



A PRACTICAL GUIDE FOR BETTER SECURITY
JULY 2004

CONTENTS

INTRODUCTION TO NETWORK SECURITY	3
What you'll get out of reading this paper	3
Security is important—take charge of it now	3
Chapter 11 - why developing your security policy is important	4
THE SECURITY PLANNING PROCESS	5
Develop your security planning team	5
Analyze your assets	7
Identify your system vulnerabilities	9
Create policies to protect your assets	14
Design and implement a security solution that fits your resources and skills	17
STAY UP-TO-DATE WITH WATCHGUARD® LIVESECURITY® SERVICE	20
Software updates	21
Technical support	21
Security broadcasts	21
Self-help resources	22
SUMMARY: EFFECTIVE SECURITY PROTECTS THE CRITICAL POINTS OF YOUR NETWORK	23
Protecting the corporate network	23
Protecting network communications	23
Protecting server content	23
Providing greater network protection with additional security services	23
WatchGuard: The Security You Really Need	24

INTRODUCTION TO NETWORK SECURITY

What if network security were as much about your bottom line as it is about deterring threats? A security plan that addresses your critical business concerns – customer confidence, data integrity, increased productivity, and cost savings – will give you the business advantage by thoroughly targeting security fissures at their source: the people and their processes.

Practical security is all about finding the right balance between protecting your business interests and resources, and letting people get their jobs done. Everyone is aware of the threats. Establishing a network security strategy is only feasible, however, if you understand that the biggest obstacles you'll grapple with may well come from within your organization.

WHAT YOU'LL GET OUT OF READING THIS PAPER

As you read through this paper, it will help you to keep a few things in mind:

- This paper is geared towards the small- to mid-sized enterprise.
- Not all recommendations in this paper are for everyone. In fact, depending on your specific needs, you may just want to ignore some of them.
- You will derive some benefit from these recommendations even if you only partially implement them. Don't be put off by the size of the job – take small steps and keep moving towards the goal of thorough security.
- Realize that you'll never reach that goal. No company anywhere is 100% successful in maintaining a perfectly secure, perfectly functioning network all of the time. Keep your eye on the destination; it's a good and worthy goal, even if you never reach it.
- Only you can determine what's best for your company. Good advice is great to have, but ultimately you need to make the final decisions and take responsibility for them.
- If you're just starting out, don't be daunted by the apparent complexity of the task. Remember that if you are smart enough to be reading this paper, you are smart enough to begin to implement its suggestions.
- Do what you can now, and keep a list of things to do later as time and resources allow. Keep another list of things you currently believe to be irrelevant, and periodically re-examine that list to see if anything has changed.

Now, on to the interesting stuff.

SECURITY IS IMPORTANT—TAKE CHARGE OF IT NOW

Internal theft and disgruntled employees are two very real dangers to your company's well being, but even they aren't the biggest problems. The real enemy is apathy. To employees, security policies are an annoying inconvenience, which is why many people don't cooperate. To those in your organization who apportion resources, security may be treated as overhead rather than a smart business move.

People tolerate seat belts because they know humans and automobiles can be a dangerous combination, and that cars are not invulnerable bubbles of protection. But many people working with critical company information expect the machines of network technology to protect their goods, and are blind to the fact that the same human fallibility that creates bad driving creates indifference to the threats against information assets.

By now you may be saying, “If only applying a security plan to increase my productivity and protect my bottom line were as simple as double-clicking!” Can we deliver on that wish? Uh, no. But reading this guide can sure make the process easier, and while it’s not an exhaustive treatise on network security protection, we hope it gives you a framework to create your own security plan.

CHAPTER 11 – WHY DEVELOPING YOUR SECURITY POLICY IS IMPORTANT

There are two critical things you should have in order to implement effective security:

- **A Security Solution:** All of the tools you need to protect the critical points of your network.
- **A Security Policy:** A documented policy statement that describes the security plan for your business.

This guide will help you develop both components. But first, a word about this “Chapter 11” business.

No, there isn’t a pagination problem. We’ve started this section with Chapter 11 because that’s where many companies are by the time they realize they need a security policy – as they’re fending off creditors after being brought to the brink of collapse by a security breach. And even if they are lucky enough to recover from a crippling attack on their business systems, they’ll be wasting their time. They’ll never get their policy manual created before they run out of money to pay wages.

