A Study On Challenges and Issues in Information Securities

Lavanya Nagarajan & Hema Senthilkumar
Computer Science and Engineering,
PITS,Thanjavur

Abstract:**This paper is based on the mistakes done by the human at the area of information system security. The new analysis of information safety have recently started to focus on the manual mistakes; Past researches show it to be a big part of issues in information security and maximum economic crisis are based on this problem. Now we did a small effective research on the role of human mistakes in this context, especially at the organizational level, peoples are not willing to share the private data due to safety concerns. Grounded theory has been worked to search the main reasons of manual mistakes in information security as a research methodology. A survey report which is based on some information security analysts around the world responses for develop a list of manual mistakes based on the non-ended coding. Our work is contributing our thoughts of the causes of manual mistakes in the information security. The present research has followed Glaser's & Strauss theory that approaches throughout the data gathering process to get the appropriate number of outcomes given by the researchers and their works related to the information security.**

I. INTRODUCTION TO INFORMATION SECURITY

As of January 2008, the internet connected an estimated 541.7 million computers in more than 250 countries on every continent, even Antarctica (Source: Internet Software Consortium's Internet Domain Survey; www.isc.org/index.pl). The internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection.Thus, individuals and organizations can reach any point on the internet without regard to national or geographic boundaries or time of day [1].However, along with the convenience and easy access to information come risks. Among them are the risks that valuable information will be lost, stolen, changed, or misused. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home; they may not even be in the same country[2]. They can steal or tamper with information without touching a piece of paper or a photocopier. They can also create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

II. BASIC SECURITY CONCEPTS:

Three basic security concepts important to information on the internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals[3]. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes. Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability[4]. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information (for example, airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When users cannot access the network or specific services provided on the network, they experience a denial of service. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is the person he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard"), or something about the user that proves the person's identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain

activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity[5]. This is known as nonrepudiation. These concepts of information security also apply to the term information security; that is, internet users want to be assured that

• They can trust the information they use
• The information they are responsible for will be shared only in the manner that they expect
• The information will be available when they need it
• The systems they use will process information in a timely and trustworthy manner In addition, information assurance extends to systems of all kinds, including large-scale distributed systems, control systems, and embedded systems, and it encompasses systems with hardware, software, and human components. The technologies of information assurance address system intrusions and compromises to information.

III. THREATS TO INFORMATION SECURITY

Technology with Weak Security
New technology is being released every day. More times than not, new gadgets have some form of Internet access but no plan for security. This presents a very serious risk – each unsecured connection means vulnerability. The rapid development of technology is a testament to innovators, however security lags severely[6].

Social Media Attacks
Cybercriminals are leveraging social media as a medium to distribute a complex geographical attack called "**water holing**". The attackers identify and infect a cluster of websites they believe members of the targeted organization will visit.

Mobile Malware – Security experts have seen risk in mobile device security since the early stages of their connectivity to the Internet. The minimal mobile foul play among the long list of recent attacks has users far less concerned than they should be. Considering our culture's unbreakable reliance on cell phones and how little cybercriminals have targeted them, it creates a catastrophic threat.

Third-party Entry – Cybercriminals prefer the path of least resistance. Target is the poster child of a major network attack through third-party entry points. The global retailer's HVAC vendor was the unfortunate contractor whose credentials were stolen and used to steal financial data sets for 70 million customers.

Neglecting Proper Configuration – Big data tools come with the ability to be customized to fit an organization's needs. Companies continue to neglect the importance of properly configuring security settings. The New York Times recently fell victim to a data breach as a result of enabling only one of the several critical functionalities needed to fully protect the organization's information.

Outdated Security Software – Updating security software is a basic technology management practice and a mandatory step to protecting big data. Software is developed to defend against known threats. That means any new malicious code that hits an outdated version of security software will go undetected.

Social Engineering – Cybercriminals know intrusion techniques have a shelf life. They have turned to reliable non-technical methods like social engineering, which rely on social interaction and psychological manipulation to gain access to confidential data. This form of intrusion is unpredictable and effective.

Lack of Encryption – Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness. The health care industry handles extremely sensitive data and understands the gravity of losing it – which is why HIPAA compliance requires every computer to be encrypted.

Corporate Data on Personal Devices – Whether an organization distributes corporate phones or not, confidential data is still being accessed on personal devices. Mobile management tools exist to limit functionality but securing the loopholes has not made it to the priority list for many organizations.

Inadequate Security Technology – Investing in software that monitors the security of a network has become a growing trend in the enterprise space after 2014's painful rip of data breaches. The software is designed to send alerts when intrusion attempts occur, however the alerts are only valuable if someone is available to address them. Companies are relying too heavily on technology to fully protect against attack when it is meant to be a managed tool.
To learn more about Georgetown University's online Master's in Technology Management program, **request more information** or contact an admissions representative at (202) 687-8888.

REFERENCE

[1] Ten Napel, Novealthy, Mano. "Wearables and Quantified Self Demand Security-First Design."
[2] Wired.com. Conde Nast Digital, 2015. Web. 12 Sept. 2015.
[3] Sterling, Bruce. "Spear-phishing and Water-holing."
[4] Wired.com. Conde Nast Digital, 10 Oct. 2012. Web. 12Sept.2015.
[5] Krebs, Brian. "The Target Breach, By the Numbers." Krebs on Security RSS. Krebs on Security, 14 May 2014. Web.12Sept.2015.
[6] "Cybersecurity Lessons from the New York Times Security Breach." GovDefenders. DLT Solutions, 2013. Web. 12 Sept. 2015.