

synnovation

Vol. 1 Issue 3

Beating the Odds

Leading an organization through a risk-laden environment is often a game of chance. But enterprise risk management can help your odds.

EDS

Unwelcome Surprises

By Al Decker

Towers Perrin

Coming of Age

By Prakash Shimpi

Microsoft

Defending the Crown Jewels

By Ron Markezich

Oracle

Protect, Detect, Deploy

By Vipin Samar

Dell

Super Power

By Dr. Reza Rooholamini

Sun Microsystems

Tapping Tag Power

By Jim Del Rossi

Xerox

For the Record

By Charles P. Brett

EMC

Reaching Out

By Gregg Therkalsen

Cisco Systems

A Matter of Self Defense

By Bob Gleichauf

EDS

Conversations

With Ron Rittenmeyer

Microsoft

Up Close and Personal

With Ron Markezich

Defending the Crown Jewels



Lessons learned from the security infrastructure Microsoft built

*I*t looked like a legitimate e-mail message. Or, more ominously, like *thousands* of legitimate e-mail messages.

It was the end of a financial quarter, in late 2004, a time when Microsoft employees expected to get e-mail statements from the financial services company that administers employee 401(k) retirement programs. And sure enough, the expected e-mail messages, apparently from that firm, were sent to thousands of Microsoft employees. The e-mail messages included links, apparently to the firm's Web site, where our employees could log in with their IDs and passwords, and update their confidential information.

While the e-mail messages looked legitimate, they were anything but. Instead, they were an example of a new twist on the already notorious "phishing" scam. While early phishing efforts involved bogus e-mail messages sent at random to hundreds of

thousands of unsuspecting users, a new variant—called "spear phishing"—was more insidious and more likely to be successful. That's because spear phishing targets specific individuals, groups, or employees of a company or organization. Because the attacks are more personalized—the attack against Microsoft addressed employees by the same naming convention we use here at the company and referred correctly to their pension plan administrator—they're often more successful in inducing their victims to part with sensitive information.

The spear phishing scam that hit us was a beauty. How was our employees' confidential information compromised? How seriously would your employees' confidential information be compromised by such an attack? >>

By Ron Markezich, Microsoft Corporation



M.D.M. S. de la Cruz, obra de D. Juan Cortes, quien fue Jefe del Gran Capitan D. Hernando Cortes y M...

The number of new and unique phishing sites on the Internet worldwide nearly tripled between March 2005 and March 2006, climbing to 9,666 new sites, according to the Anti-Phishing Working Group.¹ And that's only one of the types of online security threats facing enterprises and their employees. A joint survey of businesses by the U.S. Federal Bureau of Investigation and the Computer Security Institute found that 78 percent of businesses had been infected with a virus or worm, 37 percent had unauthorized personnel gaining access to company information, 10 percent reported theft of proprietary information, and 49 percent reported laptop thefts.² Additionally, up to 80 percent of all Internet-connected computers might have some form of spyware.³

We've Seen it All

At one time or another, we've seen every possible security threat in our IT environment here at Microsoft. And no wonder, because we have one of the largest IT environments in the world. We have more than 106,000 end users in 98 countries and more than 340,000 PCs and devices, including some 7,200 data center computers in three data centers. We receive more than 10 million e-mail messages from the Internet per day—more than 90 percent of it spam—and more than 46 million remote connections per month, including connections from more than 30,000 partners.

Our challenge is to ensure that all of those messages and connections can be implemented reliably, unimpeded by security threats, and that none of those messages or connections contain the types of threats we must guard against. As our workforce becomes increasingly mobile, the security threat grows to include not only the connections that mobile workers make to our network, but also the physical security of their mobile laptops, pocket PCs, smartphones, and other mobile devices. The types of malicious software and attacks we face have increased to include trojans,

remote access trojans (called RATs), spyware, and denial of service attacks. Preventing unauthorized access to data is a particular challenge because greater availability, which facilitates appropriate use of data, also increases risk. And hanging over this entire picture is the regulatory environment, which includes both Sarbanes-Oxley in the United States and privacy laws in the European Union and elsewhere, and with which our security program must comply.

The threats to corporate networks have grown tremendously in the past few years of course, fueled by the growth of the Internet itself. With the Internet, the bad guy trying to steal your data or bring down your network can be located anywhere within your organization—or in the world. And the exponential growth of the Internet coincides with the post-September 11 era. In contrast to the tech boom days that preceded it, when time-to-market and open environments were top-of-mind concerns for executives, world events over the last few years have sobered technology executives to the threats facing them and their networks.

