A New Risk Analysis Method for Data Backup Strategy

Bhavya Jayadevappa
Department of Computer Science
and Computer Engineering
La Trobe University,
Melbourne, Australia.
bhavya.jayadevappa@jpmchase.com

Ben Soh
Department of Computer Science
and Computer Engineering
La Trobe University,
Melbourne, Australia.
b.soh@latrobe.edu.au

***Abstract* - An organization undertakes various steps to make sure that their business runs smoothly without any difficulties. Among them, data protection procedure is the soul of an organisation to recover from a disaster. This minor research aims at proposing a new risk analysis method which facilitates in overcoming issues related to data protection.**

Keywords- Quantitative Risk Analysis, Data Backup, Information Security

I. INTRODUCTION

Over the past few years, organisations have grown interests in implementing more efficient and productive information and communication technologies. Effective risk management assists in balancing act between business and maintaining security [1, 2]. This paper looks at three main areas of concern. Firstly, Information Security being a critical part of the technology is a state of successfully protecting organisation's information assets against the threat of identified risk [3,4], also called as "confidence level". Secondly, Risk Management is an ongoing process used to identify, control and minimize the impact of uncertain events. A risk is an event which can prevent an organisation from reaching its objectives [6]. The four major steps involved in risk management are: risk analysis, risk assessment, risk mitigation and vulnerability assessment and controls evaluation [7]. Thirdly, disaster is a major site loss which has been destroyed or damaged beyond immediate repair. Any organisation cannot ignore to implement this disaster recovery plan just because of its high cost involved in building the recovery plan and hardware required to keep such a large system running safely [5].

In this paper, we attempt to exploit a quantitative risk analysis method, a process of identifying various issues/risks within a data backup strategy and the process of implementing the evolved risk analysis approach for the risks identified for a data backup strategy.

II. BACKGROUND

For any organisation to analyse the risks involved in the data backup strategy, there is a necessity to have an overview of the backup process which includes the procedure for the design of new backup and the latest risk analysis methods in which quantitative methods have been focused.

A. Data backup procedure in terms of Disaster Recovery

Data backup is usually carried out in Operations Department of an organization, whereby a copy of existing file/folder is made and saved in different location (could be onsite/off- site). Management of backup tasks can be facilitated through the policy-based backup / restore software package [9]. The backup can be scheduled with any methods depending on days of the year [10]. The different backup schedules are: daily, weekly, and monthly.

B. Risk Analysis Method in terms of Risk Management

Organisations have enormous number of risk analysis methods to choose from. Using the effective management of the security risks, organisations are better positioned to successfully achieve its objectives [16]. In this paper we focus on three aspects:

1) Quanlitative vs. Quantitave Risk Analysis

In qualitative risk analysis methods, risks are analysed by conducting survey with in an organisation; whereas in quantitative risk analysis methods, risks are analysed using mathematical formulae which are more effective to provide consistent results than the survey approach. As our paper is for a data backup strategy, which has a serious concern of the organisation's assets during a disaster, we proceed our risk analysis approach to be quantitative which gives effective results and allows calculating Annual Loss Expectancy (ALE).

2) A frame work to choose from various Risk Analysis

A number of risk analysis methodologies are available in the market and organisations often find it hard to choose a suitable obe. The work of Anita and Les [12] involves a framework for information security risk analysis methodologies.

3) Latest Quantitaive Risk Analysis methods

Information Security Risk Analysis Method (ISRAM) is a survey based approach to analyse security risks of information technologies [13]. This approach focuses on a group of an organisation's assets. There are several steps to follow which include a preparation phase, survey and risk analysis and in the final step, outcomes are assessed. ISRAM has one single equation to calculate: Risk = (Probability of occurrence of security breach) x (Consequence of occurrence of security breach). ISRAM does not support any ALE, but if the

978-1-4244-4547-9/09/$26.00 ©2009 IEEE

managers insist for the same then an easy conversion could be done by a risk analyst in terms of "dollars".

