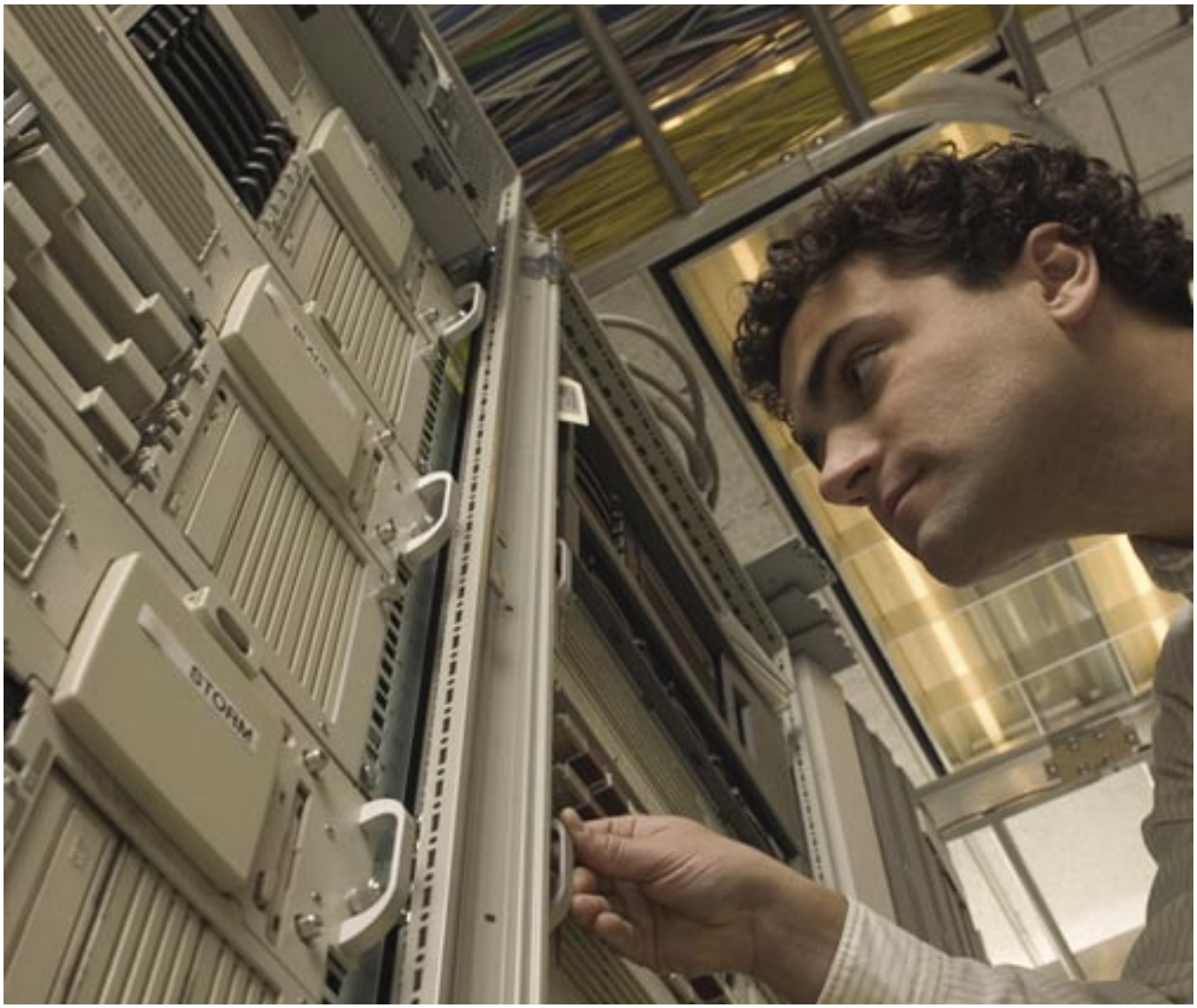
# Are You Secure?



**Contents**



As technology continues to evolve and become more complex, so do the threats to your IT infrastructure. As a mid-sized business, your resource allocation and cost margins are being stretched with an ever-increasing number of users, volume of information and 24x7 access to systems and information. And with this growth comes the increased chance for network failures and data breaches that could paralyze your business operations, affecting not only your workforce, but also vendor and customer relationships.

