Contingency planning

Contingency & Business Continuity Planning are very important aspects, not only for disaster recovery but also for computer security. Describe the key elements that might lead to an IT- related disaster and suggest ways in which the worst effects of such a disaster might well be curtailed. IntroductionAll too often businesses take their IT services for granted. While most are aware of the importance security and backing up information, the value of having an effective contingency and continuity plan is often not appreciated until it is too late.

This essay will identify factors that could trigger critical incidents and propose strategies to mitigate the effects of such a disaster. The purpose of this essay is to outline the key elements of risk management in IT, as well as provide insight into the problem from the perspective of a risk management consultant. This essay recognises that contingency and business planning are very important aspects of any company??™s overall strategy. This type of planning is especially important to computer security. In order to demonstrate the value of effective risk management, this essay will first outline the most common IT threats facing organisations and identify how these can be addressed and managed.

This essay will not only identify IT disaster triggers but also identify possible strategies to mitigate these triggers. It is possible to minimise the effects of an IT disaster by cultivating an awareness of the risks and developing strategies to address them. The conclusion will draw on the research gathered within the essay, emphasising effective IT risk management depends on the ability to identify and assess risk factors then develop strategies to either avoid or minimise these risks. Risk ManagementThe field

of risk management is a broad one, encompassing a number of industries and sectors from oil and gas to agriculture, retail to manufacturing. When the field of risk management first emerged, it focused primarily on the activities related to insurance. Over the years, however, it developed into a more important role, addressing the operational activities of an organisation. Risk management has given companies the necessary tools to identify and address risks before they become serious problems. Risk management strategies usually incorporate one of the four following approaches or a combination thereof.

Once a risk has been identified and assessed, it is possible to select the appropriate technique. The first strategy is avoidance. This strategy is characterised by abstention. Any risk activity is avoided. There are obvious drawbacks to this approach, as it can be limiting and even counterproductive. It is, however, useful in some instances.

For example, it may not be possible to avoid every activity that carries a risk, but it is possible to avoid the more significant ones. Fear of a risk should inform rather than restrict activity. The second strategy is to reduce the potential impact of the risk. This involves analysing the risk and identifying what factors can be improved or controlled. The third strategy consists of prevention. In this approach, steps are taken in order to minimise the occurrence of a risk.

It too requires careful planning. The final strategy is separation. This approach seeks to minimise the risk by identifying and separating potential hazards. In the IT sector, risk management functions in much the same

manner as it does elsewhere. There are, however, unique concerns and circumstances. Risk by its very nature is omnipresent. A failure to sufficiently acknowledge and address risks may have disastrous consequences for a business. Critical incidents or disasters in the IT sector put not only a company??™s activities in jeopardy but also its future.

It is essential that steps be taken to protect not only data but also the processes involved in IT. The second part of this essay will examine these in greater detail, drawing on research published by practitioners in the field. The Role of the Risk Management ConsultantThe role of a risk management consultant is to provide an objective assessment of the risks a company may face and provide a feasible solution to managing these risks. Most importantly, a consultant should be able to help an organisation test continuity plans and risk management strategies, as well as identify any potential weaknesses or oversights (Zawada 2008). IT Risk ManagementThis section will outline the current approaches to risk management within the IT sector. The information gathered in this portion of the essay draws on published research from practitioners and academics in the field of study. It will begin by identifying the basic principles of risk management within the IT sector, namely risk identification, analysis, reduction and monitoring. Next the chief risk factors in IT will be identified and discussed.

Finally, the importance of continuity management will be considered. This section will provide the evidence and context for the recommendations identified in the following section. Elements of Risk ManagementSome element of risk is present in almost every facet of the working environment. Risk is often determined by an organisation??™s operational activities. For

example, the construction sector is vulnerable to health and safety risks, while a financial institution??™s private data may be susceptible to security breaches. Training and safety standards may help lessen the effect of occupational hazards, and rigorous security checks may protect privileged information.

The key to risk management is identifying and evaluating a risk then taking the necessary action to address and/or control the risk. Early approaches to IT risk management suggests that a new approach is needed to meet the concerns of this sector (Halliday, Badenhorst & von Solms 1996). Halliday et al argue that conventional risk analysis strategies, which focus on the relationship amongst the asset, threat and vulnerability, are not applicable to the IT sector.

