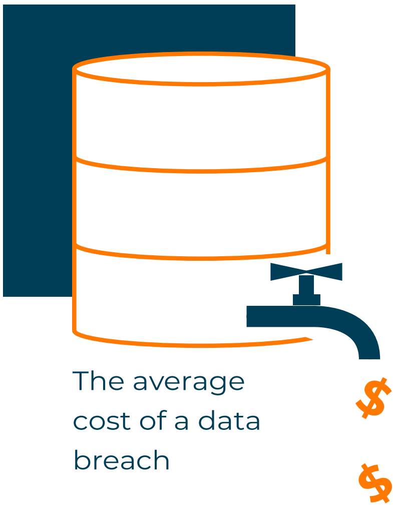
HUSH HUSH

Introduction to Data Masking and its Applications for Business

Contents

Introduction

$3.92 million



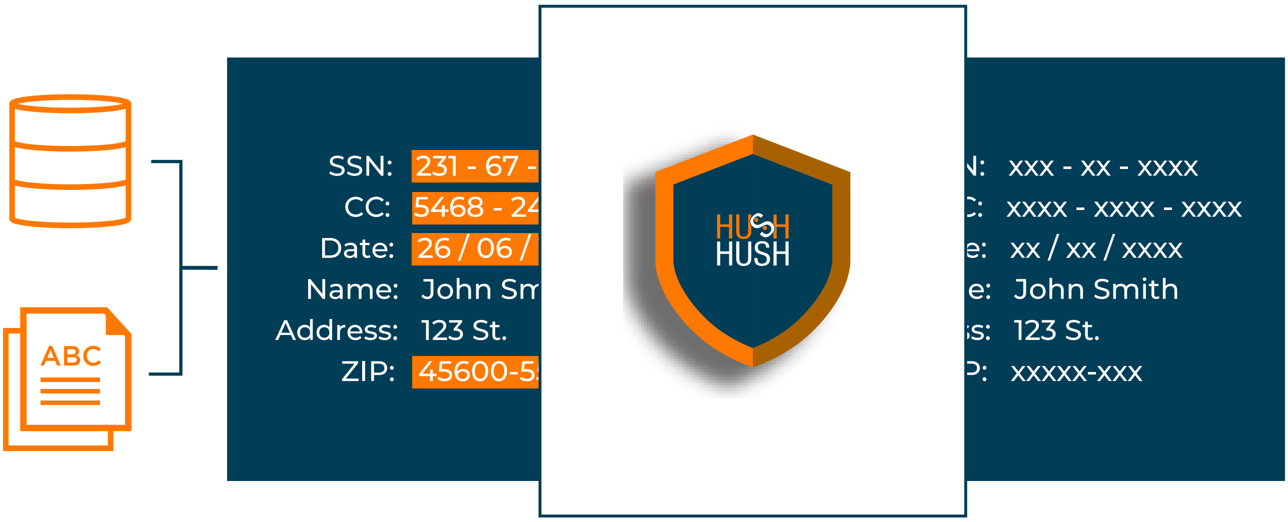
The average cost of a data breach

Data remains one of the most valuable assets a business can own, yet data breaches can cause devastating **reputational and financial damage**. According to IBM, the average cost of a data breach is $3.92 million. Protecting sensitive data has become a crucial business process, not just for the business, but for the consumer as well. More and more people are beginning to care about how their data is being used.

Having proper data privacy protection in place builds **loyalty and trust** with customers, and can make a company more attractive to investors. There are other benefits as well. According to recent research by Cisco that surveyed thousands of organizations worldwide, most businesses report very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend.

Data masking meets the **minimum compliance requirements** of numerous data privacy laws, such as GDPR and HIPAA, and can help organizations control the usage of data across the business. It also ensures secure continuous development, without the risk of disruption or data being misused.

What is data masking?



Static data masking is the process of hiding sensitive information by **replacing real values** with substitute “realistic” values. This method involves **anonymizing data** within a stable, non-changing environment that features a copy of the production database (usually called a “golden copy”). Unlike encryption, the original data cannot be retrieved.

This process protects the real data from being viewed by **changing the value** and ensures no **sensitive data** can be used outside of production. In this definition, sensitive data refers to personally identifiable information, protected health information, payment and credit card information, and intellectual property.

Data masking use cases span the entire **software development life-cycle**, from preventing insider threats and refreshing non-production environments, to end-user reporting for public agencies.

Data masking is also referred to as data anonymization, data de-identification, and data obfuscation.

On-the-fly (In Etl)

In certain stages of development, or if data has to be moved in real-time, masking algorithms can be used **on the fly**. This is a variation of SDM that does not involve a "golden copy" of the database.

Obfuscation – Extreme Masking

This involves removing sensitive values from files and databases altogether.

Data masking vs encryption

Both data masking and encryption are used to hide the data's **original values**. Yet, they are not the same, both by purpose and by implementation.

The **purpose** of encryption is to hide data from the hacker – an **external threat** with no access to encryption keys. The purpose of data masking is to hide data from the developer – an **internal threat**. The developer often has the encryption key.

