

WHITE PAPER

Disaster Recovery and Business Continuity in the Contact Centre: Sweat the Plan or Bleed the Business

Sponsored by: TELUS

Jim Westcott

Sebastien Ruest

Lars Goransson

May 2007

IDC OPINION

The contact centre, when it is part of the sales and marketing function of a business, is a critical source of competitive advantage for attracting and retaining customers. A key requirement for establishing and maintaining this competitive advantage is managing the risks and threats that can interrupt contact centre services. Disaster recovery and business continuity in the contact centre is of vital importance because it safeguards a business' most important asset – its customers. Part of what makes disaster recovery and business continuity in the contact centre difficult is the number of vulnerabilities and potential points of failure. The contact centre is exposed to safety risks associated with natural hazards resulting from natural or environmental phenomenon as well as non-intentional, human-induced hazards resulting from human error or system failure. There are also security threats based on intentional human induced hazards resulting from crime, acts of disobedience, war, and terrorism. These risks not only impact people, processes, and technologies in the contact centre, they also impact facilities (buildings and amenities) and infrastructure systems (electricity and telecommunications).

It is difficult to overstate the impact of disasters on the operations of a contact centre. Customers will often seek assurances that their suppliers are accessible and continue to provide services despite the occurrence of a natural or human induced disaster. Most businesses are aware of the dangers that can impinge business operations; however, a significant percentage of these businesses are courting disaster by underutilizing disaster recovery and business continuity planning, implementation, and management services. For example:

- ☒ In a recent IDC survey, only 25% of survey respondents (business and IT executives) indicated that their business had a disaster recovery/business continuity plan and that it was regularly tested.
- ☒ Survey results indicated that, on average, respondents allocated approximately 3% of the IT budget to disaster recovery and business continuity.
- ☒ The same group of respondents believed that the appropriate level of spending on disaster recovery and business continuity should be in the 6% range – a percentage point difference that is two times higher.

IN THIS WHITE PAPER

This IDC white paper explores the issue of disaster recovery and business continuity (DR/BC) in the contact centre. IDC research indicates that a significant proportion of Canadian businesses have underdeveloped DR/BC plans and that current levels of spending on DR/BC fall below optimal levels. As an introduction to DR/BC in the contact centre, this white paper examines the risk factors that threaten contact centre operations, it identifies strategies for categorizing risk factors, and it investigates ways in which risk can be mitigated. The paper also highlights the various sourcing strategies available to businesses as a means of finding the right balance between internal and external resources, capabilities, and management options.

SITUATION OVERVIEW

Current Business Challenges

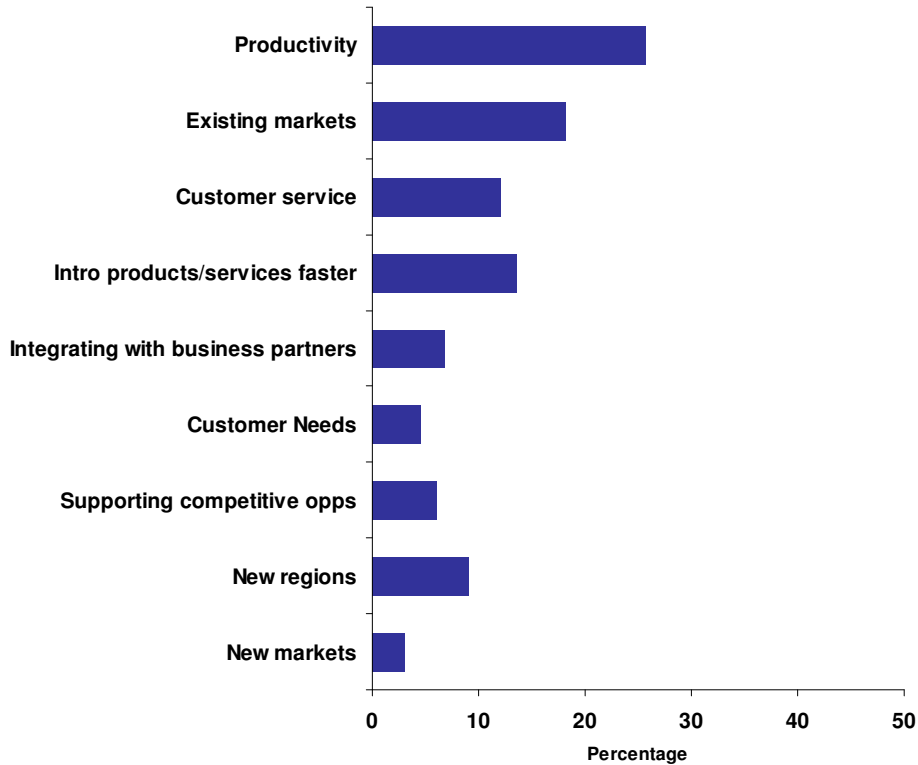
Canadian businesses are consistently challenged by one issue: productivity. This has been the top rated issue for Canadian businesses for a number of years. Productivity gains result from a combination of new technology implementation and personnel development, and commitment on the part of both managers and employees. In the case of the contact centre, where people issues are still paramount, productivity enhancements are supported by information technology solutions based on changes to internal processes and methodologies. Ultimately, the key to productivity measurement is output per worker (based on revenue) per hour worked. Central to the importance of productivity is aligning internal processes and procedures with customer requirements and demand. This is what makes the contact centre a vital component of productivity and customer satisfaction.

