African Journal of Business Management Vol. 6(26), pp. 7705-7713, 4 July, 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM11.1640
ISSN 1993-8233 ©2012 Academic Journals

Full Length Research Paper

The impact of critical business data on organizations

Taryn Schwartzel[1] and Ernest Mnkandla[2]*

[1]Accenture, Johannesburg, South Africa.
[2]Department of Business Information Technology, University of Johannesburg P. O. Box 524, Auckland Park, 2006, Johannesburg, South Africa.

Accepted 7 September, 2011

Organisations seem to assume that their employees understand what amounts to critical business data and that such data is appropriately protected. However, identification of critical business data is a rather complex undertaking and determines what data is protected in case of a disaster. Data is the company's greatest asset and is continually under threat from human error, technological failure, natural disasters and other external factors. These threats need to be identified and quantified in order to apply relevant protection techniques. Every organisation should also understand the business value of its data in order to realise the importance of protecting the data. The key to developing an effective data preservation and protection system is to identify critical business data in order to develop protection strategies relevant to the level of data criticality. Another variable that complicates the development of a comprehensive data protection system is fact that an organisation's data often reside on different mediums. This article investigates the difficulties organisations face in protecting and preserving critical business data. The research followed a qualitative approach starting with a detailed literature review to identify trends in the protection of critical business data followed by interviews to delve deeper into the possible sources of problems identified in the literature. The findings show the main problem to be a lack of understanding of what entails an organisation's critical business data and information.

Key words: Backup and restore, business continuity, data preservation, data storage, disaster recovery, data lifecycle management, critical business data.

INTRODUCTION

Data is the livelihood of an organisation, in fact it may be considered as the sole differentiating factor between organisations competing in the market place, especially in today's information age. Without data it would be impossible for business operations to run optimally. Hence, the validity and security of data is fundamental to the success of any business (Cane, 2002). Organisations have the responsibility to ensure that data is made available to business operations and in cases where the data is not immediately retrievable, recovery processes must be implemented. Such data recovery processes can be realised through the implementation of what is known as an information lifecycle (Haeusser et al., 2007).

*Corresponding author. E-mail: emnkandla@uj.ac.za. Telephone: 011 559 1217. Fax: 011 559 1239.

The concept of an information lifecycle implies that the value of information changes with time. An information lifecycle therefore, involves the creation, storage and protection of data through the application of data protection strategies using relevant technologies, processes and procedures (Haeusser et al., 2007; Hayes, Hammons, 2002). In this information lifecycle data can be stored in different formats such as hard copies, soft copies, and even emails to name a few. The soft copy of data is usually kept on a particular storage device or medium, which could pose some data access challenges. The main risk related to storage media is that as technologies change with time, the access to the data on these storage technologies could be difficult. Besides the change in technology, another risk to data access could be the exposure of storage media to a number of threats that could alter the data, and ultimately its meaning, purpose, value and integrity or even destroy the media

on which the data is stored. Such threats could be intentional or unintentional, either way the organisation is faced with a number of challenges to ensure timely access to data and eventual recovery of data if disasters occur (Kahle, 2003).

The challenges that an organisation faces if data is either unavailable for business operations or completely lost, vary from financial costs such as data re-creation costs to legal costs and impact of the loss on the customer base. Re-creation refers to the costs associated with the re-keying of lost data. The financial costs result from staff re-creating data instead of doing their usual duties in the business. Legal impacts could involve issues such as losing data that the organisation is obliged to retain for a certain period. Some of the challenges could include a competitor getting access to an organisation's key and confidential data and using that data to gain competitive advantage. It is therefore, important that stored data be protected and recoverable in order for it to be available at all times for optimal and cost-effective operation of the organisation. Anything short of this proactive approach could lead to unprecedented expenses when risks of data loss occur.

This article presents research into the challenges faced by businesses in protecting and preserving critical business data. The research followed a qualitative approach starting with a detailed literature review to identify trends in the protection of critical business data followed by interviews to delve deeper into the possible sources of problems identified in the literature.

The rest of the paper presents a literature review to data protection followed by the research methodology that was used in this research. The findings of the research are discussed leading to conclusions.

