International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 10 (October 2014), PP.01-11

INFORMATION SECURITY: AN OVERVIEW

Adewale O Adebayo
School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun, Nigeria

Abstract:- Security incidents occur because breach agents plan and execute attacks, and/or because trusted security mechanisms fail, have shortcomings or are inadequately configured. Review of information resources, and security approaches and measures, is necessary. Extant and current literature on the subject matter revealed that information security is a dynamic never ending process requiring regular review and update of information system resources, security policies, training, processes and mechanisms to ensure business continuity, and to stem information abuses and comply with regulations and standards.

Keywords:- Information Security, Data Security, Secure System, Computer Security, Secure Computing.

I. INTRODUCTION

Information security failures are due to different reasons. The main ones are unethical behaviours, mostly successful due to trusted security mechanism failures or shortcomings. There is the need to review information security approaches, to have a fresh look at it all for possible lead to improvements. A fresh look frees of prejudices which might be hindrances to innovative security solutions. A new look engenders creativity and exposes failed traditions. This will result in improved security measures and ultimately lead to more secure computing environment. Extensive literature review on the subject matter was performed. The relevant documents obtained were qualitatively analysed for convergence, and relevant details were extracted, using inductive approach.

It is true that the benefits of this research could not be entirely determined. Every reader should find useful information different from any other, as orientation and situation differ. This overview could also serve as indicator of or pointer to a research area or be a rider to a more detail research into certain aspects of information security.

II. INFORMATION SECURITY BACKGROUND

Data is raw facts, such as alphanumeric, image, audio, or video, having little or no meaning. Information is a collection of organized facts or data with added value. Information is meaningful data. It should be noted that data to one person may be information to another, depending on their objectives, and the same information may be interpreted in different ways by different people. Information becomes more useful as it becomes more accurate, complete, economical, flexible, reliable, relevant, clear or simple, timely, verifiable, accessible, and secure. Some costs may be incurred in obtaining certain information in terms of establishing necessary information system that produced it or paying outright for the information. The value of information, in that case, is its benefits over and above its costs [1].

Information is essential to the continued growth of any society. Information is an asset as important as capital or work [2]. Information is created, managed, processed, and archived by an information system. An information system is a set of interrelated components that collect, manipulate, and disseminate data and information and provide a feedback mechanism to meet an objective. Computer-based information system consists of hardware, software, databases, telecommunications, people (weakest link in information security [3]), and procedures [1]. Information is vulnerable to technical, physical and human threats, and risks to information system must be continually assessed and effectively addressed [4]. Threats to information security include errors and omissions, fraud (crime committed in order to make an unlawful gain (e.g. in e-commerce and m-commerce) or cause financial or proprietary loss to another by using deceptions and tricks) and theft, malicious hackers, malicious code, denial-of-service attacks, and social engineering [5], which may result to data alteration and damage, or access by non-authorized third parties [6]. Losing data can lead to direct financial losses, legal and regulatory issues, fines, and reputational damage [7].

Organisations that rely on information by means of information systems, therefore confront huge potential losses. A secure information system is necessary. A secure information infrastructure is also required to obtain and sustain competitive advantage. Having effective security in place could provide competitive advantage in attracting customers to use certain products and services or in providing opportunities to sell products/ services through new channels, among others [8]. Security breaches are usually perpetrated by or due to people (insiders, outsiders or third-party agents [9], or be due to hardware or software malfunctions, power

failure or natural disasters [10]. System faults are adequately addressed by provision of ample well configured resources with sufficient fault tolerance, and veritable backups. Security flaws in large and complex computer programs are addressed or reduced by encouraging programmers to code simplistically in order to make lesser or avoid programming errors.

Information security (or cyber security, as the internet becomes more prominent) relates to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction [8]. Information Security (IS) is ensuring, taking useful precautions, that the information systems perform according to stipulation and retain optimum performance, even in the face of clever wrongdoers or oppositions, and despite system failure. This covers the life cycle of every piece of information, from the information need conception to its destruction, involving data entering, creation and/or acquiring, data processing and/or deriving, data storing, replicating and distribution, data archiving and recalling, data backup and restoring, and data deleting, erasing, removing and destruction [3]. Proper methods of disposal of information that is no longer required should be in place [11]. Any company's information is as good as the security mechanisms implemented over it, and unreliable information resulting from wrong policies would generate uncertainty and mistrust [2]. Effective security is achieved by working within a proper framework, in compliance with legislation and appropriate policies, and by adherence to approved procedures and codes of practice [11]. Information system security function establishes security policies and their associated procedures and control elements over information assets to guarantee their authenticity, confidentiality, availability and integrity.

Data security is protecting data, wherever stored. The first line of defence is access control, the second good encryption program, and the third is a good back-up system [11]. Every computing device needs security to prevent it from being the weak link allowing unauthorized access to organisation's systems and information. Security related information should be kept a secret, though should not be relied solely upon for security [13]. In the end, an organisation's information security is only as strong as its weakest link [14]. Data leak prevention (DLP), a suite of technologies aimed at stemming the loss of sensitive information that occurs in enterprises, focuses on the location, classification and monitoring of information at rest, in use and in motion. This technology requires significant preparation and diligent ongoing maintenance. A strategic approach that addresses risks, impacts and mitigation steps, along with appropriate governance and assurance measures is required [15]. Network security is protecting computer networks, the essential telecommunication facilities. Computer security, database security, data security, and network security, among other perspectives, are critical and complimentary to the success of information security.

