What is data security? The ultimate guide

March 2023

TechTarget

In this guide:

Data is central to most every element of modern business -- employees and leaders alike need reliable data to make daily decisions and plan strategically. This guide to explores risks to data and explains the best practices to keep it secure throughout its lifecycle.

In this guide:

What is data security? The ultimate guide

SHARON SHEA, EXECUTIVE EDITOR

Data security is the practice of safeguarding digital information from unauthorized access, accidental loss, disclosure and modification, manipulation or corruption throughout its entire lifecycle, from creation to destruction.

This practice is key to maintaining the confidentiality, integrity and availability of an organization's data. *Confidentiality* refers to keeping data private, *integrity* to ensuring data is complete and trustworthy, and *availability* to providing access to authorized entities.

Known collectively as the CIA triad, if any of the three components is compromised, companies can face reputational and financial damage. The CIA triad is the basis upon which a data security strategy is built. Such a strategy must encompass policies, technologies, controls and procedures that protect data created, collected, stored, received and transmitted by an enterprise.

WHY IS DATA SECURITY IMPORTANT?

Data is the lifeblood of every organization. It informs decision-making, finds solutions to problems, improves the efficiency and efficacy of operations, boosts customer service and

informs marketing efforts, reduces risks, increases productivity, enhances collaboration and, in the end, is instrumental in increasing revenue and profit.

Data is often referred to as a company's crown jewels; for something so essential, its protection must be taken seriously.

Much like Coca-Cola's secret recipe that is locked away in a vault, Hershey's secret lab that concocts its famous Kisses and KFC's famous yet unknown 11 herbs and spices, it is crucial to keep certain data from prying eyes. It's not always as easy as putting something under lock and key -- especially in a digital environment. Multiple employees, stakeholders and partners need access to the data that enterprises value so highly. But more people having access means more chances for things to go wrong.

Data breaches, which occur when data is accessed in an unauthorized manner, are a major concern for organizations of all shapes, sizes and industries. In fact, 63% of respondents to a KPMG study said they suffered a data breach or cyber incident in 2021 -- and that number is only projected to grow.

Data breaches are attributed to a number of cyber incidents, including the following:

- accidental leaks or exposures
- phishing attacks

- distributed denial-of-service attacks
- physical breaches
- lack of access controls
- backdoors

Even the largest and most well-known companies are susceptible to breaches, as evidenced in the 10 biggest data breaches in history.

Data breaches can result in hefty remediation costs, as well as expenses stemming from downtime and lost business. Regulatory and legal fines may also be levied. In worst-case scenarios, companies can go bankrupt or out of business.

Data security is an important component in data compliance, the process that identifies governance and establishes policies and procedures to protect data. The process involves selecting applicable standards and implementing controls to achieve the criteria defined in those standards. Regulatory compliance -- which refers to organizations following local, state, federal, international and industry laws, policies and regulations -- is related to data compliance. Regulatory compliance standards require the use of certain controls and technologies to meet the criteria defined in them. The following are some of the most common compliance regulations:

- PCI DSS
- HIPAA
- Federal Information Security Modernization Act of 2014
- Sarbanes-Oxley Act
- GDPR
- CCPA

HIPAA, for example, outlines provisions to safeguard medical information in the U.S. Among other mandates, healthcare organizations must adhere to standards for patient data security or else face noncompliance fines and penalties. PCI DSS is a global standard aimed at protecting credit, debit and cash card transaction data. It sets guidelines for cardholder data, access controls and networks that process payment information.

Many regulations are subject to audits, during which organizations must prove they adhere to the policies set out in a given regulation.

Beyond preventing breaches and complying with regulations, data security is important to maintaining customer trust, building relationships and preserving a good company image. It is also key to sustaining a competitive advantage. After all, if everyone had the recipe and the means to make Hershey's Kisses, the chocolatier would be out a considerable amount of money.

TYPES OF DATA SECURITY

Before an organization can secure data, it has to know what data it has. This is where a data inventory -- a record of all the data created, used and stored by a company -- is key. The process starts with data discovery, or learning what and where the data is. Data classification follows, which involves labeling data to make it easier to manage, store and secure. The four standard data classification categories are as follows:

1. public information
2. confidential information
3. sensitive information
4. personal information

Data is often further broken down by businesses using common classification labels, such as "business use only" and "secret."

Sensitive data is often classified as confidential or secret. It includes these types of data:

- personally identifiable information
- protected health information
- electronic protected health information
- PCI data
- intellectual property

Compounding the difficulty of doing data inventory and classification is that data can reside in many locations -- on premises, in the cloud, in databases and on devices, to name a few. Data also can exist in three states:

1. *in motion*, meaning data that is being transported;
2. *at rest*, meaning data that is being stored, or data that is at its destination -- i.e., not transported or in use; and
3. *in use*, meaning data that is being written, updated, changed and processed -- i.e., not being transported or stored.

