Journal of Advanced College of Engineering and Management, Vol. 2, 2016

CONCERNS ON INFORMATION SYSTEM AND SECURITY AUDIT

Subarna Shakya[1] Abhijit Gupta[2]

[1]Department of Electronics and Computer Engineering, Institute of Engineering, Tribhuvan University, Nepal

Email Address: drss@ioe.edu.np

[2]Singhania University, Rajasthan, India

Abstract

Successful Information and communication technology (ICT) can cause rapid development in administrative processes. ICT strategies and ICT plans should be evaluated to align with organization visions and missions in order to achieve effective use of ICT in their organizations [1]. Efficient Software and Hardware together play a vital role giving relevant information which helps improving ways we do business, learn, communicate, entertain and work. This exposes to an environment with significant risks which are vulnerable to inside or outside attacks [2,3]. Security is a degree of protection or resistance from harm. Security can also be defined as a layer created to separate assets from threats [4]. In order to understand clearly about security, it is very important to understand important terminologies [5]. This research paper talks about important terminologies, concerns and challenges on Information System and Security Audit. This research seeks explanation from the observed phenomena, problems or behavior and thus exploratory research is used. The outcome of this research is an overview of different security concerns that must be sincerely addressed in any Information System and Security Audit.

Keywords: *information system audit; security audit; cyber threats and attacks; information system; information security;*

1. Introduction

There are three major sections that deal with security controls in any organizations and they are Management Controls, Operation Controls and Technical Controls. Managerial Controls are such techniques and concerns that deal with managerial security and focus on management of risk and computer security of the program within the organization. Operation Controls are such techniques and concerns that deal with security at operation level and focus on controls that are implemented and executed by people and often rely on management and technical controls. Technical Controls are such techniques and concerns that deal with technical security and focus on security controls that the computer system executes [6].

2. Computer Security

Computer security is the automation of IS to achieve the goal of preserving confidentiality, integrity and availability of IS resources such as information, data, firmware, software, hardware and support systems. Following are elements of computer security:

- The mission of organization should be supported.
- Sound Management should be an integral element.
- It should be cost effective.
- The responsibilities and accountabilities for computer security should be made explicit.
- It is responsibility of System owners even outside their own organizations.
- It requires integrated and comprehensive approach.
- It should be periodically reassessed.
- It is constrained by societal factor.

Followings are some of the security terms:

Integrity

Accurate, timely, consistent and complete information has integrity which is difficult for computer to protect. Integrity is narrowly discussed in two facets: data integrity and system integrity. "Data integrity is a requirement that information and programs are changed only in a specified and authorized manner [6]." System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system [7]."

Availability

A "requirement intended to assure that systems work promptly and service is not denied to authorized users [6]."

Confidentiality

Confidentiality is the maintaining of privacy or not disclosing of information to unauthorized person.

Accountability

The accountability is the explicit responsibility of users, providers and owners [8].

Awareness

Users, Providers and owners must be able to perceive, feel and be conscious to gain appropriate knowledge to maintain security of their information system [8].

Ethics

The IS and security of information should be used in a way where the legitimate interests and rights of others are respected.

Table 1 shows eight IT control requirements and possible security control tools.

Table 1 IT Control Requirements [9]

Requirement	Security Control
Non-Interference	User ID/Password, Firewall, Nondisclosure of User Access
Authentication	User ID/ Password, Token, Biometrics Device, PKI Credentials
Authorization	Access control list, attribute certification
Confidentiality	Encryption
Integrity	Message Authentication Code (MAC)/ Hash
Privacy	Policies and procedures, encryption, policy management tools.
Non-repudiation	Digital signature, time stamp
Availability	Redundancy, load balancing, policies and procedures, business continuity plan, alternate processing site.

3. Information Security

Information Security refers to the protection or safeguarding of any information from being breached against any unauthorized access and maintains integrity and confidentiality [5]. With growing dependency on the internet and email, security risks and breaches are also increasing drastically. In first six months of one year, there has been a report of 76,000 such breaches and for entire previous year there had been only 6,000 less than reported incidences [10].

Cyber threats and frauds are increasing day by day because of several reasons such as failure of internal control system and failure of organizations to update to new set of risk. Smart fraudsters, people that target weakness or holes in a system, also are a type of threats or attacks.

