Nicole P. Satiembre **April 30, 2024**

Cebu Technological University - Main Campus

Data Security

Data security is the process of protecting sensitive information from unauthorized access. It includes all of the different cybersecurity practices you use to secure your data from misuse, like encryption, access restrictions (both physical and digital), and more. The largest portion of the direct costs associated with a data breach comes from the loss of business that follows. According to Interbrand, a brand valuation agency, a large part of a brand's value comes from "the role the brand plays in purchase decisions." In other words, strong brand equity can actually enhance your customers' willingness to pay for your products or services. A data breach could cause the customers to lose trust towards the brand and we don't want that to happen.

Data Security vs. Data Protection vs. Data Privacy

These three terms can often be confused with each other. Data security refers to protecting your data against unauthorized access or use that could result in exposure, deletion, or corruption of that data. Data protection refers to the creation of backups or duplication of data to protect against accidental erasure or loss. Data privacy refers to concerns regarding how your data is handled — regulatory concerns, notification, and consent of use, etc.

Data Security Compliance and Regulations

Most countries have strict data security regulations that companies must follow. Unfortunately, regulatory compliance is often difficult to navigate, as requirements change from country-to-country or region-to-region, so one of the best things you can do is to ensure you have knowledgeable counsel on hand who can help you navigate your legal requirements.

General Data Protection Regulation (GPDR)

The GDPR is the European Union’s data protection and privacy law that states that any organization that processes personal data should implement the “appropriate technical and organizational measures” to protect that data. This means requesting consent from users to collect their data, anonymizing that data to protect users in the event it’s breached, and following specific guidelines for notifying users in the event that a breach occurs.

Health Insurance Portability and Accountability

HIPAA is the United State’s data security and protection law for regulating electronically protected health information (ePHI). It was passed in 1996 to control and modernize individual health data management, including fraud and theft protection standards, how insurance companies can and can’t use it to charge individuals for their services, and more.

Sarbanes-Oxley Act (SOX)

Designed to increase the penalty for inaccurate or incomplete financial reporting. SOX mostly applies to public corporations and the way they disclose financial information. But there are a number of elements that also apply to private companies as well — for example, falsifying financial records or retaliating against employees who report financial crimes.

Federal Information Security Management Act (FISMA)

It requires that any federal agency follow strict information security policies and auditing procedures to ensure that they are followed.

The Top Threats to Data Security

The first thing that comes into our mind when thinking about data security threats are hackers but in reality, the top threats to data security are often internal and a result of the unsafe behaviors of your employees. One of the other top causes of data breaches (phishing scams) is also something the right employee training could prevent.

Types of Data Security Technologies

Authentication. Authentication is the process of verifying a user's login credentials (passwords, biometrics, etc.) to make sure it's really them. And it's one of the most important parts of your data security strategy because it's a frontline defense against unauthorized access to sensitive information.

Encryption. Data encryption scrambles sensitive information with an algorithm so that it can't be read by someone without the specific information (the encryption key) required to unscramble it. It's an incredibly important data security tool because it ensures that even if someone gains unauthorized access to your information, they won't be able to use it.

Tokenization. Tokenization is similar to encryption. However, instead of scrambling your data with an algorithm, tokenization replaces that data with random characters. The relationship to the original data (the "token") is then stored in a separate protected database table.

Data Masking. Data masking does not transform your data into an intermediate form but rather is achieved by "masking" your data's characters with proxy characters. Software reverses it once it;s delivered to its end destination.

Physical Access Controls. Data access control is an important part of your data security strategy, as well. And while digital access control is often managed through authentication procedures (and limiting the number of authorized users who have access to your data), physical access control manages access to the physical locations where your data resides.

Best Practices for Ensuring Data Security. A comprehensive data security plan has a lot of moving parts, all working together in real-time to ensure your data is safe. These are just an overview of the heavy-hitting concepts that come together to create a good foundation for data security. These concepts include: Securing your information, Preparing for threats, Deleting Unused Data, Run Compliance Audits.

Don't Forget Mobile Data Security.

There are several steps you can take to enhance your mobile data security:

- Regularly update all apps to protect against spyware threats.
- Delete inactive apps. (Providers could have suspended or removed access to them due to a security breach.)
- Before downloading new apps, check the list of permissions requested. If these seem too invasive, employees should skip the download because it could contain mobile malware.
- Create unique passwords for every new mobile account. Never default to standard logins.
- Use communication apps that encrypt data transfers to restrict access.
- Require multi-factor authentication to access internal tools.
- Make sure employees know how to access their devices remotely. If a device is lost or stolen, being able to quickly delete or transfer information is critical.

Data Security Depends on Humans

Encouraging the right behaviors is essential to ensuring that a breach doesn't happen. One of the best ways to do that is to create a better user experience for your team. A simplified user experience makes it much easier for them to follow cybersecurity best practices, like using unique passwords for each application or using longer, more complex passwords.