Sobering Up

Certainly those events have sobered us. When the "Slammer" virus hit four years ago, it was a wakeup call to companies and organizations about the importance of securing their networks. We already had a system of software updates in place to protect our desktops, but we weren't stringent or comprehensive in our implementation of that system. A small number of machines in our lab environments were unpatched because they were configured in ways that made automatic updates impractical or impossible—and they got hit with Slammer. The experience taught us that every machine is a potential source of infection. So, now, every machine receives comprehensive antivirus protection or it's not allowed access to the network.

Of course, every organization's ideas on security

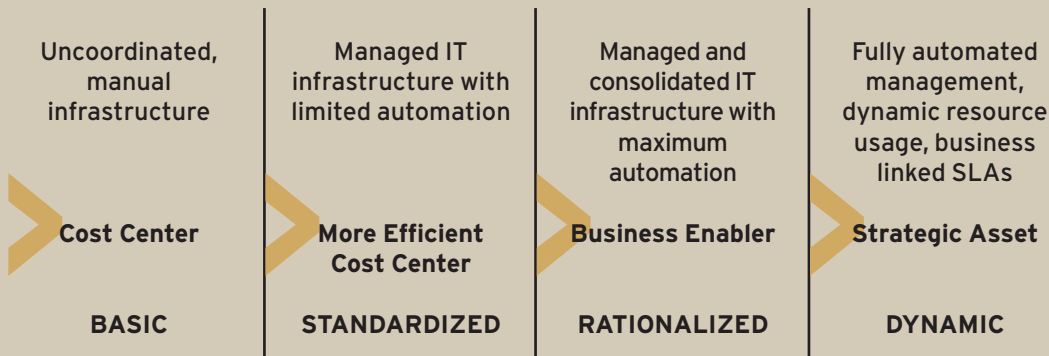


Microsoft's Bottom Line on Security

- Security must partner with the business
- Security controls should be based on risk management
- Defense-in-depth is fundamental
- Changing business and technology require flexibility
- Standards-based approach fosters mutual understanding between security and business personnel

Infrastructure Optimization Model

Figure 1



are shaped by experiences in addressing security threats. At Microsoft, our ideas on security are also shaped by our role as a leading provider of the technologies that other companies use to help run and protect their IT environments. That gives us multiple perspectives or layers of understanding on the issue of IT security. That's especially appropriate because multiple layers—called “defense-in-depth”—is a key part of our security philosophy and a key part of the approach that we recommend to others. And as a technology provider, we've also taken a multifaceted approach to our promotion of IT security throughout the industry. That approach guides the investments we make, the prescriptive guidance we provide, and the way we partner with others in the security industry, governments, and law enforcement.

How should a company apply defense-in-depth and other elements of a security program? That depends on the current state of that organization's infrastructure. Each step will be a bit different for each company, depending on its situation, but all organizations have steps to take, because security is a journey, not a destination. As the threats and the technologies continue to evolve, so must the security program that responds to them.

The Security Road Map

No journey is well-taken without a map. We call our map an infrastructure optimization model and it guides our approach to matters far beyond those of security. There are many well-known models out there, including the Gartner Group's Infrastructure Maturity Model and MIT's Architecture Maturity Model. Ours is informed by theirs, as well as by our own experiences, and the experiences of our enterprise customers. The model is a way to understand a company's current

IT infrastructure as well as the costs, risks, and benefits of optimizing it.

The model has four key stages (see Figure 1). As an organization moves from left to right in the model, it moves to more mature infrastructure levels with greater returns.

- **At the basic stage**, an organization operates in a highly reactive way to security threats. Processes are fragmented or nonexistent and costs are unpredictable. Security and IT are seen as internal taxes on business, rather than as enablers of business. And there's a big gap between the IT personnel who struggle to address security issues and the business owners who pay for that security—and for the lack of security. Microsoft was at this stage about six years ago, prior to September 11 and Slammer.
- **The standardized stage** is a more efficient version of the basic stage. Here, an organization is more proactive, processes are more evolved and even automated, and costs are more predictable—but security and IT are still viewed as cost centers. It took us about three years to evolve our security infrastructure from the basic to standardized stage.
- **The rationalized stage** is one in which formal and highly automated processes have become so predictable that they are—and are seen as—supporters and enablers of the business, rather than merely as drains on the business. Security and IT don't hold the business back; they make the business possible. Microsoft took more than two years to move to this stage.
- **The dynamic stage** is the holy grail of infrastructure optimization. Here, security and IT are strategic assets that provide a competitive advantage to the business, because fully automated and dynamic processes allow organizations to act with unprecedented >>

agility. I frankly don't know of a company that has achieved this stage in its security infrastructure, although some financial services firms seem poised to do so, as Microsoft is now also attempting to do. In the broader area of IT, Wal-Mart is a company with a dynamic infrastructure; its use of IT to track inventory down to the individual unit and to control costs has helped to enable its highly competitive pricing structure.