Management of this expanding information network is crucial to keeping your business ahead of the competition. Evaluating current IT security resources is becoming an essential part of small and mid-sized company operations. At the same time, new government and industry regulations, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA), are making businesses take an even closer look at—and possibly even re-think—their security options.

### The changing face of network security

As IT infrastructures and data networks continue to expand, so do the concerns that current security measures aren't doing enough to protect network infrastructure. Because of such rapid advancement, most IT people know that what worked yesterday might not work today and that trying to keep pace with technology is usually an exercise in futility.

***Nearly 70% of mid-sized companies say that IT infrastructure security and disaster recovery capabilities are essential, but less than 30% of those feel that the capabilities they currently have in place are complete***

For example, according to the IBM® paper "Inside the mid-market: A 2007 perspective," nearly 70% of mid-sized companies say that IT infrastructure security and disaster recovery capabilities are essential, but less than 30% of those feel that the capabilities they currently have in place are complete. [1]

In another recent security survey, conducted by the Computer Security Institute, it was found that the cost of computer crime has more than doubled from 2006 to 2007. Almost one fifth (18%) of respondents who suffered one or more types of security incidents in the past year also said that they had suffered

[1] *Inside the mid-market: A 2007 perspective*

**Highlights**

at least one targeted attack that was aimed exclusively at their organization or at organizations within a small subset of the general population.

Perhaps the most interesting finding, however, is that "only about one third of the respondents said their security policies didn't change in the wake of these incidents." [2]

***Few mid-sized businesses have the resources to keep pace with the ever-changing Internet threats that put operations and profits at risk. Escalating patch management requirements, multiple device management and the enforcement of security policies that can impact employees, vendors and customers are a 24x7 concern.***

The truth is that few mid-sized businesses have the resources to keep pace with the ever-changing Internet threats that put operations and profits at risk. Escalating patch management requirements, multiple device management and the enforcement of security policies that can impact employees, vendors and customers are a 24x7 concern.

Managing infrastructure security can be a challenge for even the most fortified network:

- Sophisticated security—With an ever-changing threat landscape, highly-skilled workers are required and are expensive to recruit, hire and retain. Many mid-sized organizations have limited IT budgets and can struggle finding the right workforce.
- Security management—Security budgeting might suffer as other core areas of the business need the funds set aside for operational growth. For many companies, patch management alone can consume hundreds of hours per month.
- New government regulations—For example, the Sarbanes-Oxley Act requires periodic disclosure of the status of internal controls on corporate financial systems.

In addition to these challenges, improperly managed network security can inadvertently block legitimate traffic, causing lost or delayed transactions, and negatively affect revenues and customer satisfaction. The spiraling and often unpredictable cost of security makes it difficult for companies to conduct proper financial planning and resource allocation.

[2] *2007 CSI Computer Crime and Security Survey*

**Highlights**

***Knowing where potential threats can manifest themselves can mean the difference in the ongoing struggle to keep your critical business information where it should be—safe and secure within your network.***

For small and mid-sized businesses, the opportunities for network vulnerabilities and information breaches will continue to rise. The good news is that if you know what to look for and where, you can stop virtually any threat. Knowing where potential threats can manifest themselves can mean the difference in the ongoing struggle to keep your critical business information where it should be—safe and secure within your network.

This coincides with having the right network assessment and capabilities in place to detect threats and defend your network, which is essential to your IT infrastructure and overall business growth.

**So what can you do?**

As your business grows, your network grows. Unfortunately, this growth increases the opportunity for unauthorized individuals to access sensitive data. You need to be aware of all aspects of your network security measures, from document confidentiality to system integrity and availability, while at the same time identifying the "security gaps," or areas where threats are the greatest to your systems.

To address your security needs fully, you also need to understand where your strengths and weaknesses lie. When assessing your current infrastructure, there are a few areas that need to be emphasized:

- Data confidentiality: Are you confident that information is shared only among those that have the proper access? Breaches of confidential information can occur when data is not handled in a manner appropriate to safeguard the information concerned. Such breaches can occur by such actions as word of mouth, printing, copying or e-mailing or creating documents and other data.
- Data integrity: Maintaining the integrity of your data means thwarting attempts by unauthorized parties to alter or forge your enterprise data.
- Data availability: You need to protect your critical data; however, it also must remain accessible to the people who need it when they need it.

