Journal of Computer Science

Original Research Paper

Assessing Information Security Vulnerabilities and Threats to Implementing Security Mechanism and Security Policy Audit

Mohammed A.M. Afifi

School of Information Technology, Skyline University College, Sharjah, UAE

Article history
Received: 29-01-2020
Revised: 12-03-2020
Accepted: 19-03-2020

Email:
mohammed.afifi@skylineuniversity.ac.ae

Abstract: In spite of the massive investment of money, time and efforts an organization devotes to growth and enhancement with continuous improvements of a sound information security strategy, the human factor is ultimately and eventually the one behind the keyboard. As a result, human beings remain the most vulnerable and weakest entity in the information security chain. A negligent and irresponsible in-house employee can be a threat even to the most breath-tight secure environment, an organization built to keep intruders away from unauthorized access. Information security is considered to be one of the most necessary and crucial issues of the field, with the rapid changes in the information technology that takes place every day and with the business models chasing it and trying to catch up, recently and for a while, it has become one of the most interesting fields to technology and business communities.

Keywords: Information Security, Network Security, Information Security Policy, Information Security Audits, Computer Security Audit

Introduction

Eventually, moving from the Personal Computing era to the necessity of having computer networks all around where the daily life cannot be carried on without having the connectivity in most if not all the time. Corporations in different sizes, large or small, look to the Internet as an essential component for conducting business. Internet explosion praised for evolution of better ways of conducting business, is at the same time denounce network security vulnerabilities. Computer systems and information security must be controlled and monitored, starting with security policy. The best security policy is not of value if it is not practically applied and it should clearly define the tools and methodology that will be employed to monitor all the network generally accessible resources to make sure that the policy rules are being followed. The security policy should include fairly and clearly outline the types of corrective actions to be enforced on the policy violators. Auditing, Monitoring and Enforcement of a well-designed and clearly-stated security policy will positively contribute to controlling any unlawful access to the network. While there is no such thing as absolute network security, there are still different ways to focus on security by constantly monitoring the network behavior and trying to prevent any unauthorized access –with good tools and skills; capabilities of the network administrators, developers and end-users that can constantly audit the computer network for vulnerabilities.

As there are many initial vulnerabilities and potential threats where attacks are becoming the headlines of our daily news, information security specialists are struggling to keep computer networks safe and secure from such attacks. The crucial and challenging mission of network administrators and security experts trying to control and prevent any unlawful entries and attacks equipped with the finest tools available. However, still getting attacked.

In the literal sense of the meaning, there is no absolute, total and an all-round computer security that does exist. Post facto computer security is a bad dream of every security specialist and there is nothing like a completely secured system. In continuous work, there are many great efforts contributing to the security measures raising the stakes to make the information security harder and harder target for intruders. With the adequate implementation of security measures, the chances of being attacked have decreased significantly.

In the past times, little more than two decades, information security was not a major issue, but later on, it has become the focus and the center of the computer networks. The information security intersects with many other disciplines, including but not limited to network system operations and administration and computer programming. Few organizations would

justify the needs and the additional expenses of recruiting an information security professional and yet, most of these organizations would be affected by the most casual penetration (Suduc *et al*., 2010).

This paper is addressing the security issues such as vulnerabilities and threats to magnify the view and contribute to taking preventive actions to the information security potential attacks, then audit the procedures to come up with a reasonably safe and sound security policy that helps in the everlasting quest to secure computers and information from harmful attacks. In addition, it will enlighten the administrators and the users to be aware and closer to remaining secure for the obvious vulnerabilities and the well-known attacks.

Security Policy Editing

Security policy should be designed and reviewed to be clear, concise, complete and accessible to all the users and groups. Once designed and reviewed, it must be followed with a thorough auditing procedure of the policy document; otherwise, there is no point in creating such a policy. It might seem normal, but the only to have a secure network infrastructure is through effective security monitoring. At this point, it is very important to state the stakeholders clearly and who is the directly responsible individual or group for the write-up of the policy and who will be a responsible entity for the continuous enforcement of such a policy.

The security policy must have signatures from all the stakeholders such as Division Managers, Technical Officers, Legal Counsel and of course, the writers of the policy, making sure to mark the date of all signatures.