LITERATURE REVIEW

According to Fogleman (1995) data is a tool that must be protected. In an Information Technology (IT) revolution there is a fundamental change in the conduct of warfare that indicates the requirement to build a defensive capability to protect the data and data exchange on which business powers have become dependent. We are reminded of an incident in ancient history in which the papyrus scrolls in the libraries of Egypt, Greece, and Rome disappeared leaving second-hand reports (Berti and Costa, 2009). There are no remains of the libraries and no one is certain about what became of them. The cause of this event was not certain but the loss was said to have been intentional (Spoon, 1999). Meanwhile the Library of Alexandria, which was the great library of Egypt with more than four hundred thousand scrolls that were used for academic purposes, lost an estimated forty thousand papyrus scrolls in a fire (MacLeod, 2004). In terms of organisations and organisational data, there are two types of organisations, those that have experienced a serious data loss and those that will lose their data at some stage (Cane, 2002). Looking back at the Library of Alexandria, the lesson learned may not be to only digitise the data but to consider different options of protection against different threats because the loss of data is disastrous regardless of the cause.

Most organisations assume that their existing data storage and backup plans protect their data from massive data loss. This notion may be false security as an estimated sixty percent of vital data is said to be stored on individual computers with little or no protection. Cane (2002) outlines the data transition path from mainframes to servers then to desktop computers and mobile computers. The emergence of technologies such as grid computing and cloud computing brings additional challenges to data protection.

There are different kinds of threats ranging from magnetic interference and condensation to fire and floods, hence best methods of protection and backup must be considered. In addition, it must be noted that the actual mediums used to provide backup may be as vulnerable as the data itself. It is important to note that anything that affects the actual premises of an organisation (such as the building and systems) is a threat to computer-based information. Fire, floods, sabotage and terrorist attacks can all destroy an organisation. Whilst it may be easier to replace the equipment, if the data has been lost it will take longer to recover. A modern organisation needs to treat its data as money and also understand patterns of 'wear and tear' and expected media lifetimes (Liang et al., 2009). The preceding statement implies that an organisation's data can be seen as an asset with an attached monetary value. Moore (2003) says "storing data is one thing; retrieving data is everything." This statement implies that critical data once stored and protected must be retrievable in case of a disaster. To reiterate the notion of data protection Burnie (2002) observed that conventional data protection methods are no longer sufficient and may succumb to the challenges that businesses face regarding the growth of data needs and the availability requirements of working twenty-four hours a day and seven-days-a-week for business operations. It is becoming increasingly difficult to protect data with tape alone, therefore additional data protection methods must also be employed.

Internationally, there are a number of data protection acts, for instance in the United Kingdom the Data Protection Act of 1984 applies to any organisation that uses computers to process data related to people, whether or not it operates for profit. Each organisation must register with the Data Protection Registry to ensure compliance with the eight data processing principles set down in the law, to ensure accuracy of data, confidentiality, and data security. Failure to comply with the law is punishable by a fine (Peers, 1985). In South Africa the Protection of Personal Information bill was published in August 2009. Data Protection and Privacy acts are typically for ensuring the privacy of personal

information.

The following areas take a more detailed review of literature relating specifically to the main objectives of this research which are (i) determining the business value of data, (ii) determining threats to digital data and the impact of data unavailability or data loss on business operations, (iii) determining measures to protect critical business data, and (iv) to evaluate the lifecycle of data preservation.

The business value of data

Organisations usually have different types of data that create business value within that particular organisation and contribute to its competitive position. Whether the business data is customer data, accounting records or billing data, it should support the organisation's core business and provide it with a competitive edge. It is important to understand how different organisations perceive their business data and whether or not they classify it in different categories. In this way, once there is an understanding of how an organisation values their data and knows where different types are stored, it is easier to ascertain whether the data and data storage itself is appropriate to protect and retrieve it accordingly.

According to Moore (2003), "data is the deoxyribonucleic acid (DNA) of the organisation in the Information Age", and in terms of the uniqueness of organisational data, each organisation's data is unique regardless of where it resides. A comparison between two users' computers can be made; both having the same type of computer with the same software installed. However, the data on each computer is unique, therefore, its base of value is created by information technology and not computation alone (Moore, 2003). Massiglia (2003) states that the knowledge of what type of data is recorded for business operations is critical to enterprise resiliency. An example of this is an airline, unable to function without passenger reservations, maintenance records and supply inventory records. In the same way a software development organisation cannot function without source code.