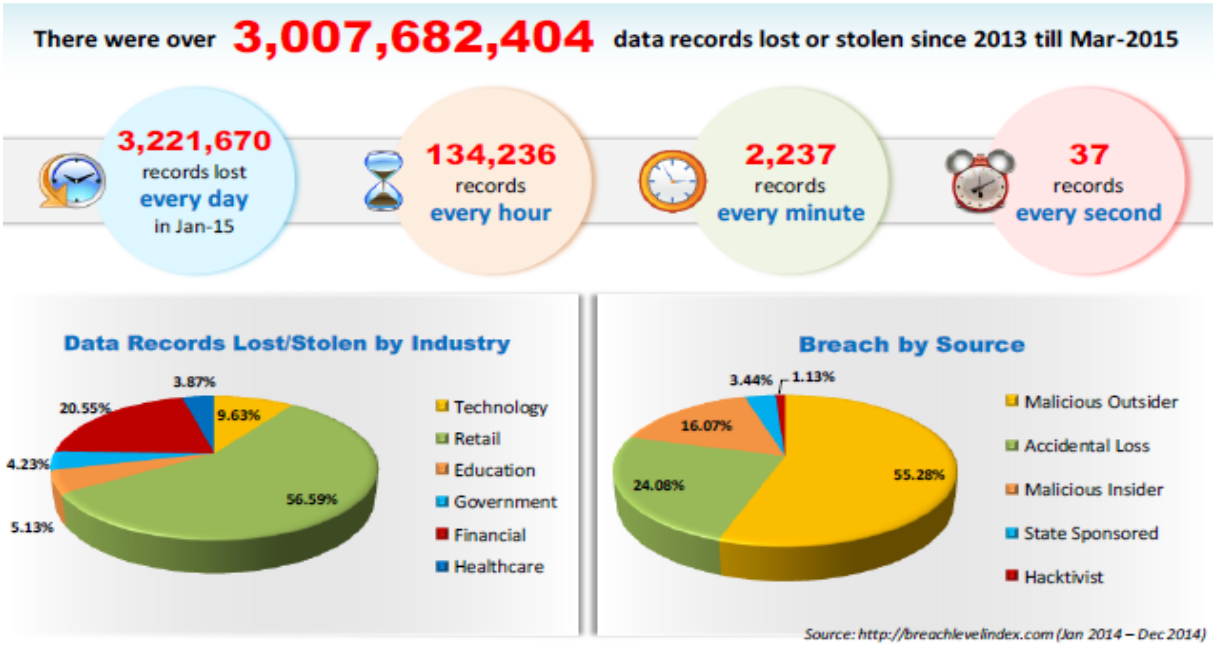

Fig 1 Data Records and Breaches

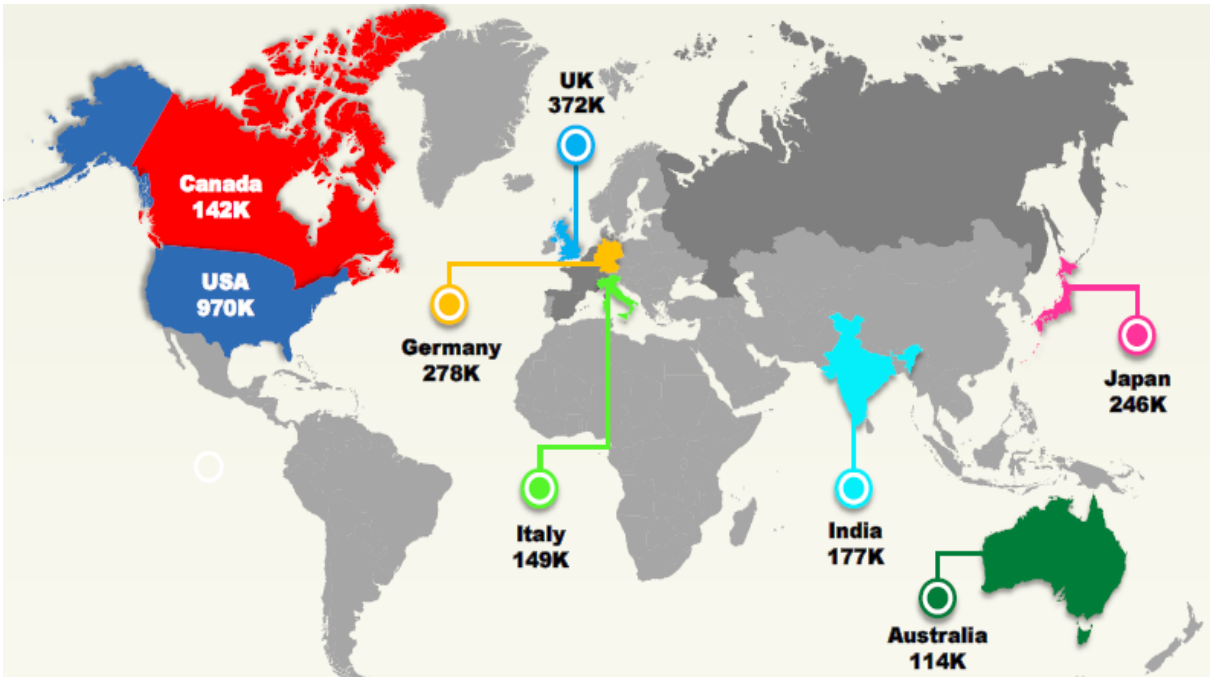

Fig 2 Financial Loss due to Trojans

A research shows that majority of data records lost or stolen by industry are for retail business, i.e. about 56.58%, as shown in Fig-1. Similarly, majority of breaches i.e. about 55.29% are through Malicious Outsider. According to the Symantec Survey 2014 report, 95% of the cases of infection, almost every type of financial institution from commercial bank to credit union, is targeted as shown in Fig-2. The rest 5% involved traditional online services like social media, ecommerce websites, web-mails, employment websites etc. Key finding of Symantec included the fact that the top 9 targeted Financial Institutions among 95% of the threats to financial institutions were targeted by more than 40% of all Trojans analyzed. "Focused Attack" and "Broader Strokes" were the two dominant strategies identified by Symantec in their reports [11].

The researcher has made a review on some common terms reflecting security, hacking, threats or cyber frauds [12].

SQL Injections