An organization optimizes its security infrastructure, and moves along our optimization model, in the way it applies technology, processes, and people to its challenges. Technology is always the easiest to mature—and people are often the hardest. Figure 2 shows how we believe an organization applies its technology, processes, and people to security challenges at each level of maturity. For example, as an organization matures, security technologies are increasingly tied to clear business objectives; security processes are explicit and automated; and security personnel have clear responsibilities and are integrated into the processes that advance business strategy.

What does the security infrastructure of a dynamic organization look like? Its business organization drives security based on business needs. The resulting security infrastructure is the result of a continuing conversation between business and security groups. Its security processes are based on ISO 9000, IT Infrastructure Library (ITIL), or, in the technology area, our Microsoft

Operations Framework version of ITIL. And the dynamic company automates technology as much as possible to let systems and data protect themselves.

For example, one way that Microsoft protects its network from threats among those 46 million monthly remote connections is by quarantining remote computers from network access until their security status can be identified and any problems cured by downloading appropriate security software. All this happens automatically between the remote computer and the Microsoft infrastructure, without the need for human intervention either by the remote user or by a Microsoft administrator.

Beginning the Journey: From Basic to Standardized

How do you begin your journey from basic to standardized security? I can tell you how we did it. Perhaps the two most important elements had nothing (well, almost nothing) to do with technology: they were executive sponsorship and an enterprise-wide awareness campaign. Without the front-and-center support of Bill Gates and Steve Ballmer for this initiative in 2000, it never would have succeeded. Improving our security infrastructure became an issue for all of us because it was clearly an issue for them.

Even with their support, we had to raise the level of awareness for security because, six years ago, people here just didn't think much about it.

Infrastructure Optimization Model: Security

Figure 2

	BASIC	STANDARDIZED	RATIONALIZED	DYNAMIC
PEOPLE	<ul style="list-style-type: none"> > IT staff taxed by operational challenges > Users come up with their own IT solutions 	<ul style="list-style-type: none"> > IT staff trained in best practices such as MOF, ITIL, etc. > Users expect basic services from IT 	<ul style="list-style-type: none"> > IT staff manages an efficient, controlled environment > Users have tools they need, availability, and access to information 	<ul style="list-style-type: none"> > IT is a strategic asset > Users look to IT as a valued partner to enable new business initiatives
PROCESSES	<ul style="list-style-type: none"> > IT processes undefined > High complexity due to localized processes and minimal central control 	<ul style="list-style-type: none"> > Central administration and configuration of security > Standard desktop images defined, not adopted by all 	<ul style="list-style-type: none"> > SLAs are linked to business objectives > Clearly defined and enforced images, security, best practices (MOF, ITIL) 	<ul style="list-style-type: none"> > Self-assessing and continuous improvement > Information easily and securely accessed from anywhere on the Internet
TECHNOLOGY	<ul style="list-style-type: none"> > Patch status of desktops is unknown > No unified directory for access management 	<ul style="list-style-type: none"> > Multiple directories for authentication > Limited automated software distribution 	<ul style="list-style-type: none"> > Automated identity and access management > Automated system management 	<ul style="list-style-type: none"> > Self-provisioning and quarantine-capable systems ensure compliance and high availability

That campaign communicated the executive sponsorship—we launched our efforts about the same time that Bill Gates issued the Trustworthy Computing Initiative memo that reoriented our entire product direction toward greater security—as well as the role we expected every employee to play in helping to achieve greater security. We went from the general to the specific, describing the basic steps that our employees needed to take both to help secure our infrastructure and to help provide greater security to our customers.

Earlier, I mentioned defense-in-depth as a fundamental element of a security infrastructure. In moving from a basic to a standardized environment, we implemented a variety of defense-in-depth measures, the top three of which I would recommend to most other organizations embarking on this same journey:

Two-Factor Authentication—In our basic stage, all a user needed to connect to our network (internally or remotely) was a password. Now, for remote users, we added two-factor authentication. Those users would need both a password and a smartcard. We rolled out two-factor authentication to our remote users first because of those 30,000 partners and 46 million monthly remote connections. In our environment, remote users posed a particular threat that we were eager to address.

