International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 10 | October - 2022 Impact Factor: 7.185 ISSN: 2582-3930

DATA SECURITY & SECURITY BREACHES: IMPACT ANALYSIS AND PREVENTION MEASURES

Pratik Barot[1], Mayura Vartak[2], Arshunnu Bare[3]

[1]Ex-Student, Electronics Engineering, Shah & Anchor Kutchhi Engineering College, India.
[2]Ex-Student, Mechanical Engineering, Vidyavardhini's College of Engineering and Technology, India.
[3]Ex-Student, Computer Department., MCT's Rajiv Gandhi Institute of Technology, India.

Abstract - The requirement for safe computer systems becomes more obvious as more tasks are automated and as more computers are used to hold sensitive data. As more systems and applications are being deployed and accessible across unsecured networks like the Internet, this requirement is becoming more and more obvious. Governments, businesses, financial institutions, and millions of daily users now depend heavily on the Internet. Computer networks provide assistance for a wide range of operations whose absence would almost bring these enterprises to their knees. As a result, cybersecurity problems have evolved into national security problems. Internet security is a challenging task. Cybersecurity cannot be accomplished via accidental, seat-of-the-pants tactics; it can only be achieved through deliberate development. In this paper we discuss the growing utility of data in the modern world, threats to personal and professional data, data security and its importance. We also give an overview into some of the biggest security breaches in the recent times as well as analyse some of their impacts and the aftermath of data breaches and what practices can be put into place to enhance data security and prevent security breaches.

***Key Words*:** data, breach, security, risk, cybersecurity

1. INTRODUCTION

Data is a collection of discrete values that convey information, describing quantity, quality, fact, statistics, other basic units of meaning, or simply sequences of symbols that may be further interpreted. The same data when considered in individual sets is known as datum. Data represents the raw facts and figures which can be used in such a manner in order to capture the useful information out of it. Data is commonly used in scientific research, finance, and in virtually every other form of human organizational activity. Examples of data sets include stock prices, crime rates, unemployment rates, literacy rates, and census data. Some might say that Data, Information and Knowledge are the same thing but in reality that is not case, Data is to information what an atom is to matter. This means that for any type of information to exist there should be some kind of data or datasets on any particular topic. To be useful, the quality of data needs to be impeccable. The main characteristics regarding data quality are: relevance; accuracy; credibility; timeliness; accessibility; interpretability; and coherence. Aside from data quality, another important aspect to data and its utility is data security.

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. Data security is crucial because it helps protect sensitive information, which might be personal or organizational. Confidentiality, Integrity, and Availability are the three primary components of data security. [1]

Confidentiality refers to keeping the privacy of the stored data as private as possible. It begins with the fundamentals, including identifying and regulating the degrees of information access both internally and externally and preventing any unauthorized access.

Integrity of the data means that it must not be modified or tampered with by an unauthorized entity. It is an essential component of data hygiene, dependability, and correctness. The best approach to ensure data integrity is to perform regular backups, monitor the audit, and encrypt your data as well as maintain the access management to the data appropriately.

Availability indicates that the system and services must be available to the authorized user(s) when they need it, regardless of the conditions, such as power outages or natural catastrophes. Other components go off without availability and can have a detrimental influence. An organization should deploy backup networks, servers, and applications to ensure availability.

2. DATA SECURITY

Data is a valuable asset that generates, acquires, saves, and exchanges for any company. Protecting it from internal or external corruption and illegal access protects a company from financial loss, reputational harm, consumer trust degradation, and brand erosion, this makes data security important. One of the reasons why data security is so critical is that the threats from hackers and malware are greater than it ever has been in the past. Just like technology has improved the daily operations of businesses, hackers have changed the way they attack data as well.

