Risk	Recovery Requirements	Recovery Options	Chosen Mitigation
potential legal disputes and financial losses due to contractual misunderstandings	Restore contract and reform of contractual agreements and employee understanding of those agreements	Create an internal program for employees to learn about contractual agreements, avoid entering in SLA agreements, risk acceptance	**Reduction** – create an internal program to learn about SLA agreements
Unauthorized access leading to breach and financial loss	Reassessment and implementation of stronger access controls	Implement role-based access controls, accept the risk, use 3rd party software for identity and access management	**Reduction** – implement role-based access controls
Inability to recover effectively from a cyber incident due to poor planning	Develop or maintain an incident response plan using experience	Hire 3rd party for planning your incident response plan, train employees on incident response and create a plan	**Reduction** – train employees and create a response plan
Malicious software compromising confidentiality, integrity, and availability of IT resources	Restoration of IT systems to functionality prior to malware infestation	Use a cloud-based security approach like MDE, have the security team maintain security products, accept risk	**Transference** – Use a cloud-based approach to keeping up to date with antivirus
Ineffective recovery from natural disasters due to poor planning	Operations can resume as normal following a natural disaster	Create a business continuity and disaster recovery plan, accept risk	**Reduction** – create a BCDR plan
Loss / destruction of facilities and equipment from natural disasters	Facilities and equipment are restored at least temporarily so employees may continue operations	Purchase insurance for facilities and equipment, purchase back up facilities and equipment, take the chances of natural disasters not happening	**Transference** – purchase insurance on facilities and equipment
Potential employee harm & loss of equipment from fires	Employees are safe and accounted for, and equipment has been restored	Employ fire safety measures and safety protocols, take the risk of a fire not happening	**Reduction** – Employ fire safety measures and protocols
Supply chain disruptions cause operational slowness	Operational speed has returned to normal	Become self-reliant by creating your own supply, acknowledge that supply chain disruptions are a part of the global economy, use multiple suppliers	**Reduction** – use multiple suppliers to avoid disruptions from a single supplier
Compromise of CIA triad due to employee security violations	Employee has been notified and possibly disciplined of violation and CIA triad returns to acceptable level	Accept that employees might make security mistakes, develop a employee training program for security	**Reduction** – Develop a security training program for continuous improvement
Reputational damage due to poor public relationship management	Public trust and reputation have been restored	Use a third party for public relations, employ well trained public relations experts, avoid talking to the public, accept that public relations might not always be the best	**Reduction** – employ experts in public relations
Poor public image because of social media attacks	Public trust and reputation have been restored	Use social media platforms that are good at handling social media attacks, accept that social media attacks happen, avoid using social media and instead only post to company websites	**Transference** – Use social media platforms that are good at handling social media attacks

Leaked sensitive information due to reduction in confidentiality.	Confirmed information leak source is stopped and notify key stakeholders. Confidentiality is restored.	Strengthen data encryption, access controls, and policies involving confidentiality, accept the likelihood of leaked information	**Reduction** - Strengthen data encryption, access controls, and policies involving confidentiality
Compromise of CIA triad due to lack of employee social training	Employee(s) is corrected and learn how to avoid the social engineering attack	Implement mandatory training programs for social engineering awareness, accept that the employees might be vulnerable even if they are trained or not	**Reduction** – implement mandatory training programs for social engineering awareness
Error and employee frustration due to confusing communication	Communication issue is resolved	Standardized communication protocols, use a third-party communication software that has an organized format	**Reduction** – use 3rd party software that has organized format, and standardize communication
Lack of employee operational awareness cause frustration	Better communication on overarching operational goals and how to obtain them is achieved	Periodically assess employees on their understand of operational goals, hire a third party to audit the communication strategy within the organization	**Transference** – Hire a third party to audit and suggest improvements on the internal communication
Inability to recover from loss of IT infrastructure availability causes increased costs	IT availability is restored	Establish redundancy according to industry standards and guidelines, take the risk of IT systems not going offline, hire a cloud service provider to handle the IT infrastructure, perform regular backups	**Transference & Reduction**– Use cloud-based IT infrastructure and perform regular back ups
Employee dissatisfaction and high turnover due to lack of pay	Employee payroll is restored	Switch to a 3rd party provider for payroll operations, create a backup system internally for payroll, accept the risk that payroll might go down	**Transference** – Switch to a 3rd party provider for payroll operations
Increased chance of workplace accidents from hazards	Employees can communicate to HR about workplace safety concerns	Switch to a 3rd party provider for HR portal operations, create a backup system internally for payroll, accept the risk that payroll might go down	**Transference** – Switch to a 3rd party provider for HR portal operations
Error in code base versions causes project slowness and confusion	Code base structure returns to normal	Implement a version control system and use regular code reviews internally, have an auditor conduct code reviews	**Reduction** – Implement version control system and use regular code reviews internally
Inability to recover vital company software	Codebase access restored	Implement code backups internally, use a 3rd party provider that saves the data to the cloud, accept the risk that the code might be deleted somehow	**Transference** – Use a 3rd party provider like Github for code storage
Undetected flaws enter the production environment causing issues	Flaws are hot fixed	Implement robust testing frameworks, accept that there might be errors in your software tests, let a third party do your tests for you	**Reduction** – implement a robust testing framework