During the **implementation** of encryption, information is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. The information does not change, but the presentation of the content does. With data masking, the information itself is changed in such a way that it presents as the same type, but the content differs entirely, rendering it **safe**.

Use cases

Data masking has become a mainstream method of protecting sensitive data in healthcare, financial, educational, government, and other types of organizations that collect and store sensitive personal data. Its many applications for the business environment are outlined below.

Protection against internal threats

According to Forrester, 53% of data breaches are the result of insider actions. Data masking proactively protects data from internal threats and allows you to control the access to information in your business.

Legislative compliance

Data masking meets the minimum compliance requirements of privacy legislation such as PCI, GDPR, CCPA, and HIPAA.

Third-party sharing

Data masking minimizes the risk of misuse of sensitive data when outsourcing or sharing with third parties as this data is effectively anonymized and cannot be used to identify individual customers or patients.

Data analytics

Data masking has a specific purpose when providing reporting in the public space. Data masking hides individual identities, transforms sensitive data into safe, but still useful data that can be applied for analytical purposes.

Privacy law

Data Masking is a key requirement in complying with **industry standards**. As the public demands a better degree of protection, the laws become more plentiful and stricter. Each country has its own legislature pertaining to data privacy. The following statutes reference the collection and private use of data in the United States.

General Data Protection Regulation (GDPR): extends to all businesses (including U.S. businesses) that offer goods and services to European residents and collect personal data in the process.

HIPAA: relates to protected patient health information such as patient history and identifiable information.

PCI/DSS: relates to payment platforms and the protection of payment information. With PCI DSS, it is mandatory to mask primary account numbers.

FERPA: The aim of the Family Educational Rights and Privacy Act is to protect the privacy of student education records.

GLBA: relates to the financial sector to ensure the security and confidentiality of customer records and information.

Privacy Shield*: set in motion by the U.S. Department of Commerce to govern the collection, use, and retention of personal data transferred from the EU, UK, or Switzerland to the United States, respectively.

PIPEDA: Covers the disclosure of personal information in the private sector in Canada.

California Consumer Privacy Act (CCPA): Gives residents of California more power over their personal data.

Benefits

The advantages of data masking over other forms of data security and protection methods include **maintaining data privacy**, ensuring **regulatory compliance** and mitigating against **insider threats**.

Unlike encryption, for example, data masking improves the cognitive aspect of development and is ideal for **ongoing, non-disruptive use** in non-production environments such as test, development, QA/demo, and staging.

Perhaps the most important benefit of safeguarding sensitive customer data, however, is increased **customer loyalty and reputational integrity**.

☑ **Mitigating against insider threats**

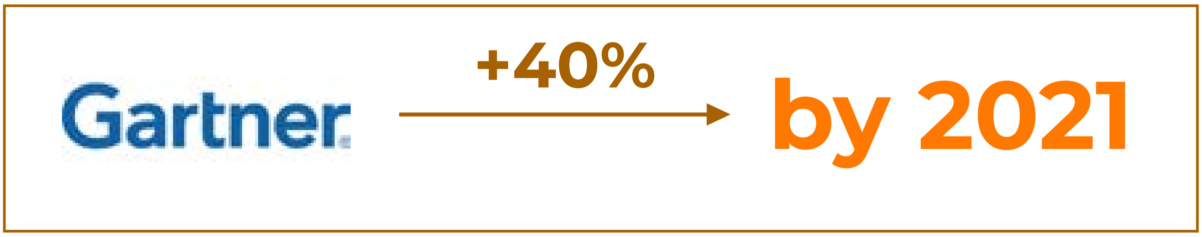
☑ **Maintaining data privacy**

☑ **Increased customer loyalty and reputation**

☑ **Improves the cognitive aspect of development**

☑ **Ensuring regulatory compliance**

Conclusion



Gartner

+40%

by 2021

Gartner predicts that the percentage of organizations using data masking will increase by 40% by 2021. Adopting data masking is one of the most effective, viable, and proven methods of safeguarding sensitive customer data in the business environment. Businesses can safely retain valuable data for testing and analytical purposes, whilst complying with the requirements of customers and legislation.

About HushHush

HushHush is a US-based technology provider of data masking and data discovery solutions for any organization that handles sensitive customer data.

The company was born as a trusted consultancy that specialized in data privacy and bespoke data masking solutions for financial institutions. After fourteen years, developing patented masking technology was a natural progression.

For more information visit https://mask-me.net

Contact details

General inquiries contact: info@mask-me.net
Sales: sales@mask-me.net
Call: (855) YOU HUSH

References

IBM Cost of a Data Breach Report (2019), https://www.ibm.com/security/data-breach

Cisco From Privacy to Profit: Achieving Positive Returns on Privacy Investments. Cisco Data Privacy Benchmark Study (2020), https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

Joseph Blankenship *(2019) Forrester, Insider Threat Gets Its Own National Awareness Month,* https://go.forrester.com/blogs/insider-threat-gets-its-own-national-awareness-month/

Gartner Market Guide for Data Masking (2019), https://www.gartner.com/en/documents/3975500/market-guide-for-data-masking

Footnotes*

* In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield, which allows the legal transfer of personal data between the EU and the U.S.