CIO 2 CIO PERSPECTIVES
Today's IT Leaders on Market Trends

IT SECURITY MEASURES

How CIOs Use Strategies, Metrics and Partnerships for Success

Headlines regularly scream of enterprise data losses from breached security. In today's networked and integrated world, security breaches and breakdowns are no longer an abstract concept. Thieves and hackers adopt new and increasingly sophisticated methods for inflicting damage and hijacking data for monetary gain. These transgressions ripple through an enterprise and beyond. According to the Computer Security Institute (CSI), 71 percent of large corporations and government agencies surveyed detected security breaches in 2006.

CIOs must confront a litany of questions, including: *How vulnerable is this system? Does this system provide absolute protection for our critical business and customer data? Are my technology vendors working to make my environment more secure? How much do I have to invest in my business to increase and improve overall security? And how do I develop sound and consistent business practices that maximize my security investment?*

There are no simple answers. A recent IDG Research survey validates the fact that security is now a primary business priority that heavily impacts IT budgets. Most CIOs peg security costs between 10 and 20 percent of their IT budgets—and the numbers escalate when considering compliance issues. IT executives must consider platform manageability and maturity, data safety and protection, a vendor's long-term commitment to addressing security issues, and their company's internal commitment to developing consistent security processes to achieve positive results over time.

Measuring Security

Security can be described as maintaining the confidentiality, integrity, and availability of information. CIOs must consider their organizational profile with respect to these three attributes, what risks they can live with and how they manage them.

There is often great debate about whether open source or closed source software is inherently more secure. This revolves around the age-old debate about whether "security through obscurity" is ever viable. For the purposes of this white paper, open source software is defined as software whose source code is available for inspection, modification and distribution. Closed source software is its opposite. The source is available to very few people—typically the vendor that created the software and possibly their partners—under tight nondisclosure agreements.

Open source software can present an opportunity for both attackers (as they have a complete view of the source code and what is fixed in a security patch) and defenders (as they, too, can inspect the code for vulnerabilities and patch them). Closed source is much more difficult to attack, arguably requiring a higher level of expertise, but defenders are now left to trust their vendor to patch things expeditiously in a manner that works within the enterprise.

Since most software has some limitations, the philosophy, skill sets and training of the team will probably go much further in determining how secure a system remains. This speaks directly to the level of trust an enterprise has in its systems vendors and support for training, certifications, best-practice documentation and tools.

Putting a Security Initiative to Work

Today's IT environment encounters a steady barrage of problems, threats and vulnerabilities. Too often, organizations wind up in a reactive mode—battling security issues as they occur. Unfortunately, this short-term approach usually leaves an enterprise vulnerable—and increases overall security costs. Today, it is imperative to take a big-picture view of manageability and platform maturity while also focusing on data safety and protection. The key is building an environment that centers on four primary factors:

Overall security quality. It's essential to focus on software that's well engineered and designed to handle the diverse needs of a business. These business-critical applications must fit business processes and provide a high level of flexibility. Of course, it's not enough to take vendors' claims and promises as gospel. An organization must substantiate information and data through independent analysis and ratings, such as the Secunia Vulnerability Study by Secunia, a leading independent source of vulnerability intelligence.

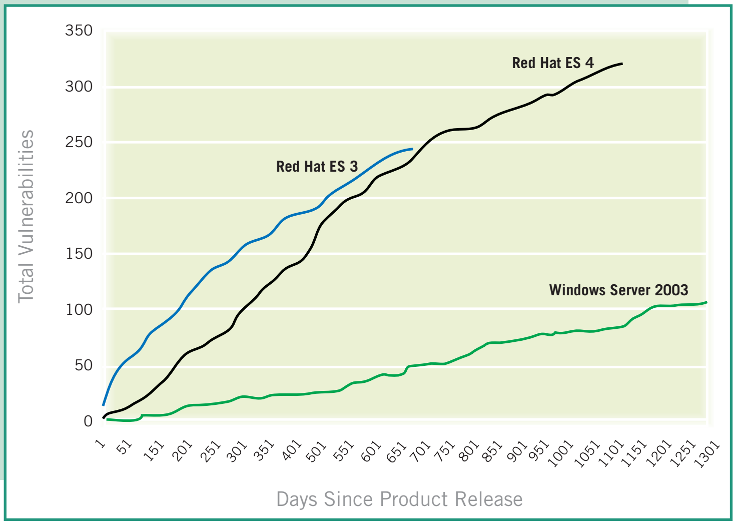
Security management. An organization must manage the operation and maintenance of various security solutions. Patch management, ongoing programming and development issues, and changes to business processes all affect the environment. Lacking a strong foundation, an enterprise can find itself struggling with inadequate or obsolete security tools. A CIO must know that the enterprise is capable of making changes and that the security infrastructure can keep up.