Business Continuity and Recovery Plan

While creating the BCDR plan make sure to be implementing the risk mitigation strategies outlined, starting with the ones that are the most known.

Phase 1: Activation

Disruption classifications

1) Catastrophic – Complete failure of business operations.
2) Significant – Major disruptions that require immediate attention
3) Moderate – Disruptions that draws attention, but won't have a sever impact on business operations
4) Minor – Disruptions that do not receive much attention that may be resolved without significant effort from the organization

Communication Plan

Pre-disruption

- Establish communication channels for employees to use during a disaster and while recovering from one.
- Identify key stakeholders
- Develop a contact list for each of the teams and create a contact tree
- Ensure the contact lists are redundant and have and saved to an off-site location

During disruption

- Crisis manager gathers relevant information by assessing the situation
- Crisis manager sends out initial notification via the established communication channel briefly describing the situation, the level of classification, and the teams activated in response
- Crisis manager gives updates to the teams throughout the disruption and contacts new team members if necessary for activation if deemed necessary

Recovery transition trigger

- Communication has been established and is effective
- The necessary teams have been activated
- All disruption is stopped or contained
- Safety of both employees and company assets is assured

Team compositions

Crisis Management team

- Purpose: Manages the overall response to a business disruption by guiding the teams through the event. Manage communication across different teams.
- Activation/Deactivation Triggers
  - Stuff
- Positions & functions
  - Crisis manager – responsible for initial activation and communication across the entire BCDR response effort teams
  - Stakeholder relations manager – manages the media accounts and stakeholder and public communication
  - Finance analyst – Assists by determining the financial impact thus far and what is to come

IT Disaster Recovery team

- Purpose: Restore IT infrastructure and all other platforms required for business operations
- Activation/Deactivation Triggers
  - Activation: IT infrastructure failure due to data corruption, security breach, network or system failure
  - Deactivation: Access has been restored. All IT systems are back to an optimal performance and any cyber security threats have been cleared.
- Positions & functions
  - IT technical lead – responsible for the overall guidance of IT teams and administration of the IT infrastructure
  - Network engineer – Tasked with maintaining network recovery and continuity
  - Database admin – restoring back-ups, and recovery processes involving data
  - ISSM – ensures data security during recovery efforts
  - Help desk – provides user support both internally and externally
  - System administrator – manages system recovery

Facilities Management team

- Purpose: Ensure the safety and security of business facilities before and after disruption.
- Activation/Deactivation Triggers
  - Activation: Safety concerns such as active shooters, fires, natural disasters, or other causes of disruption like stuck elevators or electricity outage
  - Deactivation: Safety is assured and access to facilities has been restored
- Positions & functions
  - Safety officer - Develop evacuation plans and maintenance of emergency systems like fire suppression.