Figure 1 illustrates that productivity is the top concern for business managers in Canada in 2007. The Figure also illustrates the relative importance of customer service as a top organizational priority. The relationship between customer service and the contact centre does not need any elaboration: it is one of the foundations from which contact centre operations are built.

FIGURE 1

Canadian Business Priorities, 2007

Which ONE business or organizational problem will take priority in 2007?



N= 132

Source: IDC, 2007

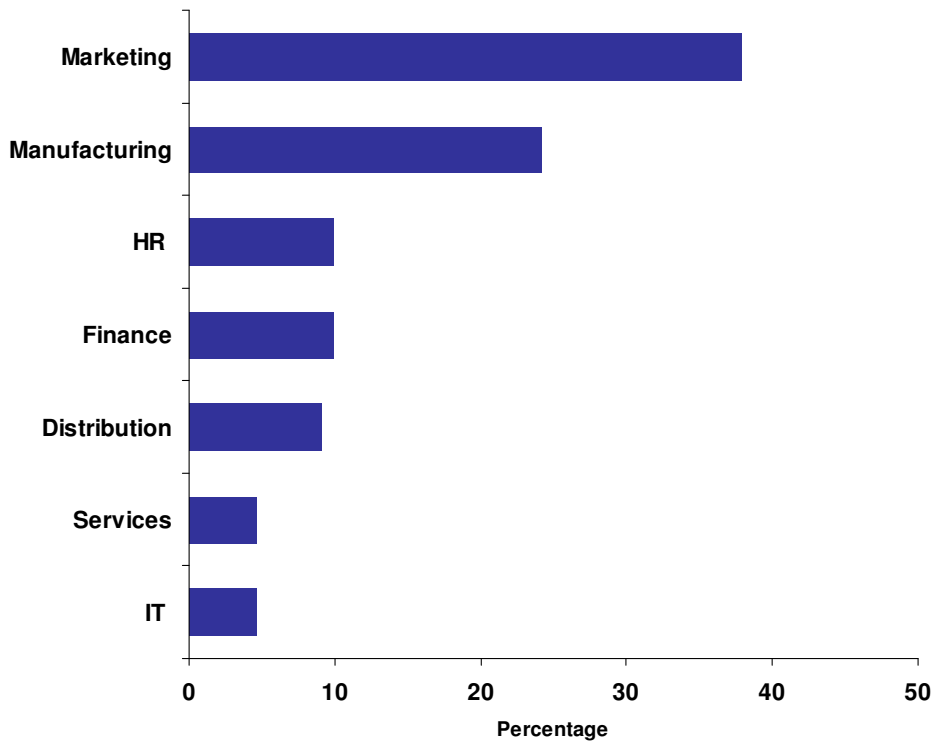
In the contact centre environment, productivity not only relates to the agents themselves, but also to the infrastructure that support the agents (both IT and non-IT assets). Productivity is critical in the contact centre because it is measured in a variety of different ways from calls answered in a given period of time, time to answer incoming calls, as well as revenue generating activities including up-selling and cross-selling products or services.

Where will productivity improvements have the biggest impact according to senior executives? There are seven functions considered in Figure 2, below. However, the department expected to contribute the most to business performance is marketing. The contact centre is a clear contributor to the marketing function and its sister function – sales. The importance of the contact centre is obvious to the success of the business, and it only makes sense for organizations to provide it with the resources it needs and the security it requires.

FIGURE 2

Department to Provide Greatest Contribution to Business Performance in 2007

Of the following seven departments, which one department do you believe will provide the greatest contribution to business performance in 2007?