Andrew Froehlich, network security expert and president of West Gate Networks, offers best practices on how to secure data in each state.

Because no single form of data exists, no single magic-bullet technique can secure all data. A defense-in-depth data security strategy is made up of a combination of tools, techniques and policies. Must-have data security technologies include the following:

- encryption
- data masking
- access control
- data loss prevention (DLP)
- data backup and resiliency

In this guide:

Encryption

Encryption is the process of converting readable plaintext into unreadable ciphertext using an encryption algorithm, or cipher. If encrypted data is intercepted, it is useless as it cannot be read or decrypted by anyone who does not have the associated encryption key.

Symmetric and asymmetric encryption are two commonly used ciphers:

- Symmetric encryption uses a single secret key for both encryption and decryption. The Advanced Encryption Standard is the most commonly used algorithm in symmetric key cryptography.

- Asymmetric encryption uses two interdependent keys: a public key to encrypt the data and a private key to decrypt the data. The Diffie-Hellman key exchange and Rivest-Shamir-Adleman are two common asymmetric algorithms.

Both symmetric and asymmetric encryption have pros and cons. Security expert Michael Cobb explains the differences between the ciphers and discusses why a combination of the two might be the fastest, most secure encryption option.

Data masking

Data masking involves obscuring data so it cannot be read. Masked data looks similar to the authentic data set but reveals no sensitive information. Legitimate data is replaced so the masked data maintains the characteristics of the data set as well as referential integrity across systems, thereby ensuring the data is realistic, irreversible and repeatable.

Below are some common data masking techniques:

- scrambling
- substitution
- shuffling
- data aging
- variance
- masking out
- nullifying

Data masking is useful when certain data is needed for software testing, user training and data analysis -- but not the sensitive data itself.

While the end result of encryption and masking are the same -- both create data that is unreadable if intercepted -- they are quite different. Expert Cobb outlines the key differences between the two, as well as use cases for each.

Access control

One of the best ways to secure data is to control who has access to it. If only authorized individuals can view, edit and delete data, it is inherently safer than an access free-for-all.

Access control involves two main processes:

1. Authentication is the process of ensuring users are who they say they are.
2. Authorization is the process of ensuring authenticated users have access to the necessary data and resources.

Authentication and authorization are components of an enterprise identity and access management (IAM) strategy. Other fundamental IAM processes and techniques include multifactor authentication (MFA), principle of least privilege access, role-based access control and privileged access management. Also important is following password hygiene best practices, such as setting minimum password lengths, requiring unique passwords and

considering regular password changes. Take a deep dive into these topics and more in our IAM guide.

Using a zero-trust access control strategy is growing in popularity. This framework provides stringent access control on a continuous basis. Get the lowdown on this up-and-coming trend in our guide to zero trust.

Data loss prevention

An integral tool for any enterprise security strategy is a DLP platform. It monitors and analyzes data for anomalies and policy violations. Its many features can include data discovery, data inventory, data classification and analysis of data in motion, at rest and in use. Many DLP tools integrate with other technologies, such as SIEM systems, to create alerts and automated responses.

Karen Scarfone, principal consultant at Scarfone Cybersecurity, explains more about the common capabilities of DLP tools and discusses the features, pros and cons of the top seven DLP options.

Data backup

Data backup involves creating copies of files and databases to a secondary, and often tertiary and quaternary, location. If the primary data fails, is corrupted or gets stolen, a data backup ensures it can be returned to a previous state rather than be completely lost. Data backup is essential to disaster recovery plans.

Learn more in our data backup guide.

Resilience is another strategy growing in popularity. The ability of an organization to adapt and recover following a cyber incident equates to how resilient it is. Read up on this up-and-coming topic from IT consultant Paul Kirvan and get help conducting a data resilience assessment.

DATA SECURITY VS. DATA PRIVACY VS. DATA PROTECTION

Data security, data privacy and data protection are overlapping but technically distinct concepts.

Data security. Data security has a broader scope, aiming to protect digital information not just from unauthorized access but also from intentional loss, unintentional loss and

corruption. While data privacy primarily focuses on the confidentiality part of the CIA triad, data security is equally concerned with information's integrity and accessibility.

For example, imagine threat actors obtain a confidential file, but encryption successfully prevents them from reading the data. The information itself stays inaccessible, and data privacy remains intact. The attackers are still able to corrupt or destroy the illegible file, however, which is a security failure.

Data privacy. The goal of data privacy is to make sure the ways an organization collects, stores and uses sensitive data are responsible and in compliance with legal regulations. Privacy policies and measures prevent unauthorized parties from accessing data, regardless of their motivation and whether they are internal end users, third-party partners or external threat actors.

