Security solutions
White paper

Acquire a global view of your organization's security state: the importance of security assessments.

April 2007

IBM Governance and Risk Management
Business alignment, visibility and control

Contents

Overview

Today, more than ever before, security is a key issue for virtually every organization. No matter the size of your enterprise and what business you are engaged in – whether a financial services company, a retail chain or a water treatment plant – threats to your information security occur daily and evolve constantly. Because of that fluidity, virtually every organization has a "security gap" – that is, a gap between the organization's current protection level and the level it should be at to meet the latest security threats.

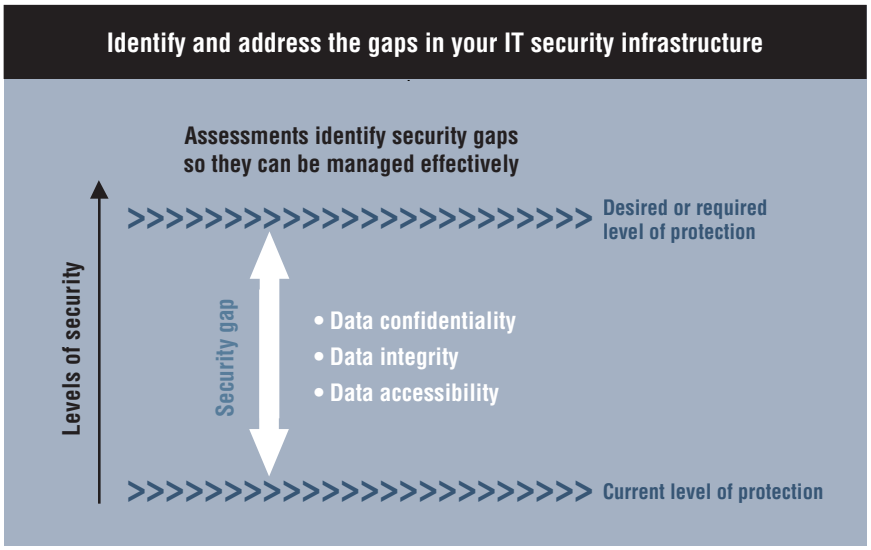
Any effective security program – one that eliminates that security gap – will concentrate on providing three attributes:

- ***Data confidentiality*** is an assurance that information is accessible only to those who should have access to it.
- ***Data integrity*** dictates that unauthorized parties should not be able to alter or forge your enterprise data.
- ***Data availability*** ensures that critical information and services will be accessible to the people who need it, when they need it.

However, as you search for a trusted advisor to help you institute an enhanced security program, you may well find that very few have the necessary expertise and the products in place to help you. This paper helps you understand the variety of assessment options that are available to you. It also provides criteria for selecting a vendor that can help you meet your security requirements.

Highlights

Almost every organization could derive value and insight from regular security assessments



One vendor that can help meet those requirements and more is IBM, which offers a broad portfolio of assessment services and products. These offerings represent one of several modular IBM security solutions, which help customers establish effective risk management strategies to manage and secure business information and technology assets, anticipate vulnerabilities and risk, and maintain timely access to information. The IBM security solutions framework – which is built on the International Standards Organization (ISO) 17799 global standard for security best practices – can help your organization safeguard the confidentiality, integrity and availability of critical business data.

Why conduct security assessments?

Almost every organization could derive value and insight from regular security assessments. Factors that drive the need for assessments include:

- Changes in the technology organizations use to do business.
- Supply chain changes.
- Mergers and acquisitions.
- The proliferation of remote office locations.
- The challenge of complying with regulations and service level agreements.
- The evolutionary nature of security threats.

Assessments are the key tools for uncovering security issues that may have been well hidden before. Often, an assessment leads to a compelling event that increases internal awareness of your organization's security shortcomings – it may uncover a prior, but undiscovered, breach; or a penetration test may "create" such an event by highlighting vulnerabilities. In addition, assessments can also help create budget resources for security enhancement – besides identifying problems, an assessment report can provide justification for making the investment necessary to solve the problems.