N= 132

Source: IDC, 2007

Disasters or business disruptions are catastrophic to the marketing department and overall performance because, according to Canadian businesses, customer service is the most important issue related to business continuity. A recent IDC Canada survey illustrates that 75% of Canadian businesses are concerned with three key business performance issues:

- Customer service
- Risk reduction
- Protection against revenue loss

Canadian businesses recognize that business continuity is critical for effective customer service and, in addition to productivity and serving existing markets, customer service is a top business priority for 2007. Since these issues – productivity,

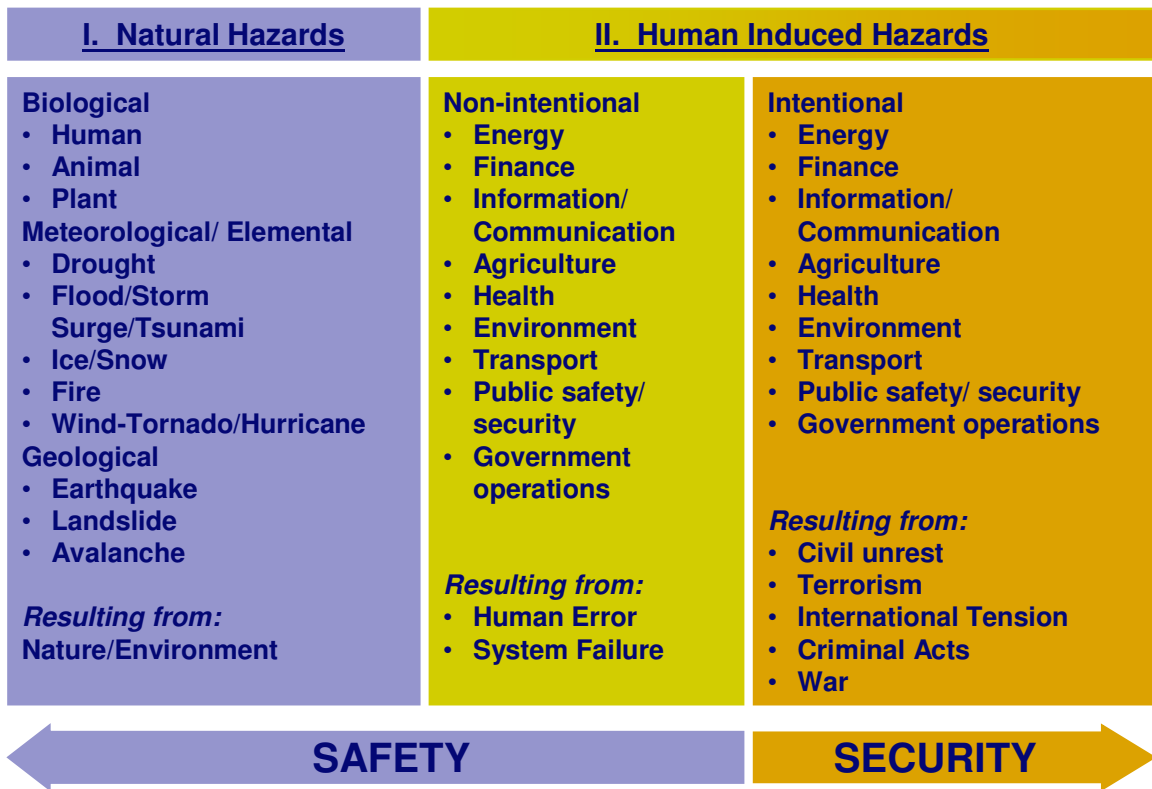
customer service, and business continuity – are linked in the contact centre, it is important to consider the risks faced by this business unit and the sources of remediation that are available.

Identifying Risk Factors

The contact centre is subject to multiple hazards that can impact productivity and customer service and result in lost business and lost opportunity. Risks can be segmented into two major groups: natural or environment risks and human-induced risks. The categorization of risk is important because it dictates the response or course of action for businesses after a disaster occurs. Figure 3 provides a summary of the types of disasters or adverse events that can impact a business in the normal course of its operations.