SQL injections refers to manipulation and execution of SQL queries through html forms or URLs where the attacker insert SQL meta-characters executed by the backend database thus providing and revealing or inserting or updating data in the database [13]. A research as shown in Fig-3 shows that SQL Injection was most prevalent vulnerability in 2012 [14].

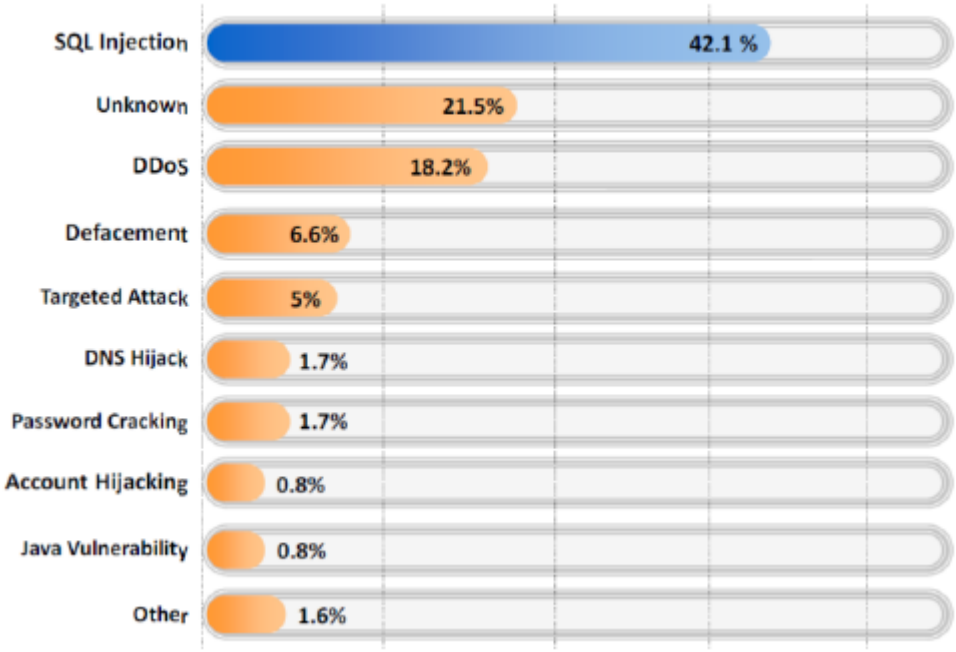

Fig 3 SQL Injection was most prevalent vulnerability in 2014

URL Manipulations

URL Manipulation is a way to access information through the vulnerabilities in the URL in an online system if the data is being sent and received using GET method. The application must validate the URL values with session token and must analyze the query string before pushing it to business logic layer [13].

Cross-Site Scripting Attack (XSS Attack)

Cross-Site Scripting Attack, also known as XSS attack is targeted to such vulnerabilities where input and output validations and file system permission has not been strictly and properly implemented. In such case, a user input can be manipulated and the result to the webpage can be printed out with user's original input thus revealing some information which was not meant to be revealed [13].

