ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Data Recovery: An Empirical Investigation of Key Executives in Small and Medium Enterprises.

Dr. Jasmin Padiya*

ABSTRACT

Data security is a prime concern for any organization. This paper aims to critically examine various facets of enterprise data security and awareness amongst key executive about potential hazards of data security. The survey probes key executives of small and medium enterprise about their awareness and preparedness pertaining to data security and recovery. Finding reveals that majority of executives are having satisfactory awareness level requiring thirst for data security policy formation and compliance.

Key Words: Data Security Awareness, Enterprise, Data Protection, Information Security

Introduction

The most essential asset in any organization is the data that is being processed and possessed. Loss of any critical information can be devastating to any organization. Hence, protection of data is the most important activity performed on any computing environment. Data security is a way of keeping data protected from unauthorized access & corruption. The aim of data security is to ensure privacy while securing personal or corporate data . In present business world, IT network is the most critical to efficient operations. Due to this dependence, networks will continue to be target for intruders outside and within an organization. To gauge the operational availability of these networks, developing an awareness of overall network security is equally vital as the operational status of the networks themselves .

Literature Review

Majority of users while disposing old computer and hard disk removes all of the files or formats it. Surprisingly, many users believes that removing files from hard disk and emptying recycle bin means permanent deletion of data. In a study recovered 300, 00000 files from 55 HDDs of donated computers. Finding reveals that there is an important need about awareness regarding data security. The strategies used for data security vary depends on the kind of data to be protected, media used and nature of industry. Organization users receive phishing messages nearly every day, and most of the users are inadequately trained to identify and safely response to them . Spear phishing is a popular way of infecting organizations with malware. A study by **PhishMe (2012)** revealed that 27% of security professionals admitted that top executives in their organizations have been attached within last 1 year. **SAI** Global's Benchmarking Survey 2008 reveals that 95% of employees consider information security is vital. However, there is a lack of knowledge and training pertaining how to identify and report incidents.

A study by **Schwartzel & Mnkandla (2012)** concluded that there are budget limitations regarding disaster recovery in the organizations as disaster recovery is not perceived as a vital business function and lack of commitment from the top management. Data preservation strategies and methods require much more attention than it has been paid.

Security awareness training only will not suffice security of an organization. Though training plays a vital role, compliance with the policy is more important. Information security must adopt a layered approach including both technical and nontechnical solutions. The biggest weak link in information security is human error or intention .

Organizations need to design and implement measures to protect their valuable data from internal misuse, without imposing blockades that confine their employees' ability to perform their duties. In present environment, those who are perceived as being incapable to protect the confidential data entrusted to them will experience loss of consumer confidence- and the related consequences.

Objectives

1. To measure awareness level among the corporate and SMEs about data recovery.

**Associate Professor - Marketing Area GLS Institute of Computer Technology (MBA) GLS Campus, Law Garden, Ellis Bridge, Ahmedabad – 380006.*

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

2. To study the corporate behaviour in post data disaster recovery.
3. To identify trends in corporate about Information security & Data confidentiality.

Methodology

Research Design: Descriptive

Population: Sr. Managers/Key executives of small and medium enterprises who are responsible for IT related decisions from following sectors in Ahmedabad city

- IT
- Multimedia
- Pharmaceutical
- 4 star and 5 star Hotels
- Govt. and private Hospitals
- Others (placement services, consultancy, etc.)

Sample unit: Key Executives who are responsible for IT related decisions

Sample size: 150

Sampling method: Non-probability purposive sampling

Research Instruments: Questionnaire & In-depth Interview

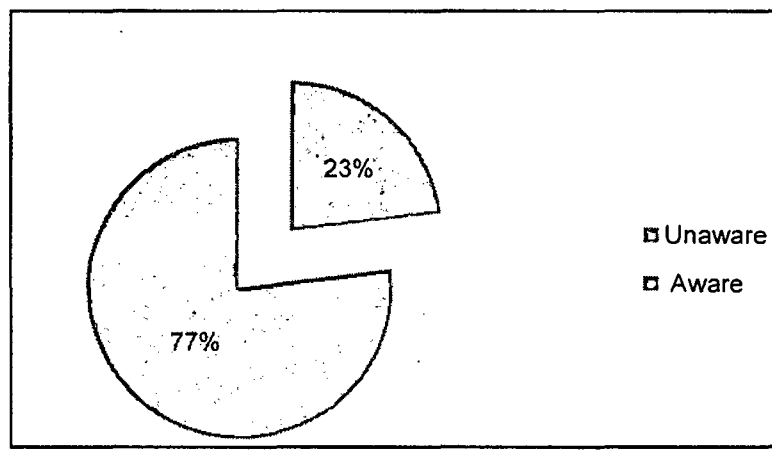
Results

Overall Awareness about Data Recovery

Table 1 Overall awareness

	Aware	Unaware
Overall Analysis of Awareness	77%	23%

Figure 1 : Overall Awareness on Data Recovery



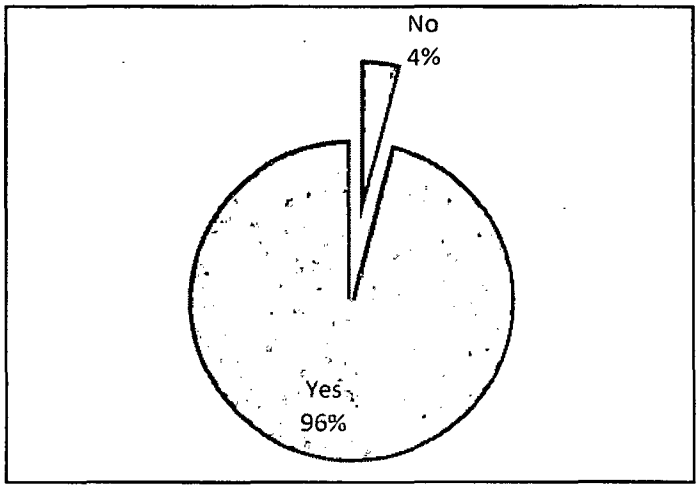
Majority of senior managers were aware about data recovery concept, however to assess their accurate awareness level further specific questions were asked.

