Data Privacy: Security Threats and Counter Measures

Divya Krishnan Iyer[1], Dr. Astitwa Bhargava[2]

[1,2]National Law Institute University Bhopal

ABSTRACT

The technological development has created innumerable opportunities for business and customers, but the downside of these opportunities it has unanticipated risks attached to them, which are vulnerable to theft or loss of data as compared to traditional processing and data storage system and create unforeseen issues such as how personal information accessed is used; how it is protected; and who is accountable for its misuse. It is important that such concerns are addressed to preserve the confidentiality of information and to establish confidence among data owners over processing of their personal information with significant guarantees of security and privacy. This research paper tends to analyze the security threats to data privacy posed by new technologies, which lead to breach of confidentiality of information and to suggest measures addressing the issues of privacy and ensuring security for electronically transmitted information and stored data.

Keywords: Data security, Technological threats, Counter measures, Data privacy.

1. INTRODUCTION

"Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data."- **Pamela Samuelson**

The development of information technology has threatened privacy and reduced the amount of control a person can have over their personal data and generate a negative consequence. The combination of increasing power of new technology and the declining clarity and agreement on privacy give rise to problems concerning law, policy and ethics. The technology allows for the storage and processing of large volume of data concerning telephone conversations, internet searches and electronic payment information, is routinely used by government agencies and private agencies, and raises various issues related to privacy such as accessing and processing of personal information.[1]Ideally, the provided information should be used only for which it has been collected but in reality this information is further processed, transmitted and exploited for unauthorized purposes without the permission of data subject and thus raise concerns for data privacy. This research paper explores the relationship between information technology (IT) and privacy and illustrates the specific threats for data security, and indicates how IT can be used to overcome these privacy issues and ensuring security of data.

2. INVASION OF PRIVACY IN DIGITAL MEDIUM

An individual's privacy can be invaded by electronic means in several ways:

- Firstly, by the information which is available in databases;
- Second, from individual by way of their online activity that identifies the individuals.
- Third, by the massive databases maintained by governments and private entities.

Users expect that their online activities are anonymous but they are not, as it is possible to make record of all activities including which files subscriber has accessed, which web sites were visited what emails were read e-mails etc. This information can be collected by a subscriber's own ISP or by the web site operator.[2]

[1] Available at<http://lex-warrier.in/2013/10/privacy-data-protection-cyber-security-india/>

[2] Available at<http://injury.findlaw.com/torts-and-personal-injuries/what-is-invasion-of-privacy-.html>

"Online communications include connecting to the Internet through an Internet Service Provider (ISP) such as America Online or EarthLink, or accessing the Internet from a public library or by community computer center. Access to the Internet by mobile is increasing via hand held Personal Digital Assistants (PDAs), pagers, and other devices. The Internet raises some privacy concerns. Information sent over internet may pass through dozens of different system on the way to its destination. Each of these systems is operated by its own administrator and may be capable of capturing and storing online communications. Furthermore, online activities can potentially be monitored by Internet Service Provider (ISP) and by web sites that users visit.[3]

Personal Computers

Computers makes access to the Internet, any information deleted from a computer is easily recoverable, whether from the machine's hard drive or elsewhere. Deletion removes data from the hard disk drives directory of files and marks the disk space where the file is still stored as available for reuse. In time, another file may be written over this area, but in the period before deleted data are overwritten, anyone with access to the computer can locate and restore the deleted file with relatively simple commands. Even if files have been "written over" or "wiped" by programs that hash over the designated disk space, software utility programs are sometimes capable of recovering the data from the computer. Moreover, deleted files can be found not only on a personal computer's hard drive but also on another personal computer or elsewhere in a networked system. This causes a further issues related to privacy, by storing of information about Internet activities. Anyone with physical access to a computer can access these data in a matter of seconds either by looking at drop down files on the browser's location bar or by accessing the "History" menu item found on both Netscape Navigator and Internet Explorer. Even more significantly, remote access to these files is possible from the Internet by exploiting security flaws in Web browsers.

