INTRODUCTION TO DATA SECURITY

Data Security refers to the set of practices and standards we use to protect digital information from accidental or unauthorized access, changes, and disclosure during its lifecycle. Data security can also include organizational practices, policies, frameworks, and technologies that can protect data against cyberattacks, malicious intrusions, or unintentional data leaks.

The practice of security data encompasses physical security of hardware and network assets containing the protected data, administrative controls and policies, and logical defense mechanism for software accessing the data.

This article will explain data security from a 1,000-foot view. We'll look at:

- Why we have to secure our data
- The components you'll need for a security strategy to actually work

Why is data security necessary?

Data security is a tricky subject, one that's often regarded as an afterthought among organizations. This approach also leaves the unprepared organizations vulnerable to cyberthreats and they often realize this too late. As the U.S. Cyber Chief puts it,

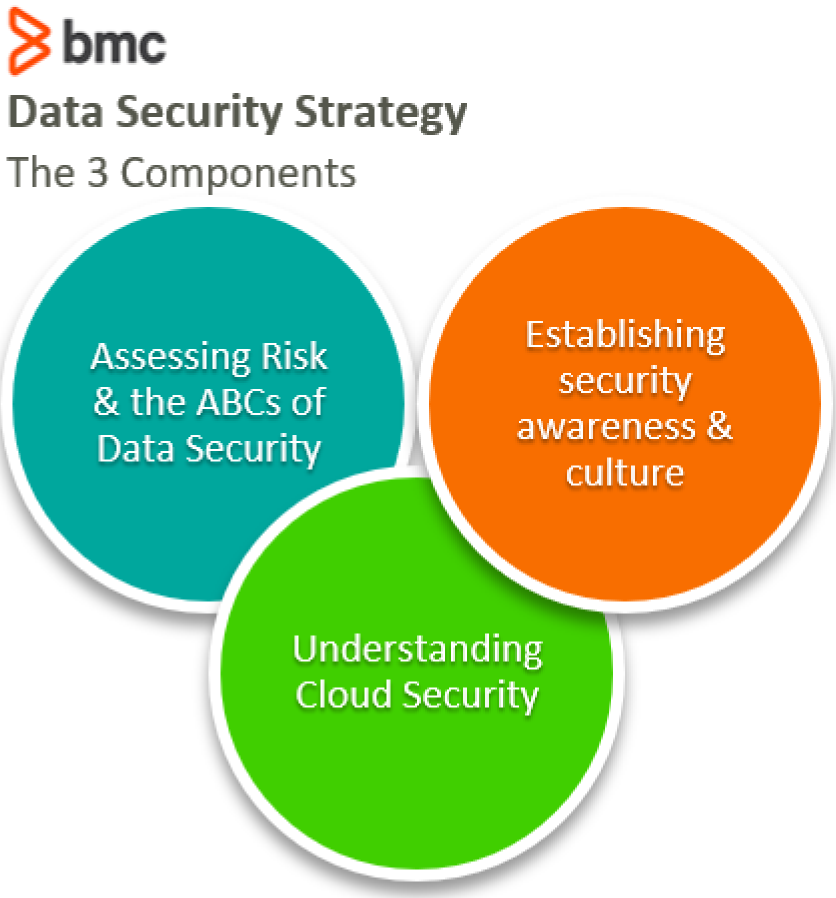
"Either you know you've been hacked, or you've been hacked and you don't know you've been hacked".

Here are a few numbers to describe the security threats last year:

- 43% of data breach victims were small business organizations (Verizon)
- The average cost of a data breach is $3.9 million (IBM)
- A cyber-attack takes place every 39 seconds—that's 2,244 times per day. (University of Maryland)
- Damages from cybercrime are projected to reach $6 trillion annually by the year 2021. (Cybersecurity Ventures)
- Cybersecurity unemployment is at 0%and over one million jobs are unfilled (CIO, Bureau of Labor Statistics)

Data security strategy in 3 components

An extensive data security strategy should contain the following key elements:


bmc
Data Security Strategy
The 3 Components
Assessing Risk & the ABCs of Data Security
Establishing security awareness & culture
Understanding Cloud Security

