



Network Security Essentials for Your New Small Business

April 2009

Congratulations! You've gone proactive, and your new business is up and running. Now it's time to master daily operations – the battle zone between your mission statement and reality. As you grapple with issues such as cash flow, time management, and inventory, don't overlook a crucial issue: the confidentiality and integrity of data on your office network.

Introduction

The reason: sloppy data security can take you out of business, fast. In fact, the US Department of Labor has warned that 93% of businesses that suffer a significant data loss go out of business within five years.¹ Further reasons network security deserves your full attention.

- **Poor network security can get you into legal hot water.** The data that you think of as “my customer contacts” is not yours. Legally, it's your customers' PII (Personally Identifiable Information). Identity thieves can use it to perpetrate crimes. Most regions have obligatory disclosure laws, which mandate that if customer PII on your network is compromised, you must inform customers.² Without proper network security, your small business might have to withstand a self-disclosed blow to its reputation, and weather the customer lawsuits that inevitably follow.
- **Poor network security can result in hefty fines and broken relationships within your industry.** Many vertical industries have unique legislation, regulations, and industry standards. Fail to comply and you're asking for trouble. For example, if you accept credit cards as payment,

¹ “[Economic Downturn Underscores Need for Proactive Measures to Safeguard Data and Minimize Risk](#),” Nov. 19, 2008.

² Examples: In the USA, 45 states have compulsory disclosure laws. Canada has PIPEDA (http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act) and other laws. The European Union has Article 8 of the ECRH, Directive 2002/58/EC, and many other privacy laws. But it's also common sense – no customer will be happy with you if your network is the reason crooks have the customer's credit card number.

but do not comply with the Payment Card Industry Data Security Standard (PCI DSS), Visa and MasterCard can revoke your right to accept credit cards. If your business relies on health care data and you violate the Health Information Portability and Accountability Act (HIPAA), the government can fine you – and recent fines have soared past six figures.³ Nearly every industry has penalties for compromising sensitive data, whether it's customer PII, a partner's proprietary research, or a client's competitive bid.

- **Poor network security makes you untrustworthy.** In a small business, competence is your biggest asset. You work hard to position yourself as nimble, efficient, and credible. One data leak can ruin all that effort. One incident where hackers access your clients' information will convince the world that you do not operate professionally, making all your marketing efforts appear hollow.

In short, a data security compromise has so many repercussions to your reputation and your finances that you literally cannot afford one slip-up. For many of the same reasons you wouldn't think of operating your business without liability insurance, you need business-grade network security.

“If you accept credit cards as payment, but do not comply with PCI DSS, Visa and MasterCard can revoke your right to accept credit cards.”

“But I'm Too Small for Hackers to Target...”

Business owners stepping up from home computer networking to business-grade networking often assume that their network will never be attacked by cyber-criminals, for two reasons:

1. The business is too new and unknown to cross the hacker's radar as a target
2. The information the small business holds is not valuable enough to incite an attack

Such thinking doesn't reflect how cyber-crooks actually work. Profit-driven attackers do not sit around surfing corporate web sites, manually picking targets. **Typical attackers do not target individuals or businesses – they target vulnerabilities.** They use automated tools that know how to exploit certain computer vulnerabilities, such as security flaws in Internet Explorer or Windows. The tools scan the Internet at super-speed, and whenever they find any computer that is vulnerable, the exploit executes automatically.

Every computer attached to the Internet is a target. Attackers don't care who you are or what you have. In 2004, the SANS Institute found that an unprotected computer running Windows XP, fresh out of the box, would be infected by malware within 20 minutes of being connected to the Internet.⁴ When the ShadowServer Foundation repeated the study in 2008, the time to infection had fallen below five minutes.⁵

³ [“Seattle system will pay \\$100K HIPAA fine after repeated breaches,”](#) July 19, 2008; [“Okla. woman faces prison, fine for HIPAA violation,”](#) May 14, 2008; [“CVS Pays \\$2.25 Million and Toughens Practice to Settle HIPAA Privacy Case,”](#) Feb. 18, 2009.

⁴ [“Infected in 20 Minutes,”](#) 19 August 2004.

⁵ [“Zombie PCs: ‘Time to infection is less than five minutes.’”](#) October 21, 2008.