The requirement to preserve people's privacy poses more challenges, which must be taken seriously, on information security. Data protection is about preserving a fundamental human right to privacy in this digital age. Privacy rights regarding information generally limit the ability of people to gain, publish, disclose or use information about others without their informed consent [16]. Personal information is information or opinion, whether true or not, whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably be ascertained, from the information or opinion [10]. The protection of data concerning persons requires that such data be collected and processed in a fair and lawful manner, and collected for determined, explicit and legitimate purposes and is not later on processed in a way that is incompatible with these purposes [6]. Appropriate security safeguards and measures for protecting personal information need to be considered in relation to all of the entity's acts and practices. This should include governance (clear procedures and lines of authority for decisions regarding information security), information and telecommunication technology security (protecting hardware as well as data that the hardware holds), data breach response plan, physical security, personnel security and training (to minimize human error and build desirable practices), integration of privacy protections into workplace policies, managing the information life cycle, compliance with international, national and industry standards, and regular monitoring and review of information security measures [10].

The implementation of a comprehensive privacy and data security plan, to reduce or eliminate vulnerabilities in order to prevent successful attacks and system failures, is necessary. This begins with understanding the network, its architecture, user population, and mission requirements. Security vulnerabilities include non-existent security architecture (no roadmap to implementing necessary protection would probably leave holes in information resources open to exploitation), un-patched software (system and application), people's baggage (social impacts, which leaves information system open to deliberate abuse, errors, and social engineering attacks), poor system configuration, mobile devices (with lagging security for operating system and application, and could be easily stolen), third-party involvement (sharing or transferring responsibility based on trust), and removable data storage media (pathway for data theft and for malware to move between networks or hosts [17]) [8]. Entities should build privacy and information security into their processes, systems, products and initiatives at the design stage, and should undertake a privacy impact assessment and an information security risk assessment for changes in existing acts or practices [10].

III. BASIC SECURITY ISSUES

A. Primary Information Security Issues

Primary information security issues are confidentiality, integrity, and availability. These three are extended to include possession, authenticity, and utility in Parkerian Hexad model [18], described as six fundamental, atomic, non-overlapping attributes of information that are protected by information security measures [19]. Confidentiality of information is maintained when it is only read or acquired by those authorized to do so. Integrity, defined differently by different information technology professionals [3], basically means content is accurate, valid and consistent, and content only altered under properly authorized and valid circumstances. Availability means resources are available when needed. Possession is exclusive (or intended) possession and control, and ability to prove it. Authenticity is validity, conformance, and genuineness. Utility is usefulness or fitness for a purpose [20]. These attributes of information must be cost effectively maintained despite malicious users, accidental misuse or non-deliberate errors, system failures, and environmental factors, among others.

B. Secondary Information Security Issues

Secondary information security issues are authentication, authorization, non-repudiation and accountability, which are concepts relating to information system users [13]. Authentication is the process of ensuring identity of entity, which could be a person, device, or programme, among others, is genuine. It is proving that an entity is what the entity claims to be. Authorization is granting of permission using authenticated identity, but based on requested resource, and security policy [21]. It is the process of determining whether a particular entity has the right to carry out a certain activity [13], and allowing or disallowing the requested action. Non-repudiation is authenticity, genuineness, being sufficiently trustworthy that it cannot be denied or refuted. Accountability is the determination of who did what, on what resource, at what time, in sufficient details [22]. Implementing a logging facility, which should not be down played, is necessary for monitoring how information system is used.

C. More on Confidentiality

Visual data security is an aspect of confidentiality concerned with ensuring that information cannot be seen or captured while displayed, whether inside or outside the office and on any devices, by unauthorized individuals [7]. This should not be overlooked because it would undermine the time and investment spent in sophisticated computer security solutions. Organisations will often never know if they have suffered a visual data security breach [7]. Measures to improve visual security includes training, screen positioning, ‘anonymizing’ data and using privacy screens, to complement standard security measures.

D. More on Data Integrity

Integrity is safeguarding information accuracy, consistency, validity and completeness [11]; [23]. Integrity, which is particularly important for critical safety and financial data, is lost when information is modified in unexpected way [13]. Database integrity is achieved through proper structuring and built-in rules, which should comply with applicable standards [23]. Guaranteed data integrity means implementing a mechanism that ensures data accuracy, completeness, and update when necessary [6]. Program of data integrity addresses Detect, Deter (2D); Prevent, Prepare (2P); and Respond, Recover (2R) [24]. Good practices to adopt include taking ownership of data and accountability for data integrity by people in the appropriate business unit, implementing appropriate access rights and privileges, and proper segregation of duties [3].

E. More on Availability

Information system resource might be unavailable for a number of reasons. Some of these are system faults, connectivity issues, bandwidth constraints (orchestrated or otherwise), the resource being overwhelmed by demand for service (orchestrated or otherwise), and malware activities. Adequate, sufficient, and well configured provision of information resources, having well designed and implemented network(s), implementing adequate fault tolerant systems, monitoring denial of service attacks and deploying sufficient resources to cope successfully (which could be handled by competent internet service provider under proper agreement), and installation of up-to-date antimalware contrivances at strategic points, should ensure acceptable availability of information resources.

F. More on Authentication

Authentication is ensuring identity of entity is genuine. Authentication is preceded by identification, usually as software entity, which allows this entity to be recognised by the system via a previous set of elements given, captured, and kept, all done securely. A foolproof digital identity is challenging to establish as immerging technology makes impersonation easier. To authenticate is to proof identity [6]. Consideration of an open trusted next generation secure computing base, at the core of this, is necessary.