It is understandable why creating a security policy is the last thing most people want to do. We’re bombarded with so much information about security that it’s difficult to keep it all in perspective. The mutable nature of business environments and the elements that threaten business assets makes the task of analyzing it all seem too overwhelming. Corporations and governments sacrifice massive amounts of money to security breaches. These breaches don’t come only in the form of viruses or worms, they also come as proprietary information theft and financial fraud. In fact, these last two offenses alone comprise some of the biggest computer crime losses in recent years.

One fifth of the organizations that experienced a security incident spent more than a week trying to recover, according to a study by PricewaterhouseCoopers (PwC). That’s a week of costly overhead and potentially no revenue. What would a security breach like this cost your business?

So we’ve started this section with Chapter 11 to reinforce the importance of developing a security policy and implementing a security solution before it’s too late. Now, let’s get down to business.

THE SECURITY PLANNING PROCESS

Your security development process should be a precise, all-encompassing, methodical approach to creating a long-term security solution. To develop your plan, you should:

- Develop your security planning team
- Analyze your business assets
- Identify your system vulnerabilities
- Create policies and plans to protect your assets
- Design and implement a security solution that fits your resources and skills

DEVELOP YOUR SECURITY PLANNING TEAM

The first thing you need to do to develop effective security is to establish a team that will work with you to gather and analyze all of the information. But before you create your team, you need to recognize and be able to explain that the most important concept underlying real-world security is the principle of least access: shut everybody out of everything on your network unless they have a solid business reason to be granted access to it.

Your development team should be made up of people who work with your network and the Internet, but who come from different functional areas of the company. Each manager in your company has a unique view of the needs and risks. You need people who know something about the technology, but also some who know about business. Include some people from the trenches, too; there is nothing less useful than a painstakingly documented security policy that, when implemented, keeps the shipping department from being able to track packages, or blocks the sales reps from network resources while they are on the road.

Here is a suggested roster for your security team:

- Senior level administrators
- Members of the management team who enforce policy
- Members of the legal staff
- User representatives
- Writers

A security policy is vital, but if your plan is too ambitious or your framework is too complicated, people will ignore it, and it will be unenforceable. One way to avoid discouraging your employees is to work with representatives from all segments of your organization.

Your network security plans will have widespread effects. Thinking about security within the context of all your company's information assets, the total risk to the organization, and the

plan's potential ROI will not only produce a more thorough security policy, but you may also find it easier to get buy-in from other department leaders for employee training.

Security Planning Principles

Your security plan should address the following simple principles:

- Security should support the goals of your entire organization.
- Security is a part of good management.
- Security is a good organizational tool.
- Security should be cost-effective.
- Responsibilities and accountability for security-related issues must be clearly defined.
- Effective security cannot be achieved without proper integration of security tools.
- Security requires cooperation between departments.
- Security solutions should be audited and reassessed every few months.

ANALYZE YOUR ASSETS

Work with representatives from other departments to identify critical assets that could be affected by IT security policies, and how your plan will mesh with their existing policies. You can use the table below to help you get started.

DEPARTMENT	INFORMATION ASSETS
Operations	
Media	
Documentation	
Finance	
Human Resources	
Development	
Quality Assurance	
Sales	
Manufacturing	

BUILD A COST ARGUMENT

While you are analyzing your assets, you will want to make a cost argument for good security. Lack of a thorough, well-implemented security plan can result in losses to the following:

- **Your Business:** Every minute your systems are down, a competitor is only a phone call or Web site visit away from your customers.
- **Your Assets:** Do you know what proprietary information has been exposed to the outside world by employees who aren't aware of security gaps?
- **Your Data:** Research, records, and other vital information are expensive (and sometimes impossible) to reproduce or recover.
- **Your Time:** When your network administrators are researching a damage trail, they're not working on other critical projects. What does your IT staff cost you on an hourly basis?
- **Your Legal Budget:** Do you really know what it will cost you if you violate BIS or HIPAA regulations, or are involved in a shareholder or vendor lawsuit?

ESTABLISH THE BUSINESS VALUE OF A SECURITY SOLUTION

One of the problems with security is that it is treated as an overhead expense rather than necessary insurance. Security should be calculated in the same way as your other business insurance policies. How much do you pay for fire insurance? And what is the risk of a catastrophic fire compared to the risk of a security breach?