In order to effectively manage risk, Halliday et al suggest a more flexible and less resource-intensive approach is needed. Later research provides a framework for incorporating risk management into IT. Bandyopadhyay, Mykytyn & Mykytyn (1999) identify the following steps: risk identification, risk analysis, risk reduction and risk monitoring.

Each of these factors will be outlined and evaluated in turn. Risk IdentificationBefore a risk can be effectively addressed, first it must be identified. Risk identification can be reasonably straightforward. For example, most users would recognise that files need to be encrypted and password-protected in order to ensure their security.

Other risks may be more difficult to identify. Consequently, it may be useful to perform this step as part of a group. The workshop setting can generate

more ideas than one individual working alone. In addition, it is important to remain current with best practises within the industry and abreast of any developing security threats. Risk AnalysisOnce a risk has been identified, it then needs to be analysed.

This analysis can help the consultant and the organisation to better understand the consequences of a particular threat or vulnerability, as well as developing appropriate strategies. Returning to the example of the password-protected file, ten years ago standard practice in selecting a security code was to pick something that would be easy to remember but hard to guess. Popular choices might include place names or unusual words. More recently, however, technology has emerged that is capable of breaking these types of passwords. Therefore, the standard for an acceptable password has changed. It is now common to create an alphanumeric sequence that is more difficult, if not impossible, for hackers or other unauthorised users to break. Risk ReductionOftentimes, once a risk has been identified and analysed, it is possible to take steps to reduce its potential impact. For example, if there is a strong likelihood that an unauthorised user may try to breach one??™s system, the risk can be reduced by either creating a firewall or limiting external access.

On occasion, the risk factor may come from within. Industrial espionage is a not uncommon occurrence in sectors where research and development are paramount. The risks posed by these individuals can be reduced in a number of ways. Firstly, applicants could be pre-screened and subjected to a security check. Secondly, photographic or copying devices could be banned from the workplace.

Thirdly, the workplace itself could be monitored as well as the activities of employees. Risk MonitoringAs the name suggest, this activity involves observing a perceived risk. The risk may exist in real time and need to be monitored. Alternatively, the risk may not be an immediate one but of potential concern in the future. For example, a company??™s operating system may be sufficient to meet current requirements; however, a sharp increase in its activities may cause the system to fail. In the retail sector, this is best illustrated by the sharp increase in activity during the holiday season. Many retailers put a halt on changes to their operating systems prior to Christmas to ensure that everything keeps running smoothly. A bug or glitch may results in hundreds of thousands pounds in lost sales or goodwill.

Effective risk management is cyclical in nature. Identifying a risk is only one part of the process. It is also necessary to establish the likelihood or frequency of a risk, as well as its potential impact. The process of risk management requires constant vigilance and careful study. Once a risk is fully understood, it is then possible to develop a strategy in order to mitigate the effects. IT Risk FactorsIn many companies, the IT system provides the framework both for the operational activities and the corporate memory. Given its importance, it is absolutely essential that any and all risk factors are clearly identified and understood.

This knowledge will enable a consultant to assist an organisation in developing an effective risk management strategy. While IT is often a powerful tool, it is traditionally more prone to failure than almost any other business system (Baccarini, Salm & Love 2004, D??™Amico 2005). This section will identify both the internal and external risk factors. InternalWithin

any organisation, there is always an element of risk; however, it is possible to identify three main categories of risk. Mair (2008) identifies the following pitfalls: ??? no people, no infrastructure, no IT??™.

The first risk factor is as follows. In general, the successful functioning of any IT systems depends largely on the performance of highly trained and competent individuals. If for any reason, i. e.

natural disaster, the skilled staff is not available to maintain the system then there will be serious problems. The second risk factor consists of the infrastructure. In the case of an emergency, it is often impossible for an organisation to carry out its normal functions.

For example, power outages or damage to buildings may destabilise the existing network. For many organisations all communication is network-based, which means this factor needs special consideration in any continuity plan or risk management strategy (Kennedy 2008). In some instances, it would be necessary to have temporary systems available to support activity and bridge the gap. The third category consists of IT. If a virus or malicious software problem attacks the IT system, it will no longer be available to support the normal functioning of the organisation. Equally, in the event of a power outage, the IT system will not be available. The strategies for dealing with these types of events will be identified later on in the essay. ExternalArguably, the greatest external threat to any IT system is a security breach.