The security policy is an organization's master document to reflect the vision, mission and the only ultimate source that steers and informs all the stakeholders of what you are protecting and how you decide to protect it. If an organization outsources or hires a consultant to draft the network security policy, this responsibility falls on the shoulders of network administrator. The network policy details can be accessed from several online resources. These online resources include:

- The Internet Engineering Task Force (IETF) Site Security Handbook (RFC 1244 obsoleted by RFC 2194). This handbook offers a comprehensive guide and information regarding security policies and the development procedure (IETF, 1997)
- Purdue University's COAST project provides policy security experts with sample security policies for reference. Samples can be checked at ftp://coast.cs.purdue.edu/pub/doc/policy (Purdue, 2012)
- There are many other good web sites with general security policy information that can be of great help to design and start the write-ups that leads to a good security policy.

If one did not have a security policy at all and just about to start writing a new one, this paper proposes some certain guidelines that have to be followed, especially when it comes to the essential components of information security policy as follows:

Version

The security policy's version number, data and owners should be clearly registered and stated at the beginning of the document to keep track of the changes and to make the amendments and updates of the policy easy to track and to know the origin of everything that the policy includes.

Introduction

This part should have a brief history of the company, its activities, purpose, vision and mission. The introduction should include all the references related to its information system and all service providers. On the top of that are; Internet Service Providers (ISP) and security solutions such as firewalls. Also, the infrastructure provider information blueprint along with the equipment provides - any other company or individuals involved with the network or system setups.

Network Layout Diagram

It should clearly show all the building blocks of the interior and exterior components. The diagram should illustrate the different groups and their blocks, their users' terminals and the clear borders with either their neighbors or the borders with the main network blocks. The diagram should also illustrate how the internal network gateway connects to the ISP's edge router. The network diagram should show the physical connections between the terminals and routers along with the connection to the servers for easy operations of troubleshooting and helping to solve day-to-day problems that occurs on the network.

Physical Security

The architectural design of the facility where the different points of entrances and exits along with any other access points for the whole building area. It should also define the areas of off-limit access for the general system users. The roles and entities of the users who will be allowed to access these areas and how secure they will gain access to it. This should secure access to the complete area, including the physical assets, including the server platforms, control panel configuration terminal, power lines, UPS systems or standby generators and console accessibility. The physical security should define the various types of access control and how they access data centers, network racks and closets areas. As a network administrator, it is vital to regulate access areas to deter any unauthorized, inexperienced and unconcerned employees from accessing the data centers or other sensitive company

resources. Lack of proper access control mechanisms can lead to damage or loss of resources.

Remote Access

It must be clearly stated in the policy whether there will be a need or necessity for allowing remote access. This part of the policy should answer a number of questions that will shape the remote access policy and if it is going to be allowed, some of these questions are: What will be the special restrictions access for remote users? Will it be allowed via normal dial-up, leased line, or public connection dedicated VPN? Who will have access remotely? How secure the connection will be? Are there any encryption techniques will be used and who will be having authorized access to the Intranet using remote access clients through the Internet?

Firewall Configuration

It is a very important component in the quest of securing the network. A firewall component can either be logical or physical; it prevents unauthorized access to network systems. The policy should include the details of the firewall detailed configuration, settings and references of all perimeters. It should also include the defense devices settings, access control rules, logging and log files facilities, different authorization and authentication methods.

Users Accounts Policy

By creating user accounts and creating groups, it will be much easier to maintain the permission and denials for accessing data controlling who accesses what. The user accounts policy should include the choice of usernames, password expiration periods and what are the termination rules, storage space quotas and allocation, process resources.

Data Usage and Access Policy

The data usage and user access along with the file permissions are collectively a very serious issue that should be cleared and extended to cover all the different types server permissions, like user access. There should be a clear distinction between the reading, writing and executing permissions of a certain file. This section of the policy should have the initial access permissions and privileges.

Monitoring Policy

A network monitoring system has the ability to detect and report failures or low performance of the system or any other devices as it happens. This section refers to the network traffic monitoring to know, review and analyze network traffic for any abnormality that may interfere with network performance and availability of network resources. Network monitoring is very important and absolutely necessary to secure the network and it may require more than one expert to be in duty around the clock to be able to detect any abnormal activities as it happens, to stop any damage to be caused and take a preventive action to secure the network saving a lot of money and eliminate many problems.

