Disaster Recovery Learning Objects

Christopher Winter

Athabasca University

COMP 601: Survey of Computing and Information Systems

Instructor: Richard Huntrods

March 23, 2024

Contents

Introduction to Disaster Recovery

This learning series will focus on Disaster Recovery procedures step by step. Disaster Recovery (DR) starts from high-level discussions among executives and high-level management about important Business Services the organization offers. These business services are key to keeping business flowing as quickly as possible in the face of a disaster. The efforts to design, implement, and test a Disaster Recovery Plan may one day prevent serious harm to any business that would have otherwise been a fatal blow to an organization.

In some areas of the world, DR plans are mandatory for organizations and businesses to establish to comply with the law. Most organizations have an Information Technology Disaster Recovery (ITDR) plan because Information Technology (IT) has become a more important and vital role in most organizations. These ITDR plans enable organizations to recover quickly, mitigate risks, and have higher up-time or availability.

Technologies in Virtual computing and Cloud computing have allowed for disaster recovery to become more accessible for organizations worldwide.

Create an Organizational Policy

With any project, you need to create a policy with clear guidelines on what you are trying to achieve. A policy is like a project charter. At the high level, you need to figure out a few key pieces of information that you can use throughout the project. In this process, the

business owner or CEO takes charge and commits to the plan. The plan will require time, resources, and money to develop and implement. Therefore, top management officials need to be on board fully with the plan (Fallara, 2004). It is important to have a few things in place in this step.

A. The organization will need to figure out who is going to sponsor this endeavor. This will depend on the size of the organization or business. A business with 30 people will have a different plan than one that has 3000 employees. In this step, it is suggested that the CEO or Business owner sign off on this policy because it is a business decision. The ITDR plan can have a lasting effect on the overall health of the organization in the event of a disaster.

   At this time, you may also assign a Disaster Recovery Leader or manager who will lead the process from a technical perspective.

B. The second consideration for this policy is to determine what the plan is going to achieve. At a high level, a description of what the plan will achieve should be written out. This will determine some of the tangibles that the project is accomplishing. This statement of what this plan will achieve should be thought of as goals.
C. Another important consideration at this phase is who will be involved in this plan. This is part of the planning for the project that will involve those who come on board to make this work.

Select Teams and Determine the Responsibilities

In this section of the project planning phase, we will discuss the importance of Team selection. While selecting the teams that will handle the different work of the project, you need to bring people in from all over the business, including management, operations, resourcing, human resources, and IT staffing. It is important to include the whole business throughout the project for information gathering and business continuity planning. Without proper input throughout the organization, you may miss out on necessary key components that are necessary to conduct business.

Business Impact Analysis

The Business Impact Analysis (BIA) is a critical part of the plan to protect assets. A BIA is a systematic approach to identify, quantify, and prioritize the potential impacts that various disruptions could have on your business or organization (Business Impact Analysis | Ready.gov, 2023; Oro, 2024). The BIA is used to assess the different scenarios that could occur and then identify the potential of those threats occurring. Lastly, the BIA outlines these potential scenarios and ranks in a manner that would assess their impact on the business. The BIA is used by RISK managers and cybersecurity personnel to gather information and assess the risk to an organization's core business processes.

There are a few steps to gather information and analyze the information in the Business Impact Analysis.

- Identify business priorities.
- Identify the risks.
- Assess the likelihood of a risk.
- Assess the impact.
- Prioritize resources.

Identify the Business Priorities

All businesses have priorities that ensure that the business functions. In this step, you need to look at identifying the business processes that make the business function. Begin by gathering critical business functions from people all over the organization. You want to gather as many different business functions as possible that help the organization meet its goals. You can ask people from different departments what the core business functions are to get a well-rounded list of the various functions of the business to move forward with.

Identify the Risks

The next round of information gathering for the business will be to identify the risks. The risks include areas both of natural occurrence and human caused. The natural risks include things like natural disasters such as earthquakes, hurricanes, tornadoes, storms, wildfires, and floods. Some human-caused risks may include terrorist attacks, government espionage, and criminal activities. Viruses and cyberattacks can also cause risks to organizations that can be crippled. There are also risks in the service and supply sectors to

the business. If you lose internet, or there is a power failure your organization will be affected. One organization will differ from another, and the risks may even be different in a larger organization with many offices in different geographical and geopolitical locations.