**Highlights**

So what is a good starting point? Reviewing your current security situation can give you a better idea of your network's health:

- What capabilities do you currently have in place to minimize the damage in the event of an attack and ensure high availability of critical business systems?
- Are you compliant with industry standards that regulate the way your customer data is managed?
- Are your costs associated with detecting and handling spam e-mail and viruses continuing to climb?
- Does your business have difficulty installing and applying the constant updates that are required to stay current with the latest security threats?

***Any disruption to your daily business operations can be detrimental. You need to understand your current situation and plan accordingly, recognizing your vulnerabilities and addressing them in an efficient, timely manner.***

Whether it's network or application unavailability, compromised or damaged customer data or even financial loss, any disruption to your daily business operations can be detrimental. You need to understand your current situation and plan accordingly, recognizing your vulnerabilities and addressing them in an efficient, timely manner.

### Safe and secure

With all the security issues that businesses have to deal with, securing data can seem a bit overwhelming to a small or mid-sized organization. Where will the next threat come from? Will there be enough resources to deal with it? Knowing your network strengths and weaknesses ahead of time can give you the visibility to plan for and fix problems before they happen. Utilizing the following approach can ease your security concerns:

- Identify security issues and create internal awareness and justification around the increasing need for increased protection.
- Secure changing networking environments and ensure the secure deployment of each new application, upgrade and business process in your organization.
- Deliver preemptive protection to support continuous business operations so that customers can stay ahead of the evolving threat landscape.

**Highlights**

- Meet or exceed regulatory compliance requirements for data protection.
- Quickly assess your security and gain expert advice on right-sized solutions to help secure your business and comply with regulations.
- Ensure data confidentiality, integrity and availability in your organization using a security framework built on global standards for security best practices.

Assessment and the formulation of plans to address discovered weaknesses are two of the multiple security solutions available that can help you implement this approach, understand your security posture and take the necessary actions to make sure that your security gap is eliminated.

***To succeed in today's world of electronic transactions and communications, all organizations must understand their security postures so that they can protect their assets while providing an available and performing infrastructure for their business applications.***

### Why conduct a security assessment?

To succeed in today's world of electronic transactions and communications, all organizations must understand their security postures so that they can protect their assets while providing an available and performing infrastructure for their business applications. If your organization is like other mid-sized organizations, it's possible that you may not know your security posture. Or recent updates or additions to your business or systems might have changed your posture without your being aware of it.

Therefore, almost every mid-sized organization can derive value and insight from regular security assessments. Factors that drive the need for assessments include:

- Changes in the technology that you use to do business
- The proliferation of remote users
- 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

**Highlights**

***Often, an assessment leads to a compelling event that increases internal awareness of your organization's security shortcomings.***

increases internal awareness of your organization's security shortcomings. In addition, assessments can also help create budget resources for security enhancement by providing justification for making the investment necessary to solve the problems.

There are two basic categories of assessments, one or both of which might be appropriate for your organization. Point-in-time assessments capture a "snapshot" of your security state at a particular moment 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.

**What you should assess?**

Security issues can affect virtually every area of your business and they can all benefit from a thorough assessment. The types of assessments you should consider as you determine your security are addressed in this section.

*Information security*

Understanding your organization's security state and identifying vulnerabilities are the first steps toward protecting the confidentiality, integrity and availability of critical data. An information security assessment, therefore, should be based on globally recognized standards and industry best practices and performed by security experts that thoroughly document the results and provide specific, actionable recommendations for mitigating the identified risks and improving overall security posture.

*Penetration*

Penetration occurs when vulnerability in your networks is exploited by an unwanted attack or intruder. Penetration testing can help determine your

**Highlights**

network's current vulnerabilities while demonstrating how attackers can harm your business. This safe and controlled exercise, performed by security experts, validates existing security controls and quantifies real-world risk. The result is a detailed security roadmap that prioritizes areas of weakness and specifies remediation steps to improve your security posture.

*Payment Card Industry data security standard compliance*

Working together, the major payment card providers have developed a set of data security standards and created a council for enforcing them. Although the Payment Card Industry Data Security Standard (PCI DSS) has become a global requirement, many organizations are lagging in compliance. A PCI compliance assessment can take you through the entire PCI compliance process, from assessment to compliance to certification, to help you meet all 12 PCI requirements for safeguarding your customer credit card data. It includes compliance gap analysis, remediation, validation, ongoing testing and reporting and makes available a range of products for security planning, management and compliance reporting.

