

SCOPE:

Whether your organization has firewalls and a security policy or not, it's prudent to regularly evaluate your security approach. Review and answer the following questions before implementing any further firewall technology and/or security policy additions or changes.

Identify which resources must absolutely be secure and in which order of priority:

- Mission critical
- Redundant back-up system(s)
- Secondary
- Base systems

Identify minimum security needs for the following WAN connections:

- Employee remote dial-up
- Office-to-office VPN
- Employee and vendor broadband (DSL, cable modem, etc.)
- Vendor access
- Business-to-business access

Does your security team have quick access to this network documentation?

- Network diagrams
- Trending data
- Protocol utilization
- Data points
- Access points
- Major vendors' point of contact information (ISP, telco, firewall vendor)

Does your security team know the order in which systems must be restored?

- The security response team must have a full understanding of which systems need to be restored to full operation and in what order.
- Does this order meet your business objectives and priorities?

Does your information disclosure policy address the following in relationship to a security issue?

- What information is shared with others?
- Is information shared internally, departmentally, externally, etc?
- Under which circumstances?
- Mission critical information?
- Secondary intrusion information?
- Who has the authority to initiate information disclosure (Chief Security Officer, legal, HR)?

Have you provided a way of documenting, distributing, and following up on security violation reports? For example:

- Denied access messages
- Failed passwords/login attempts
- Attempts to access back doors

Have you provided for alternative communication methods for intruder attacks/penetrations? Consider using:

- Cell phones
- Numeric pager codes
- Fax machines

Have you established your cycle of updates and mock drills?

- Are policies and procedures updated regularly (quarterly, bi-annually, annually)?
- Do you involve multiple departments (IT, HR, legal, upper management)?
- Do you run periodic drills to test your systems and your procedures?

Have you reviewed the legality of your security policy and procedures?

Working with your HR department and legal counsel, consider the following:

- Are your policies enforceable?
- Do your policies and practices conform to local, state, and federal laws?
- Are you providing due diligence to protect confidential information?
- Is there a clear-cut procedure for a chain of custody for documentation from an intrusion?
- Are the team and the company legitimately protected in case of a severe intrusion?
- What would be your company's risks if an attacker were to penetrate the systems of another company that uses your systems?
- Do your policies and procedures provide for proper care of customer information?
- What are your liabilities if confidential data (corporate, vendor, customer) is taken and used by an intruder?

Have you reviewed lessons learned?

- Does your firewall intruder-alert detection system work?
- Do your response procedures work?
- Do your processes provide for the correct steps to neutralize any additional threats?
- What did not work?
- What can be changed to bolster your procedures?

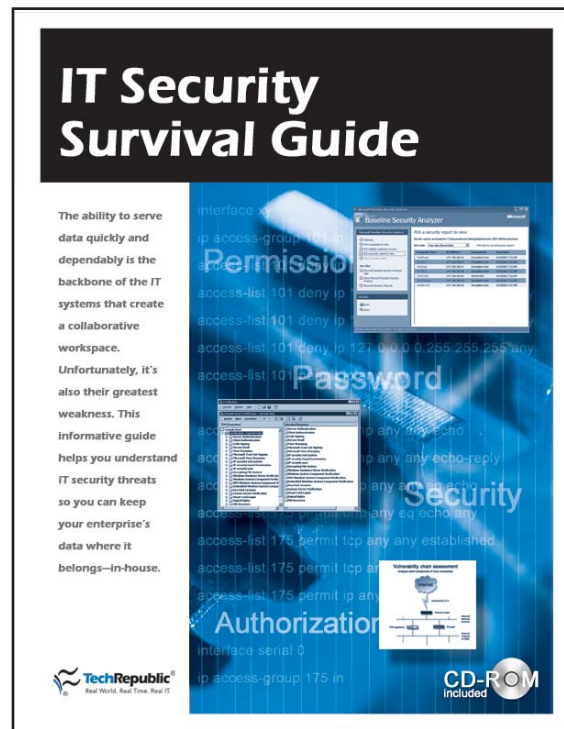
IT Security Survival Guide

Today's world is filled with threats to your information systems' security. How do you recognize and safeguard against these network threats? It takes more than a firewall, an e-mail policy, and a locked door to keep out the viruses, hackers, and worms.

Plan, deploy, and maintain responsible and airtight security measures before it starts to cost your organization money. Learn to identify and eliminate weak points in your network with TechRepublic's *IT Security Survival Guide*. The companion CD-ROM gives you the tools to teach your end users about safe computing practices.

Be prepared with information that will help you:

- Prevent workstation intrusions
- Integrate security technologies into a heterogeneous environment
- Enhance e-mail security in Outlook and Exchange
- Recognize IIS vulnerabilities and fixes
- Plug known security holes in Windows NT/2000/XP networks
- Interpret firewall log files
- Learn how crackers find and exploit network security holes



Order Today!

Yes! Please send my copy of *IT Security Survival Guide*. I'll receive my book and CD-ROM at the special Member rate of only \$69 plus \$5.95 s&h (\$8.95 s&h Canada, \$12.95 s&h international). Bonus: Free shipping in the U.S. if I pay now! If I'm not completely satisfied, I can return my copy within 30 days for a full refund.