Session Hijacking

Session Hijacking refers to exploitation where a hacker takes over the session between two computer systems for further manipulations. The attacker steals a valid session ID which can be used to retrieve the data from the system [14].

DoS & DDoS

Denial of Service (DoS) Attack is an attack on a computer resource or network by flooding it with non-legitimate service request or traffic, thus preventing it to serve genuine requests. A Distributed Denial of Service (DDoS) Attack involves a multitude of a compromised system attacking a single target, thereby causing DoS for users of targeted system [14].

Virus/ Malicious Code

Virus is such malicious code or instructions written by a programmer with a bad intention to damage, destroy, degrade or affect the performance of the computer resource or information. Viruses are usually created for inflicting damages to competitor, financial benefit, research projects, play prank, vandalism, and cyber terrorism or distribute political messages.

Trojan

Trojan is a malicious code contained insider a harmless looking program or application to get control and cause damage to the victim's computer and data. Some popular Trojans and common ports used by them are as mentioned in the Table 2. Trojan is a name coined from a similar event inn ancient Greek Mythology, where, a gift of huge wooden horse by Greece to Troy in peace and cease war was left at the gate of Troy as they could not defeat the Troy's because of their fortified Walls. The gift actually had unknown presence of a troop of army inside responsible to open the gates of Troy to let the army of Greece invade at the late night.

Table 2 Trojans and Common Ports used by Trojan

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Trojan is a security breaking and harmful malicious code in disguise of a benign. Trojan gets activated upon certain predefined actions and can create a covert communication to steal sensitive data between victim's computer and attacker [11].

Phishing

Phishing is the act of trying to acquire user access or financial credentials such as credit card information or internet banking access.

Network Scanning

Network Scanning is the process of scanning and identifying active hosts on the network for purpose of getting information such as IP address, host etc which helps in planning future attacks.

Worms

Computer worms are malicious programs which can replicate and spread within a computer or network system consuming huge resources and thus making the performance of the computer or network system slower without any human consent or interaction. Typically, a worm does not involve in any data stealth activities [11].

Wrapper

A wrapper is a tool that binds Trojan executable with a clean and trustable looking application such as games or office applications.

Hacking

Hacking refers to exploiting system vulnerabilities and compromising security control to gain unauthorized or inappropriate access to the system resources. The person responsible for hacking is termed as hackers and there are mainly 8 classes of hackers such as

- Black Hats (resorting to malicious or destructive activities)
- White Hats (for defensive purpose)
- Gray Hats (offensive and defensive at different times)
- Suicide Hats (suicide attacks for a cause without worrying for consequences or jail)
- Script Kiddies (unskilled newbie hacker using tools of real hackers)
- Spy Hackers (employed by organization to gain competitors trade secrets)
- Cyber Terrorists (motivated by religious or political beliefs to create terror with large scale disruption)
- State Sponsored Hackers (employed by government to penetrate and gain secret information) [14]

4. Security Assessment

Security Assessment is must for every organization for the assurance of validity of data and resources on the network. Security assessment might include security audit, vulnerability assessments and penetration testing or ethical hacking.

Security Audit

Security Audit focusses primarily on people and processes used to design, manage, monitor and implement security on the network. Security Audit is a systematic, measurable technical assessment on how security policy in an organization has been employed and implemented. The auditor must align properly with ICT security policies of an organization for a successful security audit. IT

management usually initiates security audit and the security audit technical assessment can be done manually or automatically by using Table-3 steps:

Table 3 Security Audit Assessment [14]

Manual Assessment	Automatic Assessment
Interviewing the Staff	Generating Audit Reports
Reviewing Application and Operating Systems Access Controls	Monitoring and Reporting the changes in the files.
Analyzing Physical Access to the systems	

Vulnerability Assessment

Vulnerability assessment is done to assess vulnerability where threats from hackers, former employees, and internal employees can be determined. This assessment helps in figuring out the security weakness by scanning the network. Vulnerability Assessment can provide information for network segments for IP enabled devices; enumerate systems, operating systems and applications, common security mistakes such as weaker password, inappropriate file/folder permissions, default services and applications that might need to be uninstalled. A vulnerability assessment must assess various network or system components such as communication failure, e-commerce failure, loss of confidential information, public facing systems websites, email gateways, remote access platforms, mail, DNS, firewalls, passwords, FTP, IIS, web servers [14].