Regarding the rate of change of data value, organisations are changing in line with the rate of change of the value and importance of their data (Croy, 2004). Some organisation data is critical to the support of business processes, whether for decision-making or to inform their employees, which makes the alignment between data value and its storage more difficult to manage. For Croy (2004) data has a lifespan and therefore decreases its value and importance to the business over time. An organisation should therefore develop a framework to identify and track its changing value of data, so as to ensure that the data is stored according to its value. Croy (2004) also points out that the responsibility of identifying the value of data lies with the IT department which is required to match the data value with the appropriate storage to support the business functions. It is difficult for organisations to determine this value due to the changing value of data in a competitive and regulated business environment.

There is a correlation between data value and storage, meaning that business data can be classified in a data valuation framework and then stored according to its value, importance and recovery needs to keep the business functioning (Croy, 2004; Myerson, 2002; Mariappan and Parthasarathy, 2009; Liang et al., 2009). This is in line with business continuity and disaster recovery plans to ensure that an organisation's most critical and important data is accessible, accurate and secure at all times. Furthermore, data storage should enable this continuity, integrity and security of valuable business data but the data management and allocation of data to data storage should be managed more effectively (Croy, 2004; Myerson, 2002).

It could be argued that a cost effective strategy would imply that an organisation would need to know the value of its business data, categorise the data according to its value and then store it using the appropriate storage medium. In this way, non-critical data is not stored on expensive storage medium.

Even if the IT department had to work closely with each business department to understand its data value, according to Croy (2004) the problem would be that most business managers say that their data needs to be highly available. Issues with this attitude are that firstly, few identify which data should be accessible and which can be stored in locations that are less accessible. Secondly, organisations have large amounts of data which change in value frequently. Thirdly, fewer organisations can afford the cost of storing all data in a highly accessible and immediately recoverable manner. It is therefore, a challenge for business continuity and disaster recovery professionals to address restoring valuable data in a way that is not only timely but also cost-effective for the business. Considering return of investment (ROI), storing data in the most highly accessible and recoverable way is not always the best option in terms of cost effectiveness. Hence, only a select set of data that is mission-critical needs to be protected in a highly available format and using replication technologies that reduce recovery times to minutes or even seconds, (EMC Education Services, 2009; Croy, 2004; Moore, 2003; Massiglia, 2003).

The next area highlights different threats to an organisation's data and the impact if business data is not available when required.

Threats to digital data

A threat is an event that can happen at any time accidental or deliberate posing potential harm to the system, including enterprise-wide network failures, local disk damage and facility destruction (Myerson, 2002). An

understanding of the threats for organisations is important in ascertaining how to appropriately protect the critical data. Literature provides some insights into the impact on business when threats occur and data is not available (Landry and Koger, 2006; Foster, 2004; Myerson, 2002). Lewis (2006) observed that data resides in different locations for different organisations as each has a unique storage environment. It is thus important for each organisation to understand where their data resides and thereby determine the corresponding cost per media. The different possible media could be e-mail servers, employee's laptops, desktop machines or organisation servers.

Literature suggests hackers, crackers, insiders, partners, competitors, terrorists, cybercrime, fires, floods, earthquakes, tornadoes, hurricanes and severe storms and malicious code as the different kinds of threats which can impact the availability of data and its business operations (Bonnette, 2003; Myerson, 2002, 2001). These types of threats can be put into four groups namely, natural threats, physical threats, intentional threats, and non-intentional threats. In addition, it must be noted that the actual media used to make the backup may be as vulnerable as the backed up data itself for example stolen laptops (Kitteringham, 2008), hence the threats to data security need to be anticipated and considered.

According to Bonnette (2003) in the data security practice it is a challenge to identify and assess threats. Performing a threat assessment is a part of a data security risk evaluation that helps in understanding threat sources and prioritisation of vulnerabilities for remediation purposes. In addition, existing security controls need to be evaluated to determine their effectiveness within the organisation. The security professionals in an organisation must understand the source of the attacks, with the likelihood of their occurrence and related impact. "This is important as one in five organisations have experienced a security breach of some nature" (Bonnette, 2003). It can therefore be argued that the criticality of performing a threat assessment within the organisation is important as the likelihood that an organisation will be a target to a threat is extremely high. Kaomea (2003) observed that the detection of many attacks is difficult until the damage has occurred in the data network and Bonnette (2003) found that each organisation has its own overall risk assessment programme to be used to develop and implement methods to evaluate threats based on its unique circumstances.