G. Other Security Issues

Other security issues are security policy, security mechanism, and trustworthiness. Security policy states what must or must not occur, to ensure that all computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that the protection is cost effective [11].

Security policy, when well thought out and articulated, is an excellent guide to security implementation. Security mechanisms are products and policies used to prevent and monitor system use and abuse. Security mechanism determines how policy is ensured at different hierarchical layers while avoiding circularity (without ambiguity in design and implementation of hardware, operating system kernel, network software, database management system, and application) [22]. Trustworthiness means that a system, an application, or network, among others, is likely to satisfy its desired requirements. These requirements must be well defined for their trustworthiness to be effectively evaluated. Security metrics should measure what matters, which would help to be proactive [25]; [26].

IV. APPROACHES TO INFORMATION SECURITY AND RELATED ISSUES

A. The First Steps

In consonant with appropriate enterprise information security architecture [27], the first step in approaching securing information system resources is to audit all aspect of system regarding possible unauthorized users and/or misuse by authorized users, and to design and implement a security plan [28]. It is also important to anticipate possible system failures and environmental misfortune. Enterprise information security architecture consists of framework of business, information, technology, and security architecture. The architecture includes business roadmap, legislative and legal requirement, technology roadmap, industry trends, risk trends and visionaries, among others [27]. What to audit include servers, user devices, software, data (offline and online), network, processes, and people, taking stock of files and personal data and the associated processing, whether they are automated or not [6]. Documented inventory of the types of data, how the data is stored, where the data is stored, how the data is moved and who has access to it, and the data controls in place, are basic [29]. Data leak prevention technologies facilitate locating and cataloguing sensitive information stored throughout the enterprise, and monitoring and controlling the movement of sensitive information across enterprise networks and on end-user systems [15]. How persons' privacy could be impacted should also be evaluated. Design and implementation of a security plan involve risk analysis, doing something about the risk, and having a disaster recovery plan. Risk analysis includes knowing the value of assets, the likelihood of breach, and probable cost of compromise against estimated costs of protection. What could be done about the risk could be risk reduction, minimization attempts or elimination/avoidance (protecting), risk acceptance (doing nothing about the risk) or risk transference (insurance, outsourcing, or other available choices). Identifying and ranking the severity of potential threats (cognisant of vulnerabilities inherent in the information systems and profiling security breach agents) to information security efforts would engender more effective security strategies [30]. The disaster-recovery plan should be implemented and tested.

B. Security Risk Reduction/Elimination Top Level Measures

Holistic risk reduction/elimination, regarding human related security breaches, includes technological, process or human-based approaches. Approaches to the security risk reduction/elimination may also be classified as technology based or non-technology based. Technology based approach is becoming the key strand to information security because of significant increases in the volume of data, speed of processing and communication technology, and the emergence of more complex and automated threats. Technological methods include physical and logical access restriction, firewall, intrusion detection and prevention, encryption, virus monitoring and prevention, audit-control software, among others, and human-based approaches include ethics, law, and effective management [28]. It should be realized that security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The best thing to do is to reduce risk of exposure regardless of the products or patches [31]. Security implementation should be managed in a way that provides capabilities to rapidly defend new vulnerabilities and threats. Any list of generic good security principles would likely include least privilege, simplicity, open design, complete mediation, white listing, separation, and ease of use [21]. Ways of measuring the effectiveness and efficiency of information security design and operations are important in making sound security decisions [32].

C. Access Control

Access control involves identification (usually as software entity), authentication, authorization (security mechanisms based on security access policy) and accountability. In order to guarantee that information technology system users only have access to the data they need to know, it is necessary to provide a unique identifier to each user, in association with authentication means (authentication method), and to apply prior access controls to data for each category of users (authorisation management). Physical and logical access restrictions include brute force or physically securing, authentication, and authorization control. Physical barrier includes doors, safes, keys, locks, and fences. Surveillance, alarm systems, and procedures are also used to physically secure and monitor. Authentication, ensuring identity of entity is genuine, requires each user entity to supply something the entity knows, something the entity has, or something the entity is [28], to match the entity's previously captured and safely stored, usually in software form, unique identifier. Something the entity

knows, which includes password (kept secret, encrypted, at least eight characters long, contains different types of characters such as uppercase, lowercase, numbers and special characters, and regularly changed) and pin, could be violated through such means as guessing, wiretapping, and social engineering. Something the entity has, which includes keys, cards, and smart badges, could be expensive and could be inconvenient because they have to be carried. Something the entity is or behavioural, which includes biometrics, comes with high security and efficiency, but could be scarce, involve expensive hardware, limited in its use by disruption of bio-configuration, and subject to abuse through biometrics replay or reuse. The biometric unique identifier of each user should also be "traceless". A combination of something the entity knows, has, or is proves more adequate for authentication, and is regarded as being strong [6]. It should be noted that authentication presupposes that identification of entity has been previously captured free of any type of errors, commission or omission. Authorization, which is the process of granting resource usage privileges to previously authenticated user entities, is usually application built-in. It may employ the use of access control list and capability list. It could use classical discretionary, classical mandatory, role-based, or a combination of these authorization approaches to restrict access [33]. Administrator user account should be very limited. Great care should also be exercised regarding Operating Systems (OS), being the ultimate enforcers of access control, and a successful attack on the OS can effectively nullify any protection built in at a higher level [21].