Record the risks on a Risk assessment form below Figure 1.

Risk to the Organization	Likelihood	Impact
Wildfire		
Building fire		
Earthquake		
DDoS attack		
Cyber event ransomware		
SAN failure		
Cyber event user data stolen		

Assess the Likelihood of a Risk

All different types of risks to your business need to be accounted for and prioritized on a scale of 1 to 5, with one being the least likely and five being extremely likely. Begin by using the chart given in Figure 1 and go through the chart and assess the likelihood the risk will have on the organization and come up with each of the risks identified.

In the second column, you will go through the list and write what the likelihood of the risk is going to occur. The likelihood of the risks is usually based on whether you know that the risk may occur. On a scale from 1 to 5 you will assess the risks:

1. Improbable – very rare, most likely will never occur.
2. Unlikely – less likely to occur than it is to happen.
3. Possible – this is just as likely to occur as it is not to occur.
4. Likely – we expect this to occur. It would be surprising if this never happened.

5. Almost certainly - There is almost no chance this will not occur. Will certainly occur within the next year to three.

This scale was acquired through the BC Government Disaster Recovery Plan from 2017 found here.

Assess the Impact

Next, we assess the impact this business process has on the organization. The impact assessment will gauge the impact the interruption has on the business achieving its goals. The impact assessment is also on a scale of 1 to 5 .

1. No Significant Impact – No significant impact beyond the regular duties of the ongoing operations.
2. Minor Impact – This will impact the organization from an administration level but will have a very minor disturbance on the organization achieving its goals.
3. Significant Impact – This is where the organization must stop providing services until an event is complete. This affects multiple departments and will require a coordinated effort to bring things back to an operational level.
4. Major Impact – This is where business processes are affected and cannot be fixed without a change in the delivery of service. Rework of the method of delivery is required.
5. Catastrophic impact – The organization takes a major blow and will result in significant damage to the credibility and integrity of the organization. There will be a loss of the ability to offer the services previously offered.

Prioritize the Resources

Once a Risk chart has been completed with the Risks to the organization and the likelihood and the impact assessments have been completed, we move on to chart the information gathered. In the chart below, a organization has completed their risk assessment. Now we will move those risks onto the graph below to show what are main risks are.

Risk to the Organization	**Likelihood**	**Impact**
Wildfire	2	3
Building fire	2	4
Earthquake	1	4
DDoS attack	3	2
Cyber event ransomware	2	4
SAN failure	3	3
Cyber event user data stolen	1	3

Use the chart you have created to put the different items on the risk matrix chart.

Likelihood	5	Low	Medium	High	Extreme	Extreme
	4	Low	Medium	High	High	Extreme
	3	Low	Medium DDos att.	Medium San failure	High	High
	2	Low	Low	Medium Wildfire	Medium Building fire CE Ransom	Medium
	1	Low	Low	Low CEStoleData	Low Earthquake	Low
		1	2	3	4	5
	Impact					

This chart will show you what to prioritize as extreme, high and medium risk items compared to those that will be low on the scale. This allows the business to prioritize higher risk items in their disaster recovery and perform some mitigation work.

Identify Support Functions for the Business

When we think of risks to our business, it is important to consider the possibility of not being able to carry out the core functions of the organization to reach its goals. Those core functions might be the ability to sell items online or to provide a service. These core business functions are supported by a range of services. We call these services the support functions of the business. Support functions are made up of anything that is required to support the function of the business. Information Technology (IT) supports most of the business functions.

During this step, we want to list the support functions the business maintains for the operational goals of the organization. List the critical services that will be needed to keep the business core functions working towards the organizational goals. These services may include areas like internet connection, database functionality, file servers, email, servers, switches, domain controllers, and many others. All services you have in place for your business or organization to keep it moving towards its goals should be included in this list.

Once the list has been created, it should be arranged in an order that prioritizes the services that support the main business functions. These high-level services should be acknowledged here to prioritize the necessary services the business needs over the nice-to-have services.

Two key features need to be discussed for each of these business services. The first is the Recovery Time Objective (RTO) and the second is the Recovery Point Objective (RPO) (The Difference between RTO & RPO, n.d.).