The following formula shows the relationship between risk, threats and vulnerabilities:

$$Risk = Threats * Vulnerabilities$$

The formula states that risk – the probability that a particular security threat will exploit a system vulnerability (Myerson, 2002), is a function of a threat acting on a vulnerability – that would allow a threat to happen or materialise (Myerson, 2002). The severity of the risk is influenced by the value of data assets that might be damaged or destroyed due to exploitation (Bonnette, 2003).

The time that data is accessible by applications when it is expected to be available is known as data availability (Massiglia, 2003). Data availability is often measured as a percentage of a year. For example, 99.95% availability equals to 4.38 h of unavailability in a year for a set of data that is expected to be available all the time (Massiglia, 2003).

High availability is the ability of a system to perform its function without interruption for a long period of time and downtime can cause different impacts for a business function, these impacts fall into three categories (Massiglia, 2003):

1) Financial impacts: This could be due to losing revenue due to the downtime, or the cost of replacing the system/function or the time taken for an employee to recreate the data therefore, the result is an increased expense, or a lost opportunity for example sales, billing, collections and service functions.
2) Organisation's customer base: Loss of a customer's trust in the product or service or the organisation's reputation are impacted by downtime.
3) Legal and regulatory impacts: This includes fines and investigations from violation of industry regulations, potential lawsuits from breach of contract, negligence, any other obligations, budget reductions or even closure.

It is important to realise that data loss is not limited to financial and customer base impacts but there could be data loss such that regain or recreation may not be possible such as data on paper that has been destroyed by fire.

Measures to protect critical business data

Critical business data is generally protected using management systems and themes such as business continuity management, backup restoration, and knowledge management.

Business continuity management (BCM) involves managing risks to ensure that an organisation can continues operating at a minimum predetermined level at all times. Business continuity is a proactive process which is the responsibility for the entire business organisation (Synergistic Online Solutions, 2009). In this way business continuity should be a business goal with the appropriate planning and tools to support it and in turn protect the organisation's data. Managing the protection of data results in minimising data loss and maximising business continuity (Cane, 2002). The most important factor to maintain continuity is to have a data

backup system, ensure the system is designed to fit the business data model and to ensure that equipment is up and running. Planning the backup and restoration of files is the most important step to protect data from accidental loss in the event of data deletion or a hard disk failure. The backup copy can be used to restore lost or damaged data (uCertify, 2009). Another aspect of BCM is managing knowledge in the organisation. Knowledge management (KM) involves spreading knowledge of individuals and groups across the organisation in ways that directly impact performance (Seiner, 2001). The challenge is that this knowledge is either kept only in hard copy format (unsearchable), on individual's local computers (unreachable), or in employees heads (unrecorded) (Seiner, 2001). Furthermore, there is no guarantee that the data is accurate and up-to-date. A knowledge steward is therefore required to manage knowledge.

According to Chin (2007), there are four approaches to long-term digital content preservation: technology preservation, technology emulation, content migration and analogue conversion. Content migration is a default option, but with a potential loss of data due to the conversion process. Converting digital content onto analogue media, such as microfilm or microfiche, is a viable strategy, but this is not a good option for frequently accessed records, or those that need to be accessible over wide geographical areas by many users. Outsourcing is an emerging alternative to the traditional four approaches, but technological innovation often lags behind what the enterprise might do on its own (Council of Europe, 2009).

According to Croy (2004), there are a number of acts and regulations such as The Sarbanes-Oxley Act, HIPAA, Graham-Leach-Bliley, and other regulatory changes which create challenges for data storage for different industries and organisations. Document retention regulations require organisations to establish, document, monitor and maintain the availability, authenticity, accessibility, security, and recoverability of their data, and sometimes retain data for some time. According to Bogossian (1998), due to the technology constantly changing, data storage issues arise from both a practical and financial point of view. Furthermore, as data file sizes grow larger, so does the need for more efficient and sizeable forms of storage mediums. Organisations and users are therefore required to constantly update their hardware in line with the rapid advancement of storage technologies.

Information has a lifecycle and over this period the value of information changes. During the lifecycle, data must be stored and protected using relevant technologies, processes and procedures and data protection strategies. Together with the lifecycles the organisation needs to ensure that this information is available for use in business operations. In the case of information not being immediately retrievable for business operations or for employees to continue with their duties, the information needs to be recoverable for business use. During the lifecycle of this information, the data is to be stored in different formats (hard copy, soft copy, and in e-mails, to name a few). A soft copy of the information may be on a particular storage device or medium. As technologies change and get out dated over time the data would not be accessible from these storage technologies. Information lifecycle management is a way to manage the lifecycle of changing information but there is currently no method to evaluate the lifecycle of data preservation. A possible digital data preservation strategy could be created using a "digital data preservation lifecycle management" to ensure that the organisation is aware of changing storage and preservation media and keeping up to date with the technology changes of media.