Before you begin planning your network security, determine the business value of your IT infrastructure, and the consequences of a security breach. A cost argument is meaningful information to those in your organization who are in charge of allotting adequate resources for security implementation.

Your outline should include:

1. The business value of the IT infrastructure as it serves your company mission
2. The business consequences of an IT security breach
3. The current solutions and remedies you have in place
4. The lifespan of each solution, and its cost
5. The estimated cost of recovery from a security incident

What do you have to lose?

Only you can estimate values for your unique circumstance, but the main risks include:

- Financial loss
- Loss of time spent rebuilding or repairing damage (none of that time enhances your bottom line, but it does permit you to stay in business)
- Loss of your competitive advantage

- Legal penalties (contractual penalties or fines, or liability if customer privacy is compromised)
- Loss of reputation and customer confidence

IDENTIFY YOUR SYSTEM VULNERABILITIES

There are some fun things you can do, and questions you can ask while investigating your system's vulnerabilities. For example, spend some time thinking about how you would attack your company. Try to determine which parts of your system are visible to external networks, modems, routers, remote access servers, etc. Where are your important systems and configurations kept and how easy would it be for you to access them? How easy would it be for you to steal passwords? Could you hack them, or could you get them from employees? If you think like a hacker, you will unearth system weaknesses you didn't know existed. You might want to include other reliable IT brains in this process to cover all the bases, or take advantage of an outside service such as Vulnerability Assessment (VA).

VULNERABILITY ASSESSMENTS

The basic point of Vulnerability Assessment (VA) is to make your network more secure. VA involves examining your network for security flaws that might allow attackers to get inside. VA follows the same simple concept described above: to figure out how an attacker would break in, you must look at your network from the hacker's perspective.

However, VA involves more than imagining attacks on your network. It also consists of documenting security holes discovered during the audit, prioritizing each vulnerability according to risk, and implementing the appropriate fixes. So how do you perform a vulnerability assessment? Unless you have experience as a hacker, you're left with two choices. Either hire a qualified third party to perform your security assessment, or use automated tools that perform *vulnerability scans* for you.

AUTOMATED VULNERABILITY SCANS

If you are a do-it-yourself type, you can perform your own quick Vulnerability Assessment with one of the many automated network security scanners available. If you don't have the time or skilled personnel who can help with this process, there are two basic types of VA you can take advantage of: outside consultant audits, or automated VA scans.

For a fee, you can hire consultants to perform penetration tests on your network to discover vulnerabilities. The best "pen-testers" are essentially "white hat" hackers—people with the skill and knowledge of network hackers, but who use their skills for good, not evil.

The newest attacks are automated, requiring no human trigger to deliver their destructive payloads. The speed with which they can then propagate outpaces the speed with which any human can deal with them, introducing the need for automated assessment and vulnerability management.

Since automated attack tools make hackers and criminals more effective, how else can you fight back unless you use automated defensive measures? Vulnerability assessment can (and should) be one of those automated defense measures on your network.

PROTECT THE NETWORK PERIMETER

Effective security protects the critical points of your network. In today's networks those critical points usually consist of the network perimeter, network communications, server content and system configurations, and individual desktops. Focus on your vulnerability levels in these areas and determine where you need to implement protection.

Routers

Routers are the first company resource the Internet traffic hits. Customize your router configuration settings and don't leave any user name, account name, or password set to its default.

Firewalls

The flip side of an Internet economy is that companies must expose parts of their systems to the public. A firewall can protect these open access zones by creating a secure perimeter around your network, and defining exactly what, and who, can get in or out of your network at any time.

When you select a firewall, keep in mind the features and screening methods you need. The size of your enterprise will also dictate the firewall you need to most benefit your business.

PROTECT NETWORK COMMUNICATIONS

Since the Internet is a public network, any confidential information you send across can be intercepted at any of the devices it passes through. Encryption turns your words into code, with only authorized parties possessing the key to decipher it, protecting your confidentiality and the integrity of the information, and verifying the sender. Since this is like creating your own private area of the Internet, these systems are known as virtual private networks (VPNs), and are much less expensive than using leased private lines.

VPNs allow businesses to take advantage of the Internet, and offer affordable broadband transmissions for secure, private communications. VPN technology can bring outstanding benefits to mobile users, branch offices, and extranets.