- **Security innovation.** Staying current with technology and processes isn't a luxury; it's a necessity. Increasingly sophisticated threats require increasingly sophisticated tools and solutions, including biometrics, two-factor authentication, analytics-based software (which uses sophisticated algorithms to detect fraud and other suspicious activity, including malware) and other tools, including more advanced network administration capabilities. Simply put, it's essential to remain one step ahead of hackers, thieves and vandals. The approach that a vendor takes in integrating products and building an overall framework for protection—including tools such as Active Directory® (which spans an array of systems and processes and builds controls into processes)—goes a long way toward reducing risk and costs.

- **Security skills and resources.** The final piece of the security puzzle is ensuring that an enterprise has access to a body of knowledge as well as outside expertise and a well-trained pool of talent to drive

THE VULNERABILITY INDEX

According to Secunia, a leading independent source of vulnerability intelligence, there's more to enterprise security than meets the eye. This chart shows the cumulative security vulnerabilities tracked in the Secunia database for three popular server operating systems—Microsoft Windows Server® 2003, Red Hat Enterprise Linux 3 and Red Hat Enterprise Linux 4. It reports that Windows Server 2003 was introduced with fewer initial vulnerabilities than either Red Hat ES 3 or Red Hat ES 4, and has fewer total vulnerabilities throughout the product life cycle. The Secunia data shows that the cumulative number of security vulnerabilities announced over the first 650 days of availability for the three products was approximately five times higher for Red Hat Enterprise Linux 3 and 4 than for Windows Server 2003.



Source: Secunia Vulnerability Data (http://secunia.com), December 2006 effective decision making. Certifications, best practices, software-based assistance, metrics and benchmarks, and a rich ecosystem of products and tools are key to implementing a world-class security program. Ultimately, achieving excellence revolves around an organization's ability to place the spotlight on security and make it the number one priority—even when financial and operational challenges loom large.

Not surprisingly, stability and reliability are far more important to CIOs than leading-edge features and promises of productivity gains. As Fernando Martinez, CIO of Mercy Hospital in Miami, observes: "I'd rather use a server platform that's mature and well distributed instead of one that's innovative and cutting-edge."

> "Internal processes–and people–pose a greater threat than vulnerabilities."
>
> JOHN PETERSON
> CIO, LONGMONT UNITED HOSPITAL

John Peterson, CIO of Longmont United Hospital in Longmont, Colorado, believes that the OS must provide an overall framework for security. "We believe internal processes—and people—pose a greater threat than vulnerabilities," he says. Consequently, Peterson scrutinizes internal workflows and business processes, and he keeps close tabs on rights, privileges and termination policies. Moreover, he and other CEOs cite the importance of data protection as it relates to regulatory and compliance issues. A single lapse can lead to severe consequences, including fines and prison terms for executives.

Achieving Results and ROI

Executives increasingly recognize that security initiatives are highly interconnected with a vendor's products and services. A critical factor for CIOs—and a basis for making decisions about products, including operating systems (OS)—is the level of OS vulnerability and a vendor's ability and commitment to include significant protection in various applications and solutions. What's more, with organizations under enormous pressure to meet budget constraints, it's essential to identify a clear technology path that provides the flexibility, scalability and overall framework required in today's business world.