As a disaster recovery plan (DRP) is created to ensure that the plan will allow work to resume with the least amount of effort and to the same standards as before the disaster (Ontrack Data Recovery, 1998; Poker, 1996; Burnie, 2002), so would some type of an information recovery plan be required to get information back to the standard and state it was in before the loss occurred. In addition, a DRP should define the scope of restoration and establish responsibilities for actions to be taken once the disaster has occurred (Myerson, 2002). Furthermore, the plan should include disaster prevention strategies because it would be easier to prevent the disaster than to repair the damage caused. A risk analysis should be performed to determine the impact and probability of each risk. Together with risk analysis, vulnerabilities should therefore be identified and the appropriate protection controls assigned to each so as to develop a proactive protection method.

According to Wrenn (2005) a business impact analysis (BIA) is used to prioritise the security efforts throughout the organisation. Alongside the BIA the appropriate human resources are assigned and prioritised for each incident-response activity. The output is a report which lists the incidents that are likely to occur with its related business or operational impact associated to time and cost. A Business Impact Analysis could be stated as a relevant concept and method to understand what incidents are likely to occur and the associated impacts if the incident were to take place. In order to understand the financial aspects of business downtime or information loss, it would be valuable for an organisation to actually understand the associated costs. According to Cougias et al. (2003), in tolerating downtime, the biggest cost factors are: time to recover, the value of the time lost to market, and value/worth of lost or unrecoverable data.

In summary, the literature suggests that commercial organisation should define and classify their business information, using a formal process to categorise their information and store the data accordingly. Such a practice would ensure that the most important data is highly available and recoverable, and the total storage

investment is more cost-effective (Silberschatz et al., 2010). The next section describes the research methodology followed to further investigate the details of identification of critical business data and the implementation of relevant data protection and preservation systems.

RESEARCH METHODOLOGY

Based on the literature review there is evidence that proper identification and subsequent classification of critical business data can enable organisations to cost-effectively protect critical business data instead of trying to protect all data, which may not only be an expensive exercise but a difficult one. In order to gain a deeper knowledge of what people understand as critical business data in their organisations and the value of protecting this data, a more detailed study of these phenomena in their natural context using interviews was undertaken in South African organisations. The interviews targeted consultants and practitioners in computer security. These consultants were selected because they had been trained in best practices and trends, as well as exposure to advisory roles and creating architectures and solutions for corporations in terms of security and business continuity. In addition these consultants had experience within the security industry for between four and twelve years. The interviews were aimed at firstly determining what organisations understood to be the business value of their data and what value they associated with the protection of the data. Secondly, to identify existing data protection strategies for critical business data. The fundamental assumption on which the interviews were based was that most organisations do not differentiate mission-critical data from other data and do not exercise standard data protection and backup practices.

The researchers undertook the problem holistically, firstly through a literature review, and secondly attaining depth through interviews. The research paradigm of choice was qualitative research following an inductive approach and using interviews for data collection. Qualitative research was chosen due to its relevance to this kind of enquiry where there is a mix between the technical (information technology and data) and the governance (security policies and compliance) aspects of information security. Qualitative research answers the complex nature of explored phenomena in natural settings with the aim of describing and understanding the multiple facets of unexplored or under-explored phenomena (Avis, 2003; Creswell, 2007; Yin, 2003; Leedy and Ormorod, 2001; Myers, 1997).

Interview participants and procedure

The researchers sought to furnish an initial understanding of the background of critical business data, threats to data, data protection and associated benefits. Interviews were performed in two streams: (i) semi-structured interviews conducted among ten participants from three South African organisations that provide storage and security solutions and (ii) structured interviews conducted among ten consultants and experts in computer security from four South African organisations that provide consultancy in information security and information systems auditing. A non-probability sampling approach was followed since qualitative research does not aim to produce a statistically representative sample or draw statistical inference. Within purposeful sampling criterion sampling was used which is very strong in quality assurance (Patton, 2001). The particular participants were chosen for a qualitative study because they were believed to facilitate the expansion of knowledge in the protection of critical business data (Henrichsen, 1997; Bogdan and Biklen, 2006).

