A Study On Data Privacy, Protection & Sanitization Practices During Disk Disposal By Indian Educational Institutes

Ramakrishnan Raman [1], Dhanya Pramod [2]

[1] Symbiosis International University, Symbiosis Center for Information Technology, Pune, Maharashtra India

[1] Symbiosis International University, Symbiosis Center for Information Technology, Pune, Maharashtra India

ABSTRACT

Information security practices are inevitable in this era of increased security breaches. With popularity of internet, cyber security issues have taken its main stay. Disk level security issues are ignored by Indian education institutes and society at large. The focus of this paper is to study data privacy, protection & sanitization practices of Indian educational institutes, vendors during disk disposal. The paper also reviews current standards, acts, policies & laws that prevail in United States, European countries and India. The study reveals that standards, acts, policies & laws are not adequate in India. The study reveals that educational organizations are still not serious about disk sanitization and lots of information remains on the disposed disks. When a disk is disposed, it is essential that data is securely removed from it so as to avoid data security breaches, data leaks and the resulting impact of loss of privacy and reputation. There is a pressing need for organizational policies to be in place. The authors have proposed a Data Privacy, Protection & Sanitization policy that can be adopted by Indian educational institutes during disk disposal.

Key words: *Data Privacy, Data Protection, Data Sanitization, Disk Disposal*

1. Introduction

Information Security revolves around confidentiality, integrity and availability. A robust information security would mean preventing unauthorized access of confidential information, while collecting, storing, retrieving and also discarding data related to a educational business processes. According to Arun Madapusi (2011) enterprise resource planning systems are still a distance dream for many educational institutes in India. Local disk drives continue to be the most commonly used storage mechanism to store all confidential data, even today. The data stored includes sensitive personal and medical information of faculty, staff and students. Pameet Singh and Peter Sandborn (2006) state - with technology obsolesce taking shorter life cycles and affordability to advanced technology gadgets becoming possible, organizations tend to dispose their used personal computers for sophisticated devices.

The disks that are disposed with out proper sanitization, on a buyback scheme or to a third party e-waste collector carry not only the business specific information but also has loads of personal information of faculty members, staff, students and vendors. In India majority of educational institutes do not sanitize the hard disks before disposal. This is a threat to data privacy and protection. The impact of disclosure of the data may result in severe consequences. This paper attempts to study the practices related to data privacy, protection & sanitization practices during disk disposal by Indian educational institutes. To understand the policies and procedures related to Data Privacy, Protection & Sanitization during disk disposal, we scanned the website of educational institutes located in India. We also purchased and analyzed 128 hard disks from third party vendors who deal with e-waste disk disposal of educational institutes. We interviewed 24 vendors to understand the procedures, policies and practices which they follow while collecting e-waste from educational institutions. The data was collected during Jan 2013. The respondents (the vendors) who participated in the interviews were in this business for more than 5 years. We also compared the Indian legal-compliance, regulations and standards with the prevailing international standards for data privacy, protection and sanitization during disk disposal.

This study is organized as follows: the **first section** discusses disk sanitization issues and Data Sanitization – standards, acts, policy & laws. Details on the Indian legal-compliance, regulations and standards, along with the prevailing international standards followed in United States and Europe have been presented. The **second section** presents the finding from the survey. Details related to the analysis of information found from the scanned websites and also analysis on the data found from the hard disks that were analyzed during the study have

been presented. The **third section** is on disk sanitization policy for Indian educational institutes. A sample policy related to data privacy, protection and sanitization during disk disposal, for educational institutions is presented in this section. The fourth and final section gives the conclusion for the study and also explore the possibility for further work that could be done.

