An Analysis of Data Security and Potential Threat from IT Assets for Middle Card Players, Institutions and Individuals

Biswajit Debnath, Jaafar M. Alghazo, Ghanzafar Latif, Reshma Roychoudhuri and Sadhan Kumar Ghosh

Abstract Information technology (IT) is one of the largest industries in the world worth $3.4 trillion. While it creates lots of job opportunities, it also creates lots of Information and Communication Technology (ICT) waste. End-of-life IT assets are termed as ICT waste; popularly known as electronic waste or e-waste. E-waste generated from IT sectors is either collected by authorized recyclers under contract or sold via auction. The storage devices contain valuable, critical and confidential data that can bring about threats to the companies. The big players such as Microsoft and others destroy their data by themselves. But the question of data security arises when it comes to the middle card players in the business. In general, they do hold auctions to give out the ICT waste. Threat starts from here because the supply chain of e-waste after that is unknown and rather always not traceable. The problem is more reckoning in the developing nations due to the domination of the informal sectors. Through this untraceable chain, the e-waste may land up in the hands of wrong people and can call for data security. The ISO/IEC 27000 guidelines are there for the information security but that does not always apply in towards the lower-middle and middle part of the pyramid. It is important to identify the possible threats coming from the storage of disposed IT assets and understand the subsequent prevention techniques for this purpose. This study focuses on the data security and possible threats coming from the storage devices of the IT assets mainly from the middle card players, institutions and in individual level. The study aims to identify the threats and proposes possible solutions to prevent any unpredicted and unprecedented activity from malicious people. The help ISO/IEC 27000 guidelines has also been taken, and a framework has been proposed which will be helpful to the concerned authorities

B. Debnath (✉)
Department of Chemical Engineering, Jadavpur University, Kolkata, India
e-mail: biswajit.debnath.ju@gmail.com

J. M. Alghazo · G. Latif
Center of the King Salman Endowed Chair of Information Security, Prince Mohammad Bin Fahd University, Al Khobar, Kingdom of Saudi Arabia

R. Roychoudhuri
Department of Computer Science, Heritage Institute of Technology, Kolkata, India

S. K. Ghosh
Department of Mechanical Engineering, Jadavpur University, Kolkata, India

S. K. Ghosh (ed.), *Sustainable Waste Management: Policies and Case Studies*,
https://doi.org/10.1007/978-981-13-7071-7_36

if implemented. In addition, the findings will also expose a new dimension to the policymakers and the researchers.

Keywords Data security · E-waste · ICT waste · ITAD · Supply chain

1 Introduction

Information technology (IT) is one of the largest industries in the world today, and it is growing very fast. Based on the findings of the consultancy IDC, in the year 2015, the global IT market surpassed $3.7 trillion and is expected to reach $3.8 trillion in 2016 which includes revenue generated from hardware sold, software services, IT services and telecommunications (CompTIA 2016). Projected global IT industry growth will be 4.1% in 2017, and the industry will cross the $3.5 trillion mark from $3.4 trillion by end of 2017 (CompTIA 2017). The global IT services market will grow at a compound annual growth rate (CAGR) of 5% or greater by 2020, another study predicts (Technavio 2016). The IT sector is one of the largest in India, and it is the world's largest outsourcing destination for the IT industry. It accounts for approximately $124–130 billion market which is nearly 67% of the total Indian market (IBEF 2017). According to NASSCOM, IT industry in India will have an expected growth at a rate of 12–14% for the financial year 2016–17 (in constant currency terms) and is expected to reach $350 billion, which is three times the current revenue, by 2025 (IBEF 2017). However, behind the silver lining lies the monster of ICT waste. As the ICT equipments reach their end of life (EoL), they become ICT waste. Outside the circle of the corporate world, ICT waste is simply known as electronic waste or e-waste. There are some controversies whether general household electronics are ICT waste or not (Adeola and Othman 2011), we choose to use both the terms synonymously.

Globally, e-waste is the speedest waste stream with a yearly growth rate of 3–5% (Kumar et al. 2017). The reason behind this is the higher rate of obsolescence of electronic equipments (Debnath et al. 2015b). The key drivers for the growing waste stream are market growth, technological advancement, short innovation cycles, change in consumer habits, urbanization, peer pressure, software development, etc. (Emmanouil et al. 2013; Debnath et al. 2015a; Ghosh et al. 2014). Global e-waste generation was nearly 41.8 MMT in 2014, and it is expected to be 50 MMT in 2018 (Baldé 2015). The BRICS nations produced nearly 25% of the global e-waste generation in 2014 (Ghosh et al. 2016). A lion's share of this waste generated is from the corporate sector, government organizations, academic and research institutions (Borthakur and Sinha 2013). The share of individuals is comparatively less as we tend to store the e-waste in our house due to some sort of emotional attachment and wealth satisfaction. In developing countries like India, it is an obvious approach to refurbish and reuse the electronics once they start malfunctioning, which in turn extends the product life cycle (Baidya et al. 2015). However, nearly one-fourth of the waste PC comes from the households only (Manomaivibool 2009).