A security breach may be perpetrated by a number of individuals or groups. For example, a criminal element may wish to obtain confidential information

from a financial institution in order to commit fraud. Alternatively, a competitor may wish to an organisation??™s files. Other security risks include terrorists, hackers or other individuals bent on creating mischief.

Information security management plays an important role in addressing these risks and reducing them to an acceptable level (Tsoumas & Tryfonas 2004). IT is often vulnerable to physical risks as well, such as flooding, fire or other natural disasters. It is important that contingency plans provide for remote storage or secondary sites in order to preserve the IT systems in the event of an incident at the company??™s primary site. Continuity Management An effective continuity plan can help an organisation to cope with almost any contingency. This section will identify best practises. The information presented her is largely drawn from the findings of practitioners in the field.

DevelopmentSuccessful continuity management depends largely on two factors: keeping things simple and ensuring that people buy into the process (Mair 2008). While a 100-page document may provide a comprehensive overview of the situation and recommended strategy, a succinct set of instructions and contact numbers printed on one side of an A4 sheet is probably more useful in an emergency, as Mair points out. It is equally important to engage staff at all levels in the process. Those with experience in the field can provide valuable insight, as well as feedback that can help improve any strategy. In addition, in order for there to be an organisational commitment to the strategy, senior management also need to buy into the process. Many people are resistant to implementing or understanding continuity plans, either because they are wildly optimistic or consider it a

waste of time (Mair 2008). It is important to make the process appealing by either clearly identifying the benefits or making the adoption of the plan more acceptable.

An effective business continuity plan should include the following details. Firstly, it needs to clearly identify who is responsible for what. Secondly, the start point needs to be well defined. For example, in the IT sector, an outage lasting more than one hour could trigger a sequence of events aimed at addressing continuity issues. Mair also recommends identifying top priorities in the event of conflict. Thirdly, it is necessary to provide a comprehensive contact list for those involved, from employees to clients, as well as suppliers and other important contacts.

This list should include primary and secondary numbers for each contact. Obviously, depending on the size of the organisation it may be necessary to provide separate contact sheets for each department. Fourthly, it is necessary to identify exactly what resources will be needed. The list may include equipment as well as staff members. Fifthly, secondary work sites need to be identified. For example, in the event of a fire, the office needs to have a place not only to meet and regroup but also continue its activities.

This secondary location may be the result of a reciprocal arrangement with another business or organisation. Sixthly, it is necessary to provide some means of recording incidents during the period. Seventhly, it is also necessary to establish general document control. AuditingIt is not enough to simply develop a plan and hope for the best. It is necessary to regularly

review and evaluate continuity measures in order to ensure that they are effective and understood by the organisation.

Auditing helps build competence within an organisation and increases its resilience (Mair 2008). In order to keep people engaged, continuity management needs to be integrated into the functioning of the organisation (Zawada 2007). Zawada suggests that companies find a way to engage with both the public as well as their own concerns in the event of an emergency; this approach not only taps into employees??™ sense of altruism but also helps strengthen the company??™s reputation in the community. It is also important to consider continuity when adopting new systems or developing new approaches (Zawada 2007). Benchmarking is also an effective strategy. Not only does it help identify best practises, but it also gives the organisation an opportunity to see how it measures up against its competitors.

AssessmentA continuity plan is only successful if it meets the needs of the organisation. If the plan is either too complicated or incomplete, it will not have the desired effect. Similarly, if the plan impedes the organisation??™s daily operations, the benefits will not merit the effort. In assessing the plan, it is important to consider whether its focus is too fixed or too vague. Does the plan imagine a disaster occurring at 9. 00 a. m. on a Monday morning, or is it always in the early hours of Sunday morning (Zawada 2007).

Similarly, the plan must be able to consider a host of factors operating either individually or in concert. For example, a network card failure may have a knock-on effect elsewhere, interrupting seemingly unrelated activities. Equally, a natural disaster may produce not only a loss of power and

structural damage but also flooding. While it is impossible to account for every variable, a successful continuity plan should be able to address a variety of factors and situations.