Auditing Policy

It usually refers to the Network Security Audit Policy process that involves the investigation of the company's security policy and the assets on the network to identify any deficiencies that put the company's system and data at risk of any type of security breach, where assets are anything that has value to the organization (ISO IEC, 2005; 2013). Policy Audit procedure help in effective determination of security to solving essential network security concerns.

What Else?

Periodical Policy Editing Review and Security Auditing is very crucial and important as the dramatic changes in the technology takes place every day, security policy cannot be a static document but very dynamic that needs to be visited and modified or even updated with the latest technologies available at the current time. As company's network infrastructure transforms, data is definitely growing every day, there grows the need that makes it necessary and mandatory to make sure that a periodical revision is conducted to the security policy parallel to the growth making sure that it is updated to reflect the needs of its purpose.

Initially, with the briefly mentioned guidelines to start the first security policy of any institution, all these sections should be included in the document so that the policy will be a long lasting document including but not limited to all the sensitive criteria covering the different policy aspects. It will need to be visited from time to time as the changes occur and the necessity is required.

Information Security Audits

Information security audit is used to evaluate effectiveness of deployed security measures and policies. The audit process is very crucial and thorough to fully understand how far the institution is secure and protected against security breaches and threats. Network systems security audit is considered to be the most important part of the whole audit process, it should be taken care of periodically to ensure the flawless and smooth operation of the entire system. The information security audit is subject to having a static and dynamic aspects to be taken in consideration, the static information such as network addresses, protocols, password rules, firewall settings and user accounts. On the other hand, the dynamic information such as data files creation,

modifications, transfer and exchange, access to databases, log files and activities.

System Architecture Audit

It usually refers to the infrastructure and the foundation that supports the information system. It consists of the physical and virtual resources that supports the smooth operation of the entire system including the system location, hardware assets, processes and the interconnection between all of them. System architecture audit process aims evaluating security measures deployed and its users, also it addresses the efficiency and robustness of the collection of hardware assets such as servers, storage and connectivity among them all.

System Integration Audit

It is to make sure of providing the right equipment and components comprising the information system hardware and putting all together in action for examining the operation of these components interaction with each other to make sure that they perform correctly and efficiently once in real operation. Now-a-days with the variety of different technologies available, one must find it a little bit difficult to make a choice among good brands. The better the choice at the very early stages is definitely the better the results and performance will be in the future until the hardware component or even the system will be commissioned. The system integration audit extremely important especially at the early stages, as it ensures the quality of system integration and how reliable it can be for processing information.

Operating System Audit

It all starts with the choice of the operating system that you intend to install and use, how transparent it can be when you start the platform-level auditing to make sure of any existing vulnerabilities and how will you fix them. At this stage, one should understand the power of open source operating systems Vs any other operating system type. The nature of the open source operating systems allows the administrators, developers and even users to constantly audit and detect flaws and vulnerabilities. Not to forget the privilege and ability to look "under the hood" that makes the open source operating systems one of the most recommended choices and the main platform for environments where security is important. Another crucial aspect is End-User License Agreement (EULA) that has to be studies carefully and thoroughly to find the gaps and potential security breaches. Then at last, look into how many viruses are effective and can harm the operating system (Afifi and Nehal, 2017).

Link Level Security Audit

It is to make sure that the messages are protected while being exchanged between queue managers. Link level security Audit is crucial to enhance confidentiality during message transmission; considering that every connection is insecure for interception or eavesdropping; so at each end, messages need to be authenticating its partner that starts while establishing the communications pathway and right before messages being transferred. Confidentiality can be achieved by ensuring that the sender encrypts the message before sending (IBM, 2020).