In Cost of Risk Analysis (CORA), a risk model [12], the data about threats, functions and assets are collected, and the vulnerabilities of the functions and assets to the threats are calculated. Also the losses due to the occurrences of the threats are identified. CORA can also be used on a group of assets. Through CORA a quick risk analysis could be performed which requires little preparation and less information. It is a methodology where the risk parameters are expressed quantitatively and where losses are expressed in quantitative monetary terms. The external risk experts are required to perform the risk analysis. CORA is a two-step process, where in the preparation phase all the contextual information is gathered; in the second step, risk analysis is performed. It is proved that CORA is simple to follow and yields absolute results. The equation: *ALE = Consequence X Frequency; w*here: Consequence = Σn (individual SOLs); *n:* the number of single loss occurrence; SOL = loss potential (worst case monetary value) x vulnerability. With this simple mathematical formula, CORA is simple to follow. Therefore, the ALE is directly obtained in this method.

Through this comparison, the new risk analysis approach proposed in this paper is to provide an easy, simple to follow method. With ISRAM having complex mathematical formula, an attempt has been made to seek a method with simple mathematical equations, so that, unlike ISRAM and CORA, the formulas could be implemented by staff to calculate ALE, and a metrics can be proposed with a scale to the given major categories in which the risks are identified.

III. Threat Identification

In an organization, data protection is a huge concern and a regular risk analysis makes data protection more efficient. This section focuses on the various threats or issues involved in a data backup process which influences the quality control of the technologies.

It is known that various elements like software applications, hardware devices, internet and people from IT teams, the original data are all required to identify threats in data backup and restoration procedure that can be characterized into four categories: File-Based; Internet-Based; Tape Management and Admin.

A. File-Based Threats

As organisation's main asset is the valuable data like client information, financial records, business procedure, employee details etc., which will be saved on to main server through their shared drive. The back-up program first scans the specified shared drive (usually depth-first), then makes a copy on to the tape in the filer*. During this process often, there are issues which cause frequent threats for the overall backup and recovery process. Few of the frequently occurring issues are: (1) restoration failed to recover the requested files, (2) repetition of same file in one or more path (or directory), (3) file open/write failed, and (4) backup restore manager failed to read the file list. From all these errors it is clear that the kind of error and the value of the files which are affected are the most important factors. It also includes the time for which the same has occurred. In order to analyse the risk for File-Based, we need to propose a metrics (see Equation 1 in Section 4).

B. Network-Based Threats

For an on-site or off-site backup process, the mode of data transfer is through internet. Even though there are dedicated lines between the locations, chances of network failure are often present. This network failure in the middle of a data backup process results in loss of time, money, memory wastage on tape and disks. The following network failures can lead to the threats for data backup process: (1) network connection broken, (2) network connection timed out, (3) single source - multiple policies, and (4) client connection refused. These identified risks are analysed (see Section 4 in Equations 2 and 3).

C. Media Management Threats

Although media management process is simple to follow, it is tedious. Each media is given a unique ID both internally by data backup application and externally by data backup administrators. The media are categorized into three types based on its location and purpose it is used for. In rotational media, the data is stored for certain period of time (called as retention period), once the retention period expires, the same media are reused till the next retention period. The archive media is one in which once data is written will be stored permanently. The bad media is one which may have some manufacture defect. Some of the frequent errors are listed below: (1) media mismatch, (2) media missing, (3) no reflection of media even after backup is complete, and (4) media reflection on multiple sites. Among all these risks, the common factors are the value of the file or data which have been copied on to the file and the amount of time involved in the error identification, processing and reaching a solution. This is analysed in Section 4 in Equation 4 of risk analysis for Media Management.