2. Disk Sanitization Issues

Hard disks have become sophisticated in terms of speed and capacity. Previous studies by researchers such as Garkunkel(2003) and Jones(2005) have addressed issues related to security awareness among end users. The technology used for read& write of data on disk still maintain backward and forward compatibility. This paves a way for some touts to buy old hard disks and retrieve the data on them by plugging them to a device. Another factor that remains favorable for these criminals are the consistency of file systems. Simson and Abhi (2003) state that most of the commonly used operating systems have compatibility to old File Allocation Table (FAT) file systems which enables reading of the files stored on old hard disks. This vulnerability needs to be plugged by removing critical information from disks before the disposal so that privacy can be ensured. If the hard disk haves FAT 16 /FAT 32 or New Technology File systems (NTFS), and are formatted, there are free tools which help in retrieving data from hard disks. The delete or erase commands are not sufficient for removal of data, as it only unlink the clusters of data storage from the metadata/file pointer /directory entry. The contents of the file will be inaccessible through the filename but remains on the disk. Smithson and Brian (2011) have mentioned that special tools can remove user data by a single overwrite of all files and free space. The format command cleans the file system and informs the operating systems to manage data again. This makes the operating system to assume that the drive is empty and hence when writing happens, the data is actually over written on those sectors which still hold data. This makes recovery of data possible even after formatting. There are tools which use algorithms to create virtual pointers, to unlinked data which makes recovery an easy job! The methods widely used for sanitization are overwriting the data with zeros or a pattern, rendering the drive unusable by degaussing the drive and physical destruction of the drive. There are sanitization tools available to erase the information on disks. However certain forensic tools can still retrieve deleted files and retained data blocks, which are not associated with a specific file.

3.Data Sanitization – Standards, Acts, Policy & Laws

Reliable, approved and accepted methods to sanitize data is critical for security and privacy reasons. As the methods and tools for data sanitization and protection are plethora in number, users find it difficult to choose the right tool. There are standards which help in selecting a appropriate framework for data sanitization. DoD5220 was the first standard from United State's (US) Department of Defense (DoD), that defined a "clearing and sanitization matrix". Gordon Huges and Daniel Cummins (2009) have referred the DoD5220 which gives a guideline, stating that two fixed-character overwrites comprising of a character and its compliment along with one random character overwrite, followed by a verify read is required before disposal of disk. With advancement in technology, general standards becomes obsolete and revision becomes inevitable. US DoD laboratory works relentlessly in to ensure that, DoD standards are updated at regular intervals. US DoD5220.22-M is the latest standard for cleaning and sanitizing information on a writable media. This standard suggests various methods for clearing magnetic tapes, hard disks, optical disk, memory, equipment and printers.

To clear data either of the three techniques mentioned below are used.

- Degauss with a Type I degausser.
- Degauss with a Type II degausser.
- Overwrite all addressable locations with a single character.

To sanitize either of the following methods is used

- Degauss with a Type I degausser.
- Degauss with a Type II degausser.
- Overwrite all addressable locations with a character, its complement, then a random character and verify.
- Destroy - Disintegrate, incinerate, pulverize, shred, or melt.

In US, DoD laboratory evaluates all processes and tools related to disk sanitization of the federal agency. The functionality is checked and approvals are given only after due diligence. NIST (National Institute of Standards and Technology) 800-88 is a standard from US government, which gives guidelines for media sanitization guidelines. NIST suggests three techniques namely Clear, Purge and Destroy to ensure media sanitization. For clearing media, user addressable storage space can be overwritten with non-sensitive data using a software or hardware product. Purging can be done using standard device sanitization commands that use media specific techniques to bypass the abstraction inherent in read and write commands by overwriting, block erase or cryptographic erase. Destruction of media can be done in three methods. First method is by applying techniques to ensure that target data is

changed so that it becomes infeasible to retrieve, through the device interface. The techniques also ensure that, the media becomes unusable for subsequent data storage and hence making the device unusable. The second method is to disintegrate, pulverize, melt, and incinerate, which will completely destruct the media. The third method is to shred. Shred is used to will destruct flexible diskettes after it is removed from its outer shield.

An organization can choose the suitable media sanitization method according to the level of confidentiality of the data stored. It is advisable to use clearing method, if the security categorization is low or moderate and the business processes ensures that media is not sent out of the organization. Purging method is suggested if security categorization is low or moderate and the business processes demand the media to be sent out of organization. When the security categorization is high, purging is advisable if the storage media is not sent out of organization. The destroy method is recommended if confidentiality is high and if the media moves out of the organization. In all above cases, verification is mandatory after sanitization of media, this is done to ensure that sanitization goal is achieved. NIST also recommends organizations to have a proper documentation of the sanitized media details.