Control Measures of Data Security:

i. Access Control: Limiting both physical and digital access to central systems and data is an example of a strategy for securing data. It involves ensuring that all computers and gadgets are password-protected and that physical places are only accessible to authorized employees.

ii. Authentication: Provide authentication measures, such as access restrictions and correct identification of people, before giving access to data. Passwords, PINs, security tokens, swipe cards, and biometrics are common examples.
iii. Backups and Disaster Recovery: Good security means you have a strategy in place to safely access data in case of a system failure, disaster, data corruption, or breach. To restore, you will need a backup data copy kept on a distinct format such as a hard drive, local network, or Cloud.
iv. Data Erasure: Appropriate discarding of data regularly is necessary. Data erasure is more secure than ordinary data wiping since data erasure uses software to wipe data completely on any storage device. Data erasure ensures that data cannot be recovered and, hence, will not fall into the wrong hands.
v. Data Masking: Data masking software obscures letters and numbers with proxy characters, concealing information. Even if a person obtains access to data illegally, it is successfully masked. Only when an authorized user acquires data, then does it revert back to its original state.
vi. Data Resilience: With comprehensive security, you can withstand or recover from failures. Avoid power outages and mitigate natural catastrophes as these factors can breach data protection. Data privacy can be implemented by incorporating resilience into your hardware and software.
vii. Encryption: With the help of encryption keys, a computer algorithm converts text characters into an unreadable format. The content can only be unlocked and accessed by authorized people who have the appropriate keys. To some extent, everything from files and databases to email conversations should be secured.

Although there are controls in place to protect data, it is not always simple to keep it safe from hackers or other security breaches.

Fig 1 : Data Security Controls

Figure 1: Data Security Controls

3. THREATS TO DATA SECURITY

In this session, we will discuss the most serious threats to data security, namely security breaches. Any conduct that allows unauthorized access to computer data, applications, networks, or devices is considered a security breach. As a result, information is leaked or accessed without authority. It mostly occurs when an intruder circumvents the security mechanisms.

There is a technical distinction between a security breach and a data leak. A security breach is essentially a break-in, but a data breach is described as a cybercriminal escaping with data. Consider a burglar: the security breach occurs when he climbs through the window, and the data breach is when he steals your wallet or laptop.

We will go over the many sorts of security breaches that might occur.

i. Weak passwords: Because they can be cracked or guessed. Even now, some people are still using the password 'password', and 'pa$$word' is not secure.
ii. Malware attacks: They are assaults in which phishing emails are used to acquire access. It just takes one person clicking on a link in a phishing email for harmful malware to proliferate across the network.
iii. Drive-by downloads: These assaults employ viruses or malware distributed via a hacked or faked website.
iv. Exploit: An exploit attacks a system vulnerability, such as an out of date operating system. Legacy systems which haven't been updated, for instance, in businesses where outdated and versions of Microsoft Windows that are no longer supported are being used, are particularly vulnerable to exploits.
v. Social engineering: Even though it is not considered as a Security Breach it can also be used to gain access. For instance, an intruder phones an employee claiming to be from the company's IT helpdesk and asks for the password in order to 'fix' the computer.

4. TARGETS OF BREACHES

Business data only becomes a target when it is valuable to a third party. Different kinds of data hold more or less value to third parties and hence represent different risk levels to businesses. The different types of target data include the following: [2]

i. Personally Identifiable Information. This includes data such as social security numbers, contact information, birth dates, education and other personal information.
ii. Financial Information. This includes charge card numbers and expiry dates, bank accounts, investment details and similar data.
iii. Health Information. This includes details on health conditions, prescription drugs, treatments and medical records.
iv. Intellectual Property. This includes product drawings and manuals, specifications, scientific formulas, marketing texts and symbols, proprietary software and other material that the business has developed.
v. Competition Information. This includes data on competitors, market studies, pricing information and business plans.
vi. Legal Information. This includes documentation on court cases the company may be pursuing, legal opinions on business practices, merger and acquisition details and regulatory rulings.
vii. IT Security Data. This includes lists of user names and passwords, encryption keys, security strategies and network structure.