Why do attackers want any and all networked computers? Because:

- *Any PC can be used as a spam relay.* Spammers can send millions of emails while making it appear someone else is the source.
- *Any PC can be used as an illegal file repository.* If a crook makes money by selling illegal software, pirated movies, or child porn, to avoid capture he'd rather offer those files from any machine other than his own.
- *Any PC can help put a foe out of business.* Some criminals are paid to keep a business or government off-line. To do so, they use thousands of computers they've already infected. They command all the infected computers to visit the targeted website at the same time. This creates an Internet traffic jam: the website gets so many requests that it can't handle them all, and thus, legitimate customers cannot reach the website. In technical lingo, it's called a Distributed Denial of Service attack, and even the slowest computer can contribute.
- *Any PC can host a phishing site.* Phishing is the word for attacks designed to make you reveal sensitive data to someone who shouldn't have it. Most often, phishing occurs as a bogus email pretending to come from a bank, asking you to verify your login credentials. If you follow the link in the email, you might think you're visiting your bank's web page, but it's an imposter site. When you enter your password and account number, you're giving it to criminals. They can serve up these fraudulent sites from any computer on the Internet – including yours.

There are other reasons why today's cyber-crooks want any computer they can control, regardless of who owns it. But you get the picture. On the Internet, every vulnerable machine looks the same, whether it belongs to a small business, a massive corporate conglomerate, or an elderly spinster. **There is no such thing as "security by obscurity."** Without adequate network security, automated cyber-tools will find your network and infect it – probably within minutes.

“Every computer attached to the Internet is a target. Attackers don't care who you are or what you have.”

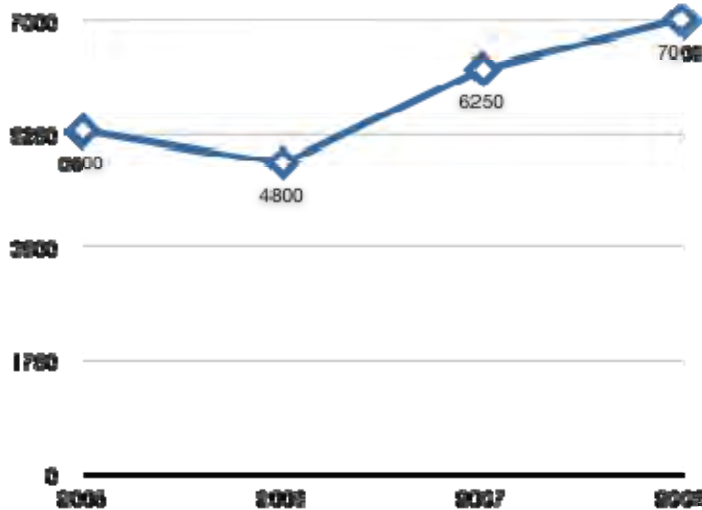
If attackers took control of your computers, wouldn't you know it? Not likely. When you get software updates from the Internet, how do you know about them? You know because the software vendor pops up a dialog box on your screen, asking permission to install. Attackers don't care whether they have your permission, so they simply skip the dialog box and execute whatever they want on your computer, stealthily. Nothing appears on your screen.

“I Have Anti-Virus, So I'm Safe, Right?”

Is anti-virus software enough to protect your business network? Sadly, no. The security threats to computer networks today are multi-faceted and go far, far beyond what anti-virus products address. Anti-virus products (called AV for short) certainly should be part of your network defenses. They certainly *should not* constitute your entire network defense. Would you ever say, “I have a lock on my front door, so I can safely leave all my windows open”?

Why isn't AV software enough? Some key reasons:

- **AV only works against previously spotted and recorded threats.** AV software works by recognizing what is unique in the programming code that allows a virus to work. This unique element is referred to as the virus's signature. AV software will fail to spot any malicious code for which the AV does not have a signature. Thus, AV never stops a brand new threat, until a security researcher spots the threat and figures out its signature.



The security trend: worsening. As the number of security holes reported in commercial software grows, business owners must learn to protect themselves.

Source: Figures from Cisco Annual Security Report, 2007 and 2008; chart from WatchGuard

- **AV only works against known versions of known threats.** Some AV signatures are very specific. Thus, if the author of a known virus modifies his code a little bit, the virus still works but it no longer matches the signature that AV vendors have on file for it. AV will fail to recognize the new version. Knowing this, many virus authors now write *polymorphic* viruses – meaning, the virus automatically changes itself to fool signature-based defenses.
- **AV only works once its signature gets to your computer.** When a new virus hits the Internet, there is a “window of vulnerability” before anyone is protected. During this window of time, the virus is spreading, while researchers race to spot it; analyze it; define a signature for it; test the signature to make sure their product can block the virus; and then distribute the signature to all their customers. Some vendors can do this in hours; some take days. Either way, if the virus gets to your computer before the AV signature does, you're infected.
- **AV only works against viruses.** Viruses still abound on the Internet, but frankly, they are among the least of today's threats. The worst threats include botnet infections, drive-by downloads, keyloggers, rootkits, and attacks against your business database. AV addresses these primary attack vectors in either a very limited fashion, or not at all.

