DATA SECURITY, PRIVACY, AND LEGAL ISSUE

Fundamental of Data Management HD repor

Tevy Tunsay

103139978

Table of Contents

Table of Figures

Introduction

The purpose of the report is to explore some common issues in database management, including data security, privacy, and legal issues. This topic is selected because data is the most valuable resource that must be strictly controlled and managed. In addition, corporate data may have strategic importance to an organization, so that data must be kept secure and confidential.
Based on IBM, there is a 10% increase in the average total cost of a data breach between 2020 and 2021. Since database security issues have risen, the scrutiny of data management practices has been scrutinized more carefully. That is when legal issues are involved.

Key findings: data security

What is data security?

Data security is the practice of protecting digital information from untheorized access or unwanted action. Its goal is to protect the organization from:

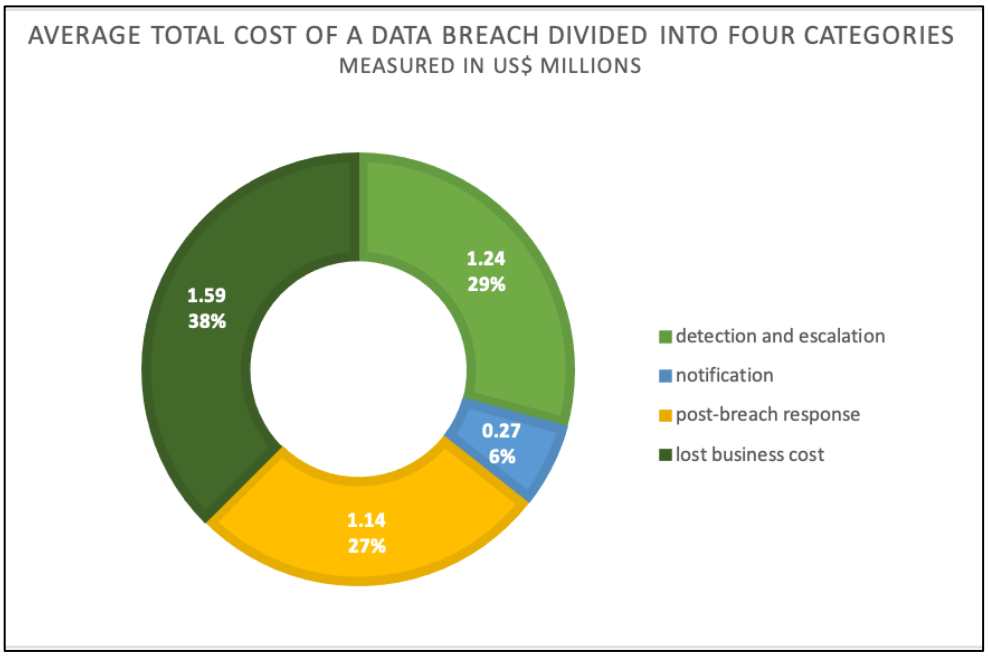
- theft and fraud
- loss of privacy
- loss of confidentiality
- loss of integrity
- loss of availability

Why is data security a serious concern?

In any firm, data security is a significant problem. If there is a security breach, it may have an impact on other aspects of the system. As a result, the entire database will be affected, leading to data being lost, stolen, released without authorization, or rendered unusable. Furthermore, a security breach can harm an organization's brand by causing customers to do their business elsewhere. The organization may also be required to pay fines and/or defend itself in court. If the organization's security is particularly poor, the leader may face criminal charges.

The above concerns have not even taken accounts of the expense of a data breach. According to IBM, the average overall cost of a data breach in 2021 is USD 4.24 million. The pie chart below depicts the total cost of a data breach in US dollars, divided into four main categories:

FIGURE 1: AVERAGE TOTAL COST OF DATA BREACH 2021



Source: (IBM Corporation, 2021)

What are threats to a database?