Third parties who value the data are interested in these forms of information. Information about one's identity, finances, and health may be sold and utilised for marketing purposes. Intellectual property can be bought, sold, and used to create goods and services that are comparable to those offered by your company. Leaked legal information may weaken your legal standing, and competitive information might be sold and exploited by rivals to thwart your ambitions. Because it gives hackers access to all other forms of information on your system, data on IT security is important in and of itself.

5. NOTABLE BREACHES

Examples of some of the major security breaches which made a ripple across the world are: [3]

i. Facebook (now Meta) saw internal software flaws lead to the loss of 29 million users' personal data in 2018. This was a particularly embarrassing security breach since the compromised accounts included that of company CEO Mark Zuckerberg.
ii. eBay saw a major breach in 2014. Though PayPal users' credit card information was not at risk, many customers' passwords were compromised. The company acted quickly to email its users and ask them to change their passwords in order to remain secure.
iii. Yahoo - 3 billion user accounts were compromised in 2013 after a phishing attempt gave hackers access to the network.
iv. Dating site Ashley Madison, which marketed itself to married people wishing to have affairs, was hacked in 2015. The hackers went on to leak a huge number of customer details via the internet. Extortionists began to target customers whose names were leaked; unconfirmed reports have linked a number of suicides to exposure by the data breach.
v. Equifax - in 2017, a website application vulnerability caused the company to lose the personal details of 145 million Americans. This included their names, SSNs, and drivers' license numbers. The attacks were made over a three-month period from May to July, but the security breach wasn't announced until September.
vi. Aadhaar Breach - During 2018, the secret and sensitive data of 1.1 billion people had been torn open and exposed, then aggregated on various dark web lists for sale. Malicious cyber-attacks and lax cyber-security protocols led to massive breaches of personal information in 2018 in India. The World Economic Forum's (WEF's) Global Risks Report 2019, says, "The largest (data breach) was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens. It was reported in January 2018 that criminals were selling access to the database at a rate of Rs500 for 10 minutes, while in March a leak at a state-owned utility company allowed anyone to download names and ID numbers." [4]

		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

Fig 2 Top 10 Biggest Breaches in 2018

6. AFTERMATHS OF DATA BREACHES

1) For Users:

Information breaches can lead (and have led) to serious impacts on the private lives of affected individuals, including but not limited to humiliation, discrimination, financial loss, physical or psychological damage or even threat to life. It can also pose a threat to other aspects of the lives of said individuals for example their businesses or jobs, their social circle, their local surroundings, etc. It can also further lead to risks in social security as well as being accused of atrocities committed by somebody else who might be “borrowing” the victim’s identity in various forms such as their credit card information, social security number, other portal details, etc.

2) For Organizations:

An organization faces 2 types of aftermaths after a data breach, immediate, short term consequences as well as long term impacts. The short term consequences include fall in market value, decline of reputation, compensation to users affected by the breach, financial losses in fines and fees, forensic investigation as well as future security outlook and costs. The organization may also immediately be scrutinized and have its activities be put on hold until further notice.

The long term effects stem from the short term effects, diminished reputation leads to loss in the trust customers have towards the organization. A good reputation is often a company’s most prized asset as a business must work constantly to build and maintain the integrity of its brand. However, one compromising episode like a data breach can tarnish even the best of reputations. The PwC report found that 85% of consumers won’t shop at a business if they have concerns about their security practices. A data breach leads to heavier investment in cybersecurity protocols and might affect the overall operations and finances of the organization. It might also give leeway to other cybercriminals to target the

organization for further attacks. It could also lead to hesitation in the stakeholders' involvement in the business as well as cast doubt for other organizations to participate in business operations with the attacked organization.