In order to manage this huge amount of e-waste, it is necessary to have proper e-waste management system (EWMS). The irony is that only 10% of this waste is properly recycled. A sustainable supply chain network (SCN) is the key ingredient for establishing a proper e-waste management system. The SCN of the EWMS is really complex with several loops. Ghosh et al. (2016) have presented the supply chain network existing in the BRICS nations. It comprises both the informal and the formal sector (EPR) for collection and treatment, inward trans-boundary movement, dismantling, refurbishing, recycling, reuse and final disposal. They have further proposed a generic SCN which includes all possible routes of collection, transition of Used Electrical and Electronic Equipment (UEEE) and Waste Electrical and Electronic Equipment (WEEE) generation, refurbishing, recycling, reusing and disposal. The collectors play a crucial role dictating the sustainability of the SCN. However, the existing SCN has certain loopholes and pitfalls which makes it difficult to trace the trail of the chain or where the loop closes. The government sectors, corporate and the institutions tend to give away their e-waste either by holding auctions or to some formal collectors who contract with those organizations. The individuals tend to sell them to the informal sector (only in those countries where informal sector exists). The threat arises from this point, because after collection, nobody knows where these ICT waste ends up. The storage devices are a part of ICT waste which calls for security threat of various types. The most reckoning of them is the data security or the information security. Garfinkel and Shelat (2003) conducted an experiment which was an eye-opener to how dangerous discarded hard drives can be. He along with his fellow researchers collected 158 hard disk drives (HDDs) from online auctions swap meetings and UEEE shops. They dug in the collected HDD and discovered thousands of financial data, credit card data, medical records, trade secrets and unauthorized data that is highly personal. Thereafter he contacted twenty organizations whose data was recovered and described them reason why it was possible to recover the data. From the feedback received, it was found that the primary fallacy is the trust of the organizations in other third parties for data sanitization. Another issue that came into front was lack of training of employees in data destruction techniques. In some cases, it was surprising that the concerned parties were least bothered about it.

Bennison and Lasher (2005) have concluded that physical destruction of the hard drive is the most thorough method to dispose of hard drive. They also list some processes to do so, namely smelting, shredding, sanding, pulverization and acid bath. Another study identified that control and preventive measures are not implemented properly is because maximum organizations have a predefined idea that their business is being espionage. An interesting fact is that espionage at industrial level costs corporate in USA almost $250 billion yearly. In 60–70% of the cases, involvement of the employees is estimated. The study recommends the need of implementation a series of preventive actions when any employee of a company resigns or dismissed in order to avoid the abuse of internal data by disgruntled employees (Helms et al. 2000). The big players in the IT industries and other corporate sectors such as HP, Amazon and Huawei destroy their storage devices or destroy the data by themselves. The real problems arise with IT asset disposal (ITAD) with the middle card players, i.e. the small- and medium-scale companies which are essentially in the second tier

of the hierarchy and/or are owned by the first-tier companies: the institutions and the individuals. They either lack the proper knowledge of ITAD or they do not own policy and infrastructure for ITAD. Sometimes, ISO/IEC 27000 series are used but it is not possible for the medium- and small-scale enterprises to adhere to these standards properly as this incurs additional cost and time for those organizations. Hence, the problem is not of technology, it is rather a science-policy case that needs to be highlighted and thus attended to. To the best of the authors' knowledge, this problem has not been addressed before. The present study aims to address the issue by answering the following questions—What are threats arising and what are the disposal methods to ensure data security? What changes are required on the policy level in this case? Can ISO/IEC 27000 series be used for this purpose? How it can be integrated to develop a better framework?

The rest of the paper has been organized into seven sections. Section 2 discusses the methodology adopted in this paper. Section 3 presents the literature review on data security in IT assets and IT asset disposal methods. Section 4 gives an overview of possible threats arising from IT assets. The succeeding section discusses the role of ISO/IEC 27000 series in the IT data security followed by the case studies. The last section concludes the paper.

2 Methodology

This paper adopted the methodology of extensive literature survey and interviewing the stakeholders. The literature survey is limited to journal publications, conference proceedings and white papers. Several search engines were explored with keywords including 'IT asset disposal techniques', 'Data security in e-waste', 'Data security in IT industries', 'Data security in storage devices', 'E-waste data destruction methods', 'E-waste recycling', etc. The relevant literature has been cited, and additional information from the associated cross-literatures has been also properly referred. Online survey was carried out in different companies, institutions and individual levels by via Google form and one-to-one interview with IT employees. The responses were collated for further analysis. Then a framework was developed via brainstorming, the interview results and considering the ISO/IEC 27000 series guidelines.

3 Literature Review

3.1 Data Security in IT Assets

Data security in IT assets is of the utmost importance to governments, institutions and individuals alike. IT experts and professionals are giving data security the highest priority. Any data left on storage devices (depending on the type of storage device) is susceptible to unauthorized access even if it is erased. The DOD 5520.22 M standard

which specifies that drives be overwritten multiple times with random 1's and 0's was proven inefficient (Aldinger and Keen 2007). An alternative standard was introduced by the US Department of Commerce through the National Institute of Standards and Technology with the NIST SP800-88 Revision 1 (Stouffer et al. 2011). In this standard, the sanitization of all storage devices of all types was specified including those deemed for reuse or those deemed for waste. Some of the methods specified in this standard include clear, purge and destroy depending on the final destination of the storage device (HP 2017).

Data must be secure on both fixed and portable devices. Institutions take measures to have data secured especially on portable devices such as laptops and personal computers. Companies realize the importance of data security for end customers whether the customer is in government, organization or just an individual; therefore, the concentration on data security to ensure customers that their data is protected. For example, Amazon Web Services (AWS) and Google Cloud storage services assure customer of both physical and digital security of their data. Only authorized individuals are allowed in their data centre and data encryption techniques are applied to the data to keep them secure (C2FO 2017). This also applies to companies that sell endpoint devices or servers such as DELL and also software companies such as Oracle. Portable devices such as phone and electronic pads receive high-security protocols for data protection (Paczkowski et al. 2015). For example, devices made by Apple receive multiple layers of encryption with multiple classes of security ranging from complete protection, to protected unless open, to protected until first user authentication and last class of no protection (Mohamed and Patel 2015).