D. Administrator Errors

Backup Administrator plays a major role in scheduling backup policies, and archiving the data for possible future restoration. There has been a diverse effect on the risks mentioned in previous three categories by administrators. Most of the errors mentioned above occur because of ignorance. There are several others which directly prove the fault of an administrator: (1) timed out waiting for media manager to mount volume, (2) client backup was not attempted because backup window closed, (3) the required storage unit is unavailable, (4) failed attempt to allocate memory and (5) Administrators have other duties and will not just be in-charge of backup process alone. With all of these identified errors in the backup application process, a set of equations are implemented to analyse risk and calculate the Annual Loss Expectancy.

* Via communications about the data backup process from my friend, who is working as data backup admin in an Organisation.

IV. PROPOSED QUANTITATIVE RISK ANALYSIS

This is the second phase of new risk analysis method of quantitative approach, a set of equations is proposed for the various risks identified in different categories of data backup strategy. Each of these equations is designed based on risks factors.

A. Risk Analysis for File-Based

According to the risks identified for the category of File-Based, the factors which have been affected are mainly the data, files, folders and time.

The underlying equation for File-Based category is based upon the outcome factors for each *risk* occurs. There are certain *files* which are being affected and also the *time* taken by the backup process in scan and copy of the same. Hence the outcome factors are *Error* (*E*), *File (F)* and *Time (T).* The level of risk depends upon the weight of error occurred. This is shown in Appendix A, Table 1: which is a reference table for the weight values of the errors and also the importance of the affected file should be known to analyse the risk. This is shown in Appendix A, Table 2: which is a proposed reference table for the weight values of files.

To analyse the risk for File-Based, we calculate: over the time period T, the product of total number of weighted errors occurred and the total number of weighted files which are being affected. This is given by:

$$\text{Analysed Risk} = \frac{\{(E_i)\}\ \{\sum W(F_j)\}}{T} \quad \textit{erroneous files / hr} \text{ - (1)}$$

where, W: weight values for Error as given in Appendix A Table 1 and for File as given in Appendix A Table2; E: The type of error occurred and which has been identified; i: the number of types of Error (E) occurred at each analysis; F: the File which has been affected due to the occurrence of Error (E); j: the number of files which are affected due to the occurrence of Error(E); T: the total time for which the error had occurred and the files were affected.

For example, if two errors have occurred Error E_1 high risk and Error E_2 low risk. Suppose, for E1 the number of files affected are 3 i.e. F_{11}, F_{12} and F_{13} and for E_2, the number of files affected are 5 with F_{21}, F_{22}, F_{23}, F_{24} and F_{25}. By applying equation 1,

Analysed Risk (File-Based)

$= [\{W(E_1) + W(E_2)\}\ \{W(F_{11}) + W(F_{12}) + W(F_{13})\}\{W(F_{21}) + W(F_{22}) + W(F_{23}) + W(F_{24}) + W(F_{25})\}] / T$

$= [\{(3)+(1)\}\ \{(2)+(1)+(4)+(5)+(3)\}] / 2$

$= [\{4\}\{15\}] / 2 = 30$ *erroneous files / hr.*

Therefore, the total risk analysed here for File-Based is given as 30 files in hour. But when the actual risk analysis process is carried out for each year the value varies highly depending on error types, and the total files affected. This has been represented in Section 5 based on different scenarios so as to compute the ALE.

B. Risk Analysis for Network Based

The outcome factors which are affected by risks identified in Section 3 for this category are cost of the internet link, delay faced by the scheduled policies which are waiting in queue, the files and time. This Network-Based category is proposed with two equations: (a) Network slows down; (b) Network fails.

1) For network slowdown, the underlying equation for this category is based on the fact that as speed of network link reduces, the rate of data transfer reduces which implies delay increases. Here delay is taken for the policies which are waiting in the queue to get fired. The cost of the network for which the policies were delayed is given by "C". Hence the network speed is inversely proportional to delay and is given as

$$\text{Risk Analysis}_{slow} = (K / d) * C \quad \$ \textit{ per hr} \text{ ----- (2)}$$

where, K: Is a constant = 1; d: the total time (in hours) for the policies to wait in the queue; C: Cost of the network delay;

For example, suppose due to the slow internet connection, the Friday backup policy running since 6 p.m. is not yet complete even after Saturday 6 p.m. and the weekly policy has been cancelled and made to wait in the queue. Total time, the weekly backup policy is made to wait in the queue is the delay time. Now if the delay is about 2 hours. Then by applying Equation 2, (assuming cost of internet is $4/hr.)