7. MEASURES TO ENHANCE SECURITY

i. For Personal Data:

a. Data Backup: Back your data up frequently. If feasible, store it on an alternate device instead of the primary workplace. Ensures prevention of loss of all data in the event of a break-in, fire, or flood.
b. Awareness of Social Engineering: Learn to recognize fraudulent emails and other social engineering tactics. You can avoid being taken by surprise by looking out for telltale signals like poor grammar, frantic pleas for action, and demands for payment. Don't believe anything that seems strange.
c. Access Secured Networks: You should always utilize a safe connection while connecting to the internet since using public Wi-Fi or an insecure connection could put personal data in jeopardy. It is recommended to use Virtual Proxy Networks (VPN) when online in order to preserve data and uphold privacy.
d. Manage data timeline as per requirement: Maintaining control over the personal data that is stored will help you save time and resources. It will also support duties for data protection. Just keep what is required for however long it holds utility. Once the data needs have been met, either archive the data or store it safely in alternate secure storages.
e. Dispose old equipment securely: Make sure there is no personal information remaining on any PCs, laptops, cellphones, or other devices before disposing of them. Think about employing deletion software or hiring a professional to erase the data. When the device is disposed of, this will guarantee that nobody may access information they are not meant to see.
f. Password Management: Use secure passwords for all of your annexes, including computers, laptops, tablets, cellphones, and email accounts. Use different passwords for different devices and services. Aim to avoid using passwords that are obvious or contain personal information. To reduce the danger of password leaks, update your passwords often.

These are some common tips to enhance data security for individual users. Other additional common practices include staying wary on remote connections, keep your devices locked when unattended, stay up to date with the antivirus, etc.

ii. For Organizational Data:

a. Protect data not just the perimeter: With approximately 90% of security resources going on firewall technology, it appears that many firms are focusing on protecting the walls around the data. However, there are several possible workarounds for firewalls, including through clients, partners, and staff. These individuals can all get beyond external cyber security and abuse sensitive data. Organizations need to ensure that their security initiatives emphasize on the data rather than merely the perimeter because of this.
b. Beware of Insider Risks: Since external dangers are frequently portrayed in the news and on television as the greatest and most expensive ones, it is simple to perceive them. The truth is that you are most vulnerable to harm from insiders. Insider assaults can be challenging to identify and stop due to their nature. It might be as easy as a worker opening an email attachment they think is from a reliable source and activating a ransomware worm. Threats of this nature are the most frequent and expensive worldwide.
c. Regular Updates: Ensure that all machines are patched and updated correctly. It is frequently better to do this to make sure it is sufficiently secured. The most current update determines how effective the security applications are. It is important to update these programs often since hackers and ransomware outbreaks are continually evolving to exploit flaws in older software versions.
d. Testing Security Protocols: It is foolish to believe that putting antivirus software on every computer or device can shield the business from threats. Hiring a qualified company to undertake a security audit will always identify vulnerabilities that weren't anticipated, as previous data breaches have demonstrated. It is advised to take the necessary precautions to properly verify the security mechanisms in place on a regular basis and to look out for other things like scribbled passwords or unsolicited papers located in inappropriate places.
e. Investment in Better Cybersecurity: Since data security continues to be the biggest risk to your IT infrastructure, many CIOs have acknowledged that investing more time and money in it is essential. With the recognition that cybersecurity must be a crucial component of all business operations, many large corporations with critical corporate data to protect are employing chief security officers, frequently to board level roles. This is related to the idea that firms may lose their advantage in the marketplace as well as suffer declines in their income and reputation if their data is compromised.
f. Organization-wide Security Mindset: Everyone who has a login and password is in charge of maintaining data security. Managers and staff

must be routinely reminded by IT administrators not to divulge login information to any outside party. Everyone has a role in data security; it is not simply the responsibility of the IT staff. To guarantee the protection of the organizational data, all personnel must get regular training on information security and other fundamental procedures, as well as refreshments.

g. Encryption: More individuals are preferring to work on their mobile or personal devices as a result of the paradigm change in remote work that has occurred globally. Make sure that all data is saved in an encrypted manner and stays encrypted during migrations to make sure that these devices are reliable. Additionally, keep the data on encrypted systems with the proper degrees of security.

h. Identity & Access Management: Every firm has a tremendous amount of data on hand. This information must be categorized based on a need to know basis. Only authorized personnel with the proper degree of security clearance must be identified and then granted access to the relevant data in order to ensure the secrecy. Without adhering to the right process to seek access to the data from a pertinent approver, no unauthorized person may be granted access to the data.