The United Kingdom (UK) Data protection act 1998 requires that the organizations have to take due care in handling employees data and other organizational data so that accidental or unauthorized disclosure of confidential data they hold can be avoided. There are organizations who are into data sanitization and disk destruction services. These organizations follow UK Government's National Technical Authority for Information Assurance (IA) CESG guidelines, policies and assistance. CESG helps in identifying appropriate countermeasures for risks and provide a basis from which informed decisions can be taken on risk management. They also help in framing various policies on security of communication and electronic data, including disposing of computer disks used for sensitive information. Several legal and federal regulations related to data protection and sanitization prevail in US and European countries. These regulations which are related to data storage devices like hard disk drives, optical drives and other disk based storage medium are revamped at regular intervals of time. US laws for data sanitization include Health Information Portability and Accountability Act (HIPAA), Personal Information Protection and Electronic Documents Act (PIPEDA) ,Gramm-Leach-Bliley Act (GLBA), California Senate Bill 1386 (2002), Sarbanes-Oxley Act (SBA), SEC Rule 17a, Fair and Accurate Credit Transactions Act etc. The Law deals with iron fist on all those who violate it. The penalty is severe which includes slapping heavy fine or in worse case financial penalty along with and imprisonment. Most European countries have strong data protection acts. United Kingdom and Netherlands have gone far ahead in meeting data protection requirements. The present day disk drives used for storage have become sophisticated and provide “in-drive” secure erase command. “In-drive” secure erase is technically superior and secure way to meet legal data sanitization requirements, and protects against attacks up to laboratory level. This method does not require additional software, as it is carried out within the hard disk drives. “In-drive” Secure erase meets the legal requirements of HIPAA, PIPEDA, GLBA, and Sarbanes-Oxley and has been approved by the US (NIST).

Indian laws/Acts/Standards : Department of Information Technology (DIT) was set up in year 2000 to implement Information Technology (IT) Policy for Government of India. Data Security Council of India (DSCI) is a focal body for data protection in India, setup as an independent Self-Regulatory Organization (SRO) by National Association of Software and Services Companies (NASSCOM). DCSI’s main objective is to promote data protection, develop security and privacy best practices & Standards. DCSI also encourages the Indian organizations to implement best practices & Standards. Data privacy and protection in India suffers from lack of legislative provisions, public and employee awareness and strong cyber laws. Unlike US or European Union, India doesn’t have dedicated data protection laws. Provisions for data protection, provided in the IT Act 2000 and its amendment in 2008 are mostly hodgepodge and does not offer any comprehensive protection to personal data .Currently data protection is governed by contractual relationship between the parties. IT Act 2000 and IT (Amendment) Act in 2008, which give provisions for dealing with information technology related issues, are generic legislations and do not provide any specifics clauses for Data Privacy, Protection & Sanitization. India does not have a proper legal framework for preserving the confidentiality, integrity, availability and/or authenticity of data. Once data is transferred outside Indian national boundary, it gets no legal protection under any of the sections or laws. Organizations in India have to resort to standards set by foreign nations in order to survive the global competition. This has to be done in order to gain global trust and credibility

Whenever an issue related to Data Privacy, Protection & Sanitization surfaces, exploiting the loop holes and technicalities in the court of law is a common practice. The fact of the matter is, provisions remain inadequate even after amendments made to IT Act in 2008. This makes, Indian organizations to fall back on standards such as BS 7799 (later adopted by ISO as ISO 17799 and is

currently ISO 27002) to standardize information security best practices. According to Christopher (2003) India attracts a lot of outsourced projects from the US. In order to generate trust and continue to flourish, Indian companies have started to adhere to European Union (EU) standards. Many organizations are now pursuing compliance in SOX, Gramm Leach Bliley Act, Safe harbor Act, HIPAA, FDCPA. There is also a positive trend for certifications from ISO on ISO/IEC 27001:2005

In the year 2006, Government of India proposed a bill for personal protection to specifically address the issue related to data protection. It is sad that the bill was not passed by the assembly but the the Indian government claimed that the critical points of the bill was incorporated into the amendments made to the IT Act in 2008. DIT is currently working on a holistic law on data protection based on the EU directive. Government plans to create a 'Common Criterion Lab' based on the report from Information Security Technology Development Council.