Cookies

While surfing the web, many web sites store data about visit to various sites, called "cookies," on the hard drive so that when a user return to that site, the cookie data will reveal that user have been there before. The web site might offer the user customized products or advertisements tailored to the users interests, based on the contents of the cookie data. A personal computer connected to the Internet can reveal users information by their acceptance of "cookies," also known as "persistent client-side hypertext transfer protocol files." These terms refer to identification tags and other blocks of data that a Web site sends to and stores on the hard drive of the user's computer. When an individual returns to this same site the browser automatically sends a copy of the cookie back to the Web site; the website identify the visitor and allow the site to match the users to details regarding the previous visit to the site.

Anyone who sits at another's computer or has remote access to it through an internal network can examine the machine's cookies to gain the names of the Web sites that were visited. Cookies are designed to report back exclusively to the Web site that placed them and to reveal only a particular identification number assigned by that site on previous visits.

Internet Service Providers (ISP)

Access to the Internet is provided by the ISP, who is an entity that supplies Internet services. ISPs can obtain access to its subscriber' sensitive information and build a profile based on customers' behavior on the Internet. This information is within its grab as the ISP generally collects the client's name, address, phone number, and credit card number at the time it assigns an account and has detailed information about the Internet behavior of each of its customers and link them to the identity of its customers. The question whether ISPs should disclose the identity of its subscribers without warrant was considered by US court in "*Timoty McVeigh v. Cohen"* where the Plaintiff, a Navy officer, sent an anonymous e-mail via AOL .The recipient searched through AOL's member profile directory, which indicated that he was homosexual. The recipient forwarded this information to the Navy. In response to this an inquiry was made with NAVY the plaintiff was identified and the NAVY held that the plaintiff should be discharged for engaging in homosexual activities. The Court held that the Navy's request to identify the identity of AOL was "likely illegal" under the Electronic Communications Privacy Act of 1996, which allows the government to obtain information from a service provider only if:

a) It has a warrant issued under the Federal Rules of Criminal Procedure;
b) It gives notice to the online subscriber or receives a court order authorizing disclosure of the information in question.
Having failed to follow the either path the court rejected the argument.

[3] Available at<https://scholarship.law.umt.edu/cgi/viewcontent.cgi?article=1150&context=mlr>

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is an, technology that uses radio signals to identify and track, objects without the need for direct contact. RFID technology can track the movements of objects through a network of radio-enabled devices over distance. RFID uses tags to store and emit information through radiofrequencies by the means of antennas. The data and other information, which is stored on the tags, are received by a transceiver (reader), which is equipped with an antenna. Antennas are the conduits between the tag and the reader, for communicating with other devices. The tag has a unique identifier and other information for identifying the device using a micro-chip to any object, animal or even a person, and the reading of this information through a wireless device. RFID systems raise privacy issues as they are used for identification of individuals and their location. Information can be extracted without having a direct link with the object. Even information indirectly linked to a person whose identity can be indirectly recognized can be personal data.

RFID tags have “electronic barcodes”; these tags use fibers that reflect the reader's signal and the signal can be used to track movement. RFID technology has three key elements:

- An RFID tag, that carries object and identify data.
- An RFID tag reader, that reads and writes tag data.
- A database, that stores records of tag contents.

Spyware and Adware

Spyware is software that secretly gathers user information without the user’s knowledge, for advertising purposes and is installed covertly on to the user’s system. Once it is installed to the system, the Spyware monitors user activity on the Internet and transmits the information to the attacker. It can gather information about e-mail addresses, passwords and card numbers. Some Spyware collect information by using “key loggers,” that capture information about the user’s computer activities, including cookies, session id, login credentials, and time spent on a particular site etc. These can record and save keystrokes in a log file that is transmitted from time to time to the attacker. When downloading adware, the user is first given an opportunity to agree to its being placed on the user’s computer and may trigger the display of pop-up or banner advertisements, and may gather and transmit information degrading system performance, tracking all activities, popping up annoying advertisements, and even stealing personal information.