8. CONCLUSIONS

In the age where the role of data is ever-growing across multifarious fields like medicine, social security, business, finances, etc. the security of the associated data also grows exponentially. The importance of data security is every bit as important for individuals as for organizations and enterprises. The indispensability of cybersecurity must be clearly realized and hence acted upon by all, individuals and businesses alike.

The compromise of either personal or organizational data leads to heavy aftershocks ranging across various aspects like financial losses, reputation plummet, loss of credibility, social boycotting, etc. Security breaches are getting more common as technology advances and creating risks for a large population. Security must be the top priority and negligence towards it should not be tolerated. To ensure smooth operations and protection of the information, proper measures must be taken for maintaining and enhancing the security.

As individuals, people should follow safe browsing as well device usage practices. They should keep their accounts safe by using strong passwords, updating them frequently, etc. for instance. Constant threat monitoring and risk analysis of your digital presence across various sites is a requisite to improve the security of personal data. Some pointers have been shared in this paper which may be used as a guideline to starting the journey towards making the storage and maintenance of personal data more secure.

The financial investments that an organization is willing to make towards its cybersecurity should reflect their sincerity to conduct business as most businesses heavily rely on their data. The investment must be comprehensive and consistent throughout. The organization must provide protection and the best guidance and training for your employees. One error is sufficient to bring down an entire network. To avoid this, keep the employees trained. It is easier to perceive tighter data restrictions as a means to protect the business. The organizational data security can be improved using some of the methods shared in this paper as well as by coming up with innovative techniques and testing them. Information security is not a one fits all for organization and must be correctly tailored to match the operations of each enterprise.

Moreover, the growth seen by the big data industry is bringing into circulation never seen before volumes and types of data. The management of this huge amount of data is not always regulated and following secure protocols. The automation of several tasks also requires access to data which is not always suitable and hence might pose a risk to data. Every step taken by users and businesses could be of some aid to protecting the important data. One must be up-to-date with the latest security breaches, risks to relevant data, measures of prevention or fixing the risks, etc. and act accordingly to gain the best outcome.

REFERENCES

1. E. Bertino, "Data Security and Privacy: Concepts, Approaches, and Research Directions," 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 2016, pp. 400-407, doi: 10.1109/COMPSAC.2016.89.
2. https://www.cloudmask.com/blog/data-breaches-threats-and-consequences
3. https://dataprot.net/articles/biggest-data-breaches/
4. https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html
5. E. Bertino, R. Sandhu, “Database Security – Concepts, Approaches,and Challenges”, IEEE Trans. Dependable Sec. Comput. 2(1):2-19(2005).
6. R. A. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., 2003, pp. 705-715, doi: 10.1109/ICSE.2003.1201257.
7. S. Pan and Z. Xiao, "Design of the Information Security System Based on the Encryption Mechanism," 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE), 2021, pp. 510-513, doi: 10.1109/ICISCAE52414.2021.9590763.
8. https://en.wikipedia.org/wiki/Data
9. https://en.wikipedia.org/wiki/Computer_security
10. https://en.wikipedia.org/wiki/Data_breach
11. P. Chauhan, N. Singh and N. Chandra, "Security Breaches in an Organization and Their Countermeasures," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 349-354, doi: 10.1109/CICN.2013.79.
12. https://en.wikipedia.org/wiki/Social_engineering_(security)
13. Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
14. A. Földvári, G. Biczók, I. Kocsis, L. Gönczy and A. Pataricza, "Impact Assessment of IT Security Breaches in Cyber-Physical Systems: Short paper," 2021 10th Latin-American Symposium on Dependable Computing (LADC), 2021, pp. 1-4, doi: 10.1109/LADC53747.2021.9672582.