Risk Analysis (Network-Based) $_{slow}$ = (K / 2) * 4 *$per hr*

= 0.5 * 4 *$ per hr* = $ 2 *per hr*

Hence, it shows how much more does company has to pay towards internet for every one hour delay. This provides a value which is used to know the effects of the network impact. The same has been represented as a scenario with a real world situation which adds up to calculate the organisation's ALE in Section 5.

2) For the network disconnected, the underlying equation is based on the fact that when the link is completely disconnected there will be major impact on the data for which the backup has stopped, the cost for the internet link and total time involved.

$$\text{Risk Analysis}_{disconnected} = \sum \{W(D) * C * T\}\ \$ / hr \text{----- (3)}$$

where, W: the weight value of the data as shown in Appendix A Table 3; D: the data affected by the error and is due to be backed up; C: the total network cost (in AUD) in both the instances before the network failure and after the network status is up till the backup process completes; T: the total time from the start of the backup till the end; this also includes the time gap between the network failure and recovery of the same.

For example, assuming there are policies belonging to different media servers that have been fired 1 hour ago and need 2 more hours to complete; and suppose if one of the backup servers' link goes down in the middle of a process, then the corresponding policies fail. There may be a time gap of 30 minutes to bring the link status up. After which the same policies will be re-fired and may take another 3 hours to

complete. The risk here is with weight value of the data affected, the cost for the network utilization from the error occurrence until the completion and total time for the same. The risk can be analysed by applying equation (3), (Suppose if the cost of the network per hour is about $ 4; then for 4 hours and 30 minutes, the cost is $18). Therefore,

$$\text{Risk Analysis}_{\text{disconnected}} = \{3*18*4.5\} = \$\,243$$

Hence when the network fails, there will be a major effect with unnecessary cost adding up to the organisation expenditure. The same has been shown in a real world situation in section 5, when added with other categories of risks as what will be the total ALE.

C. Risk Metric for Media Management

As discussed in section 3 about the various risks identified within this category, the common factors obtained are the weight of the Media (which is implied to Data). This is because there may be restoration requests of the file from the media which have any of these errors, and also the time taken to solve the problem. In order to analyse the risk factor for media management, the equation required is as follows:

$$\text{Risk Analysis} = \sum\{W(M) * T\} \quad \text{----------} \quad (4)$$

where, W: is the weight value for the type of media, as shown in Appendix A Table 4; M: is the media type for which the priorities are set based on for what kind of backup process the same is utilized; T: is the total time involved for the overall media management.

For Example: Let us consider the risk identified in the same media reflecting in multiple sites. If there are 5 rotational media and 5 archive media reflecting in two different locations for each of them, then administrator spends around 2 hours to trace those media. By applying the equation (4), the risk analysis for media management is given by:

$$\text{Risk Metric Media Management} = [\{\sum W(M)\} * T]$$

$$= [\{W(M_1)+W(M_2)+W(M_3)+W(M_4)+W(M_5)\} * 2] + [\{W(M_6) + W(M_7) + W(M_8) + W(M_9) + W(M_{10})\} * 2]$$

$$= [\{1+1+1+1+1\} * 2] + [\{2+2+2+2+2\} * 2]$$

$$\text{Risk Metric Media Management} = 20$$

With this risk analysis of media management we know as to how the media management plays a major role for the backup process in an organisation. Even with simple mistakes there could be heavy loss for the company. This has been shown in section 5 with real world situations with other categories of risk, so as to calculate ALE.