It is also important within IT that the continuity plan complements the disaster recovery plan (Bradbury 2007). An organisation must determine what its data recovery requirements are. These range from zero data loss, to start of current business day, to end of previous business day (Bradbury 2007).

A disaster recovery plan should consider not only the effect of a power loss but also change control and documentation (Kennedy 2008). The continuity plan should reflect not only the needs of the organisation but also the knowledge and experience of its employees (Zawada 2007). Ongoing self-assessment is also important to the process, as it will not only create greater awareness but also ensure a joined-up approach to strategy and continuity planning (Mair 2008). The next section will identify a series of recommendations for coping with critical incidents within IT. As indicated previously, these recommendations will be based in large part on the research discussed in this section. The findings of practitioners in the field of study will help to develop strategies to curtail the worst effects of disasters. RecommendationsDevelop a clear but concise strategy.

Continuity planning is all about identifying the essence of the organisation. The key players and activities should be clearly identified. As well, the emergency procedures should be simple to follow, in order to minimise the impact of stress. Recognise the physical vulnerability of IT systems.

Data systems are vulnerable to fire, floods and other natural disasters. Equip IT areas with adequate safety measure. Ensure backup systems are stored at a secondary or remote location. Prepare for more than one scenario.

In developing a plan, the manager should be able to imagine a variety of different factors and situations. The contingency plan should be able to cope with either flood or fire or fire and flood. While some scenarios are more likely than others to occur, and should be prepared for accordingly, it is important to keep in mind that emergencies rarely follow a script. Create early alert systems for security breaches. Ensure that these notifications reach the right people at the right time. Promote good habits within the company and help make security a chief concern for all involved. Involve all levels of the organisation. It is important to get employees and management alike to buy into the strategy.

Their input and support can mean the difference between success and failure. Create awareness of the plan. This plan should not be put on a shelf and forgotten. New staff members should be educated about the continuity plan. Existing staff members should test parts of the plan or particular scenarios. Information about the plan should be readily available on company websites or notice boards. Identify response triggers.

In IT, it is important to pinpoint exactly when a network outage becomes an incident and when an incident becomes critical or a disaster. It is possible to flag these steps by either providing flow charts or timelines. As each milestone is reached, there should be a plan of action to respond to the

situation. Be prepared for chain reactions. A failure in one part of the network may have a knock-on effect elsewhere.

It is important to ensure that the system can recover from a critical incident quickly and that the effects throughout the network can be minimised. Keep the system secure. Unauthorised access is one of the major external threats to IT. Systems need to be kept secure. The best way to ensure this happens is to remain vigilant. Create contact lists. While in a normal situation, contact information may be readily available; however, in the event of a disaster or critical incident, it can often be inaccessible. It is also important that members of the organisation know exactly who they should contact and how in the event of an emergency.

Make continuity planning part of the overall strategy. Effective continuity planning should support the long-term aims of the organisation. Equally the objectives should be sustainable. There should be a sense of connectedness between the two. If this exists, the plan is more likely to be successful.

Accept that the importance of continuity management will never be fully appreciated until something goes wrong. Some may resent the time devoted to continuity planning and testing, while others may question its value. Many people prefer not to dwell on future threats and prefer to focus on the work at hand.

For many, the importance of risk management and contingency planning does not become apparent until they experience a disaster firsthand. Consequently, it may be useful to learn from those who have had direct experience, as they will be able to clearly articulate the most important

features of continuity planning. Protection of AssetsThe consequences of a flood, fire or explosion can have devastating results for an organisation, loss of core data, personal information, customer accounts has the potential to disrupt the business, its reputation and corporate image. The security risk assessment of an installation must be the first stage to assist management identify hazards so elimination or reduction measures can be introduced. The location and construction of the installation must be assessed, will it be a remote site or based within the heart of the organisations building.

Access control to the installation should be considered a high priority, who will need access to the installation and what method of control should be used. Physical guarding, remote monitoring and access cards are ways to minimise the threat of unauthorised access into the area. A fire risk assessment under the Regulatory Reform (Fire Safety) Order 2005 will be required if the company employs more than five people. The assessment of the installation will usually form part of the overall fire management strategy, however there are specific precautions that can be undertaken to reduce a fire occurring within the premises or installation. Management must decide on the location of the installation, will it be a remote site or based within the organisation??™s premises. The vunerability of flood risk must be assessed, many companies will locate the installation within a basement, where damp and the risk of flooding may exist.