FIGURE 3

Natural and Human Disasters



Source: IDC, 2007

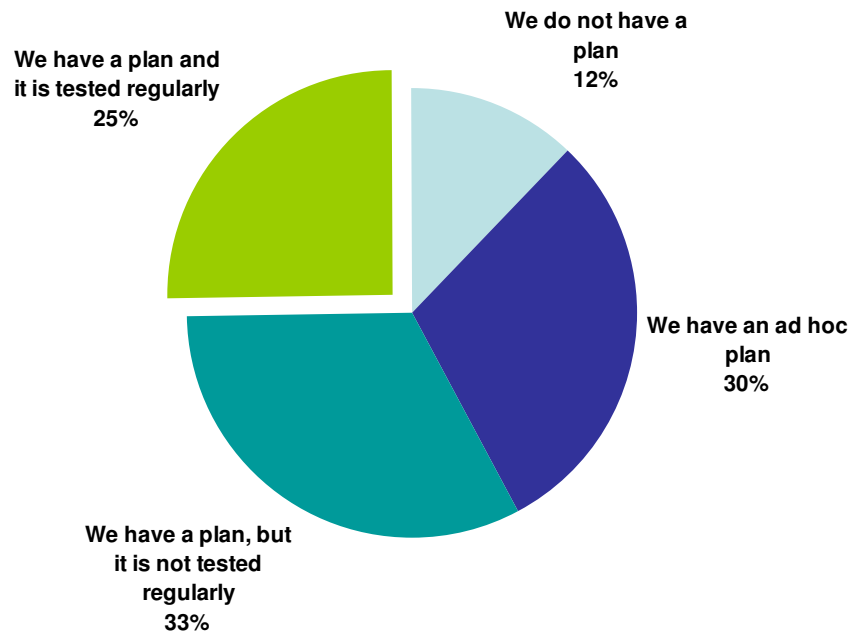
The best way to prepare and manage these hazards is by designing and implementing a disaster recovery/business continuity plan. Disaster recovery is the process of regaining access to the data, equipment, software and personnel necessary to resume critical business operations after a natural or human-caused disaster. Business continuity is a progression of disaster recovery, aimed at allowing an organization to continue functioning after (and ideally, during) a disaster, rather than simply being able to recover after a disaster.

As can be seen in Figure 4, below, three-quarters of survey respondents in medium and large Canadian businesses either lack a disaster recovery and business continuity plan, or the plan that the business has is inadequately implemented or managed. The fact is, many Canadian businesses know that the current level of spending on disaster recovery and business continuity is insufficient. IDC Canada survey data indicates that on average businesses with existing plans spend approximately 3% of the IT budget on disaster recovery and business continuity. The extent of the inadequacy of disaster recovery and business continuity is evident when the same respondents were asked what the business ought to be spending on disaster recovery and business continuity. Respondents, both IT and line of business, indicated that disaster recovery and business continuity spending would ideally account for approximately 6% of IT budgets.

FIGURE 4

Disaster Recovery/Business Continuity Planning Status

Which of the following describes your organization's business continuity planning status?



N= 255

Source: IDC, 2007

FUTURE OUTLOOK

Scenarios

Dimensions of disaster recovery/business continuity (DR/BC)

The contact centre is a visible source of failure for most businesses because it represents a primary point of contact with customers on an ongoing basis. In order to ensure continued service in the contact centre, businesses are required to address a variety of elements that are exposed to risk. In the contact centre environment this would include:

- ☒ Information systems
- ☒ Contact centre systems and applications (including ACD and PBX systems)
- ☒ Communications networks
- ☒ Personnel
- ☒ Facilities and electrical systems
- ☒ Customer and business partner service

Part of the responsibility of maintaining these assets in the event of a disaster is to plan for the possibility of some type of failure and to have alternatives in place. There can be no single point of failure. If it is a cost of doing business to implement and maintain these assets, then it is also a cost of business to ensure that adequate protection is built into the system to guard against failure.

The means of establishing the priorities of managing disasters and planning for business continuity is in identifying the risk factors to the business, categorizing the risks and then creating an action plan to mitigate and manage these risks. The assets at risk in the contact centre were illustrated above. The following section examines the means of assessing risk in its various forms and how companies can protect their contact centre operations.

Assessing the impact of a disaster or business disruption on assets

There are many questions that arise in the event of a disaster befalling the contact centre, not the least of which is how could this disaster be prevented or lessened. Given the importance of contact centres in building and maintaining customer relationships, it is too important to leave to chance or to play the odds that a low probability event will or will not occur. Disaster recovery and business continuity planning require organizations to ask themselves some very pointed questions and it also requires honest answers. Questions to ask include:

- ☒ What happens to contact centre assets in the event of a disaster?
- ☒ How do companies assess the total costs to return assets to their previous state?
- ☒ How does a business assess the cost of lost revenue and lost opportunity?
- ☒ What are the key factors that impact asset valuation in the contact centre?
- ☒ What are the costs to establish effective disaster recovery and business continuity plans for the contact centre that is managed (and paid for) internally?

