TechTarget | SearchSecurity

E-guide

PRO+ Content

Data Security Guide: Everything You Need to Know

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

In this e-guide:

This data security guide digs into data protection and privacy compliance, explaining how to construct a proactive security strategy strengthened by best practices.

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

Data security guide: Everything you need to know

Sandra Gittlen, *Editor at Large, SearchSecurity*

Data security is one of the most daunting tasks for IT and infosec professionals. Each year, companies of all sizes spend a sizable portion of their IT security budgets protecting their organizations from hackers intent on gaining access to data through brute force, exploiting vulnerabilities or social engineering. Throughout this guide are links that will help you learn more about the challenges related to securing sensitive data, ensuring compliance with government and industry mandates, and maintaining customer privacy. Along with the challenges, you'll find advice on how to solve them.

Why data security is important

The average cost of a data breach in 2019 was calculated at $3.92 million, according to a report by the Ponemon Institute and IBM Security. High-profile companies such as Capital One, Evite and Zynga experienced data breaches that exposed more than 100 million customer accounts each. The average security incident in 2019 involved 25,575 accounts, according to the report. To make matters worse, this information must be disclosed to customers, and organizations could potentially wind up as cautionary tales.

The lessons from these breaches are numerous, including the need to do the following:

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

- review credential requirements and policies;
- keep track of what data is retained and where it is stored;
- check for cloud misconfigurations regularly; and
- force password resets if a breach is suspected.

The move to the cloud presents an additional threat vector that must be well understood in respect to data security. The 2019 SANS State of Cloud Security survey found that 19% of survey respondents reported an increase in unauthorized access by outsiders into cloud environments or cloud assets, up 7% since 2017. Ransomware and phishing also are on the rise and considered major threats. Companies must secure data so that it cannot leak out via malware or social engineering.

Breaches can be costly events that result in multimillion-dollar class action lawsuits and victim settlement funds. If companies need a reason to invest in data security, they need only consider the value placed on personal data by the courts.

Sherri Davidoff, author of *Data Breaches: Crisis and Opportunity*, listed five factors that increase the risk of a data breach: access; amount of time data is retained; the number of existing copies of the data; how easy it is to transfer the data from one location to another -- and to process it; and the perceived value of the data by criminals.

Many organizations realize that the value of data and the cost to protect data are increasing simultaneously, making it near impossible to protect data by just layering on

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

more security. Instead, IT and infosec teams must think proactively and creatively about their data protection strategies.

They should also assess their risk versus the protections their current security investments provide and make decisions accordingly. To do so requires an unprecedented level of visibility that most organizations do not possess right now.

Security expert Ashwin Krishnan advised IT and security professionals to focus on three key aspects when trying to improve data security in the modern enterprise: the more data generated and collected presents a bigger "surface" for data breaches; customer rights expand with new regulatory compliance and privacy compliance mandates, such as GDPR and the California Consumer Privacy Act; and companies have to be aware if they are involved in data brokering.