***Application security is a frequently overlooked component of a security plan.***

*Application security*

Application security is a frequently overlooked component of a security plan. Developers are under pressure to bring custom applications of all kinds (such as Web applications, customer relationship management systems, accounting systems and so forth) online quickly. This often results in insufficient security testing and validation, leaving the applications vulnerable to exploitation by both internal and external attackers. An application security assessment provides a targeted code review and a comprehensive vulnerability assessment of the application and the network infrastructure directly supporting the application. It also determines security weaknesses and misconfigurations and then provides detailed recommendations for the remediation of vulnerabilities discovered.

**Highlights**

***Security assessments can be handled several ways. One option is to rely on a trusted advisor relationship. Another is to take the "do it yourself" approach.***

**Security assessment methods**

Security assessments can be handled several ways. Whether you choose just one of the following methods, or some combination of two or more, depends on your specific security needs.

*Trusted advisor relationship*

To fulfill your assessment requirements, one option is to rely on a trusted advisor relationship. In some cases, a trusted advisor relationship is critical because many regulations require the use of a third-party vendor to conduct regular security assessments. If you have decided that this method works best for you, you should seek out a trusted advisor that can offer 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. In other words, the advisor you choose should be able to provide a complete assessment solution that, depending on the requirements of your specific organization, may include consulting, products and management—all driven by security intelligence.

*"Do it yourself" approach*

Some mid-sized businesses prefer to handle their security assessments on their own. They take the "do it yourself" approach, focusing their purchases on assessment products and managing the assessment process internally. If your company prefers this method, you need to find tools that use automation and existing IT infrastructure to identify networked assets quickly, that work with third-party help-desk tools to track remediation tasks and that integrate with other security products to optimize the protection of your organization's infrastructure. Because they automate the ongoing process of asset discovery, vulnerability assessment, vulnerability remediation and reporting, these tools can also help you:

- Reduce company security risks.
- Save time.
- Decrease costs.

**Highlights**

*Outsourcing*

Your organization might not be in a position to conduct assessments in house. You might want to focus internal teams on other critical projects or wish to increase productivity by making the most of your back-end systems and processes. Therefore, another option is to outsource the point-in-time assessments, ongoing assessments or both to a managed security services provider. This approach can include product purchases and outsourcing of particular functions in addition to consulting activities. Many managed security services providers have additional capabilities for back-end processes, analysis and workflow management.

If this is the assessment route you prefer, you should seek a solution that combines managed vulnerability scanning services with expert workflow and case management—all accessible through a Web-based portal. Such a service can help protect your organization's network by identifying the vulnerabilities found in servers, firewalls, switches and other networked equipment and then assisting in the process of eliminating those vulnerabilities.

***No matter which delivery method you choose for assessment services and which area of your business you choose to assess, choosing the right vendor for assessment services will make all the difference in the validity and effectiveness of the assessments.***

**Selecting the right assessment partner**

No matter which delivery method you choose for assessment services and which area of your business 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 might be able to ascertain where weaknesses exist in your security program, far fewer will be able to uncover the problems that help you address them.

Clearly, it makes sense to search out the vendors that can discover new threats even before they emerge and that can design ways to deal with them before they become real problems. Therefore, the right assessment partner should be able to demonstrate the following attributes:

- A best-practices methodology
- Proven expertise in your market segment or industry (with references to back it up)

- Ability to address the entire security life cycle
- Integrated security intelligence
- Proven assessment tools and techniques
- Quality deliverables that provide actionable recommendations

As you search for an assessment partner that has these attributes to help you institute an enhanced security program, you might find that very few have the necessary expertise and the products in place to help you. Fortunately, there is one vendor that can meet your security challenges with every attribute necessary to make sure that your security gap is firmly closed—IBM.

**Why IBM?**

With IBM, you gain expert security consulting that is designed to accommodate your organization's unique security requirements and environment. Our highly skilled consultants, project managers, subject matter experts and architects can help you build a powerful preemptive security program so that you can significantly reduce risk and maintain business continuity. In addition, all of our professionals are security-focused and able to provide you with a hands-on approach, staff training and trusted assistance.

Only IBM and its vast network of Business Partners can provide the broadest range of IT Security solutions and solution building blocks, including hardware, software and services tailored specifically to mid-sized companies, along with deep expertise in every industry, extensive local presence and the support and backing to deliver simple, affordable, custom solutions.

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.



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

Produced in the United States of America
1-08


The IBM home page on the Internet can be found at **ibm.com**

SMW03006-USEN-00