**ESI**

# Data security


## Introduction

**What stories do you think followed these headlines?**

- **Identity theft**
- **Transaction fraud**
- **Hacking**
- **Piracy**
- **Denial of Service attack (DoS)**

**What other types of computer crime are there?**

### 1. What is Data Security?

Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, logical controls, organizational standards, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.

### 2. Why is Data Security Important?

All businesses today deal in data to a degree. From the banking giants dealing in massive volumes of personal and financial data to the one-man business storing the contact details of his customers on a mobile phone, data is at play in companies both large and small.
The primary aim of data security is to protect the data that an organization collects, stores, creates, receives or transmits. Compliance is also a major consideration. It doesn't matter which device, technology or process is used to manage, store or collect data, it must be protected. Data breaches can result in litigation cases and huge fines,

not to mention damage to an organization's reputation. The importance of shielding data from security threats is more important today than it has ever been.

### 3. Different Data Security Technologies

Data security technology comes in many shapes and forms and protects data from a growing number of threats. Many of these threats are from external sources, but organizations should also focus their efforts on safeguarding their data from the inside, too. Ways of securing data include:

**Data encryption:** Data encryption applies a code to every individual piece of data and will not grant access to encrypted data without an authorized key being given

**Data masking:** Masking specific areas of data can protect it from disclosure to external malicious sources, and also internal personnel who could potentially use the data. For example, the first 12 digits of a credit card number may be masked within a database.

**Data erasure:** There are times when data that is no longer active or used needs to be erased from all systems. For example, if a customer has requested for their name to be removed from a mailing list, the details should be deleted permanently.

**Data resilience:** By creating backup copies of data, organizations can recover data should it be erased or corrupted accidentally or stolen during a data breach.

### 4. Data Security Solutions

Micro Focus drives leadership in **data security solutions** with over 80 patents and 51 years of expertise. With advanced data encryption, tokenization, and key management to protect data across applications, transactions, storage, and big data platforms, Micro Focus simplifies the protection of sensitive data in even the most complex use cases.

- Cloud access security – Protection platform that allows you to move to the cloud securely while protecting data in cloud applications.
- Data encryption – Data-centric and tokenization security solutions that protect data across enterprise, cloud, mobile and big data environments.
- Hardware security module -- Hardware security module that guards financial data and meets industry security and compliance requirements.
- Key management -- Solution that protects data and enables industry regulation compliance.
- Enterprise Data Protection – Solution that provides an end-to-end data-centric approach to enterprise data protection.
- Payments Security – Solution provides complete point-to-point encryption and tokenization for retail payment transactions, enabling PCI scope reduction.

**ESI**

- Mobile App Security - Protecting sensitive data in native mobile apps while safeguarding the data end-to-end.
- Web Browser Security - Protects sensitive data captured at the browser, from the point the customer enters cardholder or personal data, and keeps it protected through the ecosystem to the trusted host destination.
- eMail Security – Solution that provides end-to-end encryption for email and mobile messaging, keeping Personally Identifiable Information and Personal Health Information secure and private.

**Tokenization** is the process of converting a sequence of characters (such as in a computer program or web page) into a sequence of tokens (strings with an assigned and thus identified meaning)

**PCI (**Peripheral Component Interconnect) is a standard for connecting computers and their peripherals.

https://www.forcepoint.com/cyber-edu/data-security
https://www.microfocus.com/en-us/what-is/data-security