

Talking About Security: Nine Essential Messages

www.microsoft.com/partner/securitymessages

Use these talking points to communicate with your customers and the public about security. The information included here discusses the top issues surrounding security and explains how Microsoft® and its partners—including you—are committed to addressing them. Be sure to include information about your own company's capabilities wherever appropriate.

1. Security needs to be a priority for all businesses

Recent months have seen an increase in the frequency and severity of criminal attacks on the world's computer systems. The nature of the risk is changing quickly and becoming more and more serious. Criminal hackers are becoming more sophisticated and the proliferation of high-speed broadband connections—a very positive thing in all other respects—creates an environment in which a virus or worm can spread incredibly fast, impacting businesses and consumers more quickly and significantly than ever before.

There is no silver bullet for security. Customers should take measures to get proactive and ongoing security plans in place to maintain desired security levels long term. Microsoft partners can help.

2. Microsoft is committed to improving security

Microsoft's top priority today is customer security, and the actions we have outlined here are part of ongoing activities in support of Microsoft's Trustworthy Computing initiative. Working with our partners and with the industry, we are delivering the resources, tools, and technologies to help our customers protect their PCs and secure their networks.

Microsoft and its partners are addressing the problem of security today and in the future. Improving computer security means we need to continue to invest and deliver against security threats at a higher level, and we need to simplify and drive the intelligence of security protections deeper into our software to reduce the demands on users and IT administrators. Customers tell us that they expect us to do more—we're listening, and we're working in multiple ways to innovate and address the problem.

Customers have told us they want security tools, features, and settings to be easier to implement and simpler to use,

and that they want security protections to be intrinsic to the software. Recently, Microsoft has taken specific actions to address customer security concerns, including the following:

- Improved patch management processes, policies, and technologies to help customers stay up to date and secure.
- A monthly patch release cycle, rather than weekly, in response to our customers' requests to make the process more predictable and manageable. Patches for emergencies will still be released immediately.
- Global education programs to provide better guidance and tools for securing systems.
- Updates to Microsoft Windows® XP and Windows Server™ 2003 with new safety technologies that will make Windows more resistant to attack even if patches do not yet exist or have not been installed.
- Release of Beta 1 of Windows XP SP2, which includes these safety technologies.
- Criminal prosecution of individuals who intentionally introduce widespread threats.

3. Microsoft's partners are vital to improving security

Technology exists for protecting systems, but the key is implementation. While no software is immune to all criminal attacks, computers can be set up and maintained in ways that minimize risk. To date, however, managing the existing security tools has been too difficult, too complicated, or too challenging—even though when properly implemented many of these tools are highly effective at preventing or mitigating the impact of computer attacks. Often, companies have not planned resources or budget for security plans. That's where a security partner can help.

4. Microsoft's partners can solve a wide range of security problems

Security partners offer business consultation, security risk assessments to identify top vulnerabilities, and solutions to mitigate risk. Many partners offer remote security management, so customers can reduce ongoing security maintenance tasks. Customers can choose the right security partner at <http://directory.microsoft.com>.

5. Microsoft security experts are trained and certified worldwide

Currently, 150 Microsoft Gold Certified Partners worldwide have a security specialization, which means that they not only have deep Microsoft Certified experts on staff, but they have proven experience with documented customer deployments, verified by Microsoft directly with the customer. An additional 30,000 Certified Partners have access to security training and resources.

6. Microsoft's security partners are uniquely prepared to mobilize for broad threats

Microsoft Partners are among the first to be notified of security threats—and they're among the first to be armed with the appropriate measures to stop them. Partners subscribe to key security alerts and resources from Microsoft and industry sources. Should a widespread threat occur, Microsoft Partners are aware of key steps to take with customers.

7. Partners receive specialized security information and tools from Microsoft

Microsoft builds resources that help partners identify key risks, assess IT environments, and manage and mitigate risks with appropriate technologies. Partners utilize numerous tools from Microsoft, including Microsoft Baseline Security Analyzer, Software Update Service, ISA Server, Systems Management Server, and technologies built into Microsoft Office (such as Digital Rights Management) and Windows Server (such as Internet Information Services). In addition, partners have around-the-clock access to Microsoft Technical Support, so they can get answers to tough questions around security solutions.

8. What you can do to better protect your business

Microsoft advocates a defense-in-depth approach to protect organizations against the increasing number of worms, viruses, and malicious attackers. In addition to having **firewalls** and **antivirus solutions** in place, companies should take further steps to increase their organization's security. Actions such as locking down computer and network infrastructure, proactively deploying patches, and centrally managing users and computers will enable IT professionals to reduce the potential for malicious exploits and increase control over critical corporate resources.

For defense-in-depth security, Microsoft recommends the following steps for IT professionals:

- **Conduct a security risk assessment.**

Determine where you are most vulnerable and prioritize based on our criteria such as value of data, cost to secure, or imposed regulations. See the Security Risk Assessment Checklist.

- **Lock down your servers, workstations, and network infrastructure to reduce the potential for security breaches.**

Securing both servers and workstations effectively may require disabling services, removing specific user rights, keeping the operating system up to date, and using distributed firewall products. In addition, network security requires proper configuration of network devices—firewalls, VPN gateways, routers, and switches—to protect the data it forwards.

- **Design and deploy a proactive patch management strategy to keep ahead of potential exploits.**

Proactive assessment of vulnerabilities and the application of security patches are required for increased security. Microsoft is focused on providing concise information, prescriptive techniques, tools, and templates to help organizations cost-effectively maintain an up-to-date, secure and reliable environment. Many guides and tools can help in centrally managing the deployment of critical patches to clients and servers.

- **Secure corporate users and computers with centralized identity and access management.**

Larger organizations face many challenges in identity and access management, including password management, maintaining multiple user accounts, and account policy enforcement. IT professionals can increase security and reduce complexity through: fully integrated directory and security services; single sign-on to multiple applications, Web sites, and services; the automation of account provisioning and de-provisioning; and providing interoperability with other platforms and applications. Customers can work with a Microsoft Partner or attend an IT-targeted, free Microsoft Security Briefing that can be signed-up for online at www.microsoft.com/events.