Data Security

Idea In Short

Data security protects company data from internal and external threats and is a critical element of business operations. This encompasses protecting digital information from multiple threats of unauthorized access, data corruption, or theft through its lifecycle. It's an all-encompassing term that covers hardware and its physical security and includes protection of storage devices, administrative controls, accessibility, and the safety of applications. It also covers company policies and protocols.

data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

When data security is planned and implemented correctly, a company's data assets are protected against multiple forms of cyber-criminal attacks. It also ensures that data is safeguarded from internal threats and possible human error–the latter continues to be a common cause of data breaches. The vast majority of data security breaches are caused by human error.

Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used.

As part of their data security procedures, companies deploy a range of tools and technologies to increase the visibility of their critical data and monitor its usage. These tools can protect encryption and data masking. Sensitive files are redacted, and reporting is automated to streamline audit procedures. All this helps with regulatory compliance.

Business value drivers

According to IBM1:

> The business value of data has never been greater than it is today. The loss of trade secrets or intellectual property [IP] can impact future innovations and profitability. So, trustworthiness is increasingly important to consumers, with a full 75% reporting that they will not purchase from companies they don't trust to protect their data.

Importance

Having high-end data security is essential as a breach can have dire consequences for a business. More often than not, a breach results in financial losses. The average cost of a data security breach is millions of dollars. Not only that, but most violations had a financial motivation behind them.

The most significant impact of a security breach on an organization is the financial harm. However, brand equity and the organization's brand value are also harmed. For large organizations, the impact could reach billions of dollars. Consumer surveys show that most consumers would terminate their relationship with a brand following a data security breach.

Hence, the impact of a data security breach on a company is enormous. Therefore, having solid protocols in place to ensure ongoing security is critical to a successful business.

Benefits

There are multiple benefits for organizations to invest in their data security.

Safeguard sensitive information

A company often collects a wide range of data that is not meant to be shared. These can be personal details of clients, vendors, customers, etc. Data security measures keep all kinds of information safe and within the confines of where it should be. Imagine if personal customer data was released. The consequences, both individually and for the organization, would be massive.

Protecting brand reputation

Today, people value their privacy more than ever and having a robust data security plan

helps build confidence across the organization and with all customers.

Competitive advantage

When an organization protects sensitive data from the prying eyes of hackers, it can stay ahead of the competition curve. Data leaks related to business plans can slow down business progress and development.

Cost savings

A business that does not have a good data security plan runs the risk of facing the consequences of that lapse. It may require additional investments to deal with the ramifications and invest more heavily in protecting the data in the long run. Plugging any security loopholes right at the beginning ensures that an organization does not incur these additional costs.

Avoid fines and lawsuits

When an organization is faced with a data breach, customers will opt for legal measures to protect their interests. This means that they can file legal cases against an organization, and if any non-compliance is found, it will be liable for fines. Additionally, the organization may have to pay compensation to their clients, not to mention the immense costs of a legal battle. The correct data security protocols can prevent this from happening.

Customer protection

An organization must ensure that the privacy and security of a customer's data is the ultimate pact. Not keeping this information safe can result in a loss of trust and business. Data security measures can prevent such things from happening.

Preventing data tampering

If cyber-criminals attack an organization, it's not always to steal data but could also to tamper with it. Hackers can delete, alter, and corrupt data. They can hijack processes with deadly Trojans or even introduce ransomware into information technology systems. The results can prove disastrous. Data security protocols protect a business to a large extent.

Unreliable data security systems can severely impact a business and affect day-to-day functioning. The problems can drip down the hierarchy with a domino effect leading to several complications. The need for solid data security protocols is critical.

Data Security Types

There are different kinds of data security measures, and each has a method or approach to implementation.

Data Encryption

In this security system, an algorithm scrambles text characters to an unreadable format so that authorized viewers can only read it. When there are volumes of sensitive information, solutions such as file and dataset encryption protect data with encryption or/and tokenization. Most of these solutions also come with security key management features.

Data Erasure

While data wiping is a standard procedure, it may not be thorough. This is where data erasure comes in. It utilizes software to overwrite data stored in any kind of device altogether. It verifies that data cannot be recovered. This is the modern-day equivalent of a letter self-destructing after being read.

One of the benefits of a data virtualization solution is that it doesn't store data so erasure is only required on the source systems. This enables additional governance and eliminates the potential of data inconsistency.

Data Masking

Here, personally identifiable information [PII] is masked so that various teams can continue developing applications and training recruits with accurate data. All development happens with actual data in compliant environments.

A data virtualization layer can also implement row and column based security based on users and roles at run time.

Data resiliency

Data resiliency is how fast an organization can spring back from a failure, whether hardware, power deficiencies or any other factor affecting team data availability. The speed of recovery is crucial to reducing the impact on the organization.

International laws and standards

International laws

In the UK, the Data Protection Act is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. This is particularly important to ensure individuals are treated fairly, for example for credit checking purposes. The Data Protection Act states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared.

Since the General Data Protection Regulation [GDPR] of the European Union [EU] became law on May 25, 2018, organizations may face significant penalties of up to €20 million or 4% of their annual revenue if they do not comply with the regulation.[10] It is intended that GDPR will force organizations to understand their data privacy risks and take the appropriate measures to reduce the risk of unauthorized disclosure of consumers' private information.

International laws

The international standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013 cover data security under the topic of information security, and one of its cardinal principles is that all stored information, i.e., data should be owned so that it is clear whose responsibility it is to protect and control access to that data. The following are examples of organizations that help strengthen and standardize computing security:

The Trusted Computing Group is an organization that helps standardize computing security technologies.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary international information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, automated teller machines, and point of sale cards.

The General Data Protection Regulation [GDPR] proposed by the European Commission will

strengthen and unify data protection for individuals within the European Union [EU], whilst addressing the export of personal data outside the EU.

Summary

Cyber-criminals are constantly evolving in the manner they launch attacks. With every new solution, the attacks get more sophisticated, and businesses need to ensure their data security can keep up. While there is no 100% fool-proof approach to data security, enhanced awareness among data users and proactive approach to data security will go a long way in protecting this valuable enterprise asset.