Data breaches cost institutions an average of $7.2 million per breach(Appan and Bacic 2016). There are other losses besides monetary losses such as brand reputation, customer confidence and competitive advantage. Therefore, institutions are advised to follow a holistic approach to protecting sensitive data. This may include taking extra measures such as—protecting the data physically and digitally, restricting the access to only authorized personnel, protection of intellectual property etc. (Roychowdhury et al. 2019) detail the data protection techniques in storage devices. They conclude that the problem of data security in e-waste is a complicated matter if institution does not follow the standards in the proper sanitization of data before the device enters the e-waste supply chain.

It is apparent that data security is the most critical in the IT sector and that data needs to be securely protected while in use and even in archival systems. Governments, institutions and individuals should follow standards in the disposal of their critical and sensitive data.

3.2 IT Asset Disposal Methods

As previously mentioned, the DOD 5520.22 M standard was proven to be ineffective and therefore the NIST SP800-88 Revision 1 was introduced as a standard for data sensitization for storage devices of all types. The main disposal methods for data in

NIST SP 800-88 Revision 1 include 'Clear' for devices intended for reuse within the organization and 'Purge' for devices leaving the organization but contain data that is not deemed secret, top secret or restricted. Finally, 'Destroy' for storage devices that do contain secret and sensitive data. The Clear method is simply using software or hardware to overwrite non-sensitive data, while the Purge method goes a step further using utilizing the read and write built-in functions and applying further techniques to erase the data. The Destroy method includes physical destruction through either shredding, pulverization, incineration or disintegration (HP 2017). Amazon Web Services and Google storage both utilize the Destroy option after they retire a certain storage device in order to protect their customers' information (C2FO 2017).

Magnetic storage media can be protected from data retrieval with state-of-the-art laboratory techniques with a single overwrite pass and a fixed pattern. However, this technique has proven successful only for magnetic drives and does not apply to other technologies such as flash drives. Roychowdhury et al. (2016) also explore the data deletion and destruction of storage devices in order to protect the data from unauthorized access during the e-waste life cycle. All storage devices even volatile memory storage is susceptible to unauthorized access through modern techniques. Devices must be properly processed before they enter into the e-waste recycling chain.

Standards have been developed for the proper disposal of data in storage devices of all kinds magnetic, optical, tape drives, solid-state drives and others. The methods detailed above in the NIST SP 800-88 Revision 1 essential and needed to be followed by government and private institution and also individuals in order to properly sanitize their drives from data deemed personal and sensitive.

4 Possible Threats Arising from IT Assets

IT asset disposal (ITAD) in industry and institutes is either via auction and/or through contracts with third-party vendors. The moment IT assets enter the supply chain of e-waste, the threats start expand. While holding auctions, sometimes the profiles of the bidders are not validated and sometimes the bidder may be representatives of those in the informal sector. Another scenario is where the bidder buys the e-waste from the company or institute and sells them to informal sector. This may lead to the transfer of the IT assets to the hands of wrong people which can pose security threats including the threat of reverse engineering of certain components in the e-waste equipment. Reverse engineering methods can be implemented at different levels—system level, printed circuit board level and chip level, i.e. electronic component level (Quadir et al. 2016; Grand 2014; Torrance and James 2009). Detailed discussion on reverse engineering at different levels and possible solutions has been provided in (Roychoudhury et al. 2016). Another threat can arise due to potential mixing of electronic components (ECs) recovered from e-waste with brand new ones. A brand new EC will cost more than its reusable counterparts. Adversaries present in the supply chain can mix the recovered ECs (after testing) with brand new ones. Identification of these recovered ECs is not easily done and definitely cannot been

identified visually. These people can sell the mixed volume of ECs to industries which will lead to production of electronic gadgets with recycled components and is more susceptible to becoming faulty and/or reaching EOL within a shorter period than predicted.

The threats that can arise due to e-waste disposal on the individual level are same as above, but the highest threat in this case would be the unauthorized access to the individual's private data. Data privacy is of utmost importance to individual consumers (Greenleaf 2012). It is impossible for every individual to wipe off their data and then hand it over to an authorized recycler. Most formal recyclers will give a certificate of data destruction (simsrecycling.com). But if the waste ends up in the hands of informal recyclers, then the data security may be compromised. Data privacy covers all aspects of data in general which then applies to digital data. Digital data is vulnerable to be accessed by unauthorized and unreliable people using different techniques such as decrypting encrypted data and other techniques from the discarded e-waste storage devices. Even with laws that are in place for data security and privacy, yet there are always loopholes in these laws with the presence of individuals who exploit these loopholes. Despite the implementation of best protection techniques that can secure digital data, there will be some method that can infiltrate the security layers

Table 1 Different types of e-waste and the associated threats

S. No.	Electronic items	Threats
1	Desktop, laptops, servers: hard disk contains confidential company/institute/personal information	Files are not deleted even when deleting data, and data may still be accessed even with formatting
2	Printers/Scanners/Copiers/Faxes	Nowadays, these devices have their own hard drive or memory flash card. Both these memory elements retain their data until it is overwritten with new data
3	External memory components such as CD and DVD tapes, USB sticks	Contains confidential data that is retrievable. Specially in CDs and DVDs, the only way is to destruction of the disk
4	Communications devices—mobile phones/tablet computers/GPS	These devices contain data of a very sensitive and personal nature including bank accounts, contacts, emails and even global positioning system (GPS) with home and office locations
5	Network devices such as switches and routers	Though these devices do not contain personal and confidential data, yet they still contain other private data (network-specific data) such as static IP address which can still be used to infiltrate the institution's network
6	Retail equipments which include debit/credit card terminals and point-of-sale devices	These devices may save the data of the credit/debit cards

and give access of digital data to unauthorized individuals. The issue with e-waste in the hand of unauthorized people is that they have unlimited physical access and time for experimentation with different methods and techniques to retrieve deleted data and/or to navigate through un-deleted digital data (Roychoudhury et al. 2016).