PROTECT SERVER CONTENT

With thousands of settings on a server, it only takes one critical subset to be changed without your knowledge to really mess up your day. All too often the source of these unhelpful changes is one of your employees, or even one of your IT staff. There's a lot of danger from people who have a little knowledge about IT processes and want to try applying that knowledge.

The millennium imposed a rigid discipline on IT departments. Everyone feared that if they tinkered with the systems, they would be identified as the person who caused an IT

meltdown when the dates changed. The alternative to waiting until the year 3000 to get organized is to find a management system that battens down all the hatches by protecting the critical server software and memory resources that attackers exploit in order to take control of your server.

PROTECT THE DESKTOP ENVIRONMENT

The desktop can often be the weakest link in a defense system. Antivirus software is a must for protection against known viruses, Web attacks, and e-mail intrusions to desktop environments and infrastructures. Your antivirus software should be updated regularly to be most effective.

PUT THE DANGERS INTO PERSPECTIVE

You can assess the danger to your company’s network security in terms of threat, vulnerability, and risk—threat being the degree of potential damage, vulnerability being how readily the threat can be exploited on your own network, and risk being the likelihood that the given vulnerability will be exploited by that possible threat. In other words, Risk = Vulnerability x Threat.

To counteract security dangers as effectively as possible, work out the values for these variables. What you consider a risk depends on the value you place on your information and your uptime.

Inventory sources of risk

You can use the table below to help you start assessing the risk posed by your network security.

Sources of Risk	Vulnerabilities x	Threats =	Possibility of Risk
Company procedures (Are they poor or inadequate?)	On a low-vulnerability (1) to critically weak (5) scale, rate the vulnerabilities of these risk sources. What are the big holes?	What are the dangers (viruses, hackers) to the systems related to each source, and how would you rank them on a low/high 1-5 scale?	
Business partners (How do they access shared information?)			
Third-party service providers (Which systems to they have access to?)			

Company Web site (What's protecting your Web server?)			
IT Staff (Are they under-trained and/or overworked?)			
Employees (Are they untrained in network security policy? What are they allowed to do on the corporate network?)			

Identify the risks to identify the priorities

Just how big are those numbers in the right-hand columns on the previous page? They should give you a picture of what's most vulnerable, and therefore what should be first on your list to secure.

The top computer crime losses¹ in order of occurrence are:

- Viruses
- Laptop theft
- Net abuse
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- System penetration

The largest financial losses² are caused by:

- Proprietary information theft
- Financial fraud
- Insider net abuse
- DoS and DDoS attacks

So keep in mind that the vulnerabilities are more complicated than can be addressed by virus scanning software or passwords. A security hole is a hole, whether it is an open firewall port, or a laptop someone sets on the airport floor while he digs for change for his coffee.

Identify all of these security outlets. They may be the result of hostility or benign ignorance. Either way, the risks are just as high; the prevalent abuse of Internet access privileges by employees, for example, can mean anything from downloading pornography to downloading a program that (supposedly) installs a banner of little dancing bears. So, do you want to pay for the lawsuit, or pay for the time it takes for everyone to redo the work they've done in the last six weeks? Does it matter?

¹ CSI/FBI Survey

² CSI/FBI Survey

CREATE POLICIES TO PROTECT YOUR ASSETS

After evaluating your assets, the risks, and the security systems you need, you are ready to start the policy-crafting process. Begin by listing and then outlining every policy document you will need (e.g., acceptable use, server security, VPN security, extranet, remote access, wireless communications, etc.).

Your top-level policy should state:

- What you are protecting and how you will go about it
- How policy changes will be managed
- Who has a voice in policy change

Assign each policy section to an individual staff member, then select a review group, and schedule reviews and deadlines. Your policy should be audited regularly, and should undergo a thorough periodic review. Sitting down to write a database password policy isn't easy, but luckily you can find many free templates on the Internet. When drafting your policies, consider addressing the following areas:

- Effective implementation of controls
- Internal data protection
- Standardized product selection and configuration guidelines
- Liability minimization
- Ensuring consistency of methods
- Change management process
- Company network use guidelines

IMPORTANT IT PROCESSES AND POLICIES

Documenting the tasks you already do will provide the data for your policy planning process. The rules in this list are essential to day-to-day IT security. Remember that devices cannot replace planning; software and firewalls are not ready-made security, but tools which you must wield with skill and good judgment.