Since about 2003, malicious software – often abbreviated to *malware* – has grown much more complex and sophisticated, with several kinds of attacks rolled up into one. Security experts refer to these alarming, multi-faceted attacks as “blended threats.”

Network security professionals have pushed back against blended threats with blended protection, a concept known as “defense in depth.” To fend off numerous kinds of attacks, you need layers of security. AV is just one layer. You can learn about some of the other layers later in this paper.

You might ask, “But this whole time I’ve used nothing but AV to defend my home network, and everything’s fine – so if the Internet is as bad as you say, why haven’t I been compromised?”

There are two answers to that.

- 1) If you do not know how to use diagnostic security tools, you have no way of knowing whether you’ve been compromised or not. Remember, attackers might be using your home computers, just not for activities that attack you directly. Has your computer slowed down? Do you get pop-up windows you didn’t expect and can’t explain? Has your web browser’s home page ever changed unexpectedly? Maybe all is *not* fine on your network.
- 2) You have the right to choose not to defend your home network adequately. Perhaps all you risk losing is some MP3s, and emails from your kids. But you do not have the right to put your clients’ and partners’ sensitive data at risk.

Now that you’re running a business, the stakes are higher. You need industrial-strength network security.

Essential Elements of Layered Security

What defenses does a business network need, in addition to anti-virus? Most network security professionals agree that the following are “musts”:

- Firewall
- Intrusion Prevention System
- Virtual Private Network
- Anti-spam
- Web filtering

Let’s define each of these layers of defense, so you can understand what they do and why each is necessary.

- **Firewall.** Like the strainer a chef pours his soup stock through, a firewall stops all the bones (bad stuff), but lets all the broth (good stuff) through. It does so by following a set of rules programmed into it. For example, if a data packet arrives at your network’s door trying to reach one of your user’s computers, and the packet header labels it as a Reply, a good firewall will check to see if anyone on your network ever sent the Request that this packet purports to Reply to. No Request? Then the “Reply” flag is fraudulent, so the firewall drops the packet. Another example: Every data packet contains a “Source” field that specifies what address it came from. Hackers love to hide the real source of their attacks, so they’ll use tricks to *spoof*, or enter a false address, in the Source field. A good firewall will notice if a packet coming from outside your network claims a source address inside your network – an obvious lie. Firewalls perform hundreds of such checks, to validate traffic both entering and leaving your network.
- **Intrusion prevention system (IPS).** Some security appliances can detect malformed traffic but are not sophisticated enough to do anything about it. An IPS will detect *and automatically block* bad traffic. For example, before a cyber-crook attacks a network, often he will scan every port on every IP address in that network, looking for ways in. Such an act is implicitly hostile and rarely legitimate. An IPS can notice the port scan, spot the source address doing the scan, and block that address from all access to the network. This effectively prevents an attack before it even occurs. (And is a good example of security that anti-virus does not provide.)
- **Virtual Private Network (VPN).** Almost any thriving business exchanges sensitive data with people outside the office. You might send pricing info to a sales rep on the road, or download orders from a customer who buys regularly. A VPN scrambles the data (known as *encrypting* the

data) so that you can read it, your partner on the other end of the connection can read it, but no one in between can read it. It's like sending the data through an impregnable tunnel, so no unauthorized people can get to it. VPNs solve two security problems: first, the *confidentiality* of the data is assured, because encryption defeats prying eyes; and second, the *integrity* of the data is assured, because if anyone tries to alter it en route, the decryption won't work (plus, if an attacker wanted to change your \$10 purchase order into a \$100,000 purchase order, how does he know what to change in an encrypted data stream?).

- **Anti-spam.** More than 80% of all the email that traverses the Internet is unsolicited commercial email, known by its slang term, spam. Spam wastes your time, can confuse you if it resembles your legitimate emails, and needlessly hogs up space on your computers. The best way to deal with spam is to find a spam filter that recognizes and drops spam at the gateway to your network, before it wastes your time and gums up your computers.
- **Web filtering.** Cyber-crooks spread their influence by setting up web sites as booby-traps. The moment a browser visits that site, the site crams malware onto the visitor's computer. Less dire yet still annoying, sites such as casual gaming sites or celebrity fan sites will cram spyware and adware onto visiting computers. A web filter keeps track of tens of thousands of sites known to be undesirable, and will stop you from accidentally surfing to them. If you have employees or family members using your network, a web filter can protect your network from your kids' reckless surfing, and prevent your employees from "cyber-slacking" (for example, wasting time on a Fantasy Football site instead of working).