The considerations for disaster recovery/business continuity in the contact centre are multi-faceted because they impact the three key elements of the organization: people, processes, and technology. Undertaking an ROI analysis is not really practical when considering a disaster recovery and business continuity plan for the contact centre. However, it is possible to undertake an assessment of lost revenue and opportunity

potential resulting from a disaster. The elements at risk in the contact centre are considered below.

Market Demand and Supply

Market demand considers all of the aspects of a disaster on customer relationships.

- What is the likely impact on sales if a disaster takes a contact centre off-line for an extended period of time?
 - How will an event impact sales, both direct and in-direct?
 - How will a disaster or business outage impact service/support obligations?
 - How will an adverse event impact customer perceptions and business image?
 - How will an adverse event impact business partners and their ability to service their customers?

Replacement Costs

There are replacement costs for both physical assets and human assets. In both cases there will be costs to replace the assets and personnel as well as costs to re-administer policies and procedures in the contact centre.

- What will it cost to restore (physical) assets to useful state?
- How will less tangible (i.e., data and information) be replaced and at what cost?
- How can personnel and knowledge be replaced?
- Are there other facilities available in the event of a disaster? Are these facilities in the same area or does it require setting up in a different location?

Equipment

There are obvious physical signs for the condition of assets in the contact centre. Insurance adjustments can be made for equipment and building but there are also other conditions that need consideration.

- Do damaged assets have any remaining/resale value?
- Can existing buildings or equipment be repaired/renovated?
- Can alternative sources of equipment be utilized until normal operations can resume?

Personnel

Unlike physical assets, human resources can be subject to long-term effects of disasters. Disaster recovery and business continuity planning helps to address the human issues related to providing service in difficult times, including:

- Will employees need special assistance to recover (personally and/or professionally) from a disaster?
- How will customer contacts be managed? Who is responsible and are there different expectations and/or requirements for service?
- Are there training programs in place to address how to respond to disasters or threats?
- Are there programs that address post-incident training to deal with existing employee issues as well as training new and/or replacement workers?
- Are there plans to enable alternative work strategies exist, for example work-at-home or at another site? Are there security issues that, when addressed, will resolve these issues?

Features

Even with stringent systems and structure to the operation of the contact centre, there are features that are not codified and depend on the culture and informal knowledge of people working in the organization. It is these attributes that make up the strategic or competitive advantage of a company and it could be very difficult to replace.

- Are there features/functionality that will be difficult and/or expensive to replace/recreate?
- How much knowledge resides in individual employees (contact centre agents) and how much is irretrievable in the event of a disaster?

Procedures

The contact centre is a process-driven organization and its operation can be severely damaged if procedures are not documented and employees are unaware of the policies that administer service and the continuations of business. There are important procedural issues covered in the disaster recovery and business continuity plans for the contact centre.

- How do employees respond to customer inquiries in the event of a disaster?
- Is there recourse to adding additional personnel? From other areas of the business? From external providers?
- Who is responsible for restoring the contact centre? Who is responsible for administering the disaster recovery and business continuity plan and what authority do these administrators have?
- Is there a communications policy in place for contact centre employees, informing them of when they are to resume work, and what conditions they can expect when they return?

Output

Contact centres can play an important role in generating content for both internal and external stakeholders, producing a significant impact on operations. Losing this output in a sales or marketing role could result in business failure.

- Are there specialised reports or metrics (i.e., quota attainment) that could be lost, and that affect performance or compensation?
- Will a disaster impact industry standing or recognition?
- Can contact centre agents continue to provide outstanding service in the event of a disaster?