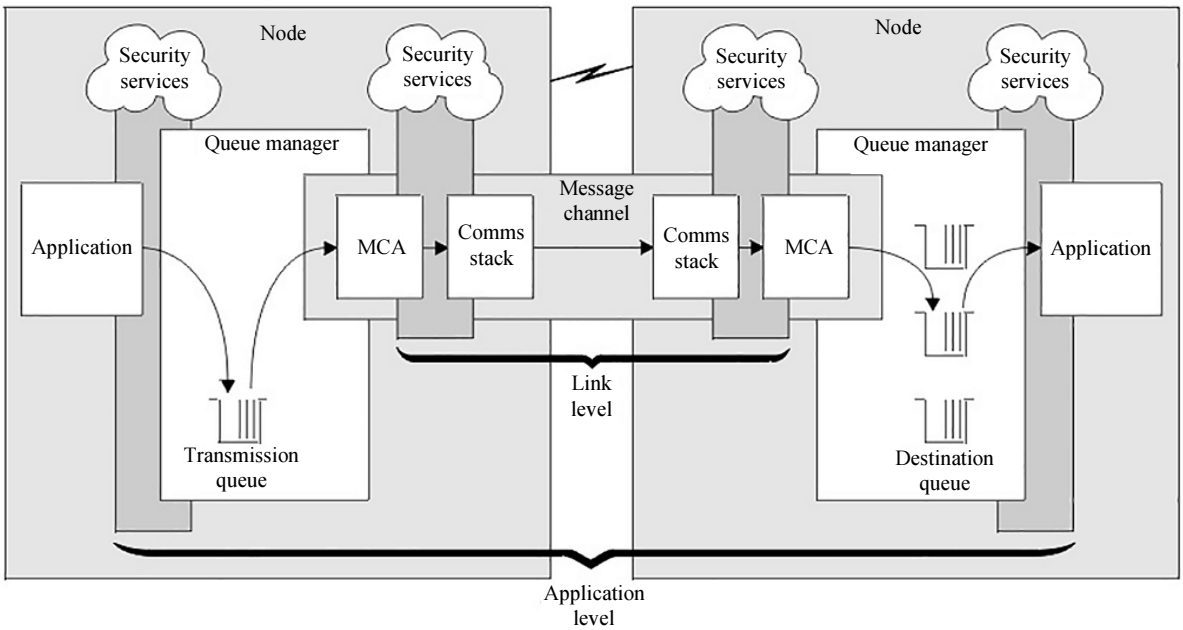

Fig. 1: Link-level security and application level security

Application Software Audit

It is to make sure that the application software is specifically, thoroughly and exhaustively tested and audited dependently and the level of control is up to what is expected to be delivered to the degree of challenges and risks involved in the incorrect or unauthorized processing of data. As shown in Fig. 1, The application software audit should deliver a detailed evaluation of the application code for many aspects, starting with network infrastructure and the possible vulnerabilities on connectivity, non-secure coding practices that may result programming bugs or runtime errors and the natural protection against all widely known attack techniques, finally the level of data encryption if needed at this level. The audit process should involve; both automated and manual penetration tests and attack-related code detection. Application level security is vital for security services invoked at the interface between application and queue manager. As shown in Fig. 1, application level security can also be referred to as end-to-end or message security (IBM, 2020).

Assessing Vulnerabilities

The information security has always been and always will be about the CIA triad that is considered as the principle and core requirements of information security for a smooth and safe utilization of storing, accessing and moving data around the same network or even to another network, where anything else comes next. CIA stands for Confidentiality, Integrity and Availability where these are the main three basic and initial objectives of having information security. Confidentiality reflects the necessity to keep the information private, to keep data concealed from unauthorized users. It includes restriction of authorized access. The opposite of confidentiality is disclosure. Data integrity involves trust that the transmitted information has not been manipulated. Availability means making data accessible to those authorized personnel when needed. Often, this implies that the resources are availed at a higher rate, over pacing normal functionalities of the wider system. The opposite of availability is basically interruption or the denial of the service (Carr *et al*., 2009).

In the early stages, all the computer networks are basically designed and interconnected to other networks with security vulnerabilities. Initially, to start the foundation and implementation of information security, is to evade and eliminate the obvious well-known vulnerabilities. Vulnerability refers to a system that is susceptible to access by unauthorized people (Kizza, 2009). A network can be vulnerable if there are no set or enough security mechanisms and policies to secure the network.

There are many aspects that information security vulnerabilities have been addressed from; as they may come from hardware and/or software security flaws, where they have not been covered in the policies and procedures stated for the network. The classification and sources of vulnerabilities developed by Kizza (2009) includes; protection barriers and vulnerability presence, among others (Weber *et al*., 2005). The possibility to study the whole list in one visit is very difficult, hence it should be a continuous improvement to keep addressing the major and obvious sources of vulnerabilities while pursuing and establishing a standard information security policy.