Table 2 Awareness about Data Recover after Deletion from Recycle Bin

Question	Yes	No
Did you know that data can be recovered after deletion from recycle bin?	144	6

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Figure 2 Awareness on Data Recovery after deletion from recycle bin

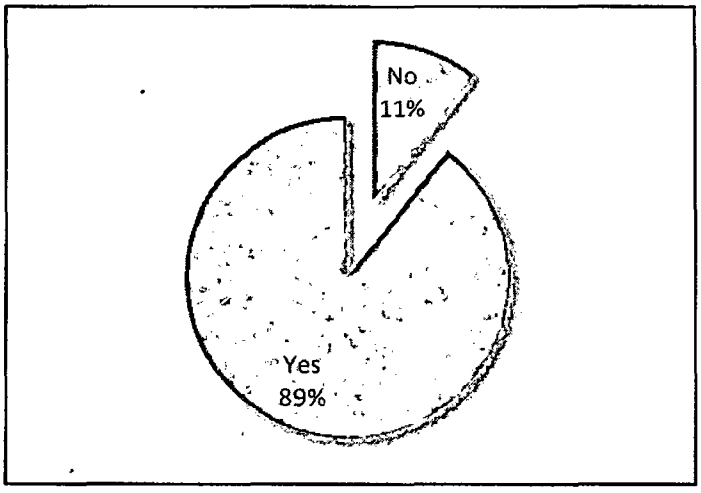


There is a great level of awareness about data recovery after deletion from recycle bin

Table 3 Awareness about Data Recovery from Formatted Hard Disk

Question	Yes	No
Did you know that data can be recovered even after formatting the HDD?	134	16

Figure 3 Awareness on possibility of Data Recovery from formatting the HDD



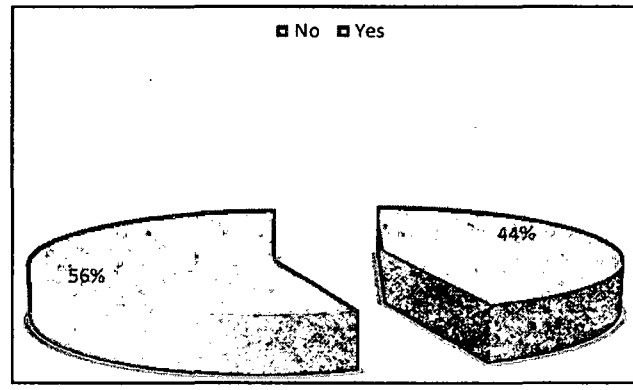
There is very high awareness level about data recovery from formatted hard disk.

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 4 Awareness on possibility of Data Recovery when HDD is note detected in BIOS

Question	Yes	No
Did you know that data can be recovered when HDD does not detect in BIOS?	84	66

Figure 4 Awareness on possibility of Data Recovery when HDD is note detected in BIOS

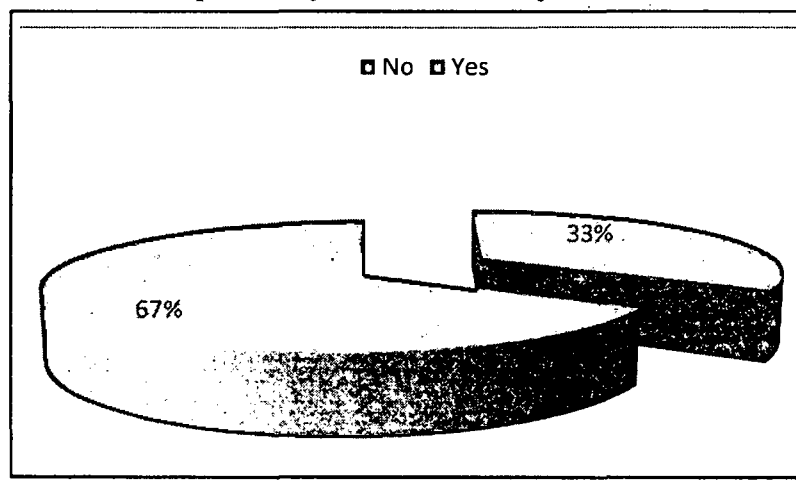


Sr. Managers are having comparatively low awareness about data recovery when HDD is not detected in BIOS.