Security Lasagna; or, Combining Your Layers of Defense

For each of these categories of network defense, you can find dozens of products, boasting a broad diversity of capabilities. Prices range from zero to "you'd better have the economy of a small country." As the owner of a small business, how much should you spend?

Professional security practitioners try to find a reasonable proportion between the value of what they're protecting, and the cost of the protection. Wisdom is in the middle: you wouldn't spend a dollar protecting data that is worth a penny. But if your expected revenue is half a million dollars per year, it is also unwise to believe a \$100 investment in a cheap firewall and some anti-virus is sufficient to deter cyber-thieves.

There are many different methods for calculating the market value of data on your small business network. Here is one quick 'n' dirty way to calculate it. In a 2008 study of 43 different companies in a cross-section of industries,⁶ the Ponemon Institute concluded that the average cost of a data breach is \$202 per victim. How many customer records do you expect to accumulate in the next three years (the minimum life of a security appliance)? Multiply that number times \$202, and you'll have a loose definition of the value on your network.

"Anti-virus products ... certainly *should not* constitute your entire network defense. Would you ever say, 'I have a lock on my front door, so I can safely leave all my windows open?'"

⁶ ["Costs of a Data Breach: Can You Afford \\$6.65 Million?"](#), Feb. 4, 2009

Further security investment guidelines:

Use the 80/20 rule to prevent overspending. Some of the brands that are most famous, or are considered “best of breed,” earned their reputation serving large enterprises. Their security devices can cost five or six figures, and many of their capabilities don’t match what small businesses need. In most cases, research will guide you to products that do 80% of what the big guys do, for 20% of the price. There’s no point in paying for features you will never need.

Don’t “cheap out.” It’s tempting to settle for free software and a “firewall” that costs fifty bucks at Best Buy. This approach, though, hides several problems. First, cheap defenses are cheap for a reason. Usually, they perform fewer security functions, and thus provide inadequate protection. They usually have a slow processor and very little RAM, meaning that if your network gets busy, your defenses can’t keep up. Beware of “solutions” that slow down your network so much, you can’t do business and security at the same time. Second, if you create your security out of a patchwork of free and cheap products, you’ll constantly have problems getting all the parts to interoperate. Your security “solution” becomes a problem and an end in itself, when what you really wanted to do was go earn money.

“Free” tools might provide false economy. Free shareware and open source tools sometimes defy the description in the paragraph above, and do a really good job. But in those cases, they usually are designed for a computer expert. To use them effectively, you’ll have to read manuals, learn to use a Command Line Interface, and experiment with various configuration settings. Free tools are usually a black hole for your time – which means, if you value your time, they aren’t really free.

Put due value on ease of use. Another quality to consider when purchasing security products is ease of use. You want to focus on your business mission, not on learning a complicated, incomprehensible management interface – much less, a separate new interface for each security product. Prefer unified management, where you (or a part-time employee) can master one interface in short order, then use it to run all your defenses.

Consider the TCO. “Total Cost of Ownership” is the term for what your defenses will cost you across their expected lifetime. Because hackers create new waves of malware every day, it is normal and expected for security firms to sell subscription-based defenses that also update constantly. However, some vendors will charge extra for features another vendor bundles in as standard. Before you purchase, inquire diligently into all licensing fees, subscription costs, and support service levels to make sure you’re getting a good value in the long run.

After deliberating on the factors above, many small business owners decide to purchase a unified threat management (UTM) solution. A UTM solution provides all five of the defenses listed in this section (and optionally, more) in one powerful yet convenient appliance.

Having an appliance that is dedicated to security at the gateway to your network moves the most processor-intensive security duties off your business machines, freeing them to earn money. Having a UTM appliance at your gateway also moves the security battle a step away from where you store sensitive data. Although

THE PROBLEM WITH MICROSOFT SMALL BUSINESS SERVER

Are you counting on Microsoft Small Business Server (SBS) for network functions such as file sharing, printer sharing, hosting your email server, and so on?

If so, you need to know that in versions of SBS released after 2008, **Microsoft removed the firewall from SBS.** They decided to focus their efforts on business application networking, and leave the security functions to vendors who function primarily on security – vendors such as WatchGuard.