- **Backup and storage** are the foundation of your road to recovery after any security breach. Data backup can be to CDs or DVDs, and should be stored offsite. There are even companies that will manage your storage and backup for you.
- **Test your backups** and make sure restoring from the backup media actually works.
- **Learn to read the logs** for your routers, firewalls, Web servers, file servers, etc., and teach yourself to recognize normal and abnormal traffic. Try to audit logs as consistently as possible.
- **Disable or remove all unnecessary services** *BEFORE* connecting systems.

- **Change passwords immediately** upon installation. Never run systems using default passwords.
- **When new faults are identified, test and update your systems** with appropriate patches as soon as you can. Remember that not all patches are created equal, and neither do they address equally severe issues. Use good judgment in deciding when to patch.
- **Consider encrypting all raw, unencrypted text** before sending it across the Internet. Remember that e-mail is raw, unencrypted text.
- **Never give passwords over the phone** without authenticating the individual.
- **Always examine new network devices** and configure them before putting them into production.
- **Create safer passwords** by using passwords with one or more of the following characteristics: many characters; using numbers, letters, and punctuation; case-sensitive; no default passwords; and no words straight from the dictionary. Make a point of protecting the repository where you store the passwords.
- **Protect password integrity** with a comprehensive set of rules. Bear in mind that the more complicated the password scheme, the more time you will spend on support. It may be more cost-effective to procure third-party technology for password management.
- **Enforce user password changes** every 60 days.
- **Change administrator passwords** every 30 days.
- **Consider encrypting data** on all laptops to prevent data theft should a laptop be stolen.

ABOUT INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) are most useful as logging and troubleshooting tools that can help you identify the types of attacks, and in some cases, the attacker, of your system. Keep in mind that IDS is Intrusion Detection, not Intrusion Prevention. Intrusion Detection is considered a passive system because although it discovers attacks, it can do nothing to prevent them. Intrusion Prevention technology, however, discovers attacks, can identify attackers and render them incapable of further attempts, and enable blocking capability against threats.

RECOMMENDATIONS FOR DISASTER RECOVERY

Despite a battery of precautions, you cannot protect against every eventuality. What if:

- You have backed up your data, but the backup is not available when you need it?
- Your backup data is destroyed along with the original?
- Your systems are in place and working, but an event occurs that prohibits employees from getting to, or into, the building?

These scenarios illustrate that, no matter how comprehensive your security measures, you should always be prepared for the prospect of your systems and your ability to conduct business being compromised. You should make plans that minimize the damage by generating the most rapid recovery possible. But how do you know what is required to recover when you've never been in that situation, and can hardly imagine what that situation would be like?

You don't have time to be creative once the event has taken place, so it's useful to orchestrate and rehearse disaster recovery, and define clear roles for each person.

Identify possible scenarios

How would you get around these problems?

- Network down
- Servers down
- All data deleted
- Acts of God (roads to work blocked, headquarters flooded, extensive fire damage)
- Senior IT staff stranded elsewhere

Share this list with acquaintances from other organizations. Can they add to it?

Appoint your recovery team

Assign key roles and discuss the breadth of functions and responsibilities. Some key roles might be:

- The **Field General**, who runs the recovery process
- The **Diagnostician**, who troubleshoots
- The **Communicator**, who logs activities and keeps everyone informed
- **Recovery Operators**, who deploy backups and implement solutions

Note: The Field General and the Diagnostician are two separate full-time functions and demand separate people, as do the Recovery Operators and the Communicator roles.

Start that well-oiled machine

- **Write and rehearse**
People serving key roles should have at least a rough set of tasks to do in the event of an emergency. Plan time to practice the responses. The more practice you get, the better. Keep thinking of new things that could go wrong, and how you would respond to them.
- **Keep communicating**
In the event of a disaster; keep department managers and remote sites informed. Recover your top ten customers fast, and keep them up-to-date.
- **Record it**
Log all events that occur during the recovery process. Your designated communicator

should log and track all internal, remote, and customer problems in a way that doesn't interrupt recovery actions.

- **Restore and recover**

Restoring the system is as important as recovery. In other words, after switching to backups, correctly restoring the primary system should follow. Failing to do this correctly prolongs the perception of unreliability. Unless the fix can be done quickly, execute the recovery first and repair the source of outage later.