Table 5 Awareness on possibility of Data Recovery –No Detection of Hard Disk

Question	Yes	No
When your maintenance engineer says HDD not detecting and it has to be replaced then are you aware data recovery is possible?	100	50

Figure 5 Awareness on possibility of Data Recovery –No Detection of Hard Disk



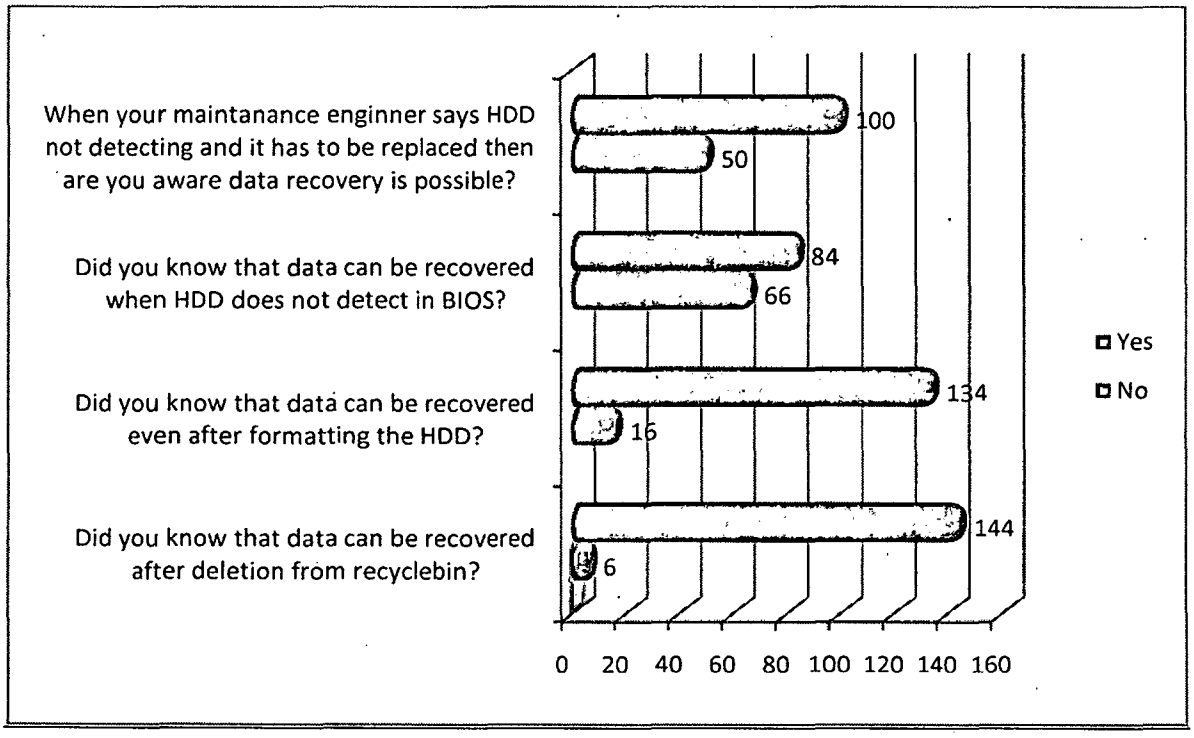
There is a moderate level of awareness about data recovery in case of no detection of hard disk amongst sr. managers.

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 6 Comparison of different types of awareness for data recovery

Question	Yes	No
Did you know that data can be recovered after deletion from recycle bin?	144	6
Did you know that data can be recovered even after formatting the HDD?	134	16
Did you know that data can be recovered when HDD does not detect in BIOS?	84	66
When your maintenance engineer says HDD not detecting and it has to be replaced then are you aware data recovery is possible?	100	50

Figure 6 Comparison of different types of awareness for data recovery



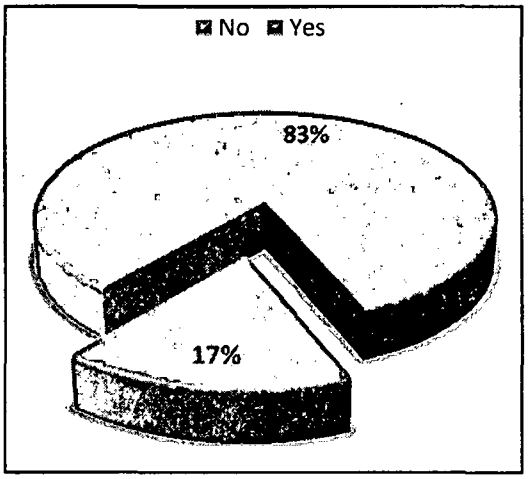
Sr. mangers are comparatively less aware about possibility of data recovery in case of no detection of hard disk by maintenance engineer and BIOS.

Table 7 Awareness -Class 100 Clean Room Environment

Question	Yes	No
Are you aware of Class 100 Clean Room Environment?	124	26

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Figure 7 Awareness of Class 100 Clean Room Environment



There is very low level of awareness about Class 10 clean room environment amongst sr. manager.