The Recovery Time Objective (RTO) is required to show how long the organization is willing to go without the service (The Difference between RTO & RPO, n.d.). The RTO sets the maximum time that the organization can wait until the service comes back online. This helps to determine realistic and achievable goals for an organization to strive towards.

The Recovery Point Objective (RPO) defines the point in time at which the data must be restored after a disaster. This will assess the criticality of the data, the regulatory requirements surrounding the data, and the acceptable level of data loss the organization is willing to tolerate. If the organization is only willing to lose twelve hours of data, the mitigation effort to collect and duplicate the data will have to be performed every twelve hours at a minimum. If the organization needs to ensure that the RPO is a small number, the more it will cost the organization to implement the plan.

When the organization combines the RTO and the RPO, the organization gets a detailed description of when the services need to be operational and how far back the information for each system is acceptably recoverable.

Implement Mitigation Strategies

Mitigation strategies are completely dependent upon the risks that an organization may face. Information Technology Disaster Recovery (ITDR) mitigation strategies are different

between organizations. Mitigation strategies are completely based on risk and risk assessments toward organizational goals and objectives (Heinz-Peter, 2010).

If you live in an area with lots of storms and potential power outages, you will want to ensure you have an alternative source of power to mitigate the risk. Downtime and business interruption can make an organization suffer data loss and bring organizations to a sudden halt without mitigating the risks.

In this stage, we look at the IT systems that run the core business processes. There is a need to implement redundant systems and backup mechanisms to protect the business in case of disaster. The organization will want to implement redundancy in most of its core systems. This can be done by always-on secondary solutions, or by backing up systems incrementally and having the ability to turn on a backup with a small amount of data loss from a few hours ago.

In this stage of the process, there is a need to decide on what to back up, how often to back it up, and if you need concurrent systems in place for automatic failover.

These services will add a cost to the organization for implementation. These costs add up quickly if you want a high level of service. For most organizations, the cost/reward analysis will need to be completed at this point. If you want a second redundant server, the organization will have to pay the upfront cost to double that system. If you want backups off-site in the cloud you will need to pay for each megabyte or gigabyte depending on the tier of service that the organization is willing to pay for. These factors will need to be addressed to implement the plan.

Create Activation Plans

Activation plans are going to be specific documents that will outline the process from the threshold event that started the disaster start of the disaster to the restoration of the IT service and including the post incident meeting. This plan will guide the ITDR recovery team leader and the recovery team through actions that will be able to bring back disrupted services.

Activation Trigger

There needs to be a sequence of events during the creation of the activation plans. First, there needs to be conditions or events which will activate a plan. This is usually called the activation triggers (B.C. Government, 2017). The triggers that could occur may be a natural disaster like an earthquake or a flood. The human-caused triggers may include a cyber-attack or ransomware against an organization. These events will cause a significant risk to the organization.

These activation triggers may have different effects later in this process. It is a good idea to organize these action triggers in a way that the organization can follow the trigger to a response.

Establish Communications Protocols

Once an Action is triggered a communication protocol must be in place. Therefore, there is a need to set up a communications protocol. A communications protocol is used to notify key personnel that the action plan has been activated. This list should also include outside

support and infrastructure vendors that may need to be contacted during the climax of the event.

To plan for the communication protocol an organization may want to have multiple methods of communication in case one of the methods is disrupted by the event. If your method of communication is email and the email server is down, then you will need a backup method to communicate such as cell phones or a satellite phone.

Some methods discussed for communications are Microsoft Teams with predefined groups, emails with email lists, and phones with email trees that include cell phones, work numbers, and home phone numbers of key personnel.

It is important to include a list of contacts whom the organization can contact in case of an emergency. This should include members of the Disaster Recovery Team, the vendors the organization uses for support, executives, insurance agencies, employees, and lastly a method to inform customers if relevant.

Recovery Team

The action plans should include those who will be responsible as recovery team members. This may include different people for different activation triggers. This phase of planning will outline who is responsible for activities during the activation phase. For example, who will be the recovery team leader, and who will be part of the technical team that will run the technical side of the recovery? This list of team members should also include a communications team element to confirm who will be responsible for communications internally and externally as required.