Though the focus of data security usually targets storage devices and solid-state drives, in reality sensitive data exists in other e-waste equipment and becomes susceptible to unauthorized individuals. Sensitive data can be retrieved from different equipments given in Table 1 (Sims Lifecycle Service 2013).

Data security issues, if not handled properly, may lead to legal lawsuits. Sensitive data released or copies of software those that are licensed may fall in the wrong hands. Critical information regarding the business could be leaked. In some second-hand markets, the value of e-waste depends on the quality and quantity of data it contains rather than on the quality the second-hand device itself. The image and reputation of a business may be compromised if sensitive data of its customers finds its way into the hands of unauthorized individuals or entities (Sims Lifecycle Service 2013).

5 Role of ISO/IEC 27000 Series in the IT Data Security

The ISO/IEC 27000 standard provides an overview of information security management systems (ISMS) and defines all the terms related to the standard. It belongs to the ISMS family of standards and are available under the *Information technology—Security techniques*. These standards are applicable to all size and types of organizations—commercial enterprises, government organizations, non-profit agencies, etc. The ISMS family of standards defines the requirement of ISMS and ISMS certification, in addition, it provides guidelines, direct support, interpretation of the whole process for establishment, implementation, maintenance and improvement of ISMS (ISO/IEC 27000:2016).

The most important standard in this family is the ISO/IEC 27001 standard. This standard known as '*Information technology—Security techniques—Information security management systems—Requirements*' is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and is dubbed as standard (ISO/IEC 27001:2013). This standard is compatible with ISO 9001 and 14001 standard. The basic PDCA cycle is also applicable for this standard. A PDCA-based model is shown in Fig. 1.

ISO/IEC 27001 details out the requirements for establishment, implementation, maintenance and continually improvement an information security management system (ISMS) (ISO/IEC 27001:2013). ISMS presents methodical approach safe keeping of sensitive information. It provides the tools for managing people, processes and IT systems by applying risk management processes. ISO/IEC 27001 is designed to be used in conjunction and in parallel with supporting controls such as the ISO/IEC 27002:2013 standard. ISO/IEC 27002 is a standard that discussed 114 security controls in detail which is further organized in 14 sections and 35 control objectives. Compliance to the ISO/IEC 27001 is formally achieved by obtaining the certifi-

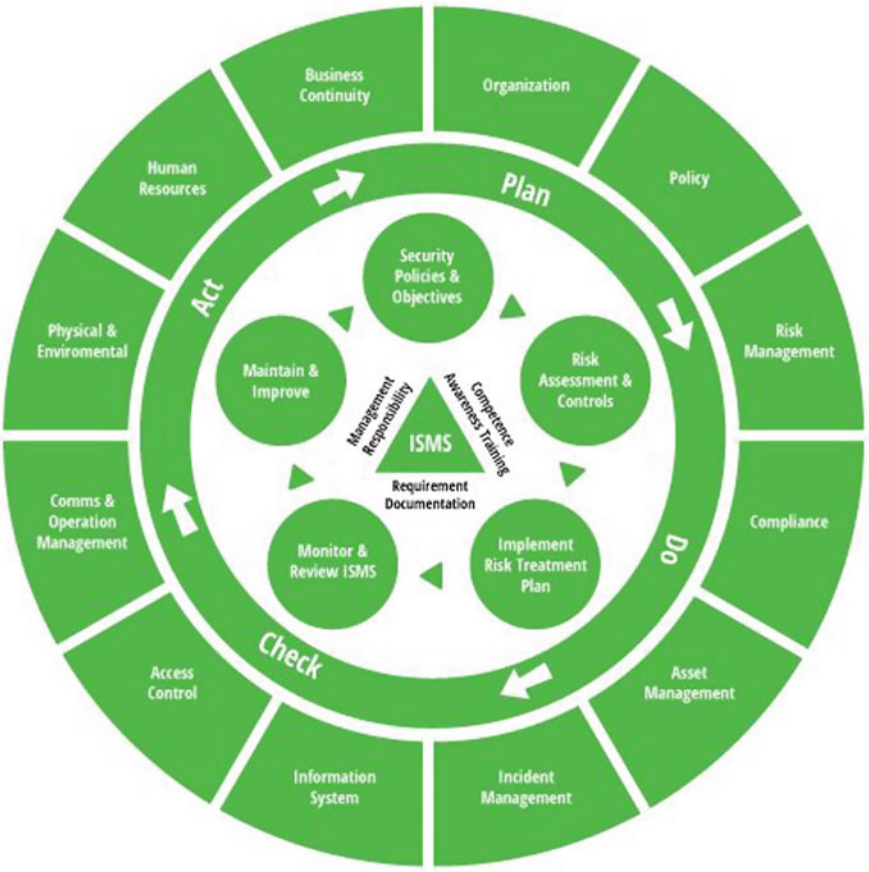

Fig. 1 PDCA model for ISO/IEC 27001:2013

cation (ISO/IEC 27002:2013). The ISO/IEC 27001:2013 certification indicates an organization's level of commitment to information security of its customers and thus provides the needed assurance to their customers, partners and stakeholders. To achieve the certification, an organization must undergo a long process which is described in Fig. 2.