D. Measures for Administrator Errors

The little ignorance or the simple mistakes can put the whole backup process and recovery into hold. As we have seen various errors or risks because of administrators, there cannot be one generic equation proposed for this category. We have to make sure that administrator's errors are reduced by a set of precautionary measures are proposed: (1) regular monitoring of the backup application used. (2) time-to-time regular tape movement (3) Prioritize the policies for the backup. (4) Keep track of the media and schedule of policies. (5) New backup policies scheduled by administrator have to be carefully designed by making sure there will be no overlap amongst them. (6) Before the backup is fired, administrator has to check whether sufficient number of medias is present in the library. Finally an administrator's goal should be to complete the backup process successfully.

V. Implementation of Model

This implementation part of our paper represents the real world situations, in which we try to identify the various risks involved in the data backup strategy. The proposed risk analysis method given in section 4 is applied to the identified risks which results in the metrics which lets the Organisation knows the level of risk attained and the loss which they have to incur. Each section's scenario represents the categories on which the equations have been derived.

A. Scenario for File-Based

The Daily backup policy for each department's files will usually be scheduled to start after their shift hours. Suppose in the time of a major audit, a user has worked hard on 3 important files with major updates in his entire shift of 8 hours and extends after business hours (may be for about 5 hours than usual). Now when the backup policy for this has started a "File write" error has occurred and the updated file is not backed up yet. To this now the user has unintentionally deleted a file. So the user's first step would be to raise a request for the restoration of the deleted file. And also if the user had created and deleted these files after the backup has started then there is no possibility to fetch these deleted files. This is the point of time it is called a risk and when analysed by applying equation (1) as given below:

$$\text{Risk Analysis} = \frac{\sum W(E_i)\} \{\sum W(F_j)\}}{T} \; \textit{erroneous files / hr}$$

Here the two errors are, E_1 being "File write" and E_2 being "File created and deleted after the backup process started". These errors are assessed by using the Appendix A Table 1 given in section 4. Now, the number of files affected by each of these errors is three given by F_{11}, F_{12}, F_{13} and F_{21}, F_{22}, F_{23}. The outcome is as below:

$$= [\{W(E_1) + W(E_2)\}] [\{W(F_{11}) + W(F_{12}) + W(F_{13})\} + \{W(F_{21}) + W(F_{22}) + W(F_{23})\}] / 5$$

$$= [\{3+2\}][\{(3) + (2) + (3)\} + \{(3) + (1) + (2)\}] / 5 = 14$$

Risk Analysis (File-Based) = 14 *files in hr*

Hence the risk analysis obtained for 2 errors with 3 files affected is 14 *erroneous files / hr.* If the same situation arises for several times a week or in a month then the risk is even higher. To calculate the loss incurred by this category with various such threats, a reference is to be made to the Table 5 as given under the section of Annual Loss Expectancy.

B. Scenario for Network-Based

As the Network-Based category has been divided based on "Slowdown" and "Disconnection", the scenarios for the same has been provided. We know that in this category we can directly calculate the Annual Loss Expectancy without the need of reference table.

1) Network-Based for Delay

Assume the policies for daily backup (which is an incremental backup) are scheduled to start at 6 p.m. on each day and finish off before 6 p.m. of next day; and the weekly backup policy (which is a full backup) are to start on every Saturday at 6 p.m. Now, when the daily backups for Friday has started and is running and in the half way, suppose if the internet link slows down then the rate of data transfer is decreased and time taken to complete is increased. In this case daily backup policies are yet to be done even after Saturday 6 p.m. But at the same time weekly backup will automatically fire up at Saturday 6 p.m. Since there is a delay, an administrative staff will manually stop (set to wait back in the queue) the weekly backup and allow the previous policies to complete. Finally the daily backup is complete on Saturday at 11 p.m. and the weekly backup can now be fired. This shows the time delay for weekly backup policies is about 5 hours. By applying equation (2), the risk of the weekly backup policies is the total time waiting in the queue for the same to start running, which is given by,

$$\text{Risk Analysis (Network-Based)}_{slow} = (1/5) * 4 = 0.2 * 4$$

$$\text{Risk Analysis (Network-Based)}_{slow} = \$\ 0.8\ /\ hr$$

There is around $1 more for every 1 hour delay and there will be cost towards internet usage as required by the backup policy as well.