4.Findings From The Survey

Having given an overview on US, European and Indian Data Privacy, Protection & Sanitization laws and standards, a study on Data Privacy, Protection & Sanitization practices in Indian educational institutes are presented in the next section. We conducted a survey by studying the web sites of Indian educational institutes, which operate in the under graduate and post graduate level. The focus was to keenly observe, the policies and procedures that exist. We interviewed the vendors who deal with e-waste collection and disposal. We also purchased the discarded hard disks from some educational institutions to understand the kind of data that are left on hard disk, which indicate the level of data sanitization practices that are adhered by them.Study of websites for Data Privacy, Protection & Sanitization Practices followed during disposal.

We studied websites of 128 educational institutions located across India. The purpose was to understand if these educational institutions have policies in place which relates to Data Privacy, Protection & Sanitization during disk disposal. We found that none of these institutions have any such policies in place. Although there are guides from Ministry of forest and environment, which deals with e-waste management and disposal, there are no norms for Data Privacy, Protection & Sanitization Practices in India.

We interviewed 24 vendors to understand the procedures, policies and practices followed to ensure data sanitization and protection, during e-waste collection and disposal from educational institutions. It was found that none of the vendors had any such policies. We also purchased and analyzed 55 hard disks from third party vendors who deal with e-waste disposal of educational institutes. Analysis was done using an online software for deleted data recovery. All hard disks had data on them which were either deleted or undeleted, which could be retrieved. On analysis we found the following details given in Table 1

Table 1: Data on Disk

Information Found	Percentage of hard disks which had this data was found
Student personal information (Like Name, Mobile Number, Date of Birth, Passport Number)	93%
Student experience details	35%
Student Health records	08%
Students Academic details (Including CGPA, Percentage, Marks etc)	43%
Students Login credentials (Email Address, Passwords , Bank Account Numbers)	36%
Employee personal information (Like Name, Mobile Number, Date of Birth, Passport Number, Qualification)	19%
Employee experience details	17%
Employee Health records	06%
Employee Salary details (Including salary slips, Percentage, Appraisals)	04%
Employee Login credentials (Email Address, Passwords , Bank Account Numbers, Network User Names, Wi-fi Login Information)	48%
Asset Information	04%
Budget Information	03%
Vendor Information	08%
Student Placement Information	07%
Faculty Feedback	07%
Student Grievances	08%
Email back ups	62%
Compliance documents	04%
Credit Card details and Pin Numbers	02%

5. Disk Sanitization Policy For Indian Educational Institutes

It is becomes necessary for educational institutes to collect and store the information of its faculty members, staff and students who are associated with them. It is voluminous information that resides on the hard disks which are on personal computers (PC) and portable devices. The information stored includes personal details, email addresses, mobile numbers,

passport numbers, Personal Account Number (PAN) education and experience details and details related to health information which are highly sensitive and unauthorized disclosure of this may lead to embarrassment, identity theft, legal noncompliance. This might also result in financial loss and defamation of the institute. Many educational institutes in India are currently resort to disposing of the obsolete PC and hard drives, to third party vendors. These vendors do not have proper data sanitization methods to sanitize devices. Many educational institutes are not aware of the consequences of disposing the obsolete disks in this manner. In the US and European countries most of the universities have taken measures to protect the information and have strong policies for data sanitization and removal. We propose a Data Privacy, Protection & Sanitization policy that can be adopted by Indian educational institutes during disk disposal.

5.1Policy

Inter-department disk/equipment transfer – When a department wishes to transfer a disks/equipment, a notification must be given to all departments and check if they require it. If a department is in need of the same a transfer of equipment could be initiated between the respective departments. When a disk /equipment is transferred from one department to other, the former department would be responsible for removing sensitive information on disks prior to transfer. Information Technology (IT) team should be requested for data removal and transfer.

