

Help Desk Calgary – April 16, 2003 Luncheon

Discussion Summary

Topic

The objective of the luncheon session was to provide a “round table” discussion forum for members to talk about Contingency Planning for the Help Desk.

Facilitator

The session was facilitated by Ron Yarwood, past president of Help Desk Calgary and Executive Director of Support Excellence Inc.

Discussion

Agenda

An agenda was set out to guide the discussions.

- Rationalizing Procrastination – why we can’t or don’t do Contingency Planning
- Risk Analysis
- Business Impact Analysis (BIA)
- Creating the Plan
- Implementation
- Testing the Plan
- Returning to Normal
- Regulatory Requirements

What Constitutes a Disaster?

A disaster is any event that puts the quality and consistency of your help desk service at risk. We tend to think of Contingency Planning as being required for the major event like:

- Earthquakes
- Floods
- Tornados
- Ice Storms
- Explosions and other earth shattering or headline grabbing events

There are few natural disasters in Calgary, and we have some of the best infrastructure in the world to support our business. Do we need to worry about Contingency Planning?

The answer is Yes, and 7 of the 10 companies represented at our meeting have some level of Contingency Plan in place. And, some companies have had to implement their plans over the last few years as a result of things like:

- The World Petroleum Congress when access to some downtown buildings was restricted.
- Same with the G8 Summit.
- HP talked about having 197 people sent home from their Toronto Help Desk because 2 people at an office event came down with symptoms of SARS and the rest had to be quarantined.

It can happen to you! If it does, you need to be prepared because Help Desk is the front line for technical support, either within your business or for your external customers (as in the case of HP). If the unexpected happens, you need to be able support your critical applications that ensure the business keeps running during the emergency.

Rationalizing Procrastination

Rationalizing procrastination is finding the multitude of reasons why we can't or won't take the time to plan for disaster. Some of the favorite reasons for postponing the Contingency Planning process are:

1. Executive Support – there just isn't enough of it.
2. Too Busy – we see the need to plan for disaster, but we just don't have time....
3. No Budget – as with time, we don't have the dollars to spend on a planning project.
4. Planning for disaster is like planning for your own funeral. You never quite get around to it until it happens, and then it costs a fortune because you're vulnerable.
5. Calgary doesn't have history of disasters, so why bother with a detailed plan?
 - a. We're not just talking about "disasters". A Contingency Plan is for any event that causes prevents us from performing our day-to-day duties.

Resources

There are plenty of books that have been written on how to sell Contingency Planning to management. The first step is to find a champion at the executive level who will back the project and sell it to the rest of the management team.

Risk Analysis

The first step in Contingency Planning is performing a risk analysis of the types of events that may cause the plan to be enacted. Once the risk of external possible external events are analyzed, the next step is to analyze the criticality of the systems and infrastructure that supports the Help Desk to determine what is critical to restore to enable service provision during the emergency.

There are several factors that need to be considered when looking at risk:

- Probability – what is the likelihood of the risk type occurring?
- Predictability – how easily can a particular risk type be predicted (e.g. a planned event like the G8 Summit is planned years in advance, whereas a flood or explosion will have little or no warning).
- Severity/duration – Define how severe each risk type is to your business and how long the risk event is likely to last. For example, a complete power outage can bring all systems and supporting infrastructure for your business to a halt, but will likely only last a few minutes to a few hours. An explosion or fire in the Help Desk could keep you away from the normal working environment for weeks/months at a time. In either case, how would you continue to operate?
- Speed of onset / forewarning – As with severity, how much forewarning would you receive for each risk type? If the risk is a toxic spill from a railway car downtown, businesses close to the railway tracks would be affected immediately. Businesses that are located away from the tracks may be affected later depending on the volume and toxicity of the spill.
- Vulnerability – you need to assess how vulnerable you are to each risk type. The risk of earthquake in Calgary is quite low compared to San Francisco or even Vancouver. The risk of fire or theft is relatively equal in all major business centres.
- Prevention – what can we do in our current environment to prevent as many risk types as possible from happening at all? The old adage, “an ounce of prevention is worth a pound of cure” is very applicable in Contingency Planning.

What Help Desk Services Are High Risk?

1. Telephone Systems

The telephony system is the life-blood of the Help Desk. Even though the industry is moving to a “contact centre” model where the customer can contact the Help Desk using email, web chat, fax and other methods to contact the Help Desk, the telephone is used 80% and more of the time. This is especially true when an emergency arises. The telephony system (PBX or key system) is the most critical link between the customer and the support team.