D. Firewall

A firewall is a contrivance that detects intrusion attempts and prevents unauthorized access to or from a private network, data, file, database or application. Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and un-trusted networks (beyond the organisation's control), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks [34]. It could be hardware or software based. Some types of firewall are packet filter, application-level filter, circuit-level control, and proxy, according to what they do and how they do what they do. Packet filter is fairly effective and transparent but takes time to setup and may slow the network. Application-level filter works for specific applications and is also fairly effective and transparent, and takes time to setup and may slow the network. Application layer filtering includes web browsing and e-mail scanning and deep content analyses, including the ability to detect, inspect, and validate traffic using any port and protocol [35]. Circuit-level control firewall checks certain type of connections, and packets flow freely without further checks after connection is permitted. Proxy server creates the appearance of an alternative server to all computers connected through it, thereby shielding them from direct access. Firewall could be implemented as software on a single computer being used, as firewall router (e.g. for a small office home office (SOHO)), or as multiple layers and types [36]. Organisations are also advised to include a layer of protection positioned closely around the data and application in the data centre, in order to stem advanced targeted attacks. This protection includes database firewall, file firewall, directory services monitoring solution, web application firewall, and secure web gateway solution, to monitor, provide real-time alert, enforce business and regulatory policies, and to block unwanted or suspicious activities [14].

A firewall can adopt one of two basic policies to control access: whatever is not prohibited is allowed (blacklisting) or whatever is not allowed is prohibited (white-listing) [37]. The ideal configuration for firewall is to simply deny all incoming traffic and then create specific rules to allow communication from specific IP addresses or ports as the need arises (white-listing). Wireless Local Area Network should disallow open access and allow only pre-authorized wireless Network Interface Cards [28], or media access control identities. Firewall at each internet connection and between any demilitarized zone and the internet network, and router with strong access control list, are necessary for a more secure needs [34]. A number of challenges are to be overcome in designing data security and privacy mechanisms for wireless body area networks (WBANs). These include balancing security, efficiency and practicality. Stringent resources constraints on WBAN devices require the security mechanisms to be very lightweight, and the open wireless channel makes the data prone to eavesdropping, modification, and injection. Data confidentiality, dependability, and integrity are the three most important requirements for distributed data storage in WBAN [38].

Data breach is probable, damaging and costly to organisations. There is a high probability that a data breach is through some form of hacking. It is, therefore, important to fortify network security. A personal computer with direct access to external network requires turning on its operating system built-in firewall, and installation of effective anti-virus software with real-time update. A small office or home office network requires a rightly configured cable or DSL router-based firewall and installed effective anti-virus software with real-time update on every host in the network to protect the perimeter and ensure maximum security for the computers. A network requiring excellent perimeter security demands at least an application gateway and an application proxy firewall. The perimeter security should also be fortified through host hardening. Effective anti-virus software with real-time update should also be installed on every host in the network [39].

E. Intrusion Detection and Prevention systems

Perimeter security implemented by the use of firewalls is never hundred percent effective, and the external traffic entering the network is not the only attack vector that requires attention. Running an intrusion

detection system (IDS) or intrusion prevention system (IPS) helps to detect malicious traffic that either slips past the firewall or originates from inside the network in the first place. IDS, a means of monitoring intrusion or alerting that an intrusion has occurred, can be network-based (NIDS) or host-based intrusion detection system (HIDS). A NIDS examines actual packets travelling the network in real time to look for suspicious activity. A HIDS examines log files and looks for entries that suggest suspicious activity. NIDS has the advantage of detecting attackers in real time. HIDS can detect attacks that do not travel the network, attempts to access files or change permissions, and changes to key system files. NIDs and HIDS can be used together to alert all the different types of attacks that might not be caught by just a NIDS [40]. An intrusion prevention system (IPS) is somewhat like a hybrid between an IDS and a firewall. When an IPS detects that there is suspected malicious traffic, it can alter or create firewall rules to simply block all traffic on the target port or block all incoming traffic from the source IP address or any number of custom responses configured. Sometimes the line between firewall, intrusion detection and intrusion prevention gets blurred as applications and devices come out that try to provide all-in-one detection or prevention. Active intrusion response system (AIRS) using behavioural analysis of inter-network communications is deployed against continuous behavioural attacks, of which distributed denial of service (DDoS) is a type. These systems employ signal processing, expert decision algorithms, statistical algorithms, and closed feedback techniques [41]. Any AIRS should be evaluated based on its self adaptive mechanism, behaviour analysis, closed feedback mechanism, countermeasures, real-time, and visualization capabilities. It is true today that firewalls, well configured routers and intrusion detection or prevention, including host hardening, will not protect from every possible computer attack, but with one or both of these technologies in place, exposure to risk is greatly reduced and security is increased. If information is highly desired or targeted for other reasons, understanding the motives, skills, and methods of probable adversaries is important to any well-considered and well-prepared defence [20].

F. Encryption

Encryption is encoding and decoding as necessary employing cryptography. Its related topics include data hiding (steganography), and watermarking (trademark hiding). Encryption works by having a code (key) scramble and a code decode the message. Sender and receiver may use the same key (symmetric secret key), which comes with key management problem at both sides. Sender may otherwise use a private key to encrypt and have a public key, known widely, to decrypt (asymmetric), thereby authenticates the sender when message sent by sender is decoded using the sender's known public key. The problem with the asymmetric method is large-scale management of public key, which is usually contracted to a certificate authority/ trusted middleman. Generally, encryption key management is important. Encryption keys should be sufficiently protected as they are vulnerable to theft or damage by malicious users or environmental hazards. Balancing encryption having strong security (large key), having high speed of encrypting and decrypting, and being portable (usable on cellular, personal digital assistant, and so on) is a challenge [28]. Encryption should be done to an acceptable standard.