To start with, several vulnerabilities occur by default once the interconnection between computers in a network has been established as a result of providing the ability to communicate among these devices. These cannot be considered as a design flaws but its basic existence is related to the networking concept existence. Hardware systems have less design flaws, after all, it was designed to execute specific instructions to perform a specific task. However, the software installed in a hardware can have vulnerabilities that might affect the hardware. The software development process might produce security flaws due to many reasons depending on the developers' ability to produce quality software. For example, programmers' memory lapses, implementation of weak algorithms, failure to conduct security testing, complacency, or installation of backdoors by the programmers (Dowd *et al*., 2006).

Another important factor of the increased vulnerabilities is the lack of knowledge and literature for the computer users that are not even aware about security. Users that leave their computers and accounts logged in and never log out, people that save their passwords and have them managed by a computer program, employees that record their login credentials on a piece of paper and stick on the computer screen for quick reference, people that allow strangers to use their computers, people that do not care about their personal information and sensitive data and the list goes on.

The lack of trustworthy software sources sums up that for more than two decades we started to find about big or even giant software companies involved and accused in many security and spying issues, scandals having access to their customers' computers without permissions, copying data, spying on usage history and invading their privacy. These companies have built different means of security breaches in their products, so that they can access their customers' computers. Ironically, when discovered and exposed, they basically admit it or announce that was a programming bug (Choi *et al*., 2008), then that will be followed with the famous multiple fixes and batches that a user will never know if it was really fixed or not.

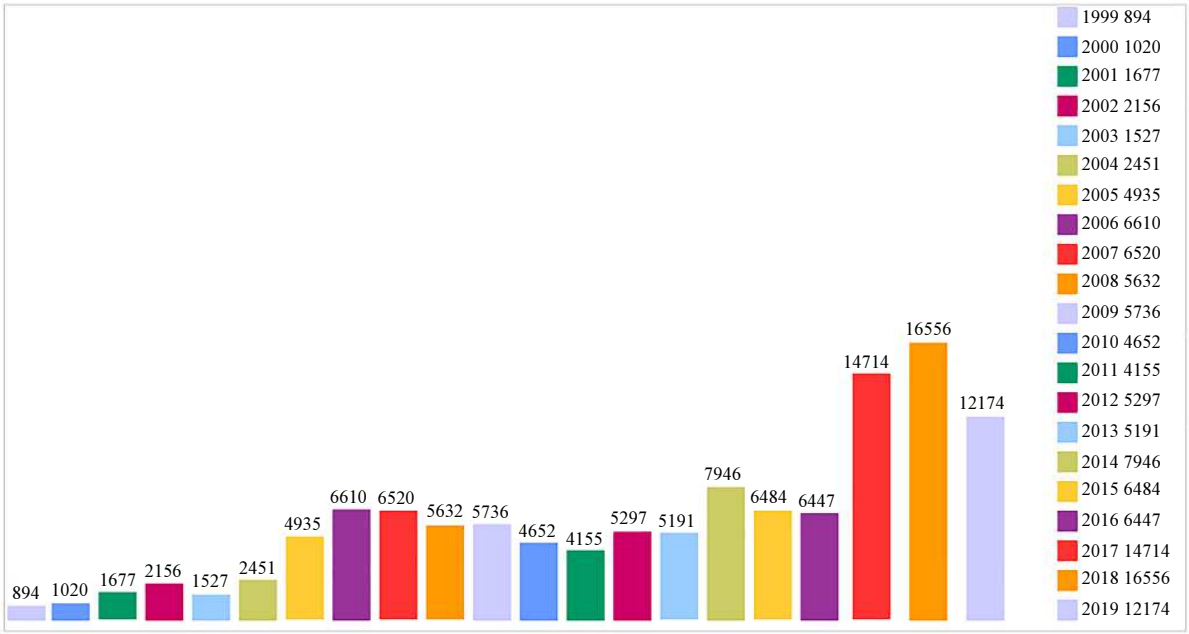

Fig. 2: CVE vulnerabilities by year

Other vulnerabilities are existing because of the weak or loose security management. Where the most likely scenario is that the computers have been connected and the users started to work and use the shared resources with no concept of security essentials or policy of who does what and how! The non-procedural implementation of network exposes it to vulnerabilities; vulnerabilities that will later require to be fixed. Such a network is more like a public park that does not require an entry pass, where everyone can simply get in and out so easily anytime, all the time.