2) Netwwork-Based for Disconnetion

Assume the policies for monthly backup (which is a full backup) are scheduled to start at 6 p.m. on Saturday and are fired accordingly. Usually monthly backup has to be completed before Monday 6 p.m. because there will be daily backup policies starting at 6 p.m. Now the policy has run for a day and on Sunday at 6 p.m. there is a connection failure between media server and the client and this may have a time gap of 20 minutes to bring the link with status UP. Now this is a risk as the monthly backup has to be re-fired, and will delay the policies scheduled for Monday backup. There is another risk in terms of the cost of the network utilized before and after the risk occurrence. By applying equation (3), Here the weight value of the data has to be considered which is most important with value as 3, this is because monthly backup policy has higher priority compared to other two. The total time taken by this single policy from first fire-up till the completion is 72 hrs and 20 minutes which is 72.3hrs. and the total cost for the entire length of the backup for the above calculated time is $289.3.

With this data when applied to the equation for Risk analysis for the Network-Based when disconnected is:

$$[\{(3) * (4) * (72.3)\}]\ \$\ /\ hr = \$\ 289.2 \text{ for total time.}$$

Hence the total risk in this category in terms of ALE is about $289 for the entire length of risk. Suppose if similar risks occur on several occasions for the whole year, then the loss incurred is very much more.

C. Scenario for Media Management

Assume there is a restoration request from a user whose data has been archived and stored in the bunker 8 months ago. For this, the administrative staff will first search for this media in the application database. In this search, the required media location details are obtained and the admin moves to storage area in search of the same. But in the physical location there may be some other media present. This is a risk of media mismatch. So, now the staff will have to make another search for the missing media (which is required for restoration) by giving the details of the mismatch media that was obtained physically. This may give the missing media location or may have some other problem. With these risks of "media mismatch" and "missing media", the staff might have spent about 1 hr. Here the risk in the media management is maybe because of ignorance of the staff or some error caused by the application database itself. This risk can be analysed by applying equation (4), which is: $\sum\{W(M) * T\}$

In this scenario, there are two risks "Media mismatch" and "Media missing", since the media is from an archive database, the weight value is also high and time spent is about 1 hr. When the same is analysed we get: (Note: There two medias for which risk has to be analysed)

$$\text{Risk Metric in Media Management} = \sum\{W(M) * T\}$$

$$= [\{(3)*(1)\}+\{(3)*(1)\}] = 6$$

Hence the risk analysis obtained for 2 rounds of media search in an hour is about 6. If the same situation arises for several times a week or in a month then the risk is further higher. To calculate the loss incurred by this category with various such threats, a reference is to be made to the Table 5 as given under the section of Annual Loss Expectancy.

D. Annual Loss Expectancy(ALE)

Annual Loss Expectancy is the loss which could be expected by an organisation where the risks are assessed and are calculated for each year. This is given by product of Single loss Expectancy and Annualized rate of occurrence.

Annual Loss Expectancy can be directly used for a cost-benefit analysis. The risk analysis calculated for File-Based in section 5.1 resulted in 35 files/hr, when we refer to Table 5, the loss to the company can be up to $2000 per year and can be realized as an important consequence and in the risk analysis calculated for media management in section 5.3 resulted in 6 volumes, when we refer to Table 5, the loss to the company can be up to $1000 per year and can be realized as Minor consequence. This assists administrators to take appropriate countermeasures in their decision making.