Table 8 Data loss causes in any organization can be classified as follow

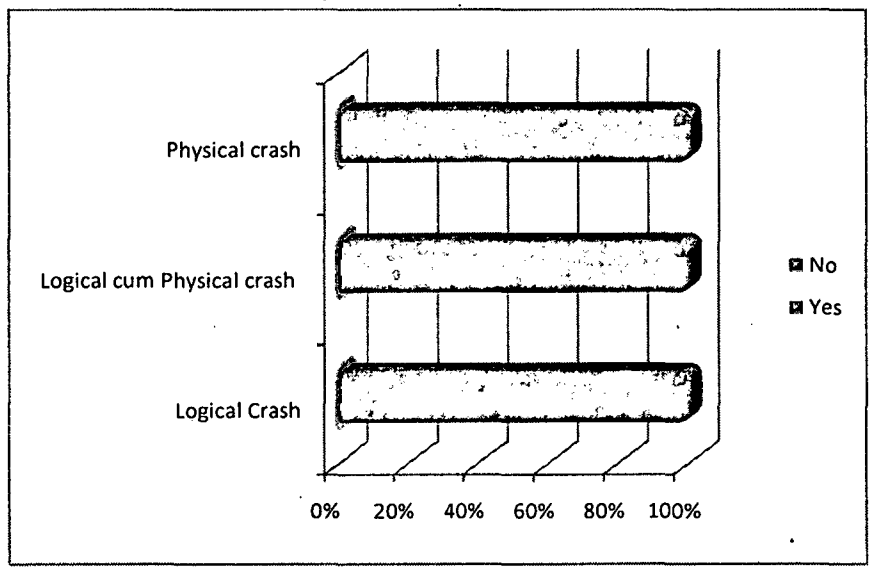
Accidental deletion of files/folders/partition Accidental format of a logical drive/ entire HDD Internal corruption of MS word/Excel/ Access / zip files Internal corruption of MS outlook/ outlook express	Logical Crash
Operating system/ application failure	Logical cum Physical crash
Physical damage of HDD	Physical crash

Table 9 Categories of data loss

Type of Crash	No	Yes
Logical Crash	62	88
Logical cum Physical crash	57	93
Physical crash	71	79

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Figer 8 Different types of crash faced by firms



Around 60% of the corporate find logical cum physical crash on their system along with the logical crashes. The combine counting of these two crashes is almost same so we can say that the corporate who find logical cum physical crash, also find logical problems.

Physical crash problems occur less as the corporate care and maintain their systems to protect from the physical damage which may cause the data unrecoverable.

Table 10 Correlation table of media crash

Particulars	Logical Crash	Logical cum Physical Crash	Physical Crash
Logical Crash	1		
Logical cum Physical Crash	0.16403	1	
Physical Crash	0.01225	0.02806	1

Here the correlation between Logical, Physical and Logical cum Physical crash is shown.

From the statistics in the table it is clear that all the variables have positive correlation among them. That means all variable tend to move in the same direction or all three variables tend to increase or decrease together. Logical crash and logical cum physical crash are significantly co-related with each other than other two combinations. Physical crashes and logical crashes are least co-related with each other.

Table 11 Table Summary Output

Regression

Regression Statistics	
Multiple R	0.998159
R Square	0.996322
Adjusted R Square	-2
Standard Error	6.615076
Observations	1

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 12 ANOVA table of media crash

Particuler	df	SS	MS	F	Significance F
Regression	2	11854.24	5927.12	270.8969	–
Residual	1	43.75923	43.75923		
Total	3	11898			

As the relationship between these two variables is linear, linear regression is the best tool to sure co-relation.

Figure 9 Linear regressions among "Logical Crash" & "Logical cum Physical Crash"

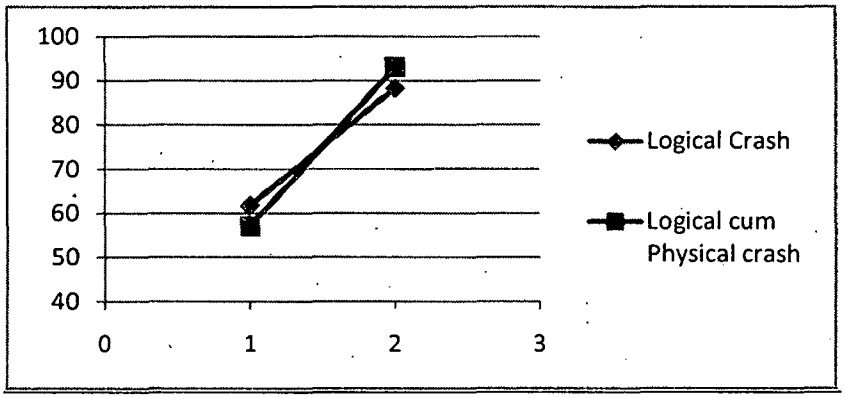


Table 13 Recovery Tool Usage & Ownership

Questions	No	Yes		
Do you use any post data disaster recovery tool?	111	39		
Did you get the data that you were looking?	111	27	12	0
		All Data	Partial Data	Irrelevant Data

Figure10 Probability of Data Recovery

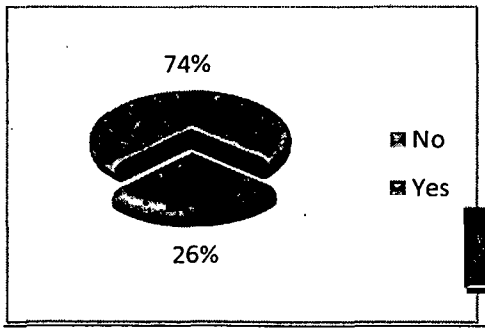
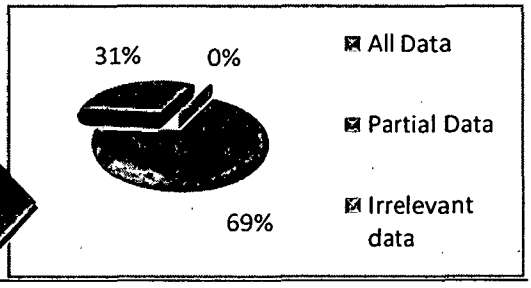