Finally, the most-likely and everlasting source of vulnerabilities that cannot be completely controlled or secured is the internet with all its available services that one can use including the web-applications. As stated by Common Vulnerabilities and Exposures (CVE, 2019); vulnerabilities reported has been on rise for the last 3 years, as shown in Fig. 2. Software is the richest host of vulnerabilities, whether it is the operating system or the application programs, both may have very crucial security breaches, opened ports vulnerabilities, web application bugs, public network connection error and client-server network protocols issues.

Assessing Threats

One cannot deny that, no matter how strong and secure we can be, all of us as individuals, companies and organizations are susceptible to information security threats as we are potentially vulnerable one way or another (somehow). Clearly, the information security awareness and education are our first line of defense besides the technical methods and strategies of protecting personal and corporate information in our possession.

For faster information exchange between business entities comes the necessity of connectivity over telecommunication technologies. Successful business operations are really difficult or nearly impossible to be achieved without information technology connectivity. As a result, the information system becomes exposed to security threats. To assess these threats and know how dangerous they can be? First and foremost, an individual or organization should be able to identify how many people out there are really going to attempt to break in to have access to their information systems. Knowing the possible dangers by studying the potential threats and their impact on the security CIA triad is relatively a good and clean start to assess the information security status.

Internal and external threats are two sets of Information security threats. In my opinion, the internal threats within an organization is much more important and severe than the external ones, described as follows:

Internal Threats

They occur when someone has an authorized access to the information system. It can be a result of an intentional or accidental act of an authorized person. These internal threats include the physical access to the facility and being near by the information system having an easy access to computers and servers, that can lead to a direct exposure to vandalism, which is a deliberate willful damage or destruction of the information system, no matter how small is the damage size appears to be, even minor damage can have a significant impact on the

information system and can cost a fortune. Physical access can lead to a direct information theft, where data can be copied on external storage of a very small compact physical size as we have seen in many cases (Snowden, google and others). Also it facilitates the implanting of any type of malicious software (malware) that causes real and severe damage to the information system either immediately or on the long run. Malware includes programs like Viruses and Worms. Taking photos of the physical equipment and hardware devices being used makes it easy to mimic and work on similar equipment to find vulnerabilities. Human factor such as errors, accidental misuse, bad habits and attitude, lack of responsibility, or lack of experience can lead to a greater impact on the information security.

External Threats

These threats involve external unauthorized access to information system, this is considered one of the most threat. Now, if that unauthorized person manages to alter or modify the data, the threat compromises the integrity of data and if manages to delete data form the information system, where no up-to-date backup is made, the threat compromises the availability of data. The situation is worse if the unauthorized access is by someone with ability to cause damage. Natural disasters and force majeure is also considered is an external threat such as fires, hurricanes, twisters, floods and earthquakes that physically damage the information system (Jouini *et al*., 2014).

Security Mechanism Implementation

Individuals and organizations having a broad range of information assets that might vary from the simplest PDA device to the most sophisticated server installed in a data center, both are considered of a value based on the information that either holds. Hence, every device is considered to be a valuable asset to an organization in terms of the data it holds and processes (ISO IEC, 2005; 2013).

In the past, information security was a purview of few individuals, but nowadays it is a responsibility of every employee of an organization (Kanatov *et al*., 2014). Therefore, everyone has an obligation to security self-awareness and to ensure availability of a secure environment (Ku *et al*., 2009). With the extremely rapid evolution of the technology, many businesses are not –if not all- capable of growing at the same pace adapting the new technologies as it happens, so that in many times, the gap between technology and business will exist and remain there as that exactly what makes information security vulnerabilities being found.

The best way to initiate the information security implementation mechanism process is to identify the system valuable areas carefully, assessing the size and level of loss if the security were breached and how long will it take to recover. Afterward, generate questionnaires (Richardson and Director, 2008), check lists and steps in the quest of forming the security mechanism full picture and building the HOW TOs strategies. The questionnaires should be simply designed in the form of Yes-No questions and answers (Suduc *et al*., 2010), where no deeply technical questions are asked keeping in mind that most of the employees conducting the questionnaires might not be information security literate people, making sure that mission-critical data is not being available to all employees, especially the naïve users. Also making sure to set the permissions and denials of data access with the right level of read/write/execute to each and every group or individual. ISO 17799 check list (SANS, 2003), provides ISO standard security testing checklist. Audit Tool (ISO IEC, 2005; 2013), offers an extensive variety of audit questions relating to advisable security practices, along with possible actions in cases where dissenting answers are provided. Though these tools are dependent on additional security measurements, they are still very useful (Kanatov *et al*., 2014).