3. SECURITY MEASURES FOR DATA PROTECTION

Regulatory and Compliance Measures

Security Policy

Organizations need to implement a security policy as a part of their administrative control. These policies should clearly state the security plan of the organization. A security policy must lays out the guidelines for employee for the use of organization resources and state the company can take action in case of any violation A security policy does not state any technical details, instead it focuses on the desired results.

Privacy Regulation

The **General Data Protection Regulation (GDPR)**[4] addresses **Privacy by Design** and states that any action by a company that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems etc., this means that the IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or process. Privacy Impact Assessments (PIAs) are an integral part of taking privacy by design approach. PIA is a tool used to identify and reduce the privacy risks. It can reduce the risks of harm to individuals through the misuse of their personal information.

Payment Card Industry Data Security Standard

PCI DSS is a standard for protecting card holder data. It has a set of requirement that the merchant who is involved in credit card transaction must follow as a control to protect credit card data and also comply with the Payment card industry data

[4] The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Available at< https://gdpr-info.eu/>

security standards. The PCI Council developed these requirements. Failure to meet the PCI DSS requirements may result in fines or penalties.

The PCI DSS 12 requirements are as follows:
1. Firewall configuration to protect cardholder data.
2. Vendor-supplied defaults passwords should not be used.
3. Cardholder data in data base should be protected.
4. Card holder data should be encrypted over network
5. Antivirus software should be update regularly.
6. Secure systems and applications should be developed and maintained.
7. Access to card holder data should be on need to know basis.
8. A unique id should be assigned to each person who has access to computer.
9. Physical access to cardholder data should be restricted.
10. Access to all network resources and card holder data should be regularly monitored
11. Security of system should be checked regularly.
12. An information security policy should be maintained.

Health Insurance Portability and Accountability Act (HIPPA)

HIPAA is a standard for protection of patient’s health information. Companies that deal with protected health information (PHI) must lay down physical and network security measures in to ensure they are HIPAA complained. It includes Covered entities (anyone providing treatment, payment, and operations in healthcare) and business associates (anyone who has access to patient information and provides support in treatment) must meet HIPAA Compliance. Other entities are the subcontractors and other business associates must also be in compliance.

According to the US Department of Health, the HIPPA Privacy Rule sets standard for the protection of certain health information. The HIPPA security standard is for protecting health information that is transferred in electronic form or transferred over network. The Security Rule addresses the technical and nontechnical controls or safeguards that covered entities must put in place to secure individuals’ electronic PHI (e-PHI). The physical technical safeguard, network security controls[5] and their regular audit should be regularly performed. The technical safeguards include access control to allow only the authorized to access electronic protected health data. Access control includes using unique user IDs, an access control procedure, automatic log off, encryption and decryption.

Generally Accepted Privacy Policy

Organizations face challenges in managing privacy on local, national and international level. They face a number of privacy laws and regulations which differ for each other and whose requirements need to be identified. The GAPP analysis the privacy requirements of all privacy frameworks and integrates into a single privacy policy that the organizations can follow to meet the regulatory and compliance requirements and to develop an effective privacy program that addresses privacy risks and identify business opportunities

ISO 27001

ISO/IEC 27001 is the international standard that describes best practice for an information security management system in the organization. Achieving accredited certification to ISO 27001 demonstrates that the organization is following information security best practice. It is a systematic and pro-active approach to effectively managing risks to the security and confidential information. The system promotes efficient management of sensitive corporate information, highlighting vulnerabilities to ensure it is adequately protected against potential threats. It encompasses people, process and IT systems. It helps to manage, monitor, audit and improve organization’s information security and manage all security practices in one place, consistently and cost-effectively. ISMS is business-driven risk assessments, which means you will be able to identify and treat security threats according to your organization’s risk appetite and tolerance.

Technical Security Measures

Logical Security Measures

[5] Network, or transmission, security is the last technical safeguard required of HIPAA compliant hosts to protect against unauthorized public access of e-PHI. Availableat<https://www.hhs.gov/hipaa/professionals/security/laws-regulations/index.html>

Firewall

A firewall is a network security device that monitors for incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. It is the first line of defense for security of network. They establish a barrier between secured and unsecured networks, such as the Internet that prevents unauthorized access to or from internal network. Rules can be created on firewall for either inbound traffic or for outbound traffic.