Data security of IT assets is a daunting issue and the ISO/IEC 27000 series of standards can be useful to combat these issues. The ISO/IEC 27000 series of standards deals with information security, which already includes the data security issues. It is important for any organization to develop an ISMS policy and to train all the employees for proper implementation. Proper training programs are required for awareness and knowledge distribution among the employees. It is crucial to execute proper monitoring and preserving of records. Perhaps, it will be best to implement the information security management systems in conjunction with ISO 9000, which can as well take care of any loop holes and will ensure continual improvement.

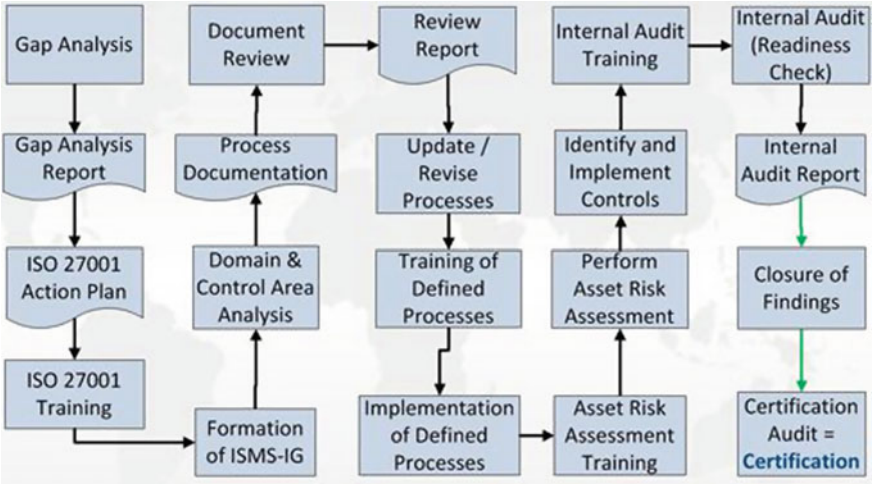

Fig. 2 ISO 27001:2013 certification process

6 Case Studies and Survey Results

6.1 Company A

Company A is an Indian multinational company that have the following services—information technology (IT) service, consultancy and business solutions. It has a capital worth of 80 billion USD and is considered one of the largest Indian IT companies expanding over 46 countries with 289 offices and over 21 countries with 147 delivery centres. As of June 2017, this company has 387,223 employees out of which nearly 120,040 employees are women, which accounts to nearly 31%. The amount of ICT waste generated is huge, and they have a proper system that manages e-waste. This company was the first in India which made necessary steps to tackle ICT waste. The company has the following ISO certifications—(a) ISO 9001:2015 certification for Quality Management Systems (QMS), (b) ISO/IEC 27001:2013 for Information Security Management Systems (ISMS), ISO 20000-1:2011 for IT Service Management and ISO 22301:2012 certification for Business Continuity Management. The company has strong commitment to the environment and health and safety of its employees and business partners, as they have implemented Environmental Management Systems (EMS) (ISO 14001:2004) and Occupational Health and Safety Management (BS OHSAS 18001:2007) throughout. They also have ISO 13485 for medical devices, TL 9000 for telecommunications and AS 9100 for aerospace which are domain specific certifications. Their implementation of several ISO standards including ISMS, QMS and EMS helps in preventing necessary risks and threats. After the electronics reach their end of life, they wipe them of any data or information in the storage devices themselves. Additionally, the storage devices have a

number of layers of encryption to prevent any data theft. Thereafter, the ICT waste is handed over to an authorized third-party vendors contracted with this company. There is no case of exchange with the OEMs or the waste going back to OEMs. Hence, they lack the implementation of EPR as well as no initiative is there from the OEM's end. The tail end of the vendors was not identified and whether the waste end up in formal sector was also not traceable. However, the profiles of the vendors are thoroughly examined before putting them in contractual practice.

6.2 Survey Results

An online survey was conducted using the Google form platform. The questionnaire was circulated among nearly 160 people in different countries who work in universities, research institutions, IT companies and other service providers. A total of 100 people responded to the questionnaire. 52% of the respondents indicated that they exchange their IT assets with better models rather than disposing of them completely. 33% of the respondents indicated that they sell their e-waste to informal sectors, 35% try to repair and refurbish and 37% keep their e-waste at home. Only 26% of the respondents indicated that they hand over their e-waste to formal recyclers (Fig. 3).

It was found that the institutions either dump their e-waste in the storage hangers (45%) or sell it to a formal sector (45%). 31% of the respondents indicated that they were selling their e-waste to informal sector and only 13% indicated that they hold auctions. The IT companies generally give it to formal sector for the proper disposal of ICT waste (61%). Only 18% of the IT companies send ICT waste to auctions, 25% sell it to the informal sector and rest of them dump in storage hangers. 47% of the respondents indicated that they do data sanitization before disposal of storage devices, 8% of the respondents indicated that they do not and the rest are not sure. This number includes both IT companies and institutions (Fig. 4). Data destruction certificates are a rare (12.7%) and many do not know about the existence of such