Knowledge base is another effectual approach for audit process. It avails necessary information for Chief Information Security Officers (CISOs) to make precise information security policy decisions. Basic knowledge base components are: Assets and vulnerabilities (Stepanova *et al*., 2009).

All the steps together will form the security mechanism implementation where every step is going to be stated as a reference for both the vulnerability and its protection standard, as well as a comparison to the cross-references with the in house guidelines. This security mechanism will provide organizational guidelines, standards and component analysis that leads to issuance of the recommendations. Consequently, the supposed meta-mode of the security standard recommendations could be created (Atymtayeva *et al*., 2012; Kozhakhmet *et al*., 2012; Atymtayeva *et al*., 2011).

Security Policy Audit

The evolution of information technology and telecommunications services in the last two decades or more, it has become compulsory for every organization regardless the nature of activities or services that they offer to use information technology, as the computer usage invaded all the fields and made the job easy for the various business models. Ever since, the need of sound information security measures has become compulsory as well. The news of organizations being attacked every day is a solid evidence for the necessity to address the issue from different perspectives. Security policy auditing has appeared to handle the majority of such events.

The content of the policy should illustrate the brevity and clarity of the content presented, especially for the

asset descriptions which are basically limited to removable media. The source of the document should signify the criteria in which the guidelines are taken. Two sources are depicted here; ISO 27002 (ISO IEC, 2005; 2013) and the UCISA Information Security Toolkit (UCISA, 2005), along with the related subclasses that define each criteria's structure.

The information security audit process should lead to produce an information security management document (manual) that will explain the details of the following information:

1. Document Version
2. Introduction
3. Network Layout Diagram
4. Physical Assets Security
5. Remote Access Policy
6. Firewall Configuration
7. Users Accounts Policy
8. Data Usage and Access Policy
9. Monitoring Policy
10. Auditing Policy
11. Review and Updates

A security policy is an organization's unique written document that describes basic best practices when dealing with information systems (Afifi, 2018). A security policy should classify all of an organization's resources, as well as all the possible and potential threats to those resources.

Conclusion

Regardless of how much resources an organization devotes to development of an enhanced security strategy for information systems, human users and operators are eventually at the control seat and they are often the most error-prone participant in the information security echo-system. The most undisputed airtight of defense rules will be surrendered and absolutely useless by an insider with a little tiny flash drive that can copy gigabytes of data faster than the time taken to drink a cup of coffee. Strong password security policies are useless if users note down their credentials on paper and leave it unsecured. Other users are habitual to storing their passwords in browsers, leaving their computers logged in and unsupervised, saving passwords in unencrypted documents and the list goes on. All these bad practices would never reward back the money, time and efforts being put to build a tight information security. With all the various security techniques and strategies that can be constructed, a well-designed security policy should be implemented and strictly deployed with the best standards and practices that specifies procedures and how it should be followed to achieve the maximum and adequate secured environment. Also visiting the security policies and procedures from time to time, even if things are fine, to find gaps and the narrow margins of security breaches that may arise in times.

Finally, planning security is very important and crucial starting all the way from the information security literacy and the proper education for the employees to be aware of the threats and the type of attacks they could be experiencing from time to time and how to avoid being vulnerable. Also the physical facility security is very important along with the choice of the hardware equipment. All of this should be sealed by the security policies and procedures which is definitely essential to complete the defense line for a sound and safe information security environment.

References

Afifi, M.A., 2018. Information security vulnerabilities analysis for having computer system security audit. Proceedings of the International Conference on Computer Auditing, (CCA' 18).