RESULTS AND DISCUSSION

On the question of the business value of data participants were asked if they understood what their organisations' critical data was. All the respondents said yes to this question. When asked if they understood the different types of data their organisations had and the value of the data only 50% the respondents said yes. When asked if they categorised their data in order to store it for example do data valuation they all said no. An important finding was that whilst the organisations did not define or categorise their data in order to store it accordingly, all the interviewees agreed that from a best practice point of view organisations should determine the value of their business data in order to store it appropriately.

On issues of threats to data all of the interviewees agreed that different types of business data have different types of threats, for example confidential data could be taken by competitors, and credit card data could be taken by hackers. The participants were further asked if they would (or had) advised their clients to perform a data threat assessments related to understanding if there was certain data that was target to specific threats. All the participants once again agreed to have advised their clients. On the question of the types of commonly encountered threats in South Africa the following threats were identified as having been experienced by all the clients of the interviewed consultants: natural disasters, man-made disasters, computer systems failure, external computer threats, and internal computer threats. Only 50% of the respondents thought that man-made threats such as war and terrorism were not a threat in South Africa. The possible impact to the business of data loss is: revenue loss, financial loss via fraud or legislative fines, reputation loss and loss of stakeholder confidence. The impact depends on the confidentiality and type of data lost, and the financial consequences to the organisation. All the interviewees indicated that the impacts differed according to the type of data. The consultants also agreed that it was important for a company to perform a business impact assessment. For example one consultant said "conducting an impact assessment will help the organisation to understand how the business is affected by the occurrence of an impact".

All consultants interviewed concurred that there was a correlation between the value of data, the threats towards the data and the impact on the organisation if it were to be destroyed or lost. The consultants indicated that they had not seen their clients perform business impact assessments. The consultants also suggested that it would make sense to align the data category, along with its associated threats and impacts in order to protect data accordingly. The alignment would however depend on the situation as it may be cost-effective for some companies to protect all data in the same way, that is, to classify all data as sensitive and apply consistent controls. Meanwhile 50% of the consultants said correctly classifying data would make data protection more cost-

Table 1. Summary of findings from the interviews.

Themes questioned	Percentage in agreement
Business value of data	
Organisations understand what critical data is	100
Organisations understand the different types of data and their value	50
Clients do data categorisation	0
Threats to data	
Different types of data have different threats	100
Natural disasters (floods etc.) are a threat to data loss	100
Man-made disasters (war, terrorism) are a threat to data loss	50
Computer system failure (hardware, software) is a threat to data loss	100
External computer threats (viruses or hackers) area threat to data loss	100
Internal threats (accidental or malicious behaviour) are a threat to data loss	100
Change control issues (e.g. patches) are a threat to data loss	100
Threats to data differ per organisation	100
Data threat assessments are important for organisations	100
Data loss impacts	
The impact to the business of data loss depends on the type of data lost	100
The impact to the business of data loss depends on the value of data lost	0
The impact to the business of data loss depends on the confidentiality of data lost	100
The impact to the business of data loss depends on the financial aspects of data lost	100
Organisations should perform a business impact assessment	40
Data protection methods	
Organisations have data protection strategy in place	0
Organisations have a data protection policy in place	50
Organisations store and retrieve data according to its value	0
Organisations have data protection procedures in place	50
Organisations have data protection processes in place	50

effective and help organise recovery priorities. The consultants agreed that it would make sense to have different but simple strategies and methods, depending on the value of data, potential threats to data, and impacts of data loss on the organisation. One consultant said “the data protection strategies cannot be the same for different types of data because the value of the data lost will determine how much the organisation is prepared to spend protecting the data”.

When asked which of these (information lifecycle management, data valuation framework, business continuity, disaster recovery, risk assessment, threat assessment, business impact analysis, and storage architectures) data protection/ storage/ preservation methods were used by their clients the consultants said that information lifecycle management and data valuation frameworks were not implemented within organisations.

The findings show that organisations do not understand or seek to understand the business value of their data. In fact organisations do not know where data reside. Since the World Trade Centre attack companies are more aware of implementing concepts such as business continuity within their departments or across organisations. Organisations are now more open to the fact that a large-scale disaster event may occur or that even a flood can lead to downtime. Either way a disaster of any scale has effect on business operations and availability of data in turn leading to different impacts on the business.