DESIGN AND IMPLEMENT A SECURITY SOLUTION THAT FITS YOUR RESOURCES AND SKILLS

SECURITY FUNDAMENTALS FOR END USERS

If you do not have a reference point for corrective action, enforcement will be very difficult. Clear instructions and a guide to the complete security policy provide the framework for regulation. Remember that security training needs to be regularly administered and updated. Management should fulfill their obligation by providing on-the-job employee training that addresses security policy, procedures, and the company's business philosophy and priorities.

Educate users about the need for the following restrictions and guidelines. Not all of these will apply in all cases, but this is a good start. Modify the list below to suit your particular environment:

- Users should not read, modify, delete, or copy a file that belongs to another person, unless formal permission is granted.
- Users should understand that the *ability* to read, modify, delete, or copy a file does not imply *permission*.
- Every user should be responsible for maintaining at least one current backup of important files.
- Users should make a backup copy of a file every time a significant change to it is made.
- Users should never download executable files from the Internet.
- Companies should prohibit users from accessing certain Web sites.
- Companies should limit time users spend personal Web surfing.
- No laptop should be connected to the network without proper antivirus software and firewall protection.
- Users should understand that exporting software is a disciplinary offense.
- Users should not share or expose their passwords to friends or family.
- Users should delete all spam and junk e-mail without forwarding it on to other users.
- Users should never open macros.

In addition, staff should be educated on:

- Access privilege policies that clearly define who in the organization is granted access and who is denied access to certain areas and systems.

- Emergency response procedures, so that in the event of an accident, security breach, or error, procedures can be easily followed.
- Legal, contractual, copyright, and data protection considerations.

POLICY ENFORCEMENT AND MANAGEMENT

Not only do you have to be able to outline a plan, but you should be able to articulate and endorse that plan to non-IT staff, including being able to answer the questions:

- What is network security?
- What is the staff's liability?
- What are the benefits and disadvantages of security?
- What are the quantifiable losses associated with security, and what do the latest case studies say?
- What are the benefits of security to management and administration?
- What are the issues end users may have with security, and how can IT overcome objections?
- What is the importance of management's commitment?
- How do we describe our security strategy?

Enlist employees and get them on your side

Because the biggest obstacle to IT security policy is employee awareness, clear communication and training are two of the most crucial responsibilities you have in getting end users to help you secure your company assets. Internal security compromises arise primarily from unwitting actions and inconvenience, rather than fraud or malice. The staff needs to feel that a security policy is in their interest, not simply a scheme to raise the profile of the IT manager.

So how do you make people aware of the importance of following the security rules? First, you need to train your company managers. Management personnel rarely support projects they don't understand, but if you make sure that management understands the benefits of security, they will support its implementation in their own departments.

Careful planning, an even-handed delivery, and a little luck will win management over to how important security is to the company mission. The next step is to deliver the same message to all employees.

The biggest security faux pas

Identifying the damage that employees are most likely to cause³ will help you craft your security education plan. The following table lists the most notable accidental actions:

End User Security Mistakes	Remedies
Opening unsolicited e-mail attachments	Issue strong warnings about the danger of attachments, or block all but the safest type of attachment with your firewall or from your e-mail server.
Failing to install security patches	Install patches for them as appropriate; many vendors offer automation installation solutions.
Installing screen savers and games without IT permission	Delete all unauthorized software, and block downloads of unauthorized software (don't forget the big lecture).
Failing to making backups or not testing to make sure the backups work	Automate centralized backup and testing.
Management Security Mistakes	Remedies
Assigning the untrained employee to carry out security-sensitive work	Make training a regular part of your professional growth plan.
Failing to understand security as a business issue	Make a list of everything you've got to lose, and how much it's worth to you.
Opting for quick fixes rather than embracing the full operational effects of security	See above.
Relying on a firewall as a universal security solution	Get the latest information about best security practices (i.e., a layered system that includes antivirus, intrusion detection and prevention, and application layer filtering).
Failing to put a value on information (and its subsequent loss) until you have to file an insurance claim	Nothing replaces planning ahead.
Pretending the problem will go away if ignored	Now about a nice hacking demo?