Encryption is used in authentication process, privacy/confidentiality, integrity, and non- repudiation, among others. Its application finds place on the internet, public telephone lines, and airwaves, among other uses. In authentication, record of what you know, have or are is encrypted during communication. Data at rest and backups are encrypted to safeguard privacy/confidentiality. Hashing result is encrypted so that a change in content material, integrity abuse, would be revealed. Encryption ensures non-repudiation in that when someone's public key is successfully used to decrypt a message there is no denying that the message was sent by that person. A virtual private network is constructed dynamically within an existing network by creating an encrypted "tunnel" to send secure data over public network. There are various types of encryption technology. An example is disc encryption, a system that encrypts all the data on a hard drive. Encrypted disk should be protected from damage by authorized or authorized users, and system failure. Disk encryption could be software or hardware based [12].

G. Virus Prevention

Virus monitoring and prevention involves having up-to-date genuine antivirus run often, avoidance of shared disks and drives, and sharewares, avoidance of downloads from non-reputable sources, deletion without opening of emails from unknown sources, following careful downloading practices, taking immediate action and reporting virus infection experience appropriately, and educating others about what to do [28]. Other technologies, such as DLP [15], exist to protect against other types of malware.

H. Auditing

Audit-control is having software that keeps track of computer activities in form of audit trail. Audit trail involves recording users and activities performed, detailing among others, who, what, how, and when [42]. By so doing it facilitates spotting suspicious activities, and engenders quick and appropriate action. A firewall does something similar automatically in real time [28].

I. Other Technological Safeguards

Other Technological Safeguards include regular backups, fast and durable storage devices, fault-tolerant systems, closed-circuit television (CCTV), uninterruptible power supply (UPS), and healthy network environment in terms of temperature, humidity, ventilation, dust and smoke, among others [28]; [43].

J. Ethics

Human-based approach to information security risk reduction includes Ethics, Law, and effective management [28]. The lack of good behaviour on the part of certain individuals is responsible for most security issues plaguing the society and needing attention. It is therefore necessary to address ethical issues in computing sciences towards more secure computing environment. Ethics, also known as philosophical ethics, ethical theory, moral theory, and moral philosophy, is a branch of philosophy that involves systematizing, defending and recommending concepts of right and wrong conduct, often addressing disputes of moral diversity. The term comes from the Greek word ethos, which means "character" [44]. It involves conscious reflection on our moral beliefs with the aim of improving, extending, or refining those beliefs in some way [45]; [46]. Any person who knows what is truly right will automatically do it, according to Socrates. While he correlated knowledge with virtue, he similarly equated virtue with joy. The truly wise man will know what is right, do what is good, and therefore be happy [47]. Christians who read the Bible are more likely to actively seek social and economic justice; believe it's important to consume or use fewer goods; and are less likely to view religion and science as incompatible, among other moral and political issues [48]. Ethics emphasizes truth, justice, and integrity (honesty and strong moral principle). Computer ethics, which are standards pertaining to information system usage, include privacy, accuracy, property, and accessibility. Responsible computer use prohibits using a computer to harm others, interfering with other people's work, snooping in other people's files, using a computer to steal, using a computer to bear false witness, copying or using proprietary software without paying for it, using other people's computer resources without authorization or compensation, and appropriating other people's intellectual output. Responsible computer use recommends thinking about social consequences of programs you write and systems you design, and using a computer in ways that show consideration and respect for others [28]. Computing professional codes of conduct are based upon loving neighbour as loving self towards more productive societies. Ethics demand that all research participants should be treated fairly and with honesty. Conditions in society are a reflection of conditions in the homes of the nation. Every effort toward personal and family wholeness is an effort in reducing security breaching behaviour. It is everybody's responsibility to propagate, encourage and support ethical living and computing [49].

K. Managing for Result

Securing information, whether technology or human based, is performed through effective and efficient management implementation. Effective management human-based security risk reduction involves system risk analysis, hiring of trustworthy employees, holistic information security planning, policies and procedures, implementation of the spelt out information policies in security measures, auditing and review of what had be done, and regular update to accommodate changing business needs. A risk is a scenario which combines a feared situation (a breach and its consequences) and the probabilities that it occurs (threats). Its level is estimated in terms of gravity (extent and number of impacts) and likelihood (possibility/probability of occurrence) [6]. System risk analysis leads to acceptable use policies with penalties well spelt for non-compliance. System risk analysis also involves assessment of current security policies and recommendation of changes for improvement. Hiring of trustworthy employees (including background screening) and treating them well is necessary to reduce internal security breaches resulting from employee abuse of authorized access. Development of holistic information security plan involves risk assessment, risk reduction/elimination planning and implementation, and ongoing monitoring. Policies and procedures detail information policy, security policy, firewall policy, security responsibility sharing with third party, strong user password, segregation of duties, use policy, backup policy, use account management policy, incident handling procedures (security breach), and disaster (natural/deliberate) recovery plan, among others. Implementation involves putting in place necessary security mechanisms, training employees on security policies and measures, and establishing effective disaster recovery measures. Auditing includes examination of policy adherence, new projects adherence to standards, security penetration tests, and vulnerability assessment [28], among others.