A threat is an item, person, or other things that pose risks of sensitive data loss or corruption to an asset. There are several types of threats:

- Human: This hazard includes unintentional errors made by employees and attackers with purposeful intent to harm your company.

  Some examples of an unintentional mistake made by employees:
- Losing/broking laptop
- Poor password use
- Careless while surfing the internet
- Deleted files on accident

  An example of the attacker who have bad intention on the organization
- On the phone, an attacker impersonates someone else, such as a manager, and convinces the employee that he has forgotten his password. And would ask the the employee to give them a password.
- Natural: it Is an unpredictable and uncontrollable threat which is a natural event such as fire, earthquakes, and floods.
- Technological and operational: Threats that operate inside information systems with the intent of harming information security goals. Technology threats include hardware and software failures. Processes that aren't operating correctly are likewise a threat. This threat might take the form of any malicious code.
- Physical and environmental: is a hazard that arises from a facility's properties, such as lax physical security and a lack of heating or cooling in the facility.

How should an organization control its security?

Physical controls, access controls, and communication controls are the three basic types of controls that an organization may use to secure its information asset.

Physical controls

Physical control stops unauthorized individuals from accessing the company's facilitator. Fences, walls, doors, locks, guards, and alarm systems are all included. Some businesses set limits on how much time and where employees can connect to their computers. They require them to log off the computer at the end of the day. Some companies even set their employees' computers to log off automatically after a period of inactivity time.

Access controls

This measure combines two functions to prevent unauthorized users from accessing information resources: authentication and authorization. Authentication is to identify the individual who needs access. The next stage is authorisation when the people have been identified.

How to implement authentication?

- Biometric: fingerprint scanning, face recognition, and iris recognition are just a few examples.
- ID card: This is also one of the most frequent types of authentications in a company. The photo and signature of the employee are usually included on the ID card. Some modern businesses now have chips that hold precise information about their employees.
- Password: In any firm, passwords pose a significant information security risk. However, a password is insufficient. Therefore, we must pick a strong password that is tough to guess for a hacker. However, if the password is difficult to remember, some employees may write it down someplace, posing a security risk. Therefore, the solution is that the company should be aware of its personnel's authentication and security risk.

What is a strong password?

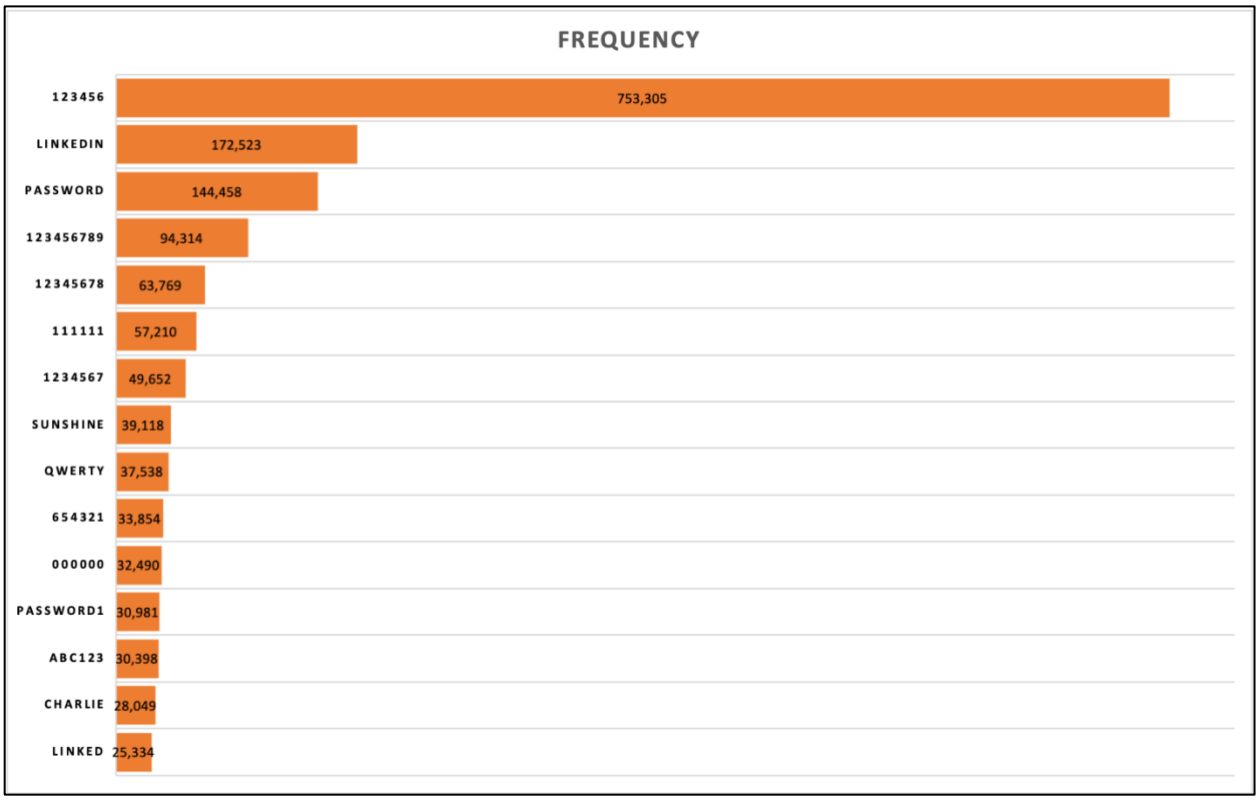
A strong password should be a password that is difficult to guess. This can mean it is:

- Long
- Complex (upper and lower case of letter, use with number and/or special character)
- Should not be a recognized word or number (such as a name, phone number and birthday)

Example of data breach due to weak password: LinkedIn

In June 2012, LinkedIn was hacked, exposing the personal information of 165 million members. Since then, it has been claimed that data including 6.5 million encrypted passwords has been offered for sale on a Russian online forum. LinkedIn spent nearly three million pounds to clean them up as a consequence. The following graph, according to Leakedsource, depicts the result of LinkedIn users' weak passwords being disclosed.

FIGURE 2: LINKEDIN USER PASSWORD HACKED 2012



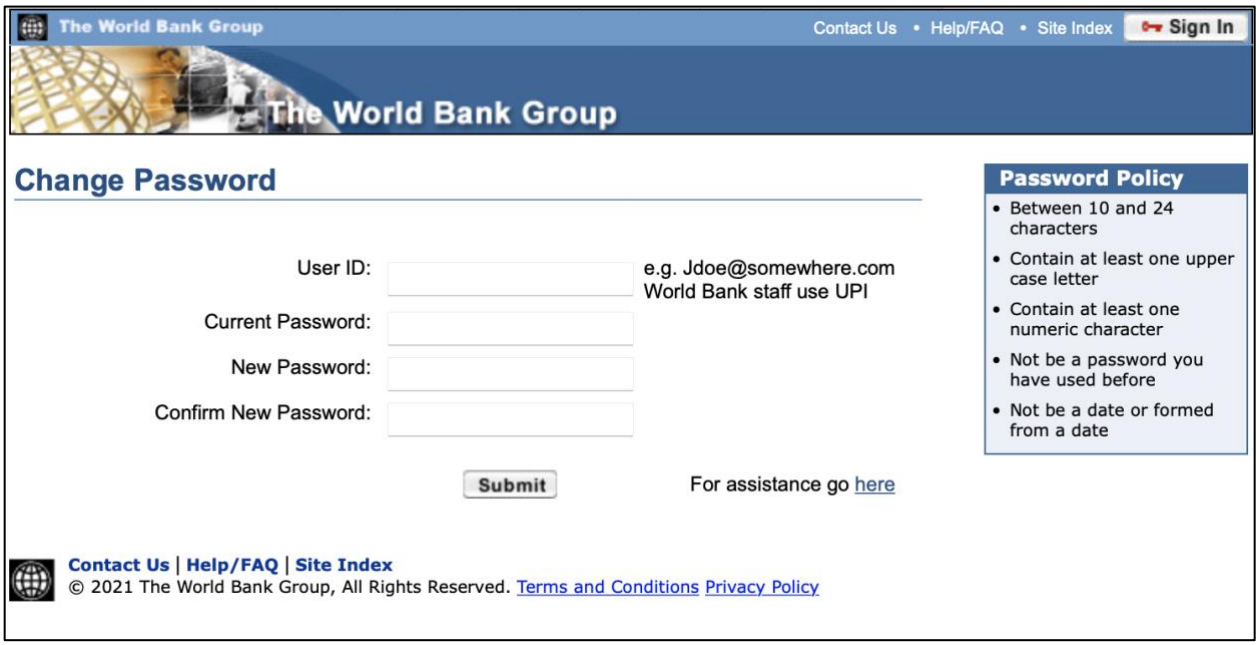
Source: (Leaked Source, 2016)