³ SANS Institute

ONGOING MANAGEMENT

The success of your security policy depends on effective internal marketing, which is a continual process, just like network security management. You can tell people what is important and what you want them to do, and they may well accept it, but then you have to constantly remind them. Fortunately, you brought representatives from other company areas into the process early on, so they're all on board with you by this time.

You should be constantly auditing what goes on in your company's IT system, assessing trends and blocking problems before they arise. Okay, we know you should do this assess/block stuff in theory, but in practice we know you'll be busy. So once you are certain you have secured your IT infrastructure as best you can, you will be far better employed educating the users. It's more realistic to identify the most common forms of mistakes your users will make than to expect that you'll be able to thinly spread yourself across the myriad maintenance tasks that appear daily.

STAY UP-TO-DATE WITH WATCHGUARD® LIVESECURITY® SERVICE

So you think you've secured your business, and you've successfully got the users to go along with the plan. You're now running a tight ship and your business is secured to within an inch of its life. Well done. You can sit back and relax. For two minutes.

That's all it takes for the security landscape to change. There are people out there dreaming up viruses and cooking up schemes to bring business crashing to a halt. There are plenty of tools available freely on the Internet that enables hackers to break into e-commerce sites and steal customer credit card information. There are obsessive individuals who, for reasons of their own, find it necessary to discover all the vulnerabilities of popular operating systems and publish the details on the Internet. If you take your eye off the ball for even a moment, you can find yourself vulnerable.

How do you stay on top of it all? Luckily there are people working to counter these threats. WatchGuard®, for example, has a team of experts tracking the latest developments in hacking, worms and viruses, malicious macros, denial-of-service attacks, and a myriad of other methods people devise to interrupt business.

Out of the box, every WatchGuard security appliance is backed by a renewable LiveSecurity® Service subscription. LiveSecurity Service is simply the most comprehensive bundled support offering in the industry. By activating your subscription, you're covered from day one with a suite of services unmatched by the competition, which includes:

- Software updates
- Technical support
- Security broadcasts
- Self-help resources

SOFTWARE UPDATES

Hackers never sleep. That's why your LiveSecurity[®] Service subscription gives you access to ongoing functional enhancements for your WatchGuard[®] product, along with updates to address specific threats when they occur. And you're not limited to minor software patches – new software versions for your products are available to active subscribers at no additional cost.

TECHNICAL SUPPORT

When you need assistance, our expert teams are ready to help. Your LiveSecurity Service subscription includes world-class WatchGuard technical support resources at no additional cost. You get:

- A highly-trained team of support representatives
- Four-hour targeted maximum response time
- Access to technical support in every global time zone through a single, convenient contact number, or by e-mail

SECURITY BROADCASTS

As the frequency of new attacks and vulnerabilities continues to surge, the task of ensuring that your network is secure becomes even more of a challenge. WatchGuard helps customers by absorbing this burden. A dedicated group of network security experts monitor the Internet to identify emerging threats, and then delivers alerts that tell you specifically what you can do to address each new menace. You can choose to receive all or any of the following broadcasts:

Editorials

The WatchGuard LiveSecurity Advisory Council, comprised of top security consultants, offers views on Internet security and provides a source of continuing education.

Foundation articles

Foundation articles are specifically written for novice security administrators, non-technical co-workers, and executives.

Information alerts

Get timely analysis of breaking Internet security events along with instructions on how to keep your network secure. With LiveSecurity Service, you are kept up-to-date, and you'll know what to do.

Virus alerts

Our strategic alliance with McAfee[®] gives you real-time virus alerts and specific information on how to protect your systems.

Threat responses

Receive valuable, detailed information on the largest and most far-reaching security vulnerabilities as they happen, and what WatchGuard® is doing to help you keep your network secure.

Support flashes

Technical tutorials offer tips for managing your WatchGuard products.

Vulnerability assessment

With WatchGuard AuditScan™, powered by Qualys®, you can run comprehensive network security audits on demand, and have the results and suggested solutions delivered in minutes without the extra cost of software or hardware deployment and maintenance.

New from WatchGuard®

When new products and services are available, LiveSecurity Service subscribers are the first to know.

SELF-HELP RESOURCES

In addition to providing you with direct personal support, your LiveSecurity Service subscription entitles you to access a variety of online tools specifically designed to answer many of the more common questions about the technical aspects of installing, configuring, and maintaining your WatchGuard products.