Disposal of unwanted disks/equipment from department- When a disk/equipment is removed from a department, the concerned department is responsible for removing sensitive information prior to the removal of the disk/equipment. IT team should be requested for handling the unused disk/equipment. The department should also ensure that IT service technician use standard methods of data removal before the disk goes the pool of central surplus equipment.

Disks or unused computer devices which are moved to central location have to be labeled ("sanitized" /"not sanitized") by IT team after ensuring that data sanitization guidelines are followed.

Disk disposed from institute- The hard disks of computers which have to be disposed should be removed and sanitized before disposal. This will prohibit data disclosure, even if individual department level sanitization does not happen. The removal of sensitive data must be carried out using standard procedures like NIST 800-88.

Disk donated to other schools or non-profit organizations- The hard disks of computers which have to be donated to other schools or non-profit organizations, have to be sanitized before donating. Remove sensitive data using standard procedures like NIST 800-88 should be adhered.

Disk sent for repairing/maintenance- A non-disclosure agreement should be in place prior to third-party getting and access to the Electronic Media. This will ensure confidentiality and non-disclosure of information.

Disk that are unusable-The disk which cannot be used any more must be physically destroyed and disposed in an environmental friendly manner

6. Conclusion And Scope For Further Work

The last decade has witnessed an unprecedented growth in information security practices across the globe in business organizations and government agencies. Laws, acts, standards and policies are being revised internationally, especially in US and European countries. However our study reveals that Indian educational organizations are not yet having adequate policies for data privacy, protection and sanitization of sensitive data during disk disposal. Our study also has revealed that laws and policies that prevail in India have to be revamped. The study gives insights on the sensitive data available in the disks that are disposed from educational institutions. Although we have suggested a data privacy, protection & sanitization policy that can be adopted by Indian educational institutes during disk disposal, there can be further study on the methods to be adopted by governing bodies of educational institutions, to ensure increased information security adhered. Further studies can also look at practical issues and implementation challenges to policy enforcement.

REFERENCES

[1] Arun Madapusi, "An Overview of ERP in Indian Production Firms", Global Journal of Enterprise Information System Volume 3, Issue 1 March 2011, pp 5-16

[2]Pameet Singh and Peter Sandborn, "TheEngineering Economist", Vol. 51, No. 2, April-June 2006, pp. 115-139

[3]Jones, A ,"How much information do organizations throw away ?" , Computer fraud and security, 2005,pp 4-9

[4]Simson L, Abhi Shelat."Remembrance of Data Passed: A study of Disk Sanitization Practices", IEEE Security & Privacy, 2003, pp 17-27

[5]Smithson, Brian (2011). "The Urban Legend of Multipass Hard Disk Overwrite and DoD 5220-22-M" Infosec Island.

[6]Gordon Huges and Daniel Cummins."Disposal of Disk and Tape data by secure Sanitization", IEEE Security & privacy 2009,pp 29-34

[7]Christopher coward "Looking beyond India:Factors that shape the global outsourcing decisions of small and medium sized companies in America", EJISDC,2003v13,issue11,pp 1-12

R Raman is a Computer Science and Engineering graduate from Madras University, he has also completed his MBA in Information Systems, Postgraduate Diploma in Software Marketing, M.Phil (Management) and Ph.D in Information Technology Enabled Services Strategy. He is a Six Sigma Green Belt and Six Sigma Black Belt Certified by RABQSA. He is a certified Green IT professional by ISEB. He has published his research finding in several refereed journals and also has presented several papers in Indian and International conferences. He has a blend of corporate and academic experience. He started his career with Godrej and Boyce and his Passion for academics made him choose teaching and research as his career. He is currently the Director Symbiosis Center for Information Technology - a constituent of Symbiosis International University, and is also the Dean of faculty of computer studies at Symbiosis International University Pune, India.

Dhanya Pramod is a post graduate in computer science from Pondicherry central university and completed her doctoral degree from Symbiosis International University. She has a strong academic foundation and was the First Rank holder of university both at undergraduate and post graduate level. She has over 10 years of experience including industry, research, academics and administration. Her research interests are networks & application security and aspect oriented programming. She has published papers in refereed journals and several conferences of international repute. She is a senior member of IACSIT, Singapore.