This demonstrates that LinkedIn users use an extremely basic password, such as "123456," which is exceedingly easy for a hacker to guess. LinkedIn should implement a password policy that requires users to use a strong password.

Good examples of strong user password

This is an example of a strong password of The World Bank Group in 2021.

FIGURE 3: WORLD BANK PASSWORD POLICY 2021



Source: (The World Bank Group, 2021)

Authorization. When a user is authenticated, the actions or privileges that person has are determined. If you want to access your mobile bank account, for example, once you've successfully signed in to your user account, you may read your profile, obtain your bank statement, perform transactions, and do a variety of other banking-related activities. Permission has been given for all of these activities. As a result, you've been given permission to carry them out.

Network controls

It is the process of safeguarding data transfer between networks. Network control includes things like firewalls, antivirus software, encryption, and virtual private networks.

A firewall is a network security device that monitors and filters inbound and outbound network traffic in accordance with an organization's security policy. A firewall is the barrier that divides a private internal network from the public Internet at its most basic level. A firewall's main objective is to let non-destructive traffic in while keeping dangerous traffic out.

Key findings: Data privacy

What is data privacy?

Data privacy relates to how a company controls who has access to sensitive data it collects, stores, and shares. Data privacy refers to the proper management, processing, storage, and use of personal information. In a nutshell, it's all about people's right to privacy.

What is the difference between data security and data privacy?

The mere fact that data is secure does not indicate that it is confidential. Similarly, just because information was collected in a way that protects privacy does not mean it is safe.

The difference between security and privacy is that security is concerned with safeguarding data from dangerous threats, whereas privacy is concerned with the responsible use of data. Because one of data security's aims is to avoid loss of privacy, data privacy is a subset of data security. There is no privacy in a database without security.

Why is data privacy important?

Because All sensitive information that firms manage, including that of customers, shareholders, and staff, is subject to data privacy issues. Furthermore, if personal data is not kept private or if people do not have control over how their information is used, it can be exploited in a variety of ways:

- Personal information can be used by criminals to scam or harass people.
- Without user consent, entities may sell personal data to marketers or other third parties, resulting in unwanted marketing or advertising.
- When a person's activities are followed and monitored, it might limit their freedom of expression, especially in authoritarian countries.
- When a person's activities are tracked and watched, it might restrict their freedom of speech, particularly in totalitarian nations.
- When a person's activities are tracked and watched, especially in authoritarian nations, it may limit their freedom of speech.
- Any of these effects can be damaging to persons. These outcomes can permanently damage a company's reputation and result in fines, penalties, and other legal implications.

How to protect the privacy of users?

As mentioned above, without data security, there will be privacy issues in the database. So, to protect the privacy of users,

1. We must ensure that the database is secure and well-controlled.
2. There are privacy laws in almost every country, and especially there is also privacy law passed by European Union EU.