Identifying and Categorizing Risk Factors

All businesses, regardless of size, industry, region, or customer demographics, face risk on a daily business. Risk is part of the fabric of business and it is important that every business manage risk in a way that is appropriate. Managing risk in the face of a disaster is multi-faceted and will require a considerable amount of work be undertaken by the organization either alone or in conjunction with an expert third-party advisor. Risk can be segmented as follows:

- Risks that can be prevented.** Even from a simple fiduciary standpoint, businesses have an obligation to fully address risks that are preventable. In the contact centre environment, the earlier list illustrates the components that should be protected, thus preventing a complete failure.
- Risks that can be lessened.** There are some risks that cannot be avoided. In these cases, risks to the contact centre can be mitigated. For example, locating contact centres in regions that are subject to different geological and environmental conditions as well as communications equipment and providers.
- Risks that can be preserved.** In some cases, retaining risk within a business is part of its competitive advantage, a way to differentiate itself from its competitors. For the contact centre, the maintenance of customer lists and proprietary information may be worth retaining internally. The use of a cold site will mitigate some of these risks while allowing the business to retain its uniqueness.
- Risks that can be transferred.** The business ecosystem is replete with organizations that specialize in service offerings that are too difficult for businesses to manage internally. Transferring risk in the contact centre environment can be as simple as creating a DR/BC plan, implementing a plan or choosing an alternative such as hosted contact centre solution.
- Reducing the risk of loss from a specific event.** There are many factors that contribute to the potential for a disaster, whether the event is natural or man-made. The contact centre is subject to conditions that can interrupt operations for short or extended periods of time. DR/BC planning is one of the best ways to mitigate the risk from a specific event by creating systems and routines that do not have a single point of failure.

There are a number of different options to consider after the contact centre has been risk assessed. The business could simply decide that it can retain sole ownership of the contact centre and manage the risk factors by instituting programs that prevent, lessen, or retain the threats. Alternatively, the business could opt for solutions that are hybrid variants in which it retains the majority ownership and uses external providers for specific threats or to minimize the impact of a specific event. A managed or hosted service would represent a hybrid alternative in which the external provider incurs the majority of risk but the business retains asset ownership. The final alternative is a fully outsourced service in which the external partner assumes all of the risk and manages the contact centre to the conditions set out in a service level agreement (SLA).

Managing Risk Factors

Once the risk factors have been identified and categorized it is possible to create a scorecard to assess the functions/assets at highest risk and to implement plans that help manage emergency situations. From a functional perspective, there are four stages of disaster/continuity management:

- ☒ **Mitigation:** The process by which threats are separated from potential targets or, alternatively, the targets are separated from potential threats.
- ☒ **Preparedness:** The actions that are focused on building capability to respond effectively and rapidly when assets are at risk due to threats or hazards.
- ☒ **Response:** The execution of the capability to minimize the losses of assets at risk. The response function is designed to provide immediate recourse to protect resources and meet basic needs.
- ☒ **Recovery:** The return to normalcy after an adverse event.

Calculating the risk factors and the developing strategies to manage the risk to the contact centre will provide the basis for developing a comprehensive disaster recovery and business continuity plan.

CHALLENGES/OPPORTUNITIES

The likelihood that a business can become entirely immune to a disaster or business outage is exceedingly low – there are simply too many factors beyond the control of most businesses to guarantee 100% accessibility to a contact centre. Past success is not a reliable indicator of future needs. A simple method of analyzing contact centre assets and the threats to these assets is presented in Table 1, below. Canadian businesses can use the scorecard to quickly rate the current level of risk exposure in the contact centre. If the risk levels seem high it probably requires that the business take some action to protect this valuable component of their business.

TABLE 1

Risk Assessment Scorecard			
Assets	Risk / Threat Level	Willingness to Incur Risk Internally	Summary / Total
Information Systems			
Contact Centre Systems & Applications			
Communications Networks			
Personnel			
Facilities and Electrical Systems			
Customer and Business Partner Services			
Summary / Total			