Secure Wireless—Wireless access was first taking off around 2000, and we wanted to ensure that our users had the business advantage of this technology and that we were not creating a new source

of security threat. Accordingly, Microsoft was among the first corporations to adopt the 802.1x standard for wireless security.

Strong Passwords—It's fundamental but, back in 2000, we didn't have strong password protection. Users could insert blanks or "password" or their names for their password. No more. We quickly required strong passwords with combinations of letters, numbers, and symbols, minimum-required lengths, and frequent changes.

In addition to these primary changes, our first effort to mature our security infrastructure also included some other steps. Because of all those remote connections we have, we implemented and enforced standards for remote access that helped protect us against machines lacking a minimum level of protection against viruses and other malware. We also implemented a network intrusion detection system to monitor network traffic and flag us when it noted suspicious activity.

This approach incorporated elements of the people-process-technology trilogy I mentioned earlier. The specific steps we took mitigated what we saw as our biggest security threats. Each organization's first steps will be somewhat different. Beyond addressing our key concerns, the biggest benefit we saw from moving to a standardized environment was the seismic cultural shift it produced throughout our company. People finally got that security was Microsoft's top priority, and they began to act in ways that reflected that.

On the downside, our security infrastructure was labor-intensive and thus expensive to >>

Bullish on Security

After **Merrill Lynch** upgraded 75,000 desktop PCs to Microsoft Windows XP Service Pack 1 in November 2004, it immediately set out to do something unexpected: upgrade them all to Windows XP Service Pack 2. A key reason: adding significant security enhancements while reducing the update maintenance and support time to install security updates.

"Security is our principal driver moving forward," says **Joe Martella**, director of product engineering for the global technology infrastructure, architecture, and engineering group at Merrill Lynch. "Our view of security isn't based on specific incidents in our company, but rather on what's happened in our entire industry. On a daily basis, our information security and privacy group monitors known security issues to help us stay ahead of problems."

The upgrade helped to enhance security for the firm by adding features, including:

- Web browser pop-up blocker to reduce unwanted online ads and content
- Zone transfer restrictions that limit what a web page can do, based on whether it came from the Internet, local intranet, or a trusted site
- Download monitoring to warn of harmful downloads and enable users to block potentially hazardous files
- Web browser add-on manager to make it easy to manage add-ons to reduce the potential for disruption

"In this business, reputation is everything, so we're doing all we can to protect ours," says Martella.

Merrill Lynch at 2 World Financial Center, where a total of 8,500 employees work.



maintain, because we were not yet as automated as we would ultimately be. For example, alerts from our automated monitoring system still went to security personnel who had to run down and address problems manually, 24x7. Occasionally, that meant security people were sleeping in their offices—not a great way to go.

Next Step: Getting Rational

From late 2003 to early 2006, we worked on the evolution from a standardized to a rational security infrastructure, which basically called for us to refine the “standardized” people, process, and technology changes we’d made, so that we supported our business in more effective ways.

The challenges during this time were massive.

For one, the threats were evolving more quickly and becoming more sophisticated. The time it took for hackers to exploit identified vulnerabilities shrank. And the Internet-wide virus attacks that had long been a threat were now joined by a new danger: the denial of service attack that could turn computers worldwide against a single corporate target. Meanwhile, at Microsoft, information security was still the responsibility of the information security department—the business groups didn’t yet accept

accountability for security, although they held the purse strings that would make security possible.

We continued our awareness campaign throughout this period and added two elements: a risk management framework and service-owner accountability. The risk management framework was tremendously important in making our security infrastructure more mature, because it was the first part of our security effort that tied security directly to business value. It did this by enabling us to decide how much to invest in security, based on the value of the particular asset we were protecting. The framework enabled us to have logical, predictable discussions about security and to begin to get on top of security strategy.

Service-owner accountability for security was another major step because it was a bridge from where we’d been to where we wanted to go in assigning accountability for security to our business groups. True, the service owners weren’t in the

business groups—they were in IT. But as the people with direct accountability to our internal business customers, they were at least closer to the business groups than the rest of our IT organization.

We continued our defense-in-depth strategy as well, building, expanding, and refining on the steps already taken. For example, we expanded our two-factor authentication requirement, previously applied to remote users, to also include internal users with heightened levels of access to our IT infrastructure or to the crown jewels of our intellectual property: our source code. These users with access to our most sensitive resources needed both passwords and smartcard authentication to gain approved access.