Figure11Extent of Data Recovery



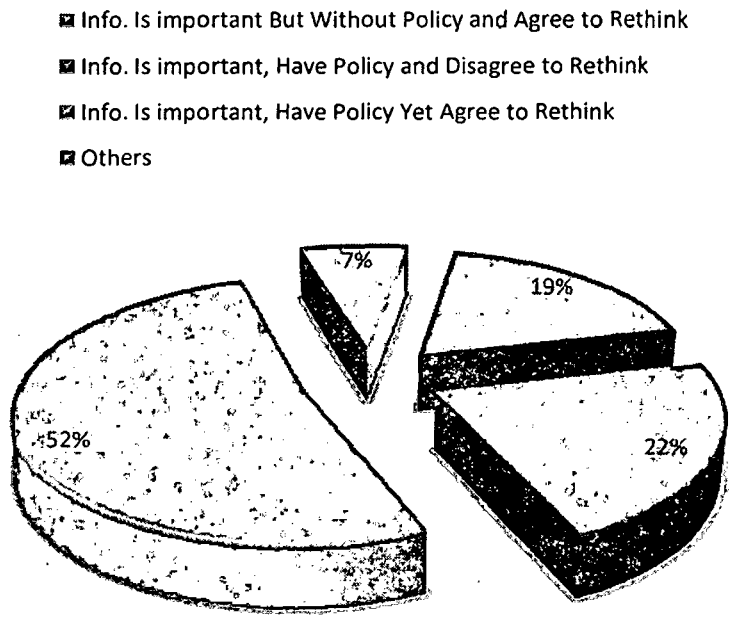
From above charts it is obvious26 % corporate are using post data disaster recovery tool and out of that 31% person were able to recover all data. Whereas 31% respondents were not able to recover 100% data, they were only able to achieve partial data around 60% to 70% on average.

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 14 Importance of Information

Types	Information Is important But Without Policy and Agree to Rethink	Information Is important, Have Policy and Disagree to Rethink	Information Is important, Have Policy Yet Agree to Rethink	Others
No. of corporate	28	33	78	11

Figure 12 Data Security Policy



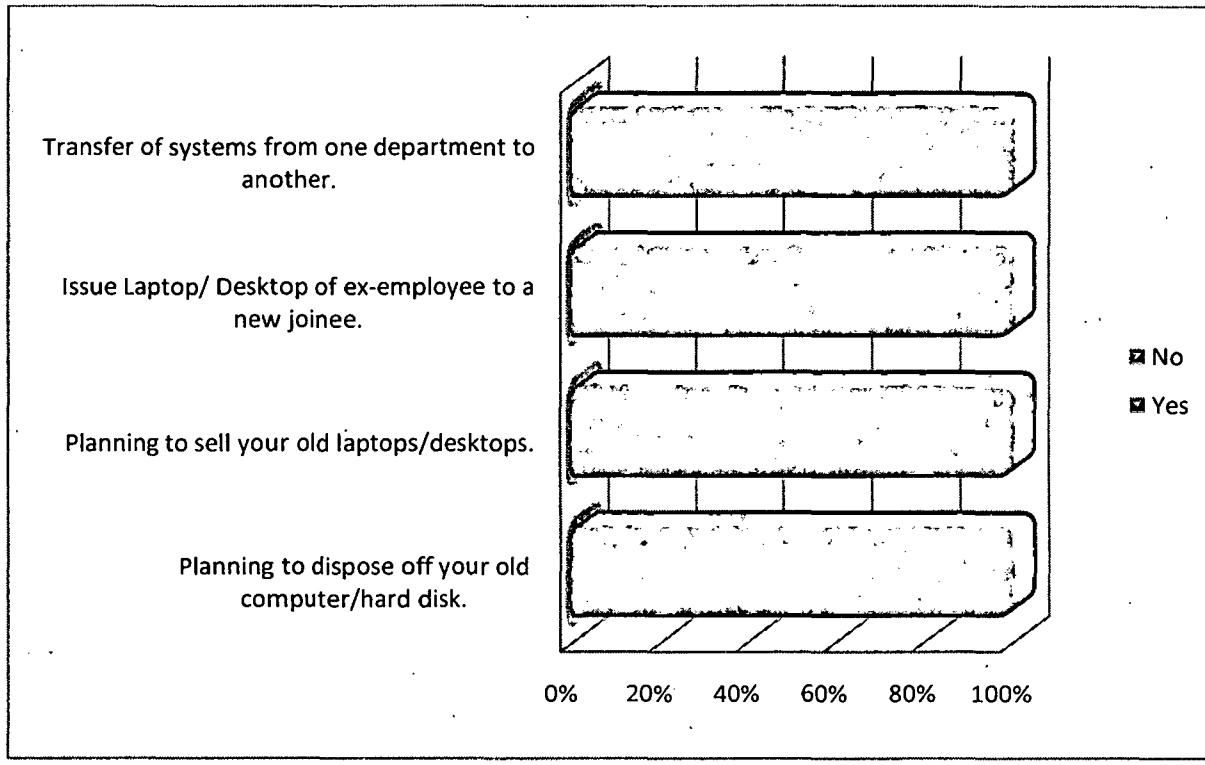
From graph one can say that around 90% of corporate finds their information important. 70% of firms are having policy for information security / data confidentiality in their organizations. Among those 90% corporate 50% are seriously thinking about Information security or data confidentiality. They still want to re-think on Information Security to save their valuable information from loss or misuse despite of having a policy to secure their data.