1= low risk, 3= medium risk, 5= high risk

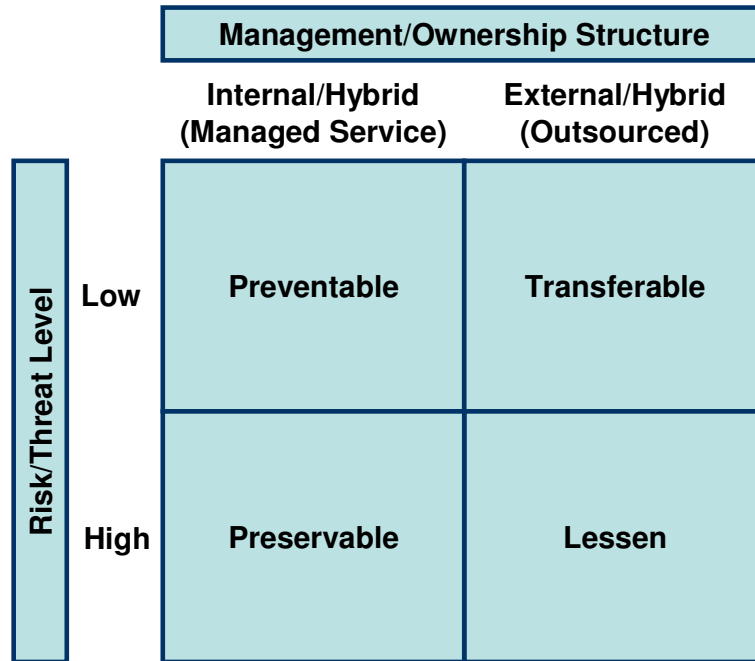
Source: IDC, 2007

Using this relatively simple methodology it is possible to take the first steps towards assessing the need for more comprehensive disaster recovery and business continuity plans. This exercise will also help to clarify some the options concerning the best practices in sourcing solutions for disaster recovery and business continuity planning. If certain assets receive a high risk score then the business can explore the various options for preventing, lessening, retaining, or transferring the risk to a partner or supplier.

Figure 5 below illustrates a model for categorizing risk and the possible sourcing strategies that businesses can utilize as a means of lower risk exposure levels. Organizations can effectively lower the exposure to threats; however, in order to facilitate exceptional disaster recovery and business continuity planning, contact centre operators will have to utilize the expertise of external specialists. The sourcing options that utilize greater outsourcing do not remove all of the responsibility from the buyer organization. Ownership of the strategy, enforcement of SLAs, governance of contracts, and suitability will still reside with the buyer organization. These critical components will account for a significant proportion of the value that contact centre managers can expect to derive from disaster recovery and business continuity planning.

FIGURE 5

Risk Segmentation Sourcing Model



Source: IDC, 2007

ESSENTIAL GUIDANCE

Best Practices

IDC believes that disaster recovery and business continuity planning is one of the most critical elements in establishing a world-class contact centre. Despite the perceived level of importance, research conducted by IDC Canada indicates that disaster recovery and business continuity planning is insufficient in many cases. In general, disaster recovery and business continuity rate high as corporate initiatives; more specifically, it is equally important to extend protection to include the contact centre. This whitepaper has examined the various forms of threats and risks to a business and its contact centre, and one fact stands out clearly: there are numerous

threats from a variety of sources making it difficult for organizations to account for all contingencies. Contact centre managers, as well as sales and marketing executives, are keenly aware of the hazards to contact centre operations and the potential impact on revenue and profit. However, most disaster recovery and business continuity plans are only given modest resources and limited capabilities.

The good news for Canadian contact centre operators is that there are options that can address the security concerns of the contact centre as well as the ownership concerns for those companies that are less willing to cede operational and managerial control to external providers. Regardless of internal preferences of organizations, there are strategies for improving contact centre performance with respect to disaster recovery and business continuity planning. The following insights are based on creating a platform from which businesses can develop stronger and more fully realized disaster recovery and business continuity plans.

Assess the situation. In order to fully grasp the extent of the issue under consideration, businesses will have to undertake a review of current disaster recovery and business continuity plans. This review will assess the costs and expenses already incurred in the contact centre and the level and status of existing investments. The assessment will also include cost projections for maintaining the status quo as well as estimates for implementing and maintaining a fault tolerant disaster recovery and business continuity plan. Another critical stage in the assessment phase is conducting due diligence on alternative sourcing options including the costs, benefits, and analysis of vendor-sourced solutions, namely managed contact centre solutions and fully outsourced solutions.

Determine what value will be gained. While it may be difficult to see tangible improvements in the day-to-day operations of a contact centre after implementing a disaster recovery/business continuity plan, there is definitely value in knowing that the continuity of the contact centre, through a disaster, is assured. The objectives for disaster recovery and business continuity in the contact centre are relatively straightforward, but are nonetheless multi-faceted, and businesses have to take a comprehensive approach to listing pertinent objectives. This list may start with improving reliability and continuous service, but it also must include sales performance metrics, SLA obligations, the value of owning and maintaining equipment and facilities, and the responsibilities owed to stakeholders in the business itself.

Determine what constraints exist. There may be limitations imposed on businesses in the development and management options of disaster recovery and business continuity plans. Businesses have to be aware of the constraints facing contact centre investments in disaster recovery and business continuity planning. Identifying the constraints – capital, executive buy-in, capacity/resources, time, etc. – will clarify the course of action open to contact centres. If there are internal constraints, then businesses can search for alternatives available in the marketplace. The important point to note is that understanding constraints will present the options that organizations can tailor to their individual needs.