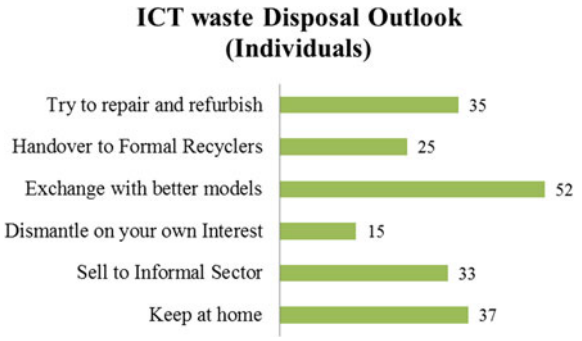

Fig. 3 Individual ICT waste disposal outlook of the respondents (numbers out of 100)

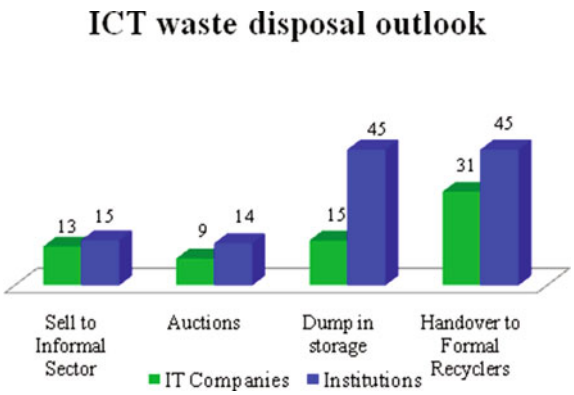

Fig. 4 ICT waste disposal outlook of IT companies and institutions (numbers out of 100)

certificate (16.5%). 37% of the respondents indicated that their organizations follow ISO/IEC 27000 guidelines and 60% are not sure whether their organizations follow these guidelines or not.

7 Discussions

7.1 Key Issues and Challenges in ICT Waste Supply Chain

There are several issues and challenges faced by the stakeholders along the supply chain of ICT waste. In most of the cases, these are due to lack of awareness or improper policy implementations. The industries, who are the major ICT waste generators, face a lot of challenges during the disposal process of their ICT waste. The basic reason is improper implementation of the policies. OEM's that supply the electronic equipments do not take back orphan products. For example, only the monitor of a PC is not working or the mouse is broken, etc. Take-back programs under the EPR are effective only when the whole system is wrecked. Despite the encryption layers that are used for the data protection, it is still subject to unauthorized access. There is always a chance for data theft via specialized equipment for data retrieval, reverse engineering or any other methods mentioned previously. The vendors who destroy the data or promises to destroy the data may or may not perform this process in a secure manner or perform it as promised. The data destruction certificates are also not a common practice. Only the formal e-waste recyclers provide proper gateway to destruction of data.

The academic and research institutions are found to be less concerned with their e-waste. Their primary attitudes towards e-waste are to either storage hangers or give away in auctions and/or collection drives. They do not have any encryption

layers in their storage devices. Defence research centres possibly do have their data encrypted but in general, the universities and other research institutes do not do that. There is also no data security policy to deal with threats of unauthorized access of data in e-waste. The EPR scheme is also not properly maintained as they are not bulk generators, and the logistics cost is estimated to be higher. A part of e-waste is dismantled by the researchers, those who are working in that area and the dismantled product disposal becomes more complex problem. Separate by-laws should be there for the purpose of institutional waste management which includes e-waste as well.

The middle card players, i.e. NGOs, start-ups, small business, medium-scale IT companies in the second tier, and even individuals face problems for disposal of e-waste and other security issues. Since, these organizations are run on low or moderate capital, their primary aim is to maintain the economics by maximizing the profit. Unless there is any strict requirement for compliance from their customers, the practice of data security by implementing any standard guideline is not maintained. The EOL storage devices and others are disposed of as is. Data sanitization is not carried out, and no track of where the waste devices are kept or where they end up. The risk of data theft increases multiple folds from these organizations. Many small IT firms are there who work as tech-support to big MNCs and their information could be at stake. Sometimes, e-waste from such organizations are sold to the unauthorized dealers and that creates a good chance that the e-waste will end up in the hands of unauthorized individuals or entities.

7.2 Proposed Supply Chain Framework Considering Data Security

There are many factors pertaining to the supply chain of e-waste. It is next to impossible to incorporate all the factors and to provide a generic framework. Based on the detailed literature review, authors' experience, case studies, survey results, some expert opinions and brainstorming sessions, a generic supply chain framework is proposed. Figure 5 presents the proposed supply chain framework for better management of e-waste considering data security issues that can arise all along the supply chain. The framework considers two major policy tools—(a) Extended Producer Responsibility (EPR) and (b) ISO/IEC 27001 standard. The supply chain of ICT waste starts from the OEMs and reaches the consumers via retailers and wholesalers. EPR comes into action in between them as the OEMs are responsible for implementing EPR with the support of retailers and wholesalers. Consumers have been divided into four groups—(a) industries (big MNCs and IT industries), (b) institutions (academic, research and government organizations), (c) middle card organizations (NGOs, start-ups, small business, medium-scale IT companies in the second tier) and (d) individuals (common people who use electronics individually or collectively in a family). The ISO/IEC 27001:2013 certification has been suggested for the first three categories. Even if these institutions choose not to go through the