Access control into the installation should be considered during the assessment, who will need access and by what means. Good standards of housekeeping within the installation coupled with regular management monitoring of the system and associated buildings are essential fire

prevention techniques. Fire detection and warning systems can be installed to give additional time to avoid worst case scenerios from occurring. The fire detection system can be monitored from a remote monitoring station to give 24 hour cover. Fire suppression systems can be installed to operate when heat or smoke are detected. Historically Halon was used, however due to environmental legislation this inert gas in now illegal. An inert gas named FM 200 is the preferred gas now used. A sprinker system can be fitted, usually operating the ??? double knock??? method where if a detection of smoke or heat identified an alarm will sound, giving the monitoring station time to alert the client that smoke has been detected, if nothing is done within a certain time frame and another detector is activated the sprinkler system will deluge the installation.

Inspection and monitoring of the installation are key management functions to minimise the risk of fire and damage occurring. ConclusionAn element of risk is present in almost any situation, including business. The effective management of risk depends on the ability to identify and assess risk factors then develop strategies to either avoid or minimise these hazards. There are a number of risks inherent in IT. The pervasiveness of the technology means that this is essential to most business activities. Consequently, any threat to IT is felt throughout the organisation. It is of great importance to both identify and monitor risks.

For example, risks posed by natural disasters, terrorists or viruses can have a significant impact on the running of an IT system. It is not possible to develop a single plan to address every risk factor. It is necessary to consider each risk in turn and decide what is and is not acceptable. Once the

threshold has been established, it is possible to identify to feasible strategy to counter risks and provide for operational continuity in the event of a critical incident or disaster. As the research discussed in this essay indicates, the success of any continuity plan depends on its ease of use and applicability to the corporate environment. ReferencesBaccarini, D, Salm, G & Love, P 2004, ??? Management of Risks in Information Technology???, Industrial Management & Data Systems, vol. 104, no. 4.

Bandyopadhyay, K, Mykytyn, P & Mykytyn , K1999, ??? A Framework for Integrated Risk Management in Information Technology???, Management Decision, vol. 37, no. 5, pp. 132-40, Bradbury, C 2007, ??? The IT Disaster Recovery Plan???, Continuity Central, retrieved 13 June 2008 from http://www. continuitycentral. com/feature0524.

htmD??™Amico, V 2005, ??? Manage Your IT Projects Like an Investment Portfolio???, Handbook of Business Strategy, vol. 6, no. 1, pp. 11-18.

Davey, B 2008, ??? Business Discontinuity: Five Common Mistakes and How to Avoid Them???, Continuity Central, retrieved on 13 June 2008 from http://www. continuitycentral. com/feature0560. htmHalliday, S, Badenhorst, K & von Solms, R 1996, ??? A Business Approach to Effective Information Technology???, Information Management & Computer Security, vol. 4, no. 1, pp.

27-38. Kennedy, J 2008, ??? The Importance of the Network in IT Disaster Recovery Planning???, Continuity Central, retrieved on 13 June 2008 from http://www. continuitycentral. com/feature0554. htmKoch, K 2007, ???

Auditing Contingency Plans???, Continuity Central, retrieved on 13 June 2008 from http://www.

continuitycentral. com/feature0521. htmLesnykh, A 2008, ??? The Impact of the Consumerization of IT on IT Security Management???, Continuity Central, retrieved 13 June 2008 from http://www.

continuitycentral. com/feature0565. htmMair, H 2008, ??? A Business Continuity Management Primer???, Continuity Central, retrieved 13 June 2008 from http://www. continuitycentral. com/ feature0568. htmRodger, C & Petch, J 1999, Uncertainty & Risk Analysis: Business Dynamics, London, PriceWaterhouseCoopers. Tsoumas, V & Tryfonas, T 2004, ??? From Risk Analysis to Effective Risk Management: Towards an Automated Approach???, Information Management and Computer Security, vol.

12, no. 1, pp. 23-29. Zawada, B 2008, ??? Overcoming Preparedness Fatigue???, continuity central, retrieved 13 June 2008 from http://www. continuitycentral. com/feature0561. htmWord count 4, 127