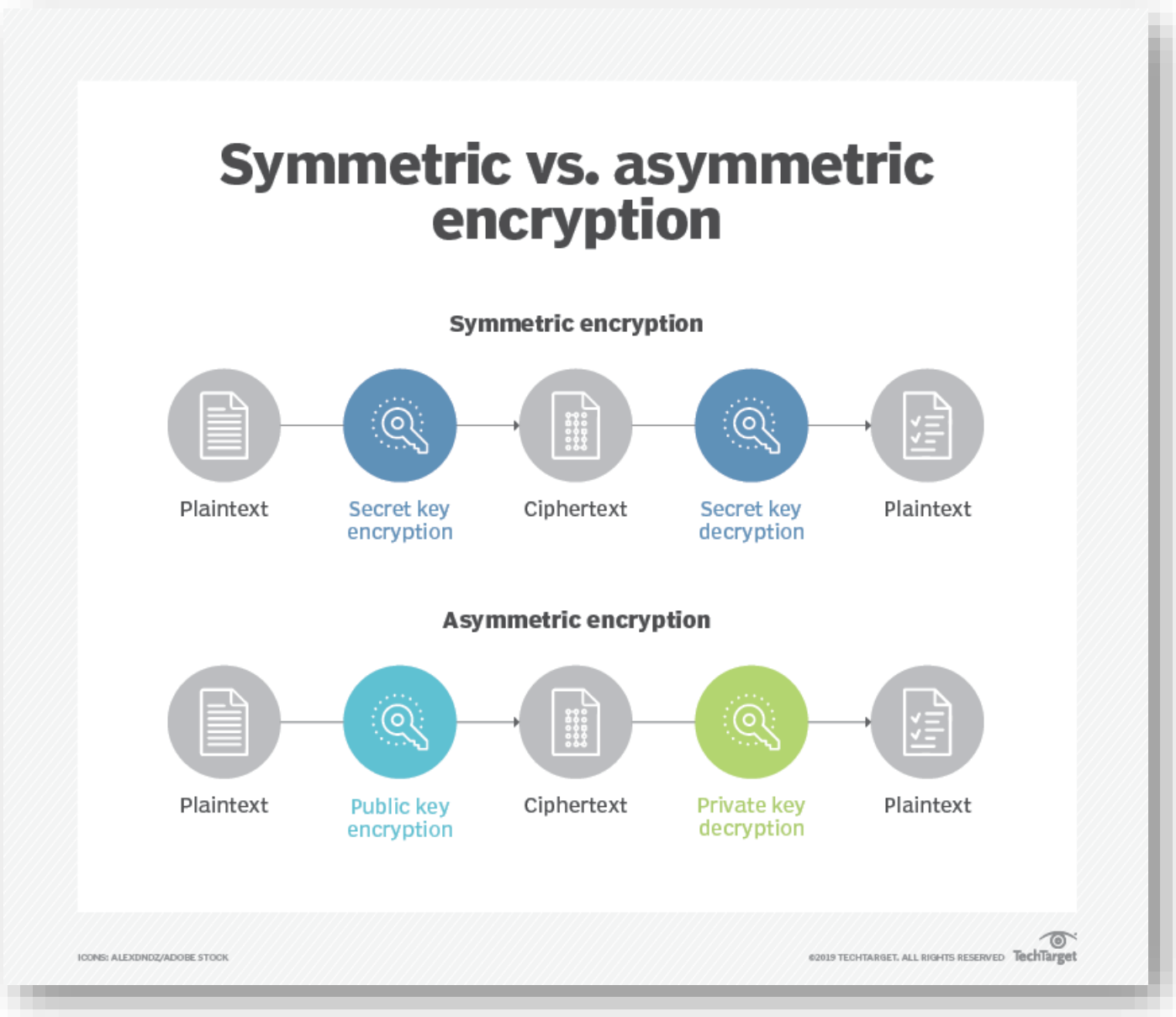
Types of data security

Data security has myriad aspects that protect information at rest, in motion and in use. Here are some technologies widely used by enterprises to protect data.

Image on the next page

In this e-guide

- Data security guide: Everything you need to know p. 2
- Why data security is important p. 2
- Types of data security p. 4
- Best practices for developing a data security strategy p. 8
- Data privacy and compliance standards p. 14
- The future of data security p. 15
- Further reading p. 17



In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

Encryption

One of the most basic concepts of data security is encryption, as simply encrypting sensitive data can go a long way toward meeting privacy and compliance mandates and keeping sensitive information safe from hackers.

Encryption is not a one-size-fits-all proposition, as organizations must select the encryption algorithm that matches their enterprise security requirements. Our encryption tutorial deciphers the differences and helps you select the best approach for your organization.

The most common form of encryption -- symmetric -- involves converting plaintext to ciphertext using the same key for encryption and decryption. Asymmetric encryption uses two interdependent keys -- one to encrypt the data and one to decrypt it. Symmetric encryption has many "flavors," including Advanced Encryption Standard and Triple DES. Asymmetric has the Diffie-Hellman key exchange and RSA, among others. Companies that don't want to encrypt all their information must determine the priority of data through classification.

Perimeter security

Intrusion detection systems and intrusion prevention systems, along with access control lists, beef up an organization's security perimeter and reduce the severity of attacks that get through. Meanwhile, endpoint security management can track malware signatures and prevent them from causing harm. Networking expert Kevin Tolly explained the need for a multipronged approach to data security, as well as the unique traits of fast-and-frontal attacks compared to low-and-slow attacks.

In this e-guide

- Data security guide: Everything you need to know p. 2
- Why data security is important p. 2
- Types of data security p. 4
- Best practices for developing a data security strategy p. 8
- Data privacy and compliance standards p. 14
- The future of data security p. 15
- Further reading p. 17

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

Data loss prevention (DLP)

DLP prevents users from transferring sensitive data, and organizations can roll it out as enterprise security software. DLP tools can be deployed as agents on endpoints or agentless at the network level. Learn how to choose DLP products as well as considerations for DLP deployment.

DLP software often includes templates to aid compliance with specific mandates, such as HIPAA and PCI DSS.

A cloud access security broker (CASB) also performs DLP tasks and can help mitigate the threat to data in the cloud. CASBs actively intervene in user-to-cloud application sessions by intercepting session traffic, helping to monitor and enforce corporate security policies. CASBs scan data objects, such as files and documents, to ensure they comply with corporate standards and government regulations.