Data protection. Data protection ensures digital information is backed up and recoverable if it's lost, corrupted or stolen. Data protection is an important part of a larger data security strategy, serving as a last resort if all other measures fail.

WHAT ARE DATA SECURITY RISKS AND CHALLENGES?

In 2017, *The Economist* declared, "The world's most valuable resource is no longer oil, but data." Unfortunately, data is more difficult to protect and easier to steal, and it presents enormous opportunity to not just businesses but also criminals.

Today's enterprises face an uphill battle when it comes to securing their data. Consider the following perennial risks and challenges.

In this guide:

Insider threats. One of the biggest threats to data security is the enterprise end user, whether that's a current or former employee, third-party partner or contractor. Malicious insiders sometimes use their legitimate access privileges to corrupt or steal sensitive data, either for profit or to satisfy personal grudges.

Unintentional insider threats are no less dangerous. An innocent click on a link in a phishing email could compromise a user's credentials or unleash ransomware or other malware on corporate systems. In fact, in nearly 40% of data breaches, attackers used either compromised credentials or phishing as initial attack vectors, according to the Ponemon Institute's 2021 "Cost of a Data Breach" report, sponsored by IBM.

Simple end-user negligence or carelessness -- absent any malicious threat actor -- can also result in accidental exposure of sensitive data. An employee might email confidential information to the wrong person, for example, or upload it to an unprotected cloud account. In addition, someone could lose a laptop and fail to report it to IT, leaving the device vulnerable to whoever happens to find it.

Misconfigurations. Technical misconfigurations pose another major threat, regularly resulting in accidental exposure of confidential data sets. The Ponemon Institute found cloud misconfigurations alone were responsible for 15% of data breaches in 2021.

Third-party risk. An organization is arguably only as secure as its least secure third-party partner, whether that's a supplier, contractor or customer. Consider the infamous Solarwinds supply chain attack, which enabled threat actors to target the vendor's customers' networks. Organizations point to vulnerable third-party software as the initial attack vector in 14% of data breaches, according to the Ponemon Institute.

Other top data security challenges organizations face today include mushrooming enterprise data footprints, inconsistent data compliance laws and increasing data longevity, according to cybersecurity expert Ashwin Krishnan.

DATA SECURITY BEST PRACTICES: HOW TO SECURE DATA

To effectively mitigate risk and grapple with the challenges listed above, enterprises should follow established data security best practices. According to Charles Kolodgy, principal at cybersecurity advisory firm Security Mindsets, organizations must start with an inventory of what data they have, where it is and how their applications use it. Only once they understand what needs protecting can they effectively protect it.

Formal data risk assessments and regular security audits can help companies identify their sensitive data, as well as how their existing security controls might fall short.

Next, enterprises should weigh how they will close any data security gaps they have flagged. Experts recommend considering tools, technologies and techniques such as the following:

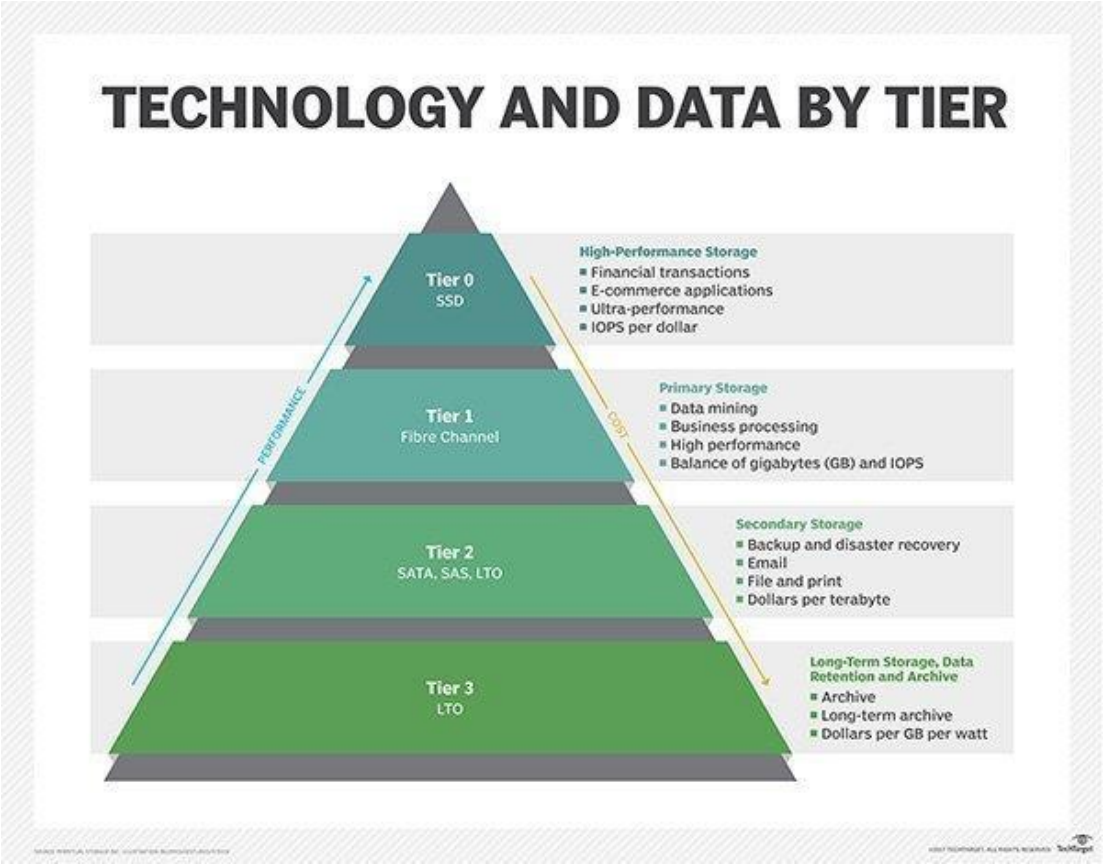
- **Access control.** Regardless of data's location and state, the ability to limit who can read, edit, save and share it is the bedrock of data security.
- **Cloud security.** While cloud use has significant benefits, such as scalability and cost savings, it also carries plenty of risk. Enterprises that use SaaS, IaaS and PaaS must