Choose assessment types that fit your needs

There are two basic categories of assessments, one or both of which may be appropriate for your organization. ***Point-in-time assessments*** capture a "snapshot" of your security state at a particular moment in time, and can serve as a basis for identifying weaknesses and formulating solutions. ***Ongoing assessments,*** made at regular intervals, can look into the effectiveness of your security policies, vulnerabilities, physical facilities and network architecture. Ongoing assessments can help ensure that you comply with security best practices, while addressing new security threats that will inevitably emerge.

You also have several options when it comes to the delivery method you choose for your assessment activities. Whether an organization chooses just one of the following methods, or some combination of two or more, depends on its specific security needs.

Highlights

- You can rely on a trusted advisor relationship to fulfill your assessment requirements. Many regulations require the use of a third-party vendor to conduct regular security assessments.
- You can take the "do it yourself" approach, focusing your purchases on assessment products and managing the assessment process internally.
- You can outsource the point-in-time and/or ongoing assessments you have deemed appropriate to a Managed Security Services Provider (MSSP). This approach can include product purchases and outsourcing of particular functions in addition to consulting activities. Many MSSPs have additional capabilities for back-end processes, analysis and workflow management.

Review the areas of your organization to assess

Security issues can affect virtually every area of your business – from your physical facilities to your network – and all can benefit from a thorough assessment. The types of assessments it may make sense for your organization to consider include:

Security policy gap assessment: Assesses the gaps between current security policies and best security practices.

Penetration testing: Simulates covert and hostile network attacks to identify specific vulnerabilities in the protection of your organization's sensitive data. A penetration test results in a clear picture of your organization's security condition, as seen from the perspective of an outsider, such as a potential hacker.

Application security is often overlooked as part of an overall security plan

Application security assessment: Provides a review of your custom applications to determine security weaknesses and recommend methods to remedy those weaknesses. Your applications house much of your organization's critical data – from customer information to human resources data to intellectual property – yet application security is often overlooked as part of an overall security plan. Security holes in Web-based and other custom applications in particular create opportunities for attackers.

Regulatory compliance gap assessment: Identifies the gaps between existing security and compliance with government and industry regulations that require security assessments. Regulations that can be addressed with this type of assessment include:

- Sarbanes-Oxley (SOX).
- Health Insurance Portability and Accountability Act (HIPAA).
- Gramm-Leach-Bliley Act (GLBA).
- Federal Information Security Management Act (FISMA).
- Federal Financial Institutions Examination Council (FFIEC).
- Supervisory Control and Data Acquisition (SCADA).
- Payment Card Data Security Standard (PCI DSS).

Network architecture assessment: Evaluates the existing network architecture to determine security weaknesses and provides a detailed security architecture design to protect the organization's IT environment.

Information security assessment: Provides a comprehensive view of an organization's overall security posture – internally and externally – including security policies, procedures, controls and mechanisms, as well as physical security, networks, servers, desktops and databases.

Physical security assessment: Determines how physical security can impact the overall data and system security of an organization, by measuring the ability to gain physical access to protected areas, systems and information. A physical security assessment should include the social engineering aspect as well as physical access considerations.

Highlights

While many vendors may be able to ascertain where weaknesses exist in your security program, far fewer will be able to uncover the problems, then help you address them

Select the right assessment partner

No matter which delivery method you choose for assessment services and which area of your enterprise you choose to assess, choosing the right vendor for assessment services will make all the difference in the validity and effectiveness of the assessments. While many vendors may be able to ascertain where weaknesses exist in your security program, far fewer will be able to uncover the problems, then help you address them. Clearly, it makes sense to search out the vendors with both capabilities.