If you run MS SBS, don’t think Microsoft has your security handled. In fact, now you need additional security more than ever. A UTM device could be your answer.

the UTM frees up your computer's memory and processor from most security duties, you still have the convenience of being able to control and manage it from your computer.

As a class, UTM solutions typically provide about the right amount of power and growth room for a small business.

Firebox X Edge: the Best UTM Solution for Small Businesses

If your new business has fewer than 20 computers and printers on a network, an ideal security solution is the Firebox X Edge e-Series UTM solution.

The Firebox X Edge provides all the essential layers of a defense-in-depth strategy, and does so through an intuitive, web-based interface. With the Edge, you get some of the best point-and-click security money can buy.

Beyond security, trusting your network to a WatchGuard Firebox offers several advantages to help you run your business:

- **Trustworthy partner, here for you today and tomorrow.** In 1996, WatchGuard Technologies, the makers of Firebox X Edge, pioneered the approach of putting a firewall into an appliance dedicated to nothing but security. Since then, customers have installed more than a half million of WatchGuard signature red security boxes. Every Firebox is backed by a reputable, enduring company, proven trustworthy.
- **Unparalleled support.** Firebox X Edge devices come bundled with premium technical support, called LiveSecurity Service. LiveSecurity includes Advance Hardware Replacement – in the rare event that your Edge breaks down, WatchGuard rushes a new Edge to you. Other manufacturers wait for you to return the broken device to them, and to prove that it really failed, before they issue a replacement. WatchGuard gets your business back up and running first, then settles the details later. The LiveSecurity Service also sends you alerts when new threats might endanger your business, with instructions on how to use your Edge to reduce the risk.
- **A way to keep home and work separate.** Each Firebox X Edge has six physical interfaces, or ports. If your home and office share space, you can put your family on a separate network from your business and keep everyone safer. If you have a good-sized office, you can keep more sensitive data, such as Human Resources or Research & Development, on separate networks from each other and the general office

LOVE WI-FI? SO DO CRIMINALS

The world has gone crazy over wireless Internet connectivity, due to its convenience and increasing speed. Road warriors can now find a quick Wi-Fi Internet connection as easily as they find a MacDonalds.

The problem is, your wireless laptop does not connect to a public wireless access point in a tightly-controlled beam. 802.11 (the standard on which wireless connectivity is based) is essentially a radio wave. Your wireless signal radiates from your laptop in all directions. Anyone within range can pluck your signal out of the air, see everything you're doing, and leave no trace of their eavesdropping. Hackers even have tools that empower them to eavesdrop on Wi-Fi connections from miles away.

That's why Firebox X Edge e-Series devices offer a secure wireless option. With an Edge at headquarters and the included Mobile VPN client on your laptop, you can establish an encrypted connection to the office from any Wi-Fi hotspot. Attackers can still eavesdrop – but all they'll intercept is scrambled gibberish they can't use. You can go about your business privately and confidently. Love Wi-Fi? Then you'll love the wireless Edge.

population. You can set up separate rules for each subnet, all through one convenient device.

- **Secures you at HQ, and on the road.** Firebox X Edge comes with mobile user VPN software. When you or your employees are on the go, you can instantly establish a VPN tunnel back to the office for secure, encrypted communications. That means that even at public WiFi hot spots, eavesdropping hackers can't see your sensitive data. The Edge protects you and your employees everywhere there is a network connection!
- **Room for growth.** With most security appliances, you buy what you need, and if your business grows, two or three years later you have to throw out what you have and purchase all over again. Not so with the Firebox X Edge! Usually, you can increase throughput or add features later, simply by purchasing a license key. Enter the license key on a Web page to unlock new power from your existing appliance. Firebox X Edge offers you the easiest, most efficient upgrade possible while protecting your investment in network security.

Even with its rich set of features, the Firebox X Edge e-Series is surprisingly affordable. Don't be caught with homemade security when industrial-strength attackers hit your small business network. To learn more and explore all the solutions, contact your WatchGuard reseller today.

For more information on WatchGuard security solutions and what they can do to protect your small business network, visit www.watchguard.com, or contact your authorized WatchGuard reseller.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard has been building award-winning unified threat management (UTM) solutions that combine firewall, VPN, and security services to protect networks and the businesses they power. Our newest appliances represent the next generation of network security: extensible threat management (XTM). All of our solutions feature reliable, all-in-one security, scaled and priced to meet the security needs of every-sized enterprise. Our products are backed by 15,000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including healthcare, education, and retail. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America..

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.

©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66617_040109