Penetration Testing

A penetration testing stimulates a process that intruders use to gain unauthorized access to an organization's network system and then compromise them. Penetration Testing is primarily used to assess the security model of entire network system and reveals potential consequences of a real hacker breaking into the network. Penetration Testing must be used in an organization

- To identify threats in organization
- To reduce an organization's expenditure on IT security and enhance Return On Security Investment (ROSI) by identify and remediating vulnerabilities or weakness.
- To provide assurance with comprehensive assessment of organization's security including policy, procedure, design and implementation.
- To gain and maintain certification to an industry regulation (BS7799, HIPAA etc)
- To adopt best practices in compliance to legal and industry regulations
- For testing ad validating the efficiency of security protections and controls
- To focus on high severity vulnerabilities and emphasize on application level security issues to development teams and management.
- To provide comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation.
- To evaluate the efficiency of network security devices such as firewalls, routers and web servers.
- For changing or upgrading existing infrastructure of software, hardware or network design.

There are basically two types of Penetration Testing such as External Testing and Internal Testing. External testing involves analysis of publicly available information, network enumeration phase and

the behavior of the security devices analyzed. Internal testing involves testing computers and devices within the company. Black-hat testing (zero knowledge testing), Gray-hat testing (partial knowledge testing), white-hate testing (complete knowledge testing), announced testing and unannounced testing are the tests that fall under internal testing. The common penetration testing techniques and areas are as shown in Table 4 [14].

Table 4 Common Penetration Testing Techniques and Areas [14]

Technique	Why?
Passive Research	To gather all the information about an organization's system configurations
Open Source Monitoring	Facilitates an organization to take necessary steps to ensure its confidentiality and integrity
Network Mapping & OS Fingerprinting	To get an idea of the network's configuration being tested.
Spoofing	To figure out whether use of one machine to pretend other is used for both internal and external penetration tests
Network Sniffing	To capture the data as it travels across a network
Trojan Attacks	To traces malicious code or programs sent into a network as email attachments or transferred via instant message
Brute-Force Attack	To trace any password cracking method in the network system which can overload system and possibly stop it from responding genuine requests
Vulnerability Scanning	For comprehensive examination of the targeted areas of an organization's network infrastructure.
Scenario Analysis	For Final phase analysis for testing, making risk assessment of vulnerabilities.

5. Conclusion

The researcher presented some of major security concerns in Information System and Security Audit and recommends use of security assessment periodically for healthy IS infrastructure and data security.

References

1. A. Gupta and S. Shakya, *"Information System Audit – An overview study of e-government of Nepal"*, International Conference on Green Computing and Internet of Things. IEEE. Noida. India., August 2015.
2. A. Gupta and S. Shakya, *"Information System Audit; A study for security and challenges"*, International Journal of Computer Science and Information Security. IJCSIS. Pp. 1-4, Vol. 13, No. 11, November 2015.

3. A. Gupta and S. Shakya, *"Information System Audit; Cloud Computing Security and Challenges"*, International Journal of Computer Science and Mobile Computing. IJCSMC, Pp 48-56, Volume 4, Issue 11, November 2015.

4. ISECOM. (2015). *"Institute for Security and Open Methodologies in the OSSTMM 3"*. Retrieved 10 21, 2015, from https://en.wikipedia.org/wiki/Security

5. Guttman, B., & Roback, E. A. *"An introduction to computer security: The NIST Handbook"*. National Institute of Standards and Technology, (1995).

6. National Research Council, *"Computers at Risk: Safe Computing in the Information Age"*. Washington DC: National Academy Press, (1991).

7. National Computer Security Centre, (n.d.), Pub. NCSC-TG-004-88.

8. OECD., *"Guidelines for the Security of Information System"*. Paris: Organisation for Economic Co-operation and Development, (1992).

9. Jain, A. K., Singh, Y., & Upadhyay, S. *"Information Systems Security: A review. Ind Jour Math & Comp Sc."* Jhs Vol. II - Pt I, 26-30, (2013)..

10. Johnson, A. M., *"The Technology Acceptance Model and the Decision to Invest in Information Security"*. Southern Association of Information Systems Conference, (2005).

11. EC-Council, *"Ethical Hacking and Countermeasures v9. In EC-Council, Malware Threats"* (p. 13). EC-Council, (2016).

12. The Institute of Chartered Accountants of India."*Information Systems Control and Audit"*, New Delhi: The Publication Department, ICAI, (2015).

13. Lim, C. C., & Jin, J. S. , *"A Study on Applying Software Security to Information Systems: E-Learning Portals"*. IJCSNS International Journal of Computer Science and 162 Network Security, VOL.6 No.3B, 162-166, (2006)..

14. CEH V8, *"Introduction to Ethical Hacking",* Module 1. In E. Council. EC-Council, (2015).