It is prevalent in the findings that some organisations have not considered cost calculations in order to determine the financial impacts related to downtime, and are therefore not aware of how much this downtime could cost their organisations. However, there is a trend that the criticality of certain protection aspects are not taken seriously within certain organisations, with IT departments commenting on the lack of support and buy-in from business (Schwartzel, 2009). This may be due to the executives not seeing cost calculations and not realising the importance of investing in preventative measures. Table 1 gives a summary of the main findings based on the interviews.

Conclusion

The research aim was to investigate the difficulties firms face in protecting and preserving critical business data. Background literature about possible threats that are relevant to organisations' data as well as to the impact that data unavailability or data loss has on the organisations was reviewed together with the interviewing of computer security consultants and experts. The findings show the main problem to be a lack of understanding of what entails an organisation's critical business data and information. Findings that remain a challenge and will probably remain so for some time are: the fact that though companies are generally involved in business continuity practices the storage mediums remain a rather high expense for the organisations, organisations generally do not understand the true value of business data and where the data resides, which affects the data protection processes. Impacts of downtime of a business operation are generally known but companies are not aware of full impact of data unavailability. Costs associated with data unavailability are unknown to organisations as no formula is available to calculate the costs. There are general budget constraints regarding business continuity/disaster recovery in the organisations as disaster recovery is not viewed as a critical business function and lack of buy-in from business as the criticality of certain proactive protection measures are not taken seriously. Data preservation strategies and methods do not get much focus in organisations.

REFERENCES

Avis M (2003). Do we need methodological theory to do qualitative research? Qual. Health Res., 13(7): 995-1004.

Berti M, Costa V (2009). The Ancient Library of Alexandria: A Model for Classical Scholarship in the Age of Million Book Libraries. In International Symposium on the Scaife Digital library (held at the VisCenter of the University of Kentucky). Lexington: Kentucky, pp. 1-26.

Bogdan RC, Biklen SK (2006). Qualitative research in education: An introduction to theory and methods. White Plains. Allyn & Bacon. pp. 15-17

Bogossian M (1998). Sorting through data in the field of data-storage formats. Available from http://albany.bizjournals.com/albany/stories/1998/08/10/smallb4.html (Accessed 12 02/2011).

Bonnette C (2003). Assessing Threats to Information Security in Financial Institutions. Available from http://www.sans.org/reading_room/whitepapers/threats/1143.php (Accessed 11/02/2011).

Burnie M (2002). Protect your data: Network Appliance outlines better ways of protecting and recovering your precious electronic data. J. Banking Financ. Serv. Available from http://www.encyclopedia.com/Journal+of+Banking+and+Financial+Services/publications.aspx?date=200204&pageNumber=1 (Accessed 23/03/2010).

Cane D (2002). Preventing the Great Data Loss Disaster: Data Protection Shouldn't Stop at the Server. Available from http://www.technologyreports.net/securefrontiers/?articleID=1007 (Accessed 9/02/2011).

Chin K (2007). Use a Digital Preservation Plan to Manage Content for the Long Term. Gartner Research Report. Gartner. pp. 6-7.

Cougias D, Heiberger EL, Koop K (2003). The Backup Book: Disaster Recovery from Desktop to Data Center. Lecanto: Schaser-Vartan Books. pp. 39-44

Council of Europe (2009). Data Preservation Checklists. Available fromhttp://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20DataPreservationChecklists_en.pdf (Accessed 10/01/2009).

Creswell JW (2007). Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks. Sage Publications, Inc.

Croy M (2004). The business value of data. Disaster Recov. J., 17(3). Available from http://www.drj.com/articles/sum04/1703-02p.html (Accessed 10/09/2010).

EMC Education Services (2009). Information Storage and Management: Storing, Managing, and Protecting Digital Information. Indianapolis: Wiley.

Fogleman RR (1995). What Information Warfare Means to You. Air Forc. Tims., 55(50): 29-31.

Foster AL (2004). Insecure and unaware. The Chronicle of Higher Education (May 7): A33-A35.

Haeusser B, Osuna A, Bosman C, Jahn D, Tarella GJ (2007). ILM Library: Information Lifecycle Management Best Practices Guide. IBM Red Books. Available from http://www.redbooks.ibm.com/redbooks/pdfs/sg247251.pdf (Accessed 9/01/2011).