VI. Conclusion

This paper proposes a new risk quantitative analysis method in relation to information security of data backup

strategy. The proposed method helps to identify repeated risks and provides an aid to take some necessary action. An application gap can also be recognized by administrator and request for better software, which in turn helps an organisation maintain its quality control and can expect more productive work from the backup team. Finally the appropriateness to Annual Loss Expectancy calculations is achieved and can be presented to the senior management. The future work includes the design of a software tool for automation, where an administrator can run the tool and gather the required information more in a cost effective manner for risk analysis.

ACKNOWLEDGEMENT

This work is produced under the auspices of La Trobe Post Graduate research. I thank my supervisor Ben Soh, my parents and family and my friend Mr. Raghuveer M Revankar for the support, encouragement and guidance.

REFERENCES

[1] M. E. Johnson and E. Goetz, "Embedding Information Security into the Organization," *IEEE Security & Privacy*, vol. 5, no. 3, 2007, pp. 16-24.

[2] D. Ruiu, "Learning from Information Security History," *IEEE Security & Privacy*, vol. 4, no. 1, 2006, pp. 77-79.

[3] T. R. Peltier, J. Peltier and J. Blackely, "Information Security Fundamentals," *Auerbach Publications*, New York, 2004.

[4] CRIM, "Data Summary Sheet - Organisation," *ISIQ,* pp. 1-5.

[5] E. G. Mallach, "Decision support and data warehouse systems," *Mc-Graw Hill Publications,* Boston, 2000.

[6] J. Sally and A. Koronios, "Information Technology Security & Risk Management," *Wiley (John Wiley & Sons)*, Australia, 2006.

[7] T. R. Peltier, "Information Security Risk Analysis," *Auerbach Publications*, New York, 2005.

[8] W. H. Baker and L. Wallace, "Is Information Security Under Control?" *IEEE Security & Privacy*, vol. 5, no. 4, 2007, pp. 36-44.

[9] J. W. Toigo, "disaster Recovery planning," *Prentice Hall PTR,* New Jersey, 2000.

[10] D. Holme and O. Thomas, "Managing and Maintaining Microsoft Windows 2003 Environment," *Prentice Hall of India,* India, 2004.

[11] J. Rees, S. Banyopadhyay and E. H. Spafford, "PFIRES: A Policy Framework for Information Security," *Communications of ACM,* vol. 46, no. 7, 2003, pp. 101-106.

[12] A. Vorster and L. Labuschagne, "A Framework for comparing different Information Security Risk Analysis Methodologies" *Proceedings of SAICIST*, 2005, pp. 95-103.

[13] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method,"*Computers & Security*, vol. 24, no. 2, 2005, pp. 147-159.

[14] D. Evans, "How to Write a Better Thesis or Report," *Melbourne University Press*, Victoria, 1995.

Appendix A

Weight Value	Explanation
3	Is a high risk error with NO countermeasure in place and contributes directly to risk factor
2	Is a medium risk error with few countermeasure in place and contributes somewhat directly to risk factor
1	Is a low risk error with enough countermeasures in place and contributes indirectly to risk factor.

Table 1: Proposed reference table for the weight values of the Errors

Status	Weight Value
Is High importance, Immediate recovery required	3
Is medium importance, some what immediate recovery required	2
Is low importance, No immediate recovery	1

Table 2: Proposed reference table of weight values of the status of affected file

Importance of Data	Weight Value
Most Important	3
Some what Important	2
Little Important	1

Table 3: Proposed reference table of the weight value of the Data.

Type of Media	Weight Value
Archive Media	2
Rotational Media	1
Bad Media	0

Table 4: Proposed reference table of the weight value of the media types

File-Based (erroneous files per hr)	Media Management	Quantitative Scale	Annual Loss Expectancy (ALE)
Less than 50	Less than 10	**Minor Consequence (1)**	**$ 1000**
Between 50 and 100	Between 10 and 50	**Important Consequence (2)**	**$2000**
More than 100	More than 50	**Serious Consequence (3)**	**$3000**

Table 5: Proposed reference table of the quantitative scale to calculate ALE for the File-Based and Media Management categories