It's not surprising that CIOs find themselves attracted to widely available and proven technology. In the quest to achieve superior protection, organizations often begin the security analysis process with a close examination of the overall computing frame-

MICROSOFT TRUSTWORTHY COMPUTING INITIATIVE

Through the Microsoft Trustworthy Computing Initiative and related programs, Microsoft has developed a wealth of tutorials, tools, and best practices to help IT professionals create and maintain a secure environment. The following list is a sampling of some of these materials:

- **The Trustworthy Computing Initiative Security Resources:** A comprehensive collection of materials to help Microsoft customers understand and enhance the security of their Microsoft software-based computers. (http://www.microsoft.com/mscorp/twc/security/resources.mspx)
- **Windows Server 2003 Security Services:** Windows Server 2003 provides improved network security with support for standardized 802.1x protocols, an integrated public key infrastructure (PKI), password or certificate-based access, and other services. (http://www.microsoft.com/windowsserver2003/technologies/security/default.mspx)
- **Microsoft Security Summit:** Online core material including the Security Training and the Security Guidance Center materials. (http://www.microsoft.com/seminar/securitysummit/default.mspx)
- **The Technet Security Center:** Tools and training for IT professionals to best secure their network. (http://www.microsoft.com/technet/security/default.mspx)

work. "The goal," says Grant Richardson, senior director of technology and services at ABX Air, a $1.3 billion transportation logistics firm based in Wilmington, Ohio, is "not only to identify the vulnerabilities, but to fix them quickly and react to them quickly. It's the ability of the server operating system to work well with third-party security applications and products and integrate with them."

Indeed, with the right combination of tools and training and a proactive approach to security, a business minimizes the risk of security breaches. Many CIOs recognize the importance of taking a standards-based approach. "From a security perspective, I tend to steer toward standards because I know that they are well tested and well vetted by companies larger than ours," explains Dave Stritzinger, CIO at wireless provider Brightstar Corp., in Miami.

A robust and mature operating system, such as Microsoft® Windows®, that supports an array of advanced management tools, often serves as the cornerstone for an effective security strategy. For example, Active Directory provides a central repository of data about all network users and the ability to assign enterprise-wide policies, procedures and workflow. It greatly simplifies the task of updating and patching systems across the enterprise. Active Directory also complements other tools, such as group policy, certificate management and public key infrastructure (PKI).

CIOs believe that day-to-day manageability is crucial. Security initiatives such as Microsoft's Trustworthy Computing Security Development Lifecycle (SDL) are expanding the boundaries of this concept. The approach focuses on deploying products that require fewer patches and a higher level of reliability. For IT departments, this translates into lower maintenance costs, increased availability and decreased security risk. Another group of products, Microsoft Forefront, offers integrated and comprehensive protection and control over client, server and edge-network systems.

A robust and mature operating system provides the management interface to enforce policies within a predetermined range of what administrators and executives deem acceptable and desirable. The combination of a platform designed to create pathways for business processes along with the tools to build and manage security fashion a powerful solution. In addition, an enterprise can develop competencies and knowledge around these sets of tools and use this information to drive further improvement.

Security has been transformed into a constant, ongoing battle. As hackers and thieves up the ante with new and more sophisticated forms of malware and intrusion techniques, organizations must keep up. However, the challenge extends beyond tools and technologies. These days, it's also essential to build strong partnerships—whether an organization purchases products directly from a vendor or turns to an outsourced or managed services model to put all the pieces together. The bottom line, CIOs say, is that all participants must work together to bring value and results to the relationship. Only then can an organization realize the full potential of its security infrastructure.

Conclusion

Stability, reliability and flexibility are the cornerstone of any security initiative. The most successful organizations develop a holistic view and establish a foundation for success through a process and technology framework. While they seek powerful solutions, they're focused heavily on using operating systems and security products that fit the business environment and help manage total cost of ownership.

They choose vendors and establish partnerships based on innovation, education and training—as well as the underlying tools. Not surprisingly, when CIOs embrace a holistic approach, they find themselves well positioned to deal with the ongoing security challenges of today's business environment.

About CIO2CIO Perspectives: This peer-based thought leadership program analyzes quantitative research and tests it via qualitative interviews with actual CIOs. The resulting executive insight is then disseminated via CXO's multimedia assets. To learn more about CIO2CIO Perspectives, please contact mavery@cxo.com.