Firewall rules are applied in the following order of priority:

- Authenticated bypass (rules that override block rules)
- Block connection
- Allow connection

Inbound Rules

Inbound rules allow explicitly or block explicitly the traffic attempting to gain access to inside. For example, configuring a rule to explicitly allow traffic secured by IPSec for Remote Desktop through the firewall but block the same traffic if it is not secured by IPSec.

Outbound Rules

Outbound traffic is allowed by default. Outbound rules explicitly allow or block traffic coming from the computer that matches the criteria in the rule. For example, a rule to explicitly block outbound traffic to a specific computer through the firewall but allows the same traffic to other computers.

Encryption

Encryption refers to transformation of information into another form or a code that, so that the users who have access to the secret key or a password can have read the data. Encrypted data is referred to as cipher text, while unencrypted data called plaintext. The purpose of encryption is to protect the confidentiality of data as it is stored on computer systems and transmitted over network. There are two types of encryption process - symmetric encryption that is a private key encryption one a single key is used to encrypt and decrypt the information and asymmetric encryption, which is public-key encryption where two keys are used for encryption and decryption of information.

Intrusion Detection Prevention System

Intrusion detection and prevention system is a network security tool that monitors the network traffic by inspecting and scanning packets for suspicious data and in real time block the packet with malicious signature. An intrusion detection system (IDS)[6] monitors all inbound and outbound network activity and generates an alert in real time that may indicate a network or system attack from an intruder attempting to break into the system. An IDS is a passive-monitoring system that only generates an alarm for suspicious activity taking place. Whereas an intrusion prevention system[7] (IPS) stops the packet from coming inside the network by blocking the suspicious packet having signatures.

Privacy Enhancing Technologies

Privacy enhancing technologies empower an individual by giving them easy access to and control over their personal information and allowing them to decide how and when this information will be disclosed to and used by third parties. Anonymity tools' allow individuals to withhold their true identity from those systems and only reveal it when absolutely necessary. These technologies help to minimize the information collected about individuals.

Examples of online anonymity tools are:

- **TOR**: Tor stands for "The Onion Routing" it is a server that keeps users anonymous on over the network. The data sent over network travels across multiple Top servers called "hops" each server move the data to another server with the final hop moves data to the end site. The information which is transmitted in this way is hard to trace.

[6] The Intrusion Detection System (IDS) provides the network with a level of preventive security against any suspicious activity. Available at<https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799>

[7] An Intrusion Prevention System (IPS) is a device that controls access to IT networks in order to protect systems from attack and abuse. Available at<https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>

- **VPN:** A virtual private network is the most effective online anonymity tool. It secures the private network from the public network, by using mechanism such as encryption to ensure that only authorized users have access to the network and ensure that the data within the network cannot be intercepted. It provides a secure tunnel that transmits the data securely between the remote user and the organization network. The information that is transmitted between the two locations is encrypted via tunnel and cannot be read by anyone as the information is securely transferred from both company's network and outside network through which the remote user connects.

- **HTTPS**: Hypertext transfer protocol for secure communication over the network. The HTTPs is a communication protocol encrypted by Transport Layer Security (TLS), it is also called as HTTP over TLS or HTTP over SSL. It protects the network from any man in the middle attack where an attacker can capture data transferring over the network. It encrypts the data between client and the server and protects the data against eavesdropping and protects tampering of communication.

- **PGP:** Pretty Good Privacy is a program used for encrypting and decrypting emails, files, directories transmitted over the network to increase the security of email communications. It is also used to sign message so that both the sender and the receiver can verify their identity and integrity of the content.