Best practices for developing a data security strategy

Data security, often thought to be about the prevention, detection and mitigation tools an organization uses, is just as much about strategy and the implementation of best practices. A good start to developing a strategy lies in focusing on the following areas.

Governance, risk and compliance (GRC)

Some companies use GRC as a framework for ensuring data security and privacy compliance. *Governance* refers to how a company uses information management

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

systems and hierarchical controls to ensure adherence. *Risk management* is the identification, analysis and response to potential risks. *Compliance* is the assurance of conformity to regulations and corporate policies when handling data. Integrated risk management takes GRC a step further to speed up decision-making and performance.

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

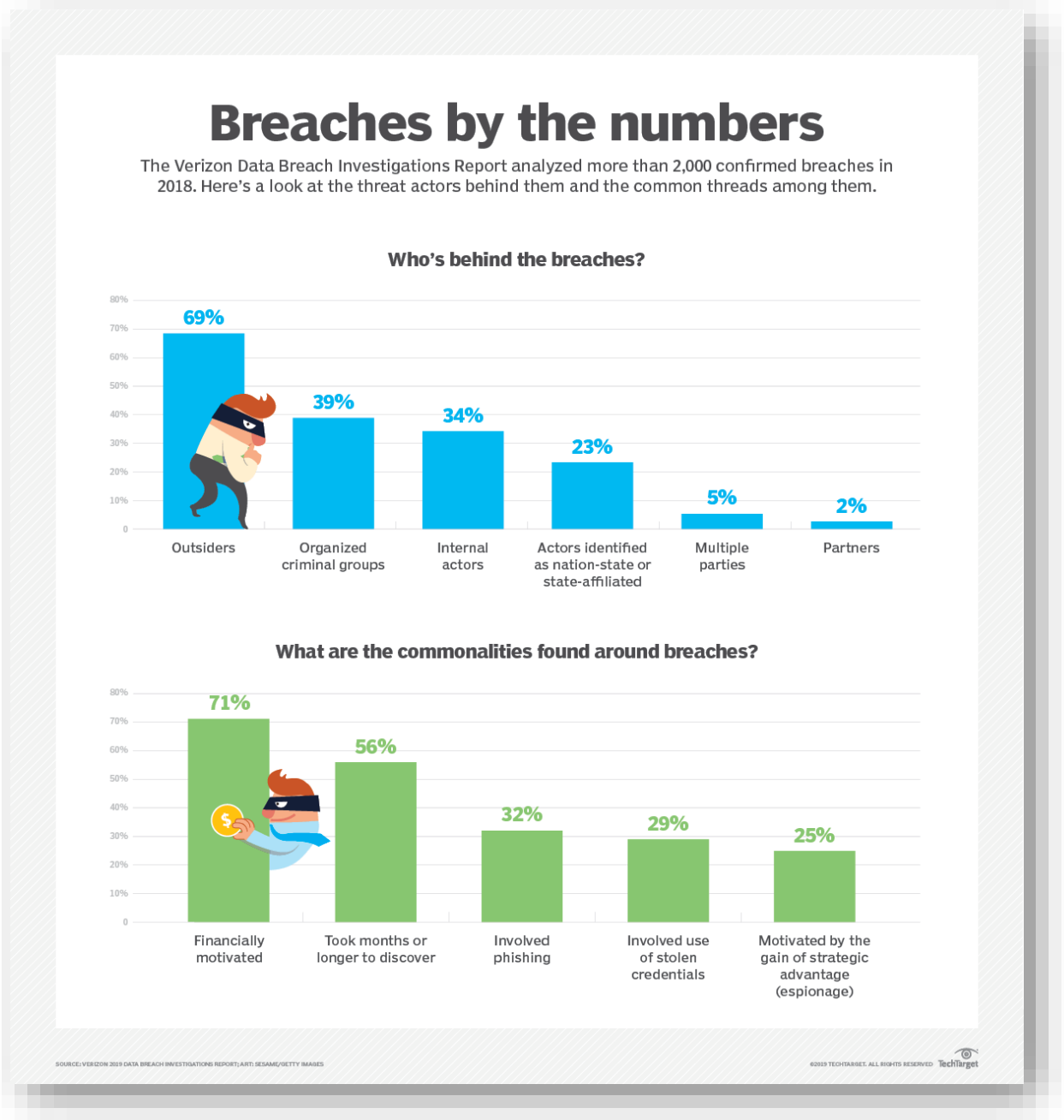
Insider threats

The human aspect -- or insider threat -- is often underestimated or even overlooked when companies develop a data security strategy. Privacy and risk management expert Sudeep Venkatesh said targeted phishing attacks and business email compromise attacks, which are aimed at top people in the organization, cause the most harm in terms of data loss. To combat this trend, companies should enact best practices that marry prevention and protection so that communication is secured and delivered to the appropriate person. If no action is taken, companies are left vulnerable to breaches initiated by an action taken by an insider -- whether malicious or accidental.