Table 15 Data Risk Perceptions

Do you think that your data is at risk due to any of the following situation?	No	Yes
Planning to dispose off your old computer/hard disk.	25	125
Planning to sell your old laptops/desktops.	34	116
Issue Laptop/ Desktop of ex-employee to a new joiner.	79	71
Transfer of systems from one department to another.	76	74

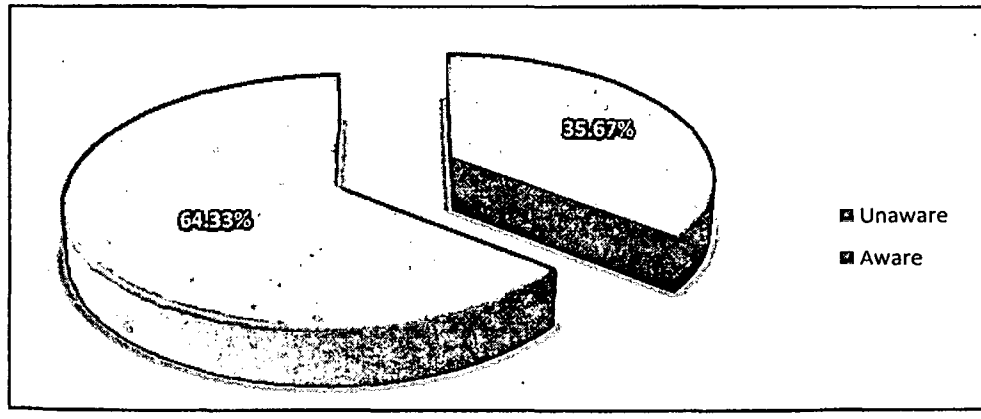
ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Figure 13 Data Risk Perceptions



Most of the corporate find risk for the first two situations. They are aware that their data is at risk if they dispose off their old computer/hard disk because the party who is going to purchase may recover their data even though the corporate had formatted their hard drive, and hence they may misuse the data. Similarly, IT managers are also aware about the risk of data security due to selling of old laptop/computers. They are measuring the risk that may occur because of data recovery from laptops/desktops. On the other hand they find issue Laptop/ Desktop of ex-employee to a new joiner less risky than 2 early scenarios. The main reason behind this measurement is that corporate are thinking that, they issue laptops of old employees to new joiner who handed over the charge of the same position so that is not risky. However, managers are not considering that personal data of the ex-employee may be revealed to new-joiner. As well as if they are not issuing laptops to the same profile the new joiner can have confidential and inaccessible data with him and he may miss use it. Managers perceive that transfer of systems from one department to another is less risky. However they are not aware that other department can derive secret data.

Figure 14 Risk Measurement Capabilities



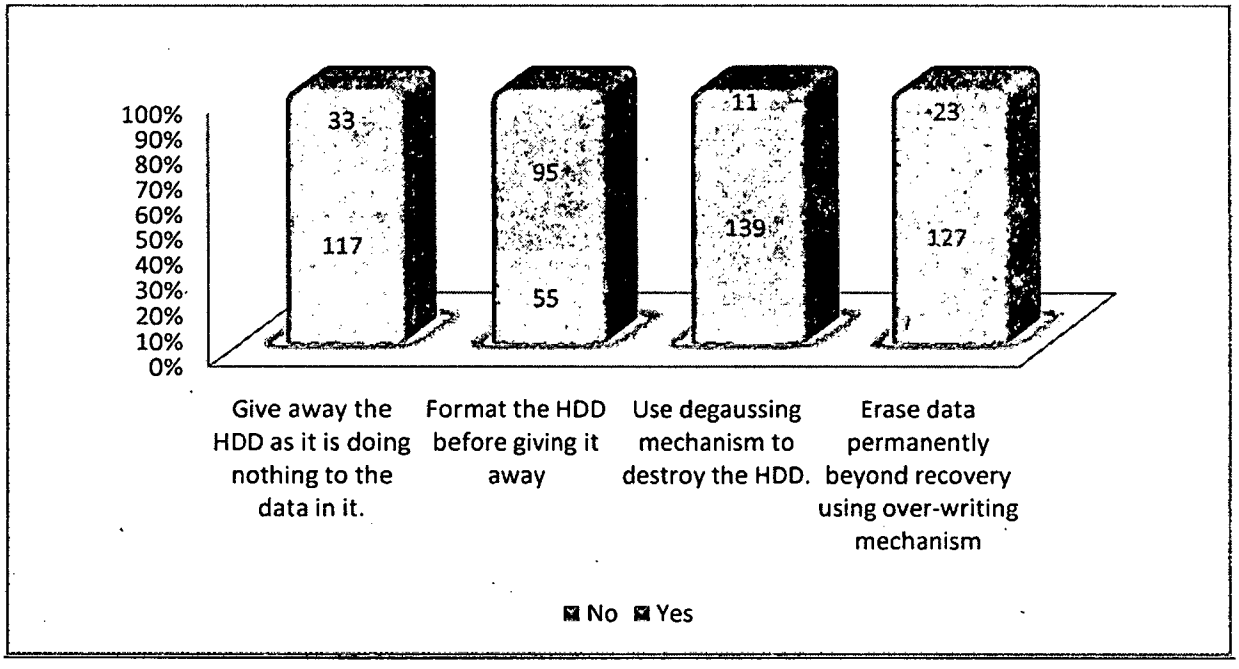
ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

The graph clearly indicates that 65% of the corporate are aware and capable of measuring the data risk due to the given scenario. 35% are still not thinking seriously about data risk. Organizations should change their risk checking approach for better information security or data confidentiality in their organization.