Hayes PE, Hammons A (2002). Picking up the pieces: utilizing disaster recovery project management to improve readiness and response time. IEEE Industry Appl. Manage., 8(6): 27-36.

Henrichsen L (1997). Taming the Research Beast, Research Methods: Panning. Available from http://linguistics.byu.edu/faculty/henrichsenl/researchmethods/RM_0_01.html (Accessed 16/01/2010).

Kaomea P (2003). Beyond Security: A Data Quality Perspective on Defensive Information Warfare. Available from http://web.mit.edu/tdqm/papers/other/kaomea.htm (Accessed 9/10/2009). Kitteringham G (2008). Lost Laptops = Lost Data Measuring Costs, Managing Threats. An ASIS International Foundation Research Council Crisp Report. Available from http://www.popcenter.org/library/crisp/Laptop-theft.pdf (Accessed 9/08/2010).

Kahle R (2003). Spreading the Digital Word. Available from http://www.extremetech.com/print_article/0,3998,a=41089,00.asp (Accessed 9/02/2009).

Landry BJL, Koger MS (2006). Dispelling 10 Common Disaster Recovery Myths: Lessons Learned from Hurricane Katrina and Other Disasters. ACM J. Educ. Resour. Comput., 6(4): 1-14.

Leedy PD, Ormorod JE (2001). Practical Research: Planning and Design, Seventh Edition, Upper Saddle River: Merrill Prentice Hall. pp. 56-58.

Liang CC, Wang CH, Hsu PY (2009). Disaster avoidance mechanism for content-delivering service. Elesevier, Comput. Oper. Res., 36(1): 27-39.

MacLeod R (2004). The Library of Alexandria. New York: I.B. Tauris and Company Ltd.

Mariappan R, Parthasarathy B (2009). An analysis of data storage and retrieval of file format system. Indian J. Sci. Technol., 2(9): 38-40.

Massiglia P (2003). The Resilient Enterprise VERITAS Software Corporation, California. pp. 21-33

Moore F (2003). Storage, New Game New Rules, Storage Technology Corporation, Louisville. pp. 11-15.

Myers MD (1997). Qualitative research in information systems. MIS Q., 21(2): 241-242.

Myerson JM (2002). Identifying enterprise network vulnerabilities. Int. J. Network Manag., 12(3): 135-144.

Myerson JM (2001). Identifying threats or assets: which come first? Int. J. Network Manag., 11(4): 207-211.

Ontrack Data Recovery (1998). The Data Recovery Solution. Available from http://www.ontrack.com/library/ontrack02wp.pdf (Accessed 10/03/2011).

Patton MQ (2001). Qualitative Research and Evaluation Methods. Thousand Oaks. Sage Publications.

Peers E (1985). Data Protection Act. Acc., 96(1108): 22-23.

Poker AM (1996). Computer system failure: planning disaster recovery. Nurs. Manag., 27(7): 38-42.
Schwartzel T (2009). A Data Protection Model to Preserve Critical Information from the Possible Threat of Information Loss. MTech Dissertation. Johannesburg: University of Johannesburg.
Seiner RS (2001). Business Impact of Knowledge Management. Available from http://www.tdan.com/view-articles/4943/ (Accessed 19/10/2010).
Silberschatz A, Korth HF, Sudharssan S (2010). Database system concept. Tata: McGraw Hill.
Spoon JC (1999). Ancient Libraries of Greece and Rome: A Summary of Research Findings. Ithaca College online Hist. J. Available from http://www.ithaca.edu/hs/history/journal/papers/sp02ancientlibraries.html (Accessed 21 March 2011).
Synergistic Online Solutions (2009). Business Continuity Issues to Consider for AS/400 Enterprises. Available from http://www.synergisticonline.com/as400_business_continuity.html (Accessed 9/11/2010).
uCertify (2009). The fastest way to IT Certification. Planning a backup and restoration of files for disaster recovery. Available from http://www.ucertify.com/article/planning-a-backup-and-restoration-of-files-for-disaster-recovery.html (Accessed 9/09/2010).
Wrenn G (2005). Data Centre Management Advisory Newsletter: Ten steps to a successful business impact analysis. Available from http://searchdatacenter.techtarget.com/tip/0,289483,sid80_gci1094071,00.html (Accessed 4/10/2010).
Yin R (2003). Case Study Research, Design and Methods. California: Sage Publications.