With some of these tasks being technical in nature, certain technical personnel will be part of many recovery teams and others may only be part of a single recovery team for one specific activation trigger. Therefore, different recovery teams may be implemented for different activation triggers depending on the technical skills needed for that recovery.

Activate the Recovery Procedure

This part of the plan aims to gather information to assess the extent to which the organization has had a disruption or disaster. When a disaster happens the recovery team leader will ask their team to gather information quickly according to assess the extent of the disaster. The recovery team will have to gather specific information based on different action triggers. The information required to be gathered should be predetermined and written as part of the action plan for a specific incident. This should be the basis for which the recovery team leader should be able to start the action items in the plan. Gather information to show the extend to the damage.

Write out the plans

There needs to be action plans in place when disaster strikes in order to restore service levels for each of the action triggers. There needs to be action plans that will be written out to restore services that the recovery team can follow. These written-out tasks may include procedures for situations like:

- Bringing backup systems online in a virtual state.
- Bringing backup systems online in the cloud.
- Restoring data from a backup.

- Restore services from natural disasters at a backup location.

Monitor the activities.

While the action plans are being carried out by the recovery team, there needs to be a process in place to monitor the activities of the recovery. As previously mentioned, there needs to be clear communication back to the recovery team leader, and from the team leader back to the rest of the recovery team. A clear path of communication may be different than discussed above, however, there needs to be a clear communication method pre-determined in the action plan.

An option is to have pre-determined team meetings to discuss steps that have already been taken and to delegate directions moving forward to have a clear understanding of all. Having meetings at intervals will allow the recovery team lead to gather information, reassess the situation, and realign staff if needed. This will keep team members informed of the overall status of the recovery. The team lead can then pass along the updated status of the recovery to the executive.

Test the Restored Function

Once all the services have been restored, it is important to confirm that they are working as expected. Begin by going through a series of tests to confirm the restored systems are operating the same as before.

Restore Normal Operations

Once the event is complete, normal operations can be restored. Sometimes this will occur during the event, however on other occasions there will need to be longer mitigation issues

that will need to be resolved before being able to put a whole system back into normal operations.

Review and Reflect

The activation event was actioned upon, and the event is now complete. The organization will participate in a post-incident evaluation. This evaluation should include what was successful, what was unsuccessful, and what can be improved upon. This discussion should include all team members. The information collected in the post-incident phase should be used to change and update the policy if needed.

No disaster recovery plan is 100% accurate. There are always ways to improve on these plans and update them with the advancement of the organization, its goals, and the technology available to the organization.

Exercise and Test the Plans

In this section of Disaster Recovery planning, the Disaster Recovery Team must perform a version of the written plan to test if it works. The plan exercise and testing phase can be done in a sandbox configuration to confirm the process and written-out procedures work.

Exercises should be done at regular intervals to ensure the strategies work and to provide training to the disaster recovery team in the event an activation trigger is triggered for real. Most insurance companies for IT-related businesses require the Information Technology Disaster Recovery (ITDR) plan to be tested yearly to be able to ensure favorable insurance rates.

These plans and exercises should be pre-planned, timed, and tracked throughout the duration of the exercise. It is important to allow these exercises to be as life-like as possible. When possible, the exercises should be spontaneous for the recovery team to see the outcome of the actions required to meet the desired goals.

The exercises and trial runs of the plans should be timed to show that the organization can meet its goals. This is a crucial testing phase to witness firsthand how the activation trigger and subsequent recovery plan processes work in real-life situations. When these plans are exercised in this testing phase, the process written out is performed exclusively which tells us if there are problems with the plans. It can also work out any old information that may no longer be relevant due to system changes that were not altered when systems were updated and changed.

The exercise test can fail. It is ok for it to fail and have a failed process during this phase. It is ok to fail in not meeting the timed outcomes. It is better to fail during the testing cycle than in the event of a real threat.

If the process that was planned is flawed, then the process that failed will need to be examined, reworked, and retested. It is very important to look at the process and work out the troubled areas and fix them during this testing phase. This is important work that will save an organization time and energy during a disaster event they might not have.