Information policy pertains to sensitive information handling, storage, transmission and proper destruction. Security policy technical controls include access limitation, audit-control software, software update and upgrade (patch management program), and computer configuration management. Computer configuration management is implementing security features through control of changes made to hardware, software, firmware, and security documentation throughout the life of an information system [17]. Use policy addresses in-house computer, internet surfing, non-employment related uses of organisational information resources, use of email, mobile devices, removable media, and social media websites, among others. Mobile devices though provide significant opportunities to increase the effectiveness of mobile workers, raise significant concerns about the security and privacy of sensitive corporate data stored on them [50]. Backup policy should state that

backup, storage and retrieval be supported by advanced data and system backup and recovery tools. Use account management guides adding new users, removing users, and fitting user rights, among others. Security mechanism should also include installation of professional enterprise-level security software for e-mail, antivirus, firewall, and so on. Employee training should include social engineering attack enlightenment/awareness, safe way to use mobile devices and removable media, password security maintenance, and social media website risks, among others. Lack of employee awareness about security policies was ranked as having the greatest impact on the security of mobile data [50]. The strength of security mechanisms, intrusion detection system, physical security, the incident response preparedness, and employee knowledge of security policies and procedures, should be properly examined and ensured to meet necessary regulations and standards.

Information security approaches need to adapt to rapidly changing threats and technology, changes in regulations and standards, and changes to business requirements and priorities (increased mobility, flexibility and shared resources [7]). It should be resilient [8]. Actors, who require and use information resources, should be involved in deciding security measures, made responsible for their choices, and made to adopt security measures they select. Custodians of information should adopt a risk-based approach to assessing the value of information handled, its sensitivity and the appropriateness of security controls in place or planned [11]. Greater needs to share information electronically require classification of information, in order to define what can and cannot be shared to protect commercially sensitive information and to comply with regulations. Classification of information into categories that reflect the business need to protect them have groups such as public, restricted to, embargoed until and secret, letting business functions take ownership [16], among others.

L. Information Security Challenges

Data protection is about protecting fundamental human right to privacy. This is particularly relevant in the context of social networking, consumer profiling, and cloud computing. Personal data means any kind of information that can personally identify, directly or indirectly, an individual or single them out as an individual. It is enough if a person is "singled out" from among other people using a combination of pieces of information or other indirect identification or inadequate anonymity set [51]. This challenges, in particular, setting up approved anti-fraud databases allowing cross-financial institution usage for verification and enlightenment, through the strict conditions for personal data processing imposed by law and legislations. This is more difficult for cross border verification. Records relating to previous conviction, satisfying "burden of proof", needed for prevention and detection of crime, or relating to matters of national security, among others, are less protected from storage on such databases [51]. Electronic funds transfer security requirements, from a user's point of view, fall into three categories relating to the privacy of the consumer, the trustworthiness of the retailer, and the safety of the payment itself [16]. It is also increasingly important that privacy protections are built into design and implementation of products and services.

Emerging security challenges are being created by ubiquitous computing, disruptive technologies such as quantum computing, wireless electricity, new man-machine interfaces and new communication protocols, among others [8]. As people spend an increasing proportion of their time online, identity becomes a greater challenge because fewer interactions will be face-to-face, a greater volume of private information may be available online and new technologies could make it easier to impersonate individuals, but innovations in artificial intelligence could enable devices make autonomous decisions on trust when connecting and exchanging data with devices and applications [8].

Social network sites, enabling people to connect with each other, obtain information quickly and participate in matters that affect them, making them more active and informed, collect peoples' data and use these data to sell targeted advertising [51]. The data collected, stored, shared, sold, bought and combined, could pose a problem if they are used to discriminate on the basis of sensitive data [51], even when supposedly 'anonymized' in keeping with laws and legislations.

The growing importance of data processing in all the spheres of society leads to the production, processing and dissemination of an increasing amount of corporate sensitive and personal data, with threats, including computer fraud, purpose circumvention, fraudulent data collection, data loss, vandalism, and environmental factors such as fire and floods, weighing on information resources/systems [6]. Staying ahead of ever-evolving threat of a data breach requires diligence on the part of the security expert in understanding and anticipating security risks, which are products of system vulnerabilities (weaknesses) and their possible attacks (threats).

Opposing forces to regulation and standardisation are globalisation (homogeneity challenge, uncertainty about legal requirements in some countries and jurisdiction ambiguities regarding responsibilities of different national authorities including consumer protection laws, record keeping and report requirements [16]) and net neutrality (all traffic must be treated equally by network carriers, without any restrictions or priorities being placed on content) against multiple internet (due to greater censorship, political motivations, need for new more secure internet, closed social networks and growth in paid content) [8].

A good law needs good enforcement to make it work. Strong data protection laws should be enforced by adequately staffed and independent data protection authorities with sufficient legal powers and necessary technical expertise [51]. Privacy protection should be made a reflex rather than an obligation for business to transform consumer expectation of privacy from hope to a demand.

Application vendors promise to protect against zero-day attack. Zero-day attack is aimed at exploiting software application vulnerability before the application vendor becomes aware of it and before the vulnerability becomes widely known to the internet security community and countermeasures applied/supplied [17].