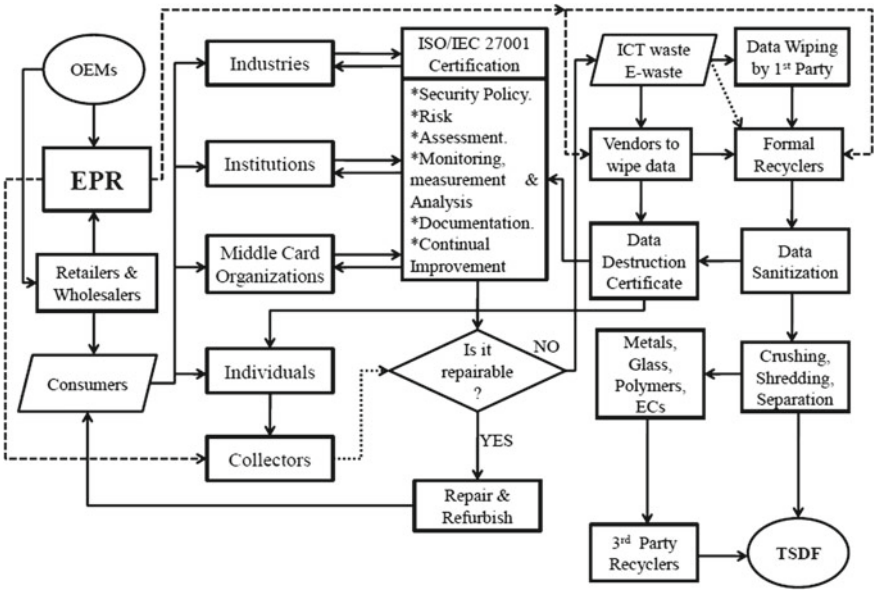

Fig. 5 Proposed supply chain framework for better management of ICT waste focusing on data security threats

certification process yet still some key points mentioned in the block has been suggested for them to follow. Development of the security policy for any organization is the first thing as the whole ISMS system revolves around that. Apart from these, risk assessment, monitoring-measurement-analysis; proper documentation and most importantly continuous improvement are necessary. Since the ISO/IEC 27001 standard is compatible with the ISO 9000 standard, a hybrid strategy may be devised. The electronics that are not working properly should go through a checkpoint to check whether it is repairable or is it beyond repair. If it is found repairable, it can be sent back to the respective consumer after being repaired and refurbished. Otherwise, it becomes ICT waste/e-waste which needs data sanitization before disposal.

The data sanitization can be done by the organizations themselves or through third-party vendors who are in contractual practice and can do that on their behalf. In both cases, data destruction certificate must be provided back to the consumers. The vendors must be in contract with the formal e-waste recyclers and under the EPR scheme of the OEMs. The formal recyclers can also be included in the EPR scheme. The existence of informal or unauthorized sector has been removed from the process to ensure environmental sustainability. The individual consumers are supposed to give their e-waste to authorized collectors appointed by the OEMs under the scheme of EPR, where it follows the same check point and path mentioned above (except data wiping will be carried out by formal recycler only) to end up with the formal recyclers. After data sanitization, formal recyclers will be responsible for mechanical processing (dismantling, crushing, shredding, magnetic and electrostatic separation)

and thereafter recovering materials and recycling them via third-party recyclers. Some waste will be generated during these processes, and those are hazardous in nature, which should be disposed of in a treatment, storage and disposal facility (TSDF).

8 Conclusion

Throughout this paper, the importance of data security was highlighted not only on devices that are in services but on devices that have reached their EOL and enter the e-waste recycling process. Though the e-waste recycling processes in some case have secure and monitored phases to ensure the data security until data destruction yet in most of the cases the recycling process is unmonitored. The recycling process includes informal recycling entities and informal recycling collectors. The background check is never and cannot be performed on these informal players within the e-waste recycling business, and therefore, some of these informal entities and collectors might be in the business of accessing personal and private data from e-waste storage devices. Due to the vast amount of e-waste generated annually and due the cost of data sanitization prior to entering the ICT waste into the recycling process, many middle card players choose to disregard the importance of the data stored on their e-waste and put trust into the recycling entities (formal or informal). In some cases, this leads to millions of dollars in lawsuits if the customers information is accessed by unauthorized entities and put to use illegally.

In this paper, we highlight the importance of standards and guidelines for the e-waste recycling process. We also show through case studies that companies especially large multibillion dollar companies have a rigorous system and usually ensure that the data stored on their devices is deemed inaccessible prior to entering their ICT waste into the recycling process. And when they do enter it to the recycling process, they ensure only to contract with authorized formal recycling entities.

We propose a supply chain framework for proper data security of data on ICT waste for middle player. Our proposed framework builds on and integrate processes from ISO/IEC 27000 Standards Series and ISO 9000 Standard. The proposed framework reduces the cost of handling of EOL equipment for middle players and at the same time ensure the protection of customers data saved on middle players devices and machines. It is important for middle players to weigh the risk assessment if for any possible reason the data on their e-waste becomes compromised. The proposed framework is recommended to be followed by middle class players and even individuals.

Acknowledgements The authors would like to acknowledge International Society of Waste Management, Air and Water (ISWMAW), Centre for Quality Management Systems (CQMS) and Consortium of Researchers for Environmental Protection and Sustainability (CREPS) for their support.

References

Adeola, A. M., & Othman, M. (2011, September). An overview of ICT waste management: Suggestions of best practices from developed countries to developing nations (Nigeria). In *2011 The 7th International Conference on Networked Computing (INC)* (pp. 109–115). IEEE.

Aldinger, M., & Keen, S. (2007, October). CAF DMO standards-based approach for achieving M&S interoperability. In *NATO Modelling and Simulation Group Conference (MSG-056) "Improving M&S Interoperability, Reuse and Efficiency in Support of Current and Future Forces"*, Prague, Czech Republic.

Appan, R., & Bacic, D. (2016). Impact of information technology (IT) security information sharing among competing IT firms on firm's financial performance: An empirical investigation. *CAIS, 39,* 12.