Image on the next page

In this e-guide

- Data security guide: Everything you need to know p. 2
- Why data security is important p. 2
- Types of data security p. 4
- Best practices for developing a data security strategy p. 8
- Data privacy and compliance standards p. 14
- The future of data security p. 15
- Further reading p. 17



In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

Social media

Social media is another vector users fall prey to when it comes to inviting malware into the enterprise. For instance, hackers will take advantage of users who search for "cheat codes" to access third-party applications, such as games on platforms like Facebook, for free. The cheat codes can be Trojans that enable a bad actor to control a device, install ransomware, activate the camera or microphone, and record keystrokes to steal passwords. Third-party applications are just one of many enterprise social media risks that should be monitored and mitigated.

Visibility and discovery

Organizations also stumble on the data governance front when they are unable to locate critical data that lives in nooks across the enterprise. For instance, protecting data is a Herculean task when users can download sensitive information onto their hard drives and out-of-sight of compliance tools. Government regulations and corporate standards are pushing companies to gain better visibility into how they are handling, storing and processing data.

Cloud-based data also requires a discovery mechanism to ensure governance. Before deploying any project into the cloud, IT and security teams should understand the data types that will be involved, and they should each be categorized and assessed for risk.

Password hygiene

One of the more straightforward data security best practices is centered around passwords, which are a universal point of vulnerability for organizations. The 2019 Verizon Data Breach Investigations Report found that 80% of hacking-related breaches

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

can be linked to stolen and reused credentials. Password spraying, keylogger attacks and other brute-force hacking techniques put on full display the weakness of traditional passwords. In addition, most users have far too many business application passwords to easily remember, resulting in poor password hygiene, which means not being unique enough or changed often enough.

Making passwords longer isn't necessarily the answer. They need to be more complex or be used in conjunction with tokens, biometrics or other types of authentication. Users also can deploy enterprise password managers, which store the encrypted passwords they use across applications, to ease the burden of remembering every application's sign-on.

Database protection

Databases require best practices to secure the data within them as well. Four simple steps can ensure sensitive information stays protected:

1. Enforce the principle of least privilege where access is limited to what is needed to carry out a job function.
2. Conduct regular access reviews to identify old and unnecessary permissions that could be compromised.
3. Monitor database activity to detect unusual user activity.
4. Encrypt sensitive data to protect it in transit and at rest to prevent snooping.

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

Data privacy and compliance standards

Developing, implementing and enforcing data security best practices is made easier if organizations fully understand the privacy and compliance mandates to which they must adhere.

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

The California Consumer Privacy Act (CCPA) went into effect January of this year. It enforces consumers' rights to control their personal information. Many experts believe a version of the CCPA will likely become federal law. CCPA itself is a take on the European Union's General Data Protection Regulation, which also protects consumers' personal data.

While companies worry that the cost to comply with government mandates could be prohibitive, many are still going forward in their efforts to ensure data is able to be discovered, reported on and erased. That way, when consumers request to see their data and then delete it, businesses will be ready.

To follow the multiple compliance mandates, organizations can create a data inventory, establish processes to get consumers their information under deadline and make updates to the organization's privacy statement.

The future of data security

AI and machine learning are going to be key in compliance efforts going forward. Companies are looking to automate some regulatory compliance processes, including data location and extraction. Inventories, as security expert Michael Cobb noted, become outdated unless automated scanning tools are deployed to sustain data discovery capture by recording regular snapshots of all applications and repositories where personal information resides. Automation, in his opinion, is the only way large

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

organizations can remain compliant with a large volume of data that is structured and unstructured and stored in data centers and in the cloud.

Next-generation technology could also help companies fall in line with other compliance mandates, such as PCI DSS. For companies that have lagged behind on compliance, some security experts suggest considering a zero-trust model as a security strategy. With zero trust, companies would look at the full lifecycle of data management and broaden their focus beyond just payment card data to other forms of personal data, including financial data, intellectual property and customer data. They would make no assumptions on where data is expected to be found or how it is being used -- only that the risk must be mitigated.

Data security will remain a significant challenge well into the future, but creative applications of AI and machine learning and zero-trust models will help IT and infosec teams protect data and ensure consumer privacy.

Next Article

In this e-guide

Data security guide: Everything you need to know p. 2

Why data security is important p. 2

Types of data security p. 4

Best practices for developing a data security strategy p. 8

Data privacy and compliance standards p. 14

The future of data security p. 15

Further reading p. 17

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading visit us at

www.SearchSecurity.com

Images; Fotalia