Information security relies on legitimate users, security mechanisms, and processes to provide a level of security. A system or an entity is trusted if relied upon for security. Security depends on trust [21]. Hardware is relied upon to perform according to what the manufacturer promised. Redundancy strategies are employed to cater for hardware failures. The question is how could one be sure that the hardware could be relied upon not to be abusing security in favour of the manufacturer? The manufacturers could have inbuilt spywares or other disruptive contrivances in purchased items. Similar doubt could be raised about software too, whether system or application. Beside bugs that are not deliberate and would expose users to security breaches, programmers could deliberately add codes that breach security, one way or the other. Firewalls, perimeter, database, file or other, are not exempts, neither are intrusion detection and prevention systems. Transparency regarding the technologies being used, open peer review by security engineering experts and responsible disclosure procedures, are necessary, and would raise standards [51]. There is also the primary need for human-to-human trust. There is an increasing need for human to trust technology, technology to trust technology, and even technology to trust human as devices increasingly act on behalf of individuals [8]. The best deal is to arrange security devices in such a way as to counteract user and manufacturer reliability doubts.

A successful attack on the OS bypasses higher-level security functions. Trusted computing base, which should be designed first and be central in one place), is everything in the OS that is relied upon to enforce security [21]. Trust have to be placed on the secure computing base that it will do what is expected and nothing more (e.g. spying or establishing hindrances) breaking one's security.

Particular security needs of various industries vary according to what they protect and what security standards and regulations dictate (health, banking, critical national infrastructure, and privacy, among others). Ensuring continued access to data collections through time and changing technology is an issue that is always rife. Storage media, necessary software, and data format become obsolete with time. Periodic reviews should be conducted to determine when data migration is needed to ensure continued access to data collections through time and changing technology [52].

Change must be managed. Elements and forces that influence change either drive it or restrain it. Awareness, management support, budget and security culture are example of change driving forces [25]. Change resisting forces include errors, lack of experience, apathy, negligence, stress, lack of communication, and lack of security policy enforcement [26]. Appropriate information security technology and measures that are able to evolve to support the changing technology landscape over time should be incorporated.

V. CONCLUSION

Securing information resources is a challenging venture. There are many aspects to the matter. What everyone does, or does not, imparts information security success, besides system failures, software bugs and environmental hazards. Information security is everyone's duty, together with the support of security experts, appropriate policies, mechanisms, procedures, and effective management, among others, to make it much more difficult for security breach agents to succeed, and much more easier to convince breach agents to do otherwise.

Information security relies on a number of things for its success. Those things are trusted to ensure security. The fact is that those things are inherently doubtfully dependable for certain reasons and because they are subject to abuses. Adequate remedy should be put in place to safeguard security contrivances manufacturer abuses. Good regulations, laws and enforcement processes would also be necessary.

Information security is a dynamic never ending process requiring regular review and update of information system resources, security policies, training, processes and mechanisms to ensure business continuity, and to stem information abuses and comply with regulations and standards. A truly secure computing environment free of abuses is only possible when all those who could access information are enlightened, faultless, and incapable of wrongs; the vision of information security.

REFERENCES

[1]. Stair, R. M. & Reynolds, G. W. (2007). *Fundamentals of Information Systems*. Boston, MA: Course Technology

[2]. Mellado, D. & Rosado, D. G. (2012). An Overview of Current Information Systems Security Challenges and Innovations. *Journal of Universal Computer Science*, Special Issue, Vol. 18, No. 12, pp 1598-1607

[3] . Gelbstein, E. (2011). Data Integrity—Information Security's Poor Relation. Retrieved from http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation.aspx, 15 Aug, 2014

[4]. Richo Security Solutions. (2010). Home Page. Retrieved from www.ricoh.com, November 17, 2010

[5]. Shostack, A & Stewart, A. (2009). *The new approach to Information Security*. Harlow, Essex: Pearson Education

[6]. CNIL. (2010). Guide Security of Personal Data. Retrieved from www.cnil.fr/fileadmin/documents/en/Guide_Security_ of_Personal_Data-2010.pdf

[7]. Honan, B. (2012). Visual Data Security White Paper. Retrieved from http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf

[8]. PricewaterhouseCoopers. (2010). Revolution or Evolution: Information Security 2020. Retrieved from https://www.innovateuk.org/documents/1524978/1814792/Revolution+or+evolution+-+Information+Security+2020/c15f89cc-405c-423d-92c4-a9295bd56720, 15 Aug, 2014

[9]. Verizon. (2012). Data Breach Investigation Report 2012. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, 15/4/12

[10]. Office of the Australian Information Commissioner. (2013). Guide to Information Security: 'Reasonable steps' to protect personal information (2013). Retrieved from http://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

[11]. UCL. (2013). UCL Information Security Policy [1]. Retrieved from https://www.ucl.ac.uk/informationsecurity/policy/public-policy/InfSec_Policy_ISGC_20130717

[12]. Stevenson, K. (2011). The Basics of Data Security. Retrieved from http://ezinearticles.com/?The-Basics-of-Data-Security&id=6078212

[13]. Pesante, L. (2008). Introduction to Information Security. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf

[14]. Imperva. (2013). Targeted Attacks: 8-Step Plan to Safeguard Your Organisation. Retrieved from http://www.imperva.com/docs/eBook_Targeted_Attacks_-_8_Steps_to_Safeguard_Your_Organization.pdf, 28/8/2014

[15]. ISACA. (2010). Data Leak Prevention. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx

[16]. Mthembu, M. A. (2010). Electronic Funds Transfer: Exploring the Difficulties of Security. *Journal of International Commercial Law and Technology*, Vol. 5, Issue 4, pp 201-205

[17]. Privacy Technical Assistant Center. (2011). Data Security: Top Threat to Data Protection. Retrieved from http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf

[18]. Kabay, M. (2011). The Parkerian Hexad. Retrieved from www.mekabay.com/courses/academic/norwich/is340/is340_lectures/csh5_ch03_parkerian_hexad.pptx