Table 16 Dispose of Old/Malfunctioned Hard Disk Drive (HDD)

Question	No	Yes
Give away the HDD as it is doing nothing to the data in it.	117	33
Format the HDD before giving it away	55	95
Use degaussing mechanism to destroy the HDD.	139	11
Erase data permanently beyond recovery using over-writing mechanism	127	23

Figure 15 Operation executed in case of HDD failure



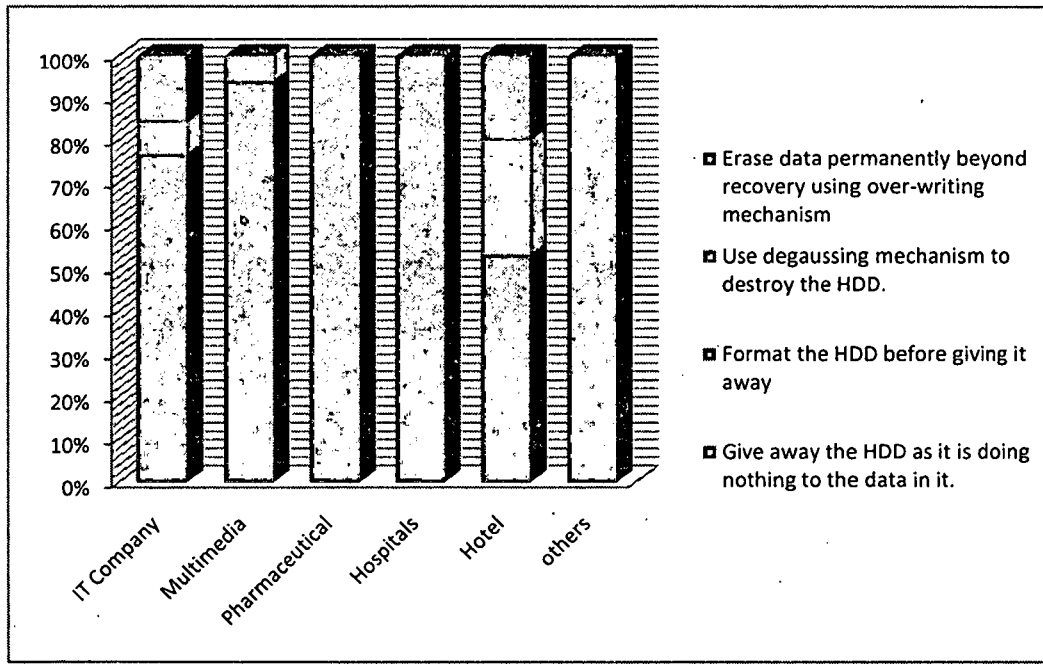
Majority of organizations are conscious enough about giving away HDD. However, only few organizations are taking utmost care while disposing hard disk.

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 17 Dispose of Old/Malfunctioned Hard Disk and Type of Industry

Option	IT y	Multimedia	Pharma.	Hospitals	Hotels	others
Give away the HDD as it is doing nothing to the data in it.	13	4	3	5	2	6
Format the HDD before giving it away	50	12	9	9	6	9
Use degaussing mechanism to destroy the HDD.	6	1	0	0	4	0
Erase data permanently beyond recovery using over-writing mechanism	13	0	2	1	3	4
Total	82	17	14	15	15	19

Figure 16 Dispose of Old/Malfunctioned Hard Disk and Type of Industry



It is quite obvious that IT Companies are more aware about their information security and data confidentiality and prefers to format HDD and over-writing mechanism before giving away it or scrapping.

Hypothesis Testing

H_0: Trend among corporate on Data Risk Measurement is significantly independent of the industries.

H_1: Trend among corporate on Data Risk Measurement is significantly dependent on the industries.

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 18 Chi-square Test- Data Risk Measurement

Particulars	Planning to dispose off your old computer/hard disk.	Planning to sell your old laptops/desktops.	Issue Laptop/ Desktop of ex-employee to a new joiner.	Transfer of systems from one department to another.	Row Total
IT Company	58	56	39	41	194
Multimedia	15	13	7	10	45
Pharmaceutical	10	8	4	4	26
Hospitals	15	13	10	7	45
Hotel	12	12	6	5	35
Others	15	14	5	7	41
Column Total	125	116	71	74	386

Table 19 Frequency Table -Data Risk Measurement

$$f_e = \frac{RT * CT}{GT}$$

$$X^2_{cal} = \sum (f_0-f_e)^2 / f_e$$

X^2_{tab} = (r-1)*(c-1) d.f. at given α

f_0	f_e	$(f_0-f_e)^2/f_e$
58	62.82	0.37
56	58.30	0.09
39	35.68	0.31
41	37.19	0.39
15	14.57	0.01
13	13.52	0.02
7	8.28	0.20
10	8.63	0.22
10	8.42	0.30
8	7.81	0.00
4	4.78	0.13
4	4.98	0.19
15	14.57	0.01
13	13.52	0.02
10	8.28	0.36
7	8.63	0.31
12	11.33	0.04
12	10.52	0.21
6	6.44	0.03
5	6.71	0.44
15	13.28	0.22
14	12.32	0.23
5	7.54	0.86
7	7.86	0.09
$\sum (f_0-f_e)^2/f_e$ =	X^2_{cal} =	5.05
D .f. = 15	X^2_{tab} =	22.307 (at α = .10)
X^2_{cal} < X2tab		

Therefore, Null Hypothesis is accepted and concluded that trend among corporate on 'Data Risk Measurement' is independent of the industries.