We also introduced least privilege access controls, which built on our previous work to limit access to key resources and, thus, the potential for unauthorized access to those resources. These

controls helped to ensure that people only had access to the information they needed for their jobs; for example, only a specific subset of developers with a need to access our source code could do so. And we took steps in new directions. For example, we used industry-standard IPSEC technology to segment our network, making it tougher for someone in—or, someone who hacked into—one part of the network to get to another part.

Automation is hugely important in the move to a rationalized environment because it drives efficiency throughout the system. We automated a range of activities, such as security event monitoring. Beyond mere monitoring, this solution also evaluated the security information it collected and, to an extent, responded automatically. For example, it could detect and shut down transmissions that matched virus signatures. And it could compare network traffic to our typical usage patterns and flag discrepancies. For example, e-mail is the life blood at Microsoft and our remote users almost always go to mail first when they log on. When our monitoring solution detected remote connections that didn’t first go to e-mail, it put the connection in a category that was likely to trigger an alert.

Security monitoring was far from the only process we automated in the move to a rationalized security infrastructure. Other systems undergoing automation included identity and access management, certificate provisioning and

Automation is hugely
important in the move
to a rationalized
environment because it
drives efficiency
throughout the system.

renewals, and vulnerability assessments. In all these processes and systems, reducing the amount of manual administration reduced our costs while increasing reliability and consistency. Taking users as well as administrators out of the equation, as we did when we made digital signature certificate renewal automatic, also meant fewer calls to the help desk and, thus, yielded another layer of savings. Automated processes are also faster and easier to confirm at audit time, yielding still more savings.

Getting security accountability one step closer to the business side was a key benefit of achieving a rationalized security infrastructure. So was automating the vulnerability assessments, because, for the first time, we had an understanding of which machines and devices were vulnerable to each type of threat—enabling us to respond with greater precision and speed to protect those machines when necessary. Where it took weeks to deploy a security update in our standardized environment, we could now do so in mere hours in our rationalized environment.

Our key remaining challenge at this point was to fully integrate service managers and business owners so that security could become a building block in the growth of the business, rather than—as it too often was—an obstacle to that growth.

Step Three: Going Dynamic

That's what Microsoft is now working on as we attempt to mature our security infrastructure to the point where it is truly dynamic, a strategic asset to the company, rather than a tax on business. One element in this effort is continuing the awareness campaigns that have served us so well in the past—only now, those campaigns are focused on the ways that business owners can exert direct accountability for the security of assets under their control.

We're also expanding our defense-in-depth strategy by extending our existing processes and adopting new technologies. For example, we first adopted two-factor authentication for remote users then expanded its use to include internal users with elevated access. Now, we'll extend it to cover all employees and users, both inside and outside the company.

We're automating network access protection so that any device—inside or outside of our network—that wants to connect to us can be checked to confirm it meets our security requirements before the connection is allowed, and can be automatically updated with security software as necessary. As with the extension of strong >>

It's in the Cards

Historically, **Gemplus**, the world's leading provider of smart card solutions, used passwords to authenticate system users internally. To reduce costs, increase efficiency, and enhance application and network security, Gemplus decided to deploy its new authentication system, called "SafeITe," based on smart card technology and Microsoft Windows Server 2003. Gemplus employees now access corporate systems by inserting a smart card and typing a four-digit PIN code. Because they no longer need to remember multiple passwords, calls to the help desk have been reduced and the IT department has realized significant operational savings. Centralized management over user profiles, e-mail systems, web servers, WIFI, and virtual private networks greatly enhances security. Users can also access the corporate network securely from external Internet connections, increasing employee productivity and opportunities for remote working.



Showcase of smart cards on display at the headquarters of the world's leading smart card maker, Gemplus.

authentication to cover all of our users, checking all of our devices is a recognition that the concept of “protecting the edge” of the network is becoming passé. Few companies can afford to have “edges” that enforce lesser levels of security inside than they do outside. The “edge” is going away as every device and every user stands at the frontline of the security effort.

We’re looking at restricting local administrator rights from some users, through something called user account control, in order to help prevent users from unwittingly allowing malware to load on their machines and to lower the cost of managing those machines.

We’re also driving protection down from the network level to the machine and data level. Digital rights management—which controls how data can be used, distributed, or printed after it leaves your computer—is one way to do this. So is something even newer, called BitLocker™ Drive Encryption. This year, there was a rash of news stories about laptops—full of credit card data, veterans’ data, and more—being stolen. With more users working on mobile systems more of the time, we’ll see more of these stories. BitLocker addresses this

threat. It’s a way to render the laptop’s hard drive completely unreadable and unusable to anyone but its authorized user.