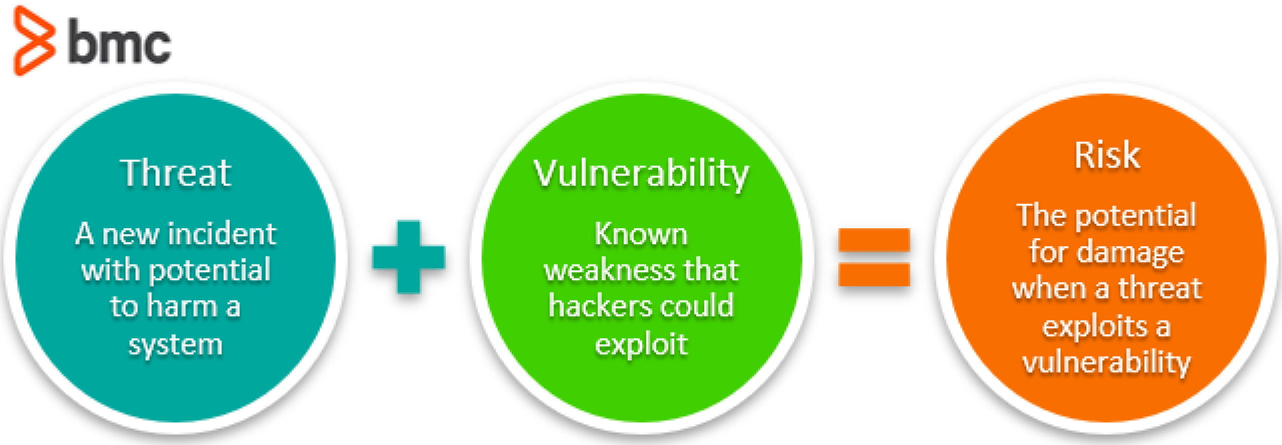
Risk assessment & the ABCs of data security

The cybersecurity landscape is evolving all the time. Its dynamic nature means there's no silver bullet solution to data security and risk management. Therefore, the first step to develop a data security strategy is to identify and understand your data security posture.

To achieve this, use these components—the ABCs of data security:

- **Align your organizational goals with IT.** Understand the security threats and quantify the business impact of the underlying risks.
- **Build future-proof security capabilities** that can help your organization mitigate risk in the near future, accounting for the changing market dynamics, scale of operations, technologies in use, and the global cybersecurity risk landscape.

- **Create an optimal tradeoff between your resource investments** across your people, processes, and technologies. Advanced security solutions cannot work if you do not have a culture of security awareness, sufficient governance controls, and the necessary skilled talent in-house.
- **Develop a thorough data security and risk management program** to mitigate the security challenges.


bmc
Threat
A new incident with potential to harm a system
+
Vulnerability
Known weakness that hackers could exploit
=
Risk
The potential for damage when a threat exploits a vulnerability

Understanding cloud security

Cloud migration is inevitable for any organization that must scale their hardware resources to meet dynamic user demands—without having the necessary CapEx and in-house talent to manage the infrastructure.

When you migrate sensitive business information and data workloads to the cloud, organizations must protect the data at rest, in transition, and during processing. A comprehensive data security strategy for cloud-based data workloads should contain the following elements:

- **Classify your cloud infrastructure.** Choose between private, public, and hybrid cloud for data workloads based on security, cost and performance requirements.
- **Encrypt data.** To avoid data leak while it moves across the Internet, data encryption ensures that only the intended recipients with the decryption keys can make sense of your business information.
- **Know your responsibilities.** Cloud vendors offer a shared responsibility model for data security: business organizations must apply strong governance controls and encrypt data, while vendors protect the IT environment from external attacks and vulnerabilities.
- **Adopt regulatory standards.** Frameworks such as HIPAA and ISO 27000 Series impose the bare minimum data security and privacy requirements for tightly regulated organizations handling sensitive data in the cloud. Many organizations lose legal battles over non-compliance to such stringent regulations. That's why it's crucial to carefully adopt security tools and processes for cloud-based data workloads that guarantee compliance to applicable frameworks.

Security awareness and culture

Data security practices are only as good as their weakest link, which often comes down to the human element. According to an IBM research study, the human element is responsible for 95% of all security incidents.

You can enhance data security by strengthening the culture of security and awareness within your organization:

- **Educate your employees on cybersecurity**, irrespective of their technical or professional background.
- **Follow the principle of least access privilege** as an organizational policy.
- **Employ and engage dedicated security professionals**, especially in the executive decision-making sections of your company. A cybersecurity perspective on the tech-business and financial decisions at the executive level is valuable in guiding the growth toward strengthened security posture.
- **Automate ITSM and governance functions to simplify routine tasks** that may open the doors to network intrusions and unauthorized data access. Keep track of the right IT Service Management (ITSM) metrics to understand the security performance of your organization.

Stay ahead of the risk with technology

Finally, it's important to keep on ahead of the curve. Use the latest and greatest technology solutions that the enterprise IT security world offers. If that feels unnecessary, consider this: cybercriminals increasingly use sophisticated means of hacking into your cloud and on-premise data center networks. Human errors will always exist despite all necessary governance controls in place.

The next generation of data security solutions rely on advanced AI capabilities for proactive and intelligent security defense, understanding the dynamic nature of IT environments and data workloads in detecting potentially anomalous activities on your network.

Related reading

- BMC Security & Compliance Blog
- BMC Machine Learning & Big Data Blog
- Cybercrime Rising: 6 Steps To Prepare Your Business
- Security Analytics Explained
- Incident Management: A Beginner's Guide