[19]. PCMag. (2014). Definition of: Parkerian Hexad. Retrieved from http://www.pcmag.com/encyclopedia/term/48859/parkerian-hexad, 28/8/2014

[20]. Verizon Risk Team. (2012). 2011 Data Breach Investigation Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[21]. Stamp, M. (2006). *Information Security: Principles and Practice*. Hoboken, New Jersey: Wiley & Sons

[22]. Neumann, P. G. (2004). Security and Privacy in Computer-Communication Systems. In Tucker, A B. (Ed.) *Computer Science Handbook*. Boca Raton, Florida: Chapman & Hall/CRC

[23]. Davis, G. (2010). Database Integrity and Database Security. Retrieved from http://www.docstoc.com/docs/164662105/Part-3-Database-Integrity-and-Database-Security

[24]. US Joint Chiefs of Staff. (2007). Joint Publication 3-28, Civil Support. Retrieved from http://fas.org/irp/doddir/dod/jp3-28.pdf, 28/8/2014

[25]. Tripwire Guest Authors (2013a). Human Factors in ISMS: Goal Driven Risk Management. Retrieved from http://www.tripwire.com/state-of-security/security-data-protection/2-human-factors-isms-background-knowledge/

[26]. Tripwire Guest Authors (2013b). Information Security Management Systems: Modelling Human Factors. Retrieved from http://www.tripwire.com/state-of-security/security-data-protection/3-information-security-management-systems-modelling-human-factors/
[27]. Gartner. (2006). Incorporating Security into Enterprise Architecture Process. In Wikipedia. (2014). Enterprise Information Security Architecture. Retrieved from http://en.m.wikipedia.org/wiki/enterprise_information_security_architecture
[28]. Jessup, L. & Valacich, J. (2007). *Information Systems Today - Managing in the digital world*. Saddle River, New Jersey: Pearson Education
[29]. Better Business Bureau. (2010). Data Security Made Simpler. Retrieved from http://www.bbb.org/data-security/intro-to-small-businesses/
[30]. Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, Vol. 46, No. 8, pp 91- 95
[31]. Schneier, B. (2000). The Process of Security. Retrieved from https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html, 28/8/14
[32]. Jansen (2009) in Mellado, D. & Rosado, D. G. (2012). An Overview of Current Information Systems Security Challenges and Innovations. *Journal of Universal Computer Science*, Special Issue, Vol. 18, No. 12, pp 1598-1607
[33]. Sandhu, R. & Samarati, P. (2004). Protocols for User Authentication, Access Control and Intrusion Detection. In Tucker, A B. (Ed.) *Computer Science Handbook*. Boca Raton, Florida: Chapman & Hall/CRC
[34]. PCI Security Standards Council. (2010). PCI Data Security standard. Retrieved from: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
[35]. Kiernan, P. (2010). Network and Perimeter Security. Retrieved from download.microsoft.com/.../June_8_ME_Network%20and%20security.ppt
[36]. Bradley, T. & Carvey, H. (2006). *Essential Computer Security*. Rockland, MA, US: Syngress Publishing, Inc.
[37]. Parenty, T. (2003). Digital Defense. Boston: Harvard Business School Press
[38]. Li, M., Lou, W., & Ren, K. (2010). Data Security and Privacy in Wireless Body Area Network. IEEE Wireless Communications, Vol. 17, No. 1, pp 51-58
[39]. Adebayo, A. O. (2013). Data Breach Risk Reduction through Perimeter Security and Smart Surfing. International Journal of Computer Science Research and Technology, Vol. 1, Issue 5, pp 46-51
[40]. Bradley, T. (2004). Host-based Intrusion Prevention. Retrieved from http://netsecurity.about.com/cs/firewallbooks/a/aa050804.htm
[41]. Chesla, A. (2011). Active Perimeter Network Security. Retrieved from www.outpost24.com/files/024_TKK_Network_Study.pdf
[42]. VERIS Community. (2013). Retrieved from www.veriscommunity.net/doku.php?id=enumerations, 30/1/13
[43]. Microsoft. (2000). Networking Essentials Plus. Redmond, Washington: Microsoft Press
[44]. Wikipedia. (2013). Ethics. Retrieved from: http://en.wikipedia.org/wiki/Ethics
[45]. Hinman, L. M. (1997). *Ethics: A Pluralistic Approach to Moral Theory*. 2nd Ed. Forth Worth, Texas: Harcourt, Brace
[46]. ISWorld (2000). Ethics. Retrieved from www.cityu.edu.hk/is/ethics/ethics.htm
[47]. Sahakian, W. S. & Sahakian, M. L. (1993). *Ideas of the Great Philosophers*. London: Barnes & Noble
[48]. Adventist .org, (2012) Not Your average Novel. Retrieved from: http://www.adventist.org/spirituality/bible-study/
[49]. Adebayo, A. O. (2014). Ethics towards Secure Computing Environment. Researchjournali's Journal of Computer Science, Vol. 1, No. 2, pp 1-7
[50]. Dimensional Research. (2012). The Impact of Mobile Devices on Information Security: A Survey of IT Professionals. Retrieved from www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
[51]. European Digital Rights. (2013). An Introduction to Data Protection. The EDRi papers, Issue 06. Retrieved from www.edri.org/files/paper06_datap.pdf
[52]. Data-PASS (2011). Data Security Standards: Integrity and Availability - Introduction. Retrieved from http://www.data-pass.org/sites/default/files/DataSecurity.pdf