If telephone systems are not available, some options for continued service are:

- b. Leave the phones on “Night Service” where the customer is sent to voicemail.
- c. Transfer the calls to a cell phone (either at the PBX or directly from the Telco’s central office) to enable calls to be answered remotely.
- d. If the capability exists, have agents dial in to the PBX from home and use their home PCs to provide service.
- e. Have a Help Desk backup site available, either as a “Hot Site” that is reserved in case a disaster strikes, or use a second site within the company (usually reserved for the largest companies) to take over the calls for the centre where the disaster has occurred.

2. IVR/ACD

If the Help Desk has an IVR or ACD, these systems should also be classified as critical to the operation of the Help Desk. The IVR or auto attendant in the ACD can be used to provide announcements of the problem and expected duration, thereby alleviating the Help Desk of having to answer calls from people who are simply wondering what is going on. The IVR can also provide self-help options for customers during the emergency period.

What Help Desk Services Are Medium Risk?

1. Problem Tracking

The problem tracking system is the core of our ability to capture problems, dispatch and track them, and document problem resolutions. However, in the event of a disaster, the ability to track and report is less critical than the ability to talk to our customers. Help Desk analysts can take notes manually and update the problem tracking system later if required. You must recover the phone capability immediately. Problem tracking can be recovered afterwards.

2. Chargeback

For a Help Desk with external customers, the chargeback (billing) system is of high importance. However, calls can be tracked and bills issued manually during a crisis. For an internal Help Desk, the chargeback mechanism can be suspended throughout the event.

Levels of Disaster

When evaluating risk in the event of a disaster, there are 3 things that you can do:

1. Remove the Risk

- a. Once a risk element has been defined, find ways to remove the risk. For example, if the raw power to your server farm is inconsistent and causes power spikes, the purchase and implementation of a Universal Power Supply (UPS) with enough battery supply to keep conditioned power supplied to your computing equipment to smooth out power bumps and provide sufficient battery backup to withstand typical power outages. A UPS will also allow you to gracefully shut down non essential systems in the event of an extended power problem.

2. Reduce the Risk (policy/procedures)

- a. Where a risk element cannot be removed, develop and implement policies and procedures that will reduce the risk when it does occur. For example, if the risk is from internal employee vandalism, implement strong policies regarding company computing infrastructure usage and the tools to monitor and manage policy compliance. These policies and procedures, in conjunction with proper management tools, provide the incentive to avoid potentially harmful or malicious events from occurring within the company.

3. Accept the Risk

- a. There are some risks that, upon evaluation, are not worth the cost or effort to either remove or reduce. For these risks, the company agrees that they will

bear the cost of dealing with the risk if it should occur. Often, insurance may be taken out to offset the potential cost of recovery. For example, in Calgary the risk of earthquake is very small, as compared with the risk of fire, flood or power interruptions. A company may consider a minimum amount of insurance to cover the results of earthquake in Calgary but not try to protect itself in other ways because the risk is so small. In Vancouver or San Francisco, the same company might do more to reduce the risk by occupying a building designed to withstand an earthquake or other risk reducing strategy.

When Do You Declare An Emergency?

SLA Checkpoint

Emergencies are often declared as the result of a Service Level Agreement targets based on the severity and impact of the incident in question. If a serious event occurs, the SLA will initiate a time monitoring process during which escalations occur while the issue remains unresolved. As more time is consumed, the Contingency Plan may be initiated.

Options for handling a critical event may include:

- Putting phones on “night service” where calls are routed to voicemail or a cell phone.
- Agents may be asked to work from home (where the capability to take calls in a home office exists).
- Agents may be sent to a “Backup Site” or hot site that contains infrastructure to receive and handle trouble calls when access to the main office is not available.

Business Impact Analysis (BIA)

What Is It?

The Business Impact Analysis (BIA) is created as a result of the evaluation of the impact of losing any of the people, processes or technologies that support the Help Desk. Each element is evaluated for the value of recovering the service against the cost of maintaining an alternative service delivery capability in the face of a major outage or other event.

The Business Impact Analyst should contain:

- **Philosophy**
A statement of the company’s approach to handling a critical event and the importance of Help Desk recovery to the business
- **Mission**
A statement of the mission of the Help Desk, and the overall business. All the actions and decisions regarding the scope of disaster recovery should be measured back against the company and Help Desk mission statements.

- **Requirements**

In the case of a disaster or the initiation of the Contingency Plan, what are the base requirements to ensure that the business continues to function and survive the event? Issues should be considered against the following principles;

- Relate to cost/time – Use the Risk Analysis to define what will be recovered and how long the recovery will take.
- Impact – Define the impact of the service or affected people, processes and technologies on the business and recover as required. You need to determine:
 - i. How long can you go without the Help Desk
 - ii. Costs of the event, both hard and soft costs.