Example of Privacy issue: Google Glass

Google Glass is a computer that can be worn. It resembles a pair of glasses, but it has a camera, microphone, and voice command capabilities. As a result, it can capture audio, video, and photos, as well as link to a smartphone to make phone calls, send texts, and read email.

What is the privacy risk posed by Google glass?

What if this glass is being worn by someone in your close surroundings? You may be uneasy about your actions since you don't know if they were recorded or not. The power to choose how and to whom one expresses oneself is referred to as privacy. If a person can't control who they're expressing themselves to, they'll change the way they express themselves. Individuals will be afraid of retaliation for non-conforming, unconventional, or unprofessional behavior if they do not

have control over their audience. Creativity, innovation, and self-discovery will be stifled as a result of this chilling impact.

Some questions to consider are:

- Who owns those data after generated by Google glass?
- What happens after they are captured?
- What if those data were leaked by a hacker?
- What if this glass was used by a stalker or a weirdo to record you?
- Will a stranger be able to recognize you using the glass's face recognition feature?

Google was discovered to be collecting data from unprotected WiFi networks all around the world in 2010. As a result of this behavior, many investigations against the company were conducted, and consumers were left perplexed. Following that, Google agreed to pay $7 million to 38 states to settle charges that it was gathering data from unencrypted Wi-Fi networks without permission. Google also admitted that it failed to safeguard user privacy adequately and that it has changed its procedures to address the issue.
In 2021, a Google glass named "GLASS ENTERPRISE EDITION 2" is still on the market, but it is exclusively available to developers, businesses, and enterprise clients.

Key findings: EU General Data Protection Regulation (GDPR)

What is GDPR?

The European Union devised and approved GDPR, the world's most stringent privacy and security regulation (EU). On May 25, 2018, the regulation came into action.

Does an organization always need user consent?

No, if an entity has a valid reason to use user personal data, it does not necessarily require user agreement. There are six valid grounds based on Article 6 of the GDPR:

1. Consent
2. Contract
3. Legal Obligation
4. Vital interests
5. Public task
6. Legitimate interests

What consent do you need store user personal data?

There are three concent that an organization need from user

1. Consent for Cookies
2. Consent for Sending Marketing Material
3. Consent for Third Party Marketing

Key finding: Intellectual Property Law

What is Intellectual Property Law?

Intellectual property refers to the product of human creativity in the industrial, scientific, literary, and artistic fields.

Why is Intellectual Property Law is important?

It is essential to understand what is intellectual property because:

- You must be aware of and value your rights as a creator of original works or ideas, whether you are an individual or an organization.
- To be aware of the methods for safeguarding and profiting from such work
- To be aware of legal options for defending against unauthorized usage of your work

How to protect Intellectual Property Law?

Patent

A patent gives you the legal right to create, use, sell, or import an invention for a specific period of time. The government grants patents to individuals or organizations who can show that their invention is novel, useful, or includes an innovative step.

software patent

A software patent is a property right that protects computer programs or computer performance. A software patent is a sort of utility patent that lacks a clear legal definition. Patents on software are a contentious matter in the United States and across the world.

Why does the software need a patent?

Patents on software can be strategically applied in a variety of ways. Patents can be utilized to block rivals from getting too close. When revenue is needed, patents can be licensed for added income streams. When companies need access to a competitor's technology, patents can be cross-licensed. Counterclaiming for breaking and then settling a patent infringement case is the most successful approach to get out of it, as demonstrated by Stac Electronics' $120 million patent infringement award against Microsoft for data compression or Apple's $1 billion verdicts against Samsung.

Copy right

Copyrights provide you the legal right to reproduce and distribute a literary, musical, audiovisual, or other work of authorship for a certain length of time. Copyright protection may apply to a database, but only under specific conditions.

To begin with, the structure of a database may be protected if it is the author's own intellectual production as a result of the contents' selection or arrangement.

Secondly, depending on what is contained in the database, copyright might exist independently in the contents of the database.

