IBM Information Security

Your enterprise is dependent upon a continuous flow of information. This flow of data to employees, customers, business partners, and suppliers enables collaboration, innovation, and better decision making.

At the same time, information is one of your greatest sources of risk. Whether intentional or not, data security breaches can expose you to regulatory fines or legal actions and damage your brand.

Traditionally, information is primarily secured through a perimeter-based approach that relies on firewalls and other point products. But today's Web-based technology both enables and extends the need to share information beyond perimeter borders.

A business-driven approach to information security is a smarter approach.

Business-driven information security begins not with technologies and tactics, but with intelligence.

It begins with a holistic, lifecycle approach that helps you find the balance between information availability and risk, and brings proper focus to the potential exposures and vulnerabilities most relevant to your unique business and industry needs.

There are five key steps you can take to help determine your information risk tolerance, better understand potential security issues, and help minimize the breadth and potential impact of those issues.

Step one: define controls.

Creating an effective information security infrastructure begins with defining appropriate controls and related processes based on relevant standards, data security requirements, and business needs. This step includes comparing your current security posture against risk assessment results to determine gaps, and identifying the strengths and weaknesses of your current security practices.

Step two: discover and classify.

To protect information effectively, you need to identify sensitive data, and determine where it resides and who can access it. These decisions must take into account the need to protect data and applications across your entire infrastructure, including network, end points, and physical security.

Compliance requirements must also be considered. Many mandate storing documents for a specified amount of time, classifying data by sensitivity, and ensuring proper controls – like encryption – are in place for those assets.

Step three: enforce controls.

To protect the confidentiality, security, and availability of information, you need to validate the authenticity of all users who access resources, define what they may access, and monitor to help ensure that access controls are consistently enforced.

Step four: address data retention.

The number of specific information storage requirements continues to escalate. You need secure, scalable, and integrated archiving solutions to carry out established retention policies and reporting.

These solutions should provide index and search capabilities to make it easier to locate data when it's needed.

Step five: monitor, audit, and report.

To help ensure existing controls and policies are adequately protecting your data, you should constantly monitor your security posture relative to your end goal. This final step closes the loop on the information security lifecycle by enabling you to monitor, audit, and report on activities related to information security.

IBM's business-driven approach to information security is a smarter approach. It allows you to balance availability and risk as you safeguard your information assets, support compliance efforts, and enable dynamic collaboration.

No matter where you are in the process, IBM can work with you to help ensure you have a better understanding of what type of information you have, how to control access to it, and how to report on and manage how it's being used.

To learn more, contact your IBM representative or visit ibm.com/itsolutions/security.