These various technologies—network access protection, user account control, and BitLocker drive encryption—aren’t just for Microsoft’s infrastructure. They’re also key features of our new wave of Windows Vista and Longhorn products.

Private Business in a Public World

The key element in our drive to achieve a fully mature, fully dynamic security infrastructure is a new set of processes we call information security governance (ISG). With ISG, we seek to enable the conduct of private business in a public world. That’s a tall order, because it includes not only our intellectual property, but also the IP and other private information of our customers, employees, partners, suppliers, and others with whom we do business. It also requires us to apply security technology in a new way—by designing that technol-

Flying High

In 2004, **Austrian Airlines** launched a project to create a secure web-enabled portal that delivered pilot documentation to tablet PCs. Working with Microsoft Gold Certified Partner, **mii**, Austrian Airlines created an electronic flight rules and communication portal named “eFORCE” and deployed handheld devices running Microsoft Windows XP with Service Pack 2. The highest security settings ensure that key documents on the tablet PCs are read-only

and protected against any modification. The organization’s portal solution meets aviation industry guidelines for document security. In addition, Austrian Airlines has gained a flexible client operating system with advanced stability and security controls, plus a programming technology that delivers industry-standard protection at the coding level.

“With the many policy settings available under Windows XP with SP2, it was a simple and cost-effective process to harden the client devices,” says **Dr. Philipp Haller**, pilot and head of IT coordination flight operations for Austrian Airlines. “By using .NET technology such as ASP.NET in creating our applications, we’ve established a system where security begins right at the system’s very foundation.”



Austrian Airlines Chief Executive Officer Vagn Soerensen

ogy from the ground up to meet newly identified business needs. We also see ISG as a way to protect shareholder value by reducing the shrinkage of our digital assets. And ISG is the mechanism through which we'll meet regulatory and statutory requirements around the world that call for us to demonstrate due care in regard to security and privacy issues.

Implementing ISG calls for new processes, methodologies, policies, and frameworks—all of which help to ensure that our security response covers every conceivable business requirement and does so in a consistent and repeatable way. For example, our ISG “due care” requirements are based on U.S. federal case law and guidelines for judging the effectiveness of corporate regulatory compliance. Our security safeguards—which span areas such as communications security, digital assets, personnel security, physical assets, and so on—are based on standards of the International Standards Organization (specifically, ISO/IEC 17799:2000(E)). The bottom line on ISG is that we're building a system to ensure that security does everything we need it to do, and that it does so in the most effective ways possible.

Back to Phish

In the midst of evolving and maturing our security infrastructure, we were hit with that spear phishing scam. How badly was our employees'

confidential information compromised? It could have been a disaster. A few years earlier, it would have been a disaster.

But now, the answer was: not at all. E-mail software technology called the Sender ID Framework, which can determine whether an e-mail message really originates from its apparent source, detected and deleted the thousands of fraudulent messages before they ever got to our employees in-boxes. No Microsoft employee personal information was put at risk.

Our security infrastructure shielded our employees from the debacle of massive identity theft. They worked that day to deliver value to our customers and shareholders as though nothing had happened. As we continue to mature our security infrastructure, that's what security threats will increasingly mean to our employees: nothing, nothing at all. It's a future well worth working toward. |s|

FOOTNOTES:

¹ Anti-Phishing Working Group, www.antiphishing.org, cited in *Protecting a Business from Online Threats*, Microsoft White Paper, April 2006.

² 2004 CSI/FBI Computer Crime and Security Survey.

³ *Microsoft Technology Investments: Helping Customers Mitigate Security Risk*, October 2005.

About the Author: **Ron Markezich** is chief information officer and vice president of managed solutions at Microsoft.

Security Rx

Wake Forest University Baptist Medical Center, one of the leading academic medical centers in the United States, uses networking, PCs, and mobile technologies extensively to access electronic medical records, computerized physician order entry, and online curriculum. Its staff and student population uses more than 11,500 computers, 15 percent of which are mobile. In 2003, a series of virus attacks cost the center tens of thousands of hours in lost productivity in a single month. In response, and to comply with new regulations protecting patient information, the center deployed a security solution that includes Microsoft Windows XP Service Pack 2. The software's easily configurable automatic firewall helps protect computers both on and off the network, and works with the center's update management system to help prevent future virus attacks.