Another area where a test can fail is in the recovery time objectives. If the test fails in the Recovery Time Objective (RTO) or the Recovery Point Objective (RPO), there will be a need to modify the Disaster Recovery Plan. There are a few ways to change the plan and how it

functions. The recovery plan leader will need to either change the way the mitigation pieces have been implemented, or they will have to change the action plan to meet the desired goals. These are both technical functions of the plan which will need to be changed to meet the time requirements.

Ongoing Changes and Maintenance of the Plans

All things in our world change over time. Benjamin Disraeli said “Change is inevitable. Change is constant.” As organizational systems change so will the disaster recovery plan. As part of an organization’s change management procedure, the disaster recovery plan should be updated at pre-determined intervals or as the change occurs. If there is a major change to a major system, the disaster recovery plan should be updated immediately. However, for systems with low risk, and low impact, these updates to the disaster recovery plan should be carried out at least once a year at a minimum.

Ongoing Changes

Ongoing changes to the Information Technology Disaster Recovery (ITDR) plan should be made on systems that fall into a medium to extreme risk to the overall goals of the organization. The organization will want these systems immediately brought into mitigation strategies with activation plans included in the ITDR plans.

Maintenance of the Plans

The maintenance of the ITDR plan should be done yearly to confirm the documentation is up to date with relevant information. The maintenance should include reviewing and updating:

- Risk assessments.
- Team members.
- Contact information.
- Mitigation strategies.
- Activation plans.
- Test plans.

In doing this review and maintenance on this critical document the ITDR Plan, an organization will be ready for a disaster when it strikes.

Major review

The last item to discuss in this section on ongoing changes and maintenance of the plans is that of a major review that goes beyond the scope of regular maintenance. A major review or revision of the ITDR Plan should come if the organization changes its strategic goals. Laura Saalmuller suggests executives should update their organization's strategic goals every five years. With that in mind, there should be a major review if something changes in the organization that is a major change to the way the organization does business. This may include changes that are done on the business process side of things, or it may include a shift in the way IT delivers its resources or mitigation techniques. During

any of these major changes the organization is going through, the ITDR plan should be re-evaluated from start to finish. This will ensure the IT Disaster Recovery plan is up to date with business processes and the technology that supports the organization to get the processes done.

Conclusion

Information Technology (IT) has become an integral part of organizations and businesses to provide their goods and services to meet their strategic goals. The risks associated with not being prepared for an IT related outage or disaster grows as more organizations digitize their workflow and processes. We are in a world that provides a consistent number of natural disasters besides the number threat actors who try to steal data and cause cyber security events. It is essential that organizations take the time to assess their reliance on IT services and develop a Disaster Recovery plan to help in the recovery of the organization when disaster strikes. The question is not if a disaster will strike or not, the question is when a disaster strikes, is the organization going to be ready to respond. This will greatly help in reducing the core business process downtime and help maintain data integrity.

References

(2017). Disaster Recovery Plan [Review of Disaster Recovery Plan]. In https://www2.gov.bc.ca. BC Government. https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/defensible-security/2017-04-18_--_drp-servicename-template.docx

Business Impact Analysis | Ready.gov. (2023, September 7). Www.ready.gov. https://www.ready.gov/business/planning/impact-analysis

Fallara, P. (2004). Disaster recovery planning. *IEEE Potentials*, *23*(5), 42–44. https://doi.org/10.1109/mp.2004.1301248

Heinz-Peter Berg (2010). Risk management: procedures, methods and experiences. Reliability: Theory & Applications, 5 (2 (17)), 79-95

Oro. (2024, February 21). Your comprehensive guide to a business impact analysis (BIA). Thoropass. https://thoropass.com/blog/compliance/business-impact-analysis/

The Difference Between RTO & RPO. (n.d.). Rubrik. https://www.rubrik.com/insights/rto-rpo-whats-the-difference

Saalmuller, L. (2022, December 20). Who's Responsible for Strategic Planning? | HBS Online. Business Insights Blog. https://online.hbs.edu/blog/post/who-is-responsible-for-strategic-planning

Setyawan, A., Giri Sucahyo, Y., & Gandhi, A. (2020, November 1). *Design of Disaster Recovery Plan: State University in Indonesia*. IEEE Xplore. https://doi.org/10.1109/ICIC50835.2020.9288543