ANOVA

H_0: Overall Risk measurement trend among corporate is same for all industries.

H_1: Overall Risk measurement trend among corporate is different for all industries.

Here, $\alpha = 0.05$

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Table 20 ANOVA Summary

Groups	Count	Sum	Average	Variance
Planning to dispose off your old computer/hard disk.	6.00	125.00	20.83	335.77
Planning to sell your old laptops/desktops.	6.00	116.00	19.33	327.07
Issue Laptop/ Desktop of ex-employee to a new joiner.	6.00	71.00	11.83	181.37
Transfer of systems from one department to another.	6.00	74.00	12.33	201.47

Table 21 ANOVA - Data Risk Measurement

Source of Variation	SS	df	MS	F	P-value	F Crit.
Between Groups	391.50	3.00	130.50	0.50	0.69	3.10
Within Groups	5228.33	20.00	261.42			
Total	5619.83	23.00				

Here, $n_T = 24$

$K = 4$

$n_T - k = 20$ d.f. =denominator

$k-1 = 3$ d.f = numerator

$$F_{cal} = \frac{130.50}{261.42}$$

$$= 0.50$$

$$\text{Now, } F_{tab} = \frac{\text{df of numerator}}{\text{df of denominator}}$$

$$= \frac{3 \text{ d.f.}}{20 \text{ d.f.}}$$

$F_{tab} = 3.10$

Here,

$F_{cal} < F_{tab}$.

Overall Risk measurement trend among corporate is almost same for all industries.

H_0: No significance difference in trend among different industry sectors about data risk measures.

H_1: At least one industry sector has significant difference in trend from corporate of other industry about data risk measures.

Table 22 ANOVA Different Industry Sectors

ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	391.5	3	130.5	0.5	0.69	3.1
Within Groups	5228.33	20	261.42			
Total	5619.83	23				

ISSN 2249-4103 GGGI Management Review
A Bi-annual Refereed International Research Journal

Here, From the ANOVA table,

$p = 0.69$

But, $\alpha = 0.05$

So, $p > \alpha$

Null Hypothesis is not rejected and concluded that there is no statistically significant difference

Findings

- General awareness on Data Recovery among corporate is around 77% meaning that all IT manager are very well knowing the data recovery possibilities for different situation.
- Proportion of corporate aware about Class 100 Clean Room is less than 25% to be exact it was around 17.33% so many corporate are unaware of 100% data recovery possibility of their HDD.
- 90% of corporate finds their information important, whereas the 70% of the firms have policy for information security / data confidentiality and 50% are seriously re-thinking about Information security to save their valuable information from loss or misuse despite of having a policy to secure their data.
- Around 65% of the corporate are aware and capable of measuring the data risk in the given scenario.
- Trend among corporate on data risk measurement is independent of the industries.
- Overall risk measurement trend among corporate is almost same for all industries.
- Trend among the corporate on executing any of the given operation for dispose off their HDD is directed towards the formatting their HDD before giving it away.
- IT Companies are more aware about their information security and data confidentiality hence they are more favouring to the option of first formatting the HDD and then either give away it or put it as a scrap.

Conclusion

Awareness about data security and potential hazard is very high. Majority Organizations are having their information security policy in place. However, thirst is required in area of training of technical as well as nontechnical employees about data security policy and measures. Another area requires attention is compliance with the existing policy and continuous updating of information security policy. As the proverb goes 'Prevention is better than cure'.

Reference:

Chang, C.-Y. (2005). A survey of data protection technologies . IEEE International Conference 2005 on Electro Information Technology (p. 6). Lincolin, USA: IEEE.

Driml, S. (2003). Enhancing Security with an IT Network Awareness Center. ISACA, IV.

Medlin, B. D., & Cazier, J. A. (2010). A Study of Hard Drive Forensics on Consumers' PCs: Data Recovery and Exploitation. Journal of Management Policy and Practice , 12 (1), 27-35.

Moynihan, J. (2008). Managing the Insider Threat: Data Surveillance. ISACA, I.

PhishMe. (2012, August 7). www.finance.yahoo.com. Retrieved August 16, 2012, from www.yahoo.com: http://finance.yahoo.com/news/survey-conventional-security-awareness-training-130200079.html

Quagliata, K. (2011). Impact of Security Awareness Training Components on Perceived Security Effectiveness. ISACA, IV.

Schwartzel, T., & Mnkandla, E. (2012). The impact of critical business data on organizations. African Journal of Business Management , 6(26), 7705-7713.

Survey. (2011, May 9). Retrieved August 16, 2012, from www.infosecurity-magazine.com: http://www.infosecurity-magazine.com/view/1844/survey-shows-information-security-awareness-is-high-yet-compliance-is-low-/

Teotia, S., Punia, R., & Awasthi, M. (2012). A Survey on Data Security & Computer Networks. International Journal of Management, IT and Engineering , 2 (6), 233-244.