contend with a number of cloud security concerns, including credential and key management, data disclosure and exposure, and cloud storage exfiltration.
    - Expert Dave Shackleford, principal consultant at Voodoo Security, explains how organizations can achieve data security in cloud computing using encryption, MFA, cloud access security brokers, IAM and more.

- **Data backup.** The best advice is to expect the best and plan for the worst. Data backup acts as an insurance policy in case digital information is corrupted, lost or stolen, as in the case of a ransomware attack.
- **Data encryption.** If access control is the bedrock of a data security policy, then encryption is the cornerstone. Experts say it should be non-negotiable for sensitive data, whether at rest, in use or in transit. If access control fails and an unauthorized entity views a confidential file, encryption makes its contents illegible.
- **Data masking.** Data masking complements data encryption by selectively replacing sensitive digital information with fake information. This is helpful if an organization needs to share a nonconfidential version of data with certain users, for reasons such as database administration, research and development, software testing and user training.
- **Database security.** If an organization's most sensitive data sets are its crown jewels, then its databases should be as impenetrable as the Tower of London. Cybersecurity expert Mike Chapple shares best practices for keeping databases secure, including enforcing the principle of least privilege, conducting regular access reviews and monitoring database activity.
- **DLP.** Data loss prevention plays a critical role in enforcing data security policies at a granular level -- blocking a user from emailing or downloading a protected file, for example. DLP can prevent unauthorized access and alert cybersecurity staff to violations and suspicious behavior.

- **Data lifecycle management.** DLM is an automated approach to keeping massive amounts of digital information accurate, confidential, secure and available -- and destroying it in a safe and timely fashion, in keeping with enterprise policies -- all while meeting relevant compliance requirements. DLM policies are based on data attributes such as type, size, age and classification. The main phases of the data lifecycle in a DLM framework include the following:
    - generation and collection
    - processing and storage
    - usage
    - archiving
    - destruction

In this guide:



- **Patch management.** Leaving a known vulnerability unpatched is like failing to fix a broken lock on the side door of an otherwise secure home. Patch software quickly and often to limit the ways attackers can gain access to enterprise property.
- **Security awareness training.** Intentional and unintentional mistakes of staff, contractors and partners represent one of the greatest threats to data security.

Security awareness training is therefore of utmost importance to educate users on organizational security policies and topics such as phishing attacks.

- **User behavior analytics.** UBA, also known as user and entity behavior analytics (UEBA), flags attempts to gain unauthorized or unusual levels of access to sensitive data. Among top UEBA use cases, the technology can help detect lateral network attacks, identify compromised user accounts and uncover insider threats.

How to create a data security policy

It's important to develop an overarching strategy for deploying data security tools, technologies and techniques such as those listed above. According to consultant Kirvan, every enterprise needs a formal data security policy to achieve the following critical aims:

- codify data security expectations and responsibilities; and
- demonstrate compliance with relevant data privacy and security laws and standards.

Explore key elements of a data security policy and download our editable template.

Prepare for the worst

When it comes to data security, an ounce of prevention is worth a pound of cure. But while following best practices can help prevent a data breach, it can't guarantee one won't occur. Organizations therefore also need to develop thorough breach response plans to manage and minimize the financial, legal and reputational fallout if preventive measures fail.

In this guide:

CONTINUED READING

The importance of data security in the enterprise

5 data security challenges enterprises face today

How to create a data security policy, with template