The right assessment partner should be able to demonstrate the following attributes:

- Use of a best-practices methodology
- Proven expertise in the organization's market segment or industry (with references to back it up)
- Ability to address the entire security life cycle
- Integrated security intelligence — able to discover new threats even before they emerge and design ways to deal with them before they become real problems
- Utilization of proven assessment tools and techniques
- Quality deliverables designed to provide actionable recommendations

Understand the unified IBM strategy for security

Drawing on extensive customer experience, broad technical knowledge and deep understanding of today's security threats, IBM provides a unified strategy for enterprise security that incorporates assessments as one of four essential functions:

Assess: *to understand an organization's security exposure.* Assessment solutions accurately inventory enterprise assets, review security policies, identify and prioritize vulnerabilities and manage the workflow to remediate vulnerabilities.

Highlights

Defend: *to protect the organization from external and/or internal threats.* Solutions for security defense are designed to support effective threat detection and fraud prevention while helping to protect data, Internet-based systems, physical environments and applications.

Access: *to implement and manage user identities and to provide access authority across applications and data sources in a secure environment.* Access solutions help protect assets and information from unauthorized access – but without diminishing business productivity.

Monitor: *to manage and prevent security exposures and intrusion attempts.* Monitor solutions include management and reporting capabilities to help organizations proactively prevent, detect, analyze and remediate threats.

Advanced, modular and affordable IBM technology and service offerings help organizations stay ahead of security threats while supporting compliance and business requirements

IBM believes that today's enterprise security solutions should address all four of these functions but enable customers to implement them at their own pace. Advanced, modular and affordable IBM technology and service offerings help organizations stay ahead of security threats while supporting compliance and business requirements.

Leverage assessment solutions from IBM to obtain useful, tailored recommendations

IBM can deliver a complete assessment platform that, depending on the requirements of your specific organization, may include consulting, products and management – all driven by unsurpassed security intelligence. The fact is, IBM can address the complete security life cycle.

IBM products and services that address security assessment can be acquired on either an ongoing or point-in-time basis, and can represent any of the three assessment delivery methods previously described.

Trusted security advisor approach

IBM Professional Security Services delivers expert security assessment and consulting services that help organizations of all sizes reduce risk, facilitate regulatory compliance, maintain business continuity and reach their security goals. Highly skilled IBM Professional Security Services consultants focus solely on security and utilize proven consulting methods based on ISO 17799 best security practices. They can help organizations perform any types of assessments described in the "Review the areas of your organization to assess" section of this paper.

The IBM Internet Security Systems X-Force® research and development team supports IBM Professional Security Services in deploying proprietary toolsets, the latest threat intelligence and advanced countermeasures to help organizations build effective security programs that protect and enhance business operations.

"Do it yourself" approach

IBM Proventia® Network Enterprise Scanner helps reduce enterprise security risk, saves time and decreases costs by automating the ongoing process of asset discovery, vulnerability assessment, vulnerability remediation and reporting. Proventia Network Enterprise Scanner leverages existing IT infrastructure to quickly identify networked assets, works with third-party help-desk tools to track remediation tasks and integrates with other IBM Proventia security products to optimize the protection of an organization's infrastructure.

Outsourced approach

Part of the IBM Managed Security Services portfolio, the turnkey vulnerability management service combines managed vulnerability scanning, security expertise and integrated security intelligence with expert workflow and case

management – all accessible through a Web-based portal. This service helps organizations proactively strengthen and protect their networks by identifying the vulnerabilities found in servers, firewalls, switches and other networked equipment. It then helps eliminate those vulnerabilities resulting in minimized downtime, lower total cost of ownership, and increased productivity and operational efficiency.

Summary

Assessment is the first step in creating a security program for all aspects of your enterprise that will be effective now and in the long term. By choosing IBM to perform assessments or to deliver assessment tools, you can gain a global view of your current security state, formulate plans for correcting weaknesses and devise a schedule for ongoing assessments that will facilitate compliance efforts and help protect against evolving security threats – far into the future.

For more information

To learn more about how IBM security solutions can help you understand the weaknesses in your security infrastructure and provide a plan to improve security – or to find the IBM security solutions entry point that is right for your organization – contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
4-07

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

GMW10351-USEN-00