Baidya, R., Ghosh, S. K., & Debnath, B. (2015, March). Analysis of parameters for green computing approach using the analytical hierarchy process. In *2015 International Conference on Energy Economics and Environment (ICEEE)* (pp. 1–4). IEEE.

Baldé, C. P. (2015). The global e-waste monitor 2014: Quantities, flows and resources. United Nations University.

Bennison, P. F., & Lasher, P. J. (2005). Data security issues relating to end of life equipment. *Journal of ASTM International, 2*(4), 1–7.

Borthakur, A., & Sinha, K. (2013). Generation of electronic waste in India: Current scenario, dilemmas and stakeholders. *African Journal of Environmental Science and Technology, 7*(9), 899–910.

C2FO Security Whitepaper, C2FO, Financial Technology Company, March 2017.

CompTIA's IT Industry Outlook. (2016). Retrieved October 2, 2017 from https://www.comptia.org/resources/it-industry-outlook-2016-final.

CompTIA's IT Industry Outlook. (2017). Retrieved October 2, 2017 from https://www.comptia.org/resources/it-industry-trends-analysis-2017.

Debnath, B., Baidya, R., Biswas, N. T., Kundu, R., & Ghosh, S. K. (2015a). E-waste recycling as criteria for green computing approach: Analysis by QFD tool. In *Computational Advancement in Communication Circuits and Systems* (pp. 139–144). New Delhi: Springer.

Debnath, B., Baidya, R., & Ghosh, S. K. (2015b). Simultaneous analysis of WEEE management system focusing on the supply chain in India, UK and Switzerland. *International Journal of Manufacturing & Industrial Engineering, 2*(1), 16–20.

Emmanouil, M. C., Stiakakis, E., Vlachopoulou, M., & Manthou, V. (2013). An analysis of waste and information flows in an ICT waste management system. *Procedia Technology, 8,* 157–164.

Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. *IEEE Security and Privacy, 99*(1), 17–27.

Ghosh, S. K., Singh, N., Debnath, B., et al. (2014). E-waste supply chain management: Findings from pilot studies in India, China, Taiwan (ROC) and the UK. In *ICWMT9: Proceedings of the 9th International Conference on Waste Management and Technology* (pp. 1131–1140), Beijing, China, 29–31 October. China: Basel Convention Regional Centre for Asia and Pacific.

Ghosh, S. K., Debnath, B., Baidya, R., De, D., Li, J., Ghosh, S. K., & Tavares, A. N. (2016). Waste electrical and electronic equipment management and Basel Convention compliance in Brazil, Russia, India, China and South Africa (BRICS) nations. *Waste Management & Research, 34*(8), 693–707.

Grand, J. (2014, August). Printed circuit board deconstruction techniques. In *WOOT*.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108. *International Data Privacy Law, 2*(2), 2011–2039.

Helms, M. M., Ettkin, L. P., & Morris, D. J. (2000). The risk of information compromise and approaches to prevention. *The Journal of Strategic Information Systems, 9*(1), 5–15.

HP, Storage Device Sanitization Methods and Applications, 4AA6-6273ENW, March 2017.

IBEF. (2017). Retrieved October 2, 2017 from https://www.ibef.org/industry/information-technology-india.aspx.

ISO/IEC 27000. (2016). Information technology—Security techniques—Information security management systems—Overview and vocabulary.
ISO/IEC 27001. (2013a). Information technology—Security techniques—Code of practice for information security controls.
ISO/IEC 27001. (2013b). Information technology—Security techniques—Information security management systems—Requirements.
Kumar, A., Holuszko, M., & Espinosa, D. C. R. (2017). E-waste: An overview on generation, collection, legislation and recycling practices. *Resources, Conservation and Recycling, 122,* 32–42.
Manomaivibool, P. (2009). Extended producer responsibility in a non-OECD context: The management of waste electrical and electronic equipment in India. *Resources, Conservation and Recycling, 53*(3), 136–144.
Mohamed, I., & Patel, D. (2015, April). Android vs iOS security: A comparative study. In *2015 12th International Conference on Information Technology-New Generations (ITNG)* (pp. 725–730). IEEE.
Paczkowski, L. W., Parsel, W. M., Persson, C. J., & Schlesener, M. C. (2015). U.S. Patent No. 9,049,186. Washington, DC: U.S. Patent and Trademark Office.
Quadir, S. E., Chen, J., Forte, D., Asadizanjani, N., Shahbazmohamadi, S., Wang, L., & Tehranipoor, M. (2016). A survey on chip to system reverse engineering. *ACM Journal on Emerging Technologies in Computing Systems (JETC), 13*(1), 6.
Roychowdhury, P., Alghazo, J. M., Debnath, B., Chatterjee, S., & Ouda, O. K. M. (2019). Security threat analysis and prevention techniques in electronic waste. In *Waste Management and Resource Efficiency* (pp. 853–866). Springer, Singapore.
Sims Lifecycle Services. (2013). IT Asset Disposal. Version 2.0.
Sims Recycling. Retrieved November 5, 2017 from http://www.simsrecycling.com/Services/Data-Destruction/Safeguarding-Data.
Stouffer, K. A., Falco, J. A., & Scarfone, K. A. (2011). Sp 800-82. Guide to industrial control systems (ICS) security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC).
Technavio. (2016). Retrieved October 2, 2017 from https://www.technavio.com/report/global-it-professional-services-it-services-market.
Torrance, R., & James, D. (2009, October). The state-of-the-art in IC reverse engineering. In *CHES* (Vol. 5747, pp. 363–381).