Research the alternatives. Understanding the objectives and constraints will lead to the search for alternative sourcing strategies. Not only are there alternative risk

management strategies, there are a variety of sourcing strategies that can be led, either internally or externally, and in whatever proportion, to suit the buyers' organizations. Disaster recovery and business continuity solution development and deployment do not have to take contact centre operators out of their comfort zone because there are specialist organizations that can customize solutions that respect the limitations imposed by Canadian businesses while providing the necessary protection for the contact centre.

Utilize external experts. The earlier point highlighted the importance of understanding alternatives and it illustrated the potential involvement of partners and advisors. The burden on an organization to test and deploy disaster recovery and business continuity would extend beyond the contact centre to include the IT department, human resources, facilities, marketing, and sales. Each of these departments (or functions) will have an inherent interest in a disaster recovery and business continuity plan for the contact centre, and their expertise in developing, implementing, and maintaining these plans will likely extend beyond their core capabilities. It is incumbent on buyers to protect themselves and the interests of their stakeholders to leverage the skills and expertise of providers that specialize in the design, deployment, and support of disaster recovery and business continuity plans.

CONCLUSION

This white paper is intended to be a primer for Canadian businesses to further their understanding of the importance of disaster recovery and business continuity in the contact centre. The effective use of disaster recovery and business continuity plans serves as a form of insurance for contact centre operations in the event of a disaster occurring. While the immediate benefit of effective disaster recovery and business continuity planning is fairly obvious, there are other benefits that, when considered collectively, can account for significant competitive advantages.

As discussed at the outset of this white paper, productivity is a key performance indicator for a large segment of businesses in Canada. Companies that can maintain productivity levels while operating under adverse conditions resulting from a disaster or business outage will enjoy strategic benefits not available to competitors that are not as well prepared. Productivity improvements benefit businesses directly from an internal perspective by maximizing revenue and output in a specific time period. Productivity can also have a positive impact on external factors such as improvements in customer retention levels by ensuring consistent quality of customer interactions ranging from initial sales to after-sales support.

There are also operational benefits associated with disaster recovery and business continuity in the contact centre. One of the chief benefits in the operational realm is the reduction (or improved management) of risk. Lowering or maintaining risk factors to contact centre operations benefits the overall business by improving the utilization of assets, including human assets. The white paper discussed at length the importance of identifying and managing risk factors to the contact centre as well as the strategies available to buyers in categorizing the risk factors and the ways in which risk, when managed successfully, can be turned into a positive, differentiating attribute rather than a liability.

Improved contact centre operations, from a disaster recovery and business continuity perspective, also generate benefits that are visible in the marketplace. While disasters and business outages may be low probability events, the damage inflicted on a business after an adverse event can have lasting and negative consequences. Improving and ensuring business continuity in the contact centre is beneficial to a business because it can lead directly to stronger customer relationships. The foundation of any business is its customers and its ability to foster long-term relationships. If the business relies on a contact centre for customer interactions then it has an obligation to itself and its stakeholders to prepare, respond, mitigate and recover from disasters and threats to its operation.

The final consideration in the initial phase of evaluating the importance of disaster recovery and business continuity solutions is the finding the optimal mix of sourcing capabilities and expertise internally and externally. Executing effective disaster recovery and business continuity planning will often require significant commitments in the form of time, capital expenditures, and other resources. In some cases, the requirements needed for disaster recovery and business continuity may not be available internally, and the use of external providers will be necessary. Buyers can be assured that there are numerous sourcing and contract options available from suppliers that can be tailored to the specific needs and operating conditions of most buyer organizations. These external providers bring a level of expertise that will far surpass that of individual businesses and further lower the level of risk.

APPENDIX

Sources

Strategic Outsourcing. A Structured Approach to Outsourcing Decisions and Initiatives, Maurice Greaver, AMACOM, 1999, New York.

Definitions

The business continuity category includes the following:

Business continuity services:

- Disaster recovery is defined as a number of services elements that allow a business to get back up and running in the event of a major incident that temporarily puts its operations completely out of action. These elements include standby provision (such as hot site and cold site) and restart services.

- Backup services are defined as the transfer of company data from a "live" medium to a protected medium in case of a corruption of the original "live" medium. This process can be internal (the backup is conducted in-house and stored in-house), external (the backup is conducted in-house and stored at an offsite location), or remote (the backup is conducted electronically to another location). These services may encompass a variety of methods, including traditional backup-and-restore, archiving, and vaulting services, among others.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.