Authentication

Authentication is used to ensure that the person who is accessing the information is indeed the person who they claim to be. Authentication can be accomplished by identifying someone through one or more of three factors i.e., *"something user know, something user have, or something user are.*" For example, the most common form of authentication is the user ID and password. In this case, the authentication is done by confirming something the user knows that is user ID and password. This form of authentication is easy to compromise and more strong form of authentication is required, if the user ID or the password is compromised then the intruder can gain access to the information. The second form of authentication is "*something user have"* that is the token card or ID cards used to gain access. This form of authentication has risk as the identification card can be stolen or lost. The third form of authentication is "*something user are",* this form of authentication is much harder to compromise as it identifies a user through its physical traits such as an eye-scan or fingerprint i.e., biometrics. The most secure way of authentication is multi-factor authentication[8] it is done by combining two or more factors and therefore it becomes difficult for someone to misrepresent themselves. Adaptive authentication is a way that two-factor authentication or multi-factor authentication that can be configured and deployed. It's an authentication method depending on a user's risk profile and tendencies - for adapting the type of authentication according to the situation.

Password Security

Password policies must be in place to ensure that passwords cannot be easily compromised. Common policies that organizations should put in place are:

- **Require complex passwords**. One of the reasons for which password is easily compromised is that they can be guessed easily. A password should not be simple. It should not be that it can easily be compromised by dictionary attack or brute force attack. It should be minimum of eight characters and should be combination of upper case, lower case, numbers, alphanumeric characters and special characters.

- **Change passwords regularly:** The users should change their passwords on a regular basis for every 60 to 90 days ensuring that the password which might have been guessed or stolen earlier by the attacker will not be able to use it again for gaining access.

- **Phishing attacks:** One of the primary methods used to steal password is simply by asking to the users or administrators. For example if an attacker calls the helpdesk or security administrator and pretends to be a particular user having trouble logging in and provides personal information about the authorized user, the attacker

[8] Multi-Factor Authentication, one-time-passwords, and biometrics can improve security, but may not be as user friendly and convenient as the employee would like. Available at< https://www.globalsign.com/en/blog/what-is-multi-factor-authentication-mfa/>

convinces the security person to reset the password and tell him the new password. This method is called as misrepresentation where the attacker pretends to be a legitimate user.[9]

- **Password salting**: Password salting is a form of password encryption that appends a random string of characters to the password and then the new string of character is then hashed to make a strong password. It is more secure form of password encryption model considered a more secure password encryption model.

Physical Security Measures

Physical security is the protection of the actual hardware and networking devices that store and transmit information. An organization must identify all the resources that are venerable and take measures to ensure that these resources cannot be physically tampered with or stolen. These measures include the following:

- **Physical Locks**: Physical locks should be implemented to secure information assets to prevent from being stolen.

- **Physical intrusion detection:** Security cameras should be placed to monitor the information assets to detect unauthorized access to information resources.

- **Environmental monitoring**: Organization’s servers and other high-value equipments should be kept in a room that is monitored for temperature, humidity, and airflow as there arises a risk that server failure might occur when these factors go out of a specified range.

- **Employee training:** the most common ways thieves steal corporate information is by stealing employee laptops. Employees should be trained to secure their devices.[10]

CONCLUSION

The growth of technology criminal has brought criminals to perpetrate the privacy of individuals. The traditional technique of physically isolating the raw data alone is no longer effective in ensuring data security. Organizations must plan and review policies and procedures to protect their data. A variety of measures can to be adopted like providing training and educating the employees, restricting access to protected data, regularly auditing the log data, encrypting data over network and database, implementing network security tools and incident response procedures should be in place.

ACKNOLEDGEMENT

I gratefully acknowledge the contributions of Dr. Astitwa Bhargava for his work on the original version of this document.

REFERENCES

[1] Claudine Guerrier, “*Security and Privacy in the Digital Era*,” ISTE Ltd and John Wiley & Sons, Inc,2016, ISBN 978-1-78630-078-2

[2] Carey, Peter, *“A Practical Guide to UK and EU Law*” Edition 3. Oxford: Oxford University Press. 2012. ISBN: 978-0-19-956354-8

[3] Alan Charles Raul ,”*The Privacy, Data Protection and Cyber security Law Review”*, Edition 1, ISBN 978-1-909830-28-8

[9] Phishing occurs when a user receives an e-mail that looks as if it is from a trusted source, such as their bank, or their employer. Available at< https://www.us-cert.gov/ncas/tips/ST04-014>

[10] Available at< https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120>