        - Facilities manager - Inspect facilities for potential damages before and after evacuation
        - Security guard - Ensure the continuity of physical security of the facilities

Human Resources Team

- Purpose: Ensure employee safety and well-being, establish communication, maintain compliance.
- Activation/Deactivation Triggers
    - Activation: A disruption affects employees in a way that involves employee safety, or organizational communication is necessary
    - Deactivation: Employee safety and concerns is no longer an issue and communication at the organization level is no longer required
- Positions & functions
    - HR manager: Leader of the HR team and responsible for engaging in communication and ensure employees' needs are being met
    - Training and Development coordinator: Responsible for employee awareness in emergency procedures, safety procedures, etc.
    - Compliance officer: helps to maintain regulator and law requirements during disasters. Example: labor laws

Software Development team

- Purpose: Restoring software products to their intended design after errors have been pushed to production
- Activation/Deactivation Triggers
    - Activation: Errors in the code pushed to production have caused disruption to operations
    - Deactivation: Issues with the production code have been confirmed as resolved and documentation has been updated
- Positions & functions
    - SCRUM master – Works with the team to facilitate smooth recovery and guides efforts to recovery within the MTD
    - Software engineer – Creates emergency software patches to fix errors pushed to production
    - Documentation / dependencies engineer – determines if the software patches worked on could create more issues

Phase 2: Recovery

Recovery checklist (in no particular order)

Assessment of disruption

- Appropriate information has been gathered
- Financial & operation impact analysis completed
- Disruption classification assigned

Communication established

- Initial notification is sent out to team members and stakeholders
- Activations are made based on team activation triggers

Disruption mitigation

- Key IT infrastructure has been restored via temporary fix
- Access to facilities, physical security, and employee safety is restored
- Critical applications necessary to business functions operational
- Data has been recovered
- Errors in production code have been patched

Impact assessment

- Determine if the disruption is still a threat or if any other threats will result from it
- Assess the damages and resources needed to repair
- Document all the damages caused by the disruption

Resource gathering

- Begin gathering the resources needed to repair the damages
- Gather operational requirements need to begin repairs
- Gather timeline information from teams for repairs

Recovery review

- Review documentation of the impact from the disruption and summarize to key leadership
- Use information learned to create new training plans and protocols
- Update BCDR documentation and plans

Phase 3: Business Continuity

Begin workaround systems

Natural disasters: Begin a remote work policy. If using an internal on-prem IT systems to conduct business operations, switch to a cloud provider until the natural disaster is deemed to be over and IT infrastructure and safety are ensured

Supplier disruptions: Begin identifying alternatives for suppliers and engage with them.

Loss of IT infrastructure: Leverage the redundant systems used for case of emergency

Production Code Issues: Roll back to an old patch version while a hot fix is created

Lost access to critical company applications: Transition to a third-party application (cloud) or begin using a temporary application

Implementation testing and training

This plan will be activated regardless of whether a disruption is to occur. Maintenance needs to be done no matter what on a regularly scheduled basis to ensure organizational readiness.

Training

Creation & maintenance of training

- Training and development coordinator is responsible for the creation of new training documents and programs
- Training and development coordinator is also responsible for identifying who is required to take the training
- Training is updated during the same time as maintenance (quarterly)
- Any lessons learned from previous disruptions should be incorporated into new training

Maintenance

Review of BCDR plan

- Review the BCDR quarterly to determine if any changes need to be made because of the following:
    - Updated regulations and laws
    - Changes in IT infrastructure that were made internally (IP address changes, host names, etc)
    - Creation of new best practice methods in certain fields
    - Development of new technology
    - Changes in organizational structure
    - Business process changes

Update documents

- Use results of quarterly review of BCDR to make changes to the BCDR plan
- Only authorized personnel such as the crisis manager can make changes to this plan
- Before any changes are made to the BCDR document, a backup must be made of the old version
- Any new changes to the BCDR documentation will require a version change clearly stated in the document

Resource assessments

- Do an annual review of company resources to determine if any action should be taken
- All resources identified should be accounted for
- Any projects that have been disrupted previously should be identified and an assessment should be made to see if any further resources are needed to continue recovery efforts

Testing

Tabletop exercise

- This type of test will be conducted annually and will be led by the crisis manager.
- It consists of partial activations that simulate real life disruptions
- Results of the tabletop exercise must be documented and will be used to update the BCDR plan during the next maintenance phase
- Testing must meet regulatory compliance

Works Cited

Snedaker, Susan, and Chris Rima. *Business Continuity and Disaster Recovery Planning for IT Professionals*. Amsterdam ; Boston, Syngress, 2014.