The owner of the copyright has the only right to:

- Copy the work
- Issue copies to the public

- Rent or lend to the public
- Communicate to the public
- Adapt or do any of these other acts in relation to an adaptation

Software Copyright

In 1976, the copyright legislation only applied to tangible items, but in 1980, it was expanded to include a definition of software. We can secure the software, but not the algorithm. Although copying the code is illegal, we may rewrite the algorithm in another programming language. Copyright just prevents copies from being made, yet it is insufficient to protect or safeguard. As a result, we must strengthen the security of our data.

Trademarks

Tradmeards means a term, phrase, design, or a mix of words and phrases that describes your products or services. It assists you with stopping others from using a similar trademark with related items or services by stopping others from registering the trademark without your permission.
The benefit of trademark protection is that it may be awarded for any product based on its uniqueness and originality. If a company's legal protection is revoked, it might maintain its market position by employing objects that develop into a trademark.

References

GPDR.EU, 2021. *GPDR.EU.* [Online]
Available at: https://gdpr.eu/tag/gdpr/
[Accessed 05 11 2021].
PrivacyPolicies, 2021. *PrivacyPolicies.* [Online]
Available at: https://www.privacypolicies.com/blog/gdpr-consent-examples/#When_Is_Consent_Required
[Accessed 08 11 2021].
Rainer, Prince & Cegielski, 2015. *Introduction to Information Systems.* 5th Edition ed. s.l.:John Wiley & SOns, inc..
Connolly, T. & Begg, C., 2015. *Database system: A practical aprroach to Design, Implementation, and Management.* 6th Edition ed. England: Pearson.
Grama, J. L., 2022. *Legal and Privacy Issues in Information Security.* 3rd Edition ed. Burlington: Jones & Bartlett Learning.
Google, n.d. *Glass.* [Online]
Available at: https://www.google.com/glass/start/
[Accessed 06 November 2021].
IBM Corporation, 2021. *https://www.ibm.com/downloads/cas/OJDVQGRY,* Armonk: IBM Corporation.
Leaked Source, 2016. *Blog:.* [Online]
Available at: https://leakedsource.ru/blog/linkedin
[Accessed 05 November 2021].
The World Bank Group, 2021. *Change Password.* [Online]
Available at: https://wbssoext.worldbank.org
[Accessed 5 November 2021].

UpCounsel Technologies, Inc., 2021. *Intellectual Property Law: Everything You Need to Know.* [Online]
Available at: https://www.upcounsel.com/intellectual-property-law
[Accessed 5 November 2021].
Tysver, D. A., 2021. *Guidance: WHY PROTECT SOFTWARE THROUGH PATENTS?.* [Online]
Available at: https://www.bitlaw.com/software-patent/why-patent.html
[Accessed 6 November 2021].
MILLER IP LAW, 2021. *Is software protected by copyrights or patents?.* [Online]
Available at: https://milleripl.com/blogs/patents/is-software-protected-by-copyrights-or-patents
[Accessed 6 November 2021].
Jeff, P., 2020. *Data Privacy Guide: Definitions, Explanations and Legislation.* [Online]
Available at: https://www.varonis.com/blog/data-privacy/
[Accessed 6 November 2021].
BBC, 2016. *Tech: Millions of hacked LinkedIn IDs advertised 'for sale'.* [Online]
Available at: https://www.bbc.com/news/technology-36320322
[Accessed 6 November 2021].
Data Privacy Manager, 2021. *Data Privacy vs Data Security [definitions and comparisons].* [Online]
Available at: https://dataprivacymanager.net/security-vs-privacy/
[Accessed 6 November 2021].
Epic.org, n.d. *Google Glass and Privacy.* [Online]
Available at: https://archive.epic.org/privacy/google/glass/
[Accessed 6 November 2021].
iPleader, 2021. *Blog: Data privacy vs. data security.* [Online]
Available at: https://blog.ipleaders.in/data-privacy-vs-data-security/
[Accessed 4 November 2021].