Online training

Get up to speed quickly on network security issues with a series of interactive online training courses. Learn exactly what to do to protect valuable information assets and make the most of your WatchGuard products.

Online forums

Your LiveSecurity Service subscription gives you access to forums reserved for customers only.

Knowledge base and documentation

Get 24-hour access to valuable resources, FAQs for experts and novices alike, user guides and online help, a searchable knowledge base, and a centralized index of essential reading are available to subscribers online.

In summary, you might think your company is secure, but the landscape is constantly shifting. WatchGuard® LiveSecurity® Service keeps you on terra firma.

SUMMARY: EFFECTIVE SECURITY PROTECTS THE CRITICAL POINTS OF YOUR NETWORK

There is no single solution that cures every security problem. Today's network security requires a wide reach, including VPN, intrusion prevention, application layer inspection, antivirus, and content security. Yet none of these protections alone can do the entire job. To be effective, security solution tools must work together to secure the critical points of your network: the perimeter, your servers, your communications, and your desktop environments. These solutions must also be adaptable enough to easily incorporate new functionality to meet emerging threats.

Security solutions should also be powerful and scalable, and turn management and maintenance processes into an easy, hassle-free experience. WatchGuard® bundled security solutions are designed to meet the needs of the SME by offering:

- An Integrated security appliance designed to grow as your business grows
- Proven protection through Intelligent Layered Security
- An intuitive user experience that lets you get on with your business
- Expert guidance and support

PROTECTING THE CORPORATE NETWORK

The new Firebox® X products bring high-speed network security to SMEs, remote offices, service providers, and data centers. It offers enterprise-level protection at a price small- to medium-sized enterprises can afford.

PROTECTING NETWORK COMMUNICATIONS

WatchGuard VPN solutions provide private business communications to branch offices, mobile users, and telecommuters, allowing businesses to take advantage of the Internet and affordable broadband transmissions.

PROTECTING SERVER CONTENT

Firebox® X appliances come with 3 active network ports and are designed to be upgradeable to 6 active ports with the 3-port upgrade option. Additional ports allow you to sub-segment your network by device types or user groups, and enforce unique security policies to each group. Since approximately 90% of intellectual property loss can be attributed to company employees, sub-segmenting your network gives you an added layer of protection for your server content.

PROVIDING GREATER NETWORK PROTECTION WITH ADDITIONAL SECURITY SERVICES

Firebox® X Intelligent Layered Security architecture allows you to deploy the following services outside of your appliance to protect your network before attacks even begin:

- AuditSca™, powered by Qualys® **vulnerability assessment** service identifies vulnerabilities in your network so you can fix them before hackers discover them. Run comprehensive network security audits on demand, and have the results and suggested solutions delivered in minutes without the extra cost of software or hardware deployment and maintenance.
- SpamScreen gives you an advanced **anti-spamming filter** to help you fight back and stop receiving the growing deluge of junk e-mail that wastes your employees' valuable time.
- WebBlocker **URL filtering software** is a customizable management tool with a point-and-click interface that lets you control Web surfing and deny access to objectionable material. Filtering is transparent to users and requires no additional client software or configuration.
- **Antivirus protection** based on McAfee® innovative Active Virus Defense and VirusScan® technology, VirusScan® ASaP delivers continuous protection against known viruses, Web attacks, and e-mail intrusions to desktop environments and infrastructures.

WATCHGUARD: THE SECURITY YOU REALLY NEED

You understand the importance of protecting your business against Internet threats. We hope this paper has given you some good tools for implementing a security solution you can use and trust. Once you have developed your security plan, we invite you to take a closer look at WatchGuard® products. Our total focus is on meeting the security needs of small- to medium-sized businesses everywhere, and we'll be happy to help you bring your security solution from concept to completion.

For more information about WatchGuard products, visit us at www.watchguard.com

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

E-MAIL:

information@watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.521.8340

FAX:

+1.206.521.8342

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with affordable, effective security. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

FOR MORE INFORMATION

Please visit us on the Web at www.watchguard.com or contact your reseller for more information.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

©2004 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, LiveSecurity, and AuditScan are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. Network Associates, McAfee, and VirusScan are registered trademarks of Network Associates. Qualys is a registered trademark of Qualys, Inc. All other trademarks and tradenames are the property of their respective owners.

Part. No. WGCE66014_0604