- **Business Relevance**

- The BIA musts reflect the needs and strategic requirements of your business. What's right for Company A may be inconsequential to Company B

- **Scope**

- Plan for most realistic occurrences of outages in your environment
- The Help Desk needs to work with business that you're supporting to plan for disaster.
 - Impact on Internal/External customers
 - Contractual requirements for service delivery
 - Consider any financial penalties that may be incurred as the result of an extended service interruption.
 - Availability SLA (Internal) – what have you committed to?
 - Force Majeure – acts of nature are usually considered as beyond the control of the service provider. However, be aware that invoking a Force Majeure clause does NOT relieve liability.
 - Not having a plan is not an excuse
 - Tied in with Business Disaster Recovery Plan (Contingency Plan) – Help Desk is usually part of the broader plan.

Other Considerations

- **Regulatory Requirements**
 - Is your company publicly traded? If so, what types of plans are you obligated to have in place?
- **Financial commitments** – can drive the requirement for Contingency Planning.
- **Partners Plans**
 - If your partners have Contingency Plans, you may have to develop plans to mesh with the partners' requirements.
 - Your partners may require you to provide contingency plans as a term of the business relationship.
 - Internal or external SLAs may require a Contingency Plan and escalation process is in place.
 - Financial penalties for non-availability may be significant enough to require a Contingency Plan be put in place.

Contingency Plan Development

The BIA requires that a Contingency Plan be prepared containing the following elements:

- Scope
- Team
 - Staff roles and responsibilities
 - Vendors' responsibilities
- Checklists to determine the sequence and timing of tasks to be performed.
- Timing and cost of planning.
 - Some plans as are inherent in current business practices
 - These plans should be referenced by the Contingency Plan
- Gradual implementation
- Cost Estimates:
 - You can base the amount to spend on a Contingency Plan as a percentage of the Information Technology budget as follows:
 - 4% Entry Level – This is the industry standard and usual benchmark.
 - 6% Best Practice – For those companies who want to be seen as being in the forefront of the industry.
 - 10% Financial – where there is a significant financial impact of loss of service.

Implementation

Once the Contingency Plan has been developed, it should contain definitive criteria for declaring a disaster that will trigger the implementation of the Plan. The Implementation Plan should contain:

- A plan of when to declare a disaster.
- A definition of the impact of the event on the business
- Timing of escalation. Is this a slow motion disaster?
- Interim Call Handling (ICH) procedures.
 - How can calls be handled in the interim period before a full implementation of the Contingency Plan is declared?
- Real Time Minimum Operation (RTMO) – what is the minimum operations that can be tolerated?
- Should Help Desk be restored prior to systems if both are affected?
 - E.g. do the phones first – people want to hear a voice on the phone when they call.
 - Other contact methods later or not at all depending on the BIA results.
- Strategies
 - Drive out disaster scenarios on paper – plan for the worst.
 - Use of analog phones – no power required if the event is a major power outage.
 - Implementation of a UPS to survive brief (1-2 hour power outages) or a generator to survive unlimited power outages.

- Use tools such as PC Anywhere from home to access critical company systems.
- Pre-test any infrastructure or procedures before a real disaster.
- Determine real power needs and plan backup accordingly.
- Contingency Planning and Implementation is neither cheap nor easy. However, in the event of a disaster, it can make the difference in the company's survival.
- Everyone must know their role in the Contingency Plan, from senior executive to front line staff.
- People priorities should take precedence.
 - Consider the personal needs of the staff. They will be under a lot of stress in the event of a disaster, and their creature comforts are of utmost importance to allow the staff to perform in these conditions.
 - Stoke the home fires – make them comfortable.
 - If people stuck in an office as a result of an event.
 - Make sure they have lots of
 - Food
 - Lighting
 - Cash
 - Emergency Kit
 - Provide transportation for staff as required.

Testing

There are four types of testing for a Contingency Plan. Choose the tests that you require to prove the plan and practice so that the plan can be executed under stress.

- Simulated Input Evaluation (Talk Through) – prepare an event on paper and talk the process through.
- Physical Verification (Walk Through) – prepare an event on paper and physically walk through the plan.
- Evacuation (Backup, Hand Over and Walk Out) – Perform all the technical planned tasks and walk out of the building to test the plan.
- Full Function Tactical Evaluation – Implement the plan fully, including making people and facilities un-available and the initiation of “hot site” facilities.

Return to Normal

Take the time to test the processes for returning to normal after the disaster has been completed. Ensure that any data captured during the tests can be restored in the production environment and that the Help Desk environment runs as planned once fully restored.

Conclusion

We ran out of time again, but covered the basic tasks for performing a Contingency Plan. There are lots of books about Contingency Planning for further information, and some web sites that can provide basic information. Contingency Planning is something that every Help Desk should do. Make sure you can recover when a major business disruption occurs.