Afifi, M.A. and K. Nehal, 2017. Linux platforms as a secure desktop solution. Int. J. Comput. Applic., 164: 9-11. DOI: 10.5120/ijca2017913597

Atymtayeva, L., A. Akzhalova, K. Kozhakhmet and L. Naizabayeva, 2011. Development of intelligent systems for information security auditing and management: Review and assumptions analysis. Proceedings of the 5th International Conference on Application of Information and Communication Technologies, Oct. 12-14, IEEE Xplore Press, Baku, Azerbaijan, pp: 1-5. DOI: 10.1109/ICAICT.2011.6110898

Atymtayeva, L.B., G.K. Bortsova, A. Inoue and K.T. Kozhakhmet, 2012. Methodology and ontology of expert system for information security audit. Proceedings of the 6th International Conference on Soft Computing and Intelligent Systems and 13th International Symposium on Advanced Intelligence Systems, Nov. 20-24, IEEE Xplore Press, Kobe, Japan, pp: 238-243. DOI: 10.1109/SCIS-ISIS.2012.6505287

Carr, H.H., C.A. Snyder and B.N. Bailey, 2009. The Management of Network Security. 1st Edn., Pearson Education India, Upper Saddle River, N.J., ISBN-10: 0132234378, pp: 380.

Choi, M.K., R.J. Robles, C.H. Hong and T.H. Kim, 2008. Wireless network security: Vulnerabilities, threats and countermeasures. Int. J. Multimedia Ubiquitous Eng., 3: 77-86.

CVE, 2019. Common Vulnerabilities and Exposures (CVE).

Dowd, M., J. McDonald and J. Schuh, 2006. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. 1st Edn., Pearson Education, ISBN-10: 0132701936, pp: 1200.

IBM, 2020. IBM Knowledge Center, Comparing Link and Application Level Security.

SANS, 2003. Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003 BS 7799.2:2002 (2003). SANS.

ISO IEC, 2005. ISO IEC 27002 2005 Information Security Audit Tool.

ISO IEC, 2003. ISO/IEC 27002:2013 [ISO/IEC 27002:2013] Information technology — Security techniques— Code of practice for information security controls.

Jouini, M., L.B.A. Rabai and A.B. Aissa, 2014. Classification of security threats in information systems. Proc. Comput. Sci., 32: 489-496. DOI: 10.1016/j.procs.2014.05.452

Kanatov, M., L. Atymtayeva and B. Yagaliyeva, 2014. Expert systems for information security management and audit. Implementation phase issues. Proceedings of the Joint 7th International Conference on Soft Computing and Intelligent Systems and 15th International Symposium on Advanced Intelligent Systems, Dec. 3-6, IEEE Xplore Press, Kitakyushu, Japan, pp: 896-900. DOI: 10.1109/SCIS-ISIS.2014.7044702

Kizza, J.M., 2009. Guide to Computer Network Security. 1st Edn., Springer, London, ISBN-10: 184800916X, pp: 476.

Kozhakhmet, K., G. Bortsova, A. Inoue and L. Atymtayeva, 2012. Expert system for Security Audit using fuzzy logic. Proceedings of the Midwest Artificial Intelligence and Cognitive Science Conference, (CSC' 12), pp: 146-146.

Ku, C.Y., Y.W. Chang and D.C. Yen, 2009. National information security policy and its implementation: A case study in Taiwan. Telecommun. Policy, 33: 371-384. DOI: 10.1016/j.telpol.2009.03.002

Purdue, 2012. Purdue University's COAST Project offers a number of sample, real-life security policies.

Richardson, R. and C.S.I. Director, 2008. CSI computer crime and security survey. Computer Security Institute.

Stepanova, D., S.E. Parkin and A.P. van Moorsel, 2009. A Knowledge Base for Justified Information Security Decision-making. Proceedings of the 4th International Conference on Software and Data Technologies, Jul. 26-29, Sofia, Bulgaria, pp: 326-331.

Suduc, A.M., M. Bîzoi and F.G. Filip, 2010. Audit for information systems security. Inform. Econom., 14: 43-48.

IETF, 1997. The Internet Engineering Task Force's (IETF) site security handbook (RFC 1244).

UCISA, 2005. Universities and Colleges Information Security Association (UCISA). UCISA Information Security Toolkit.

Weber, S., P.A. Karger and A. Paradkar, 2005. A software flaw taxonomy: aiming tools at security. ACM SIGSOFT Software Eng. Notes, 30: 1-7. DOI: 10.1145/1083200.1083209