

The Security Journal

"Common Sense Security for Common Businesses"



Inaugural Issue: Volume 1

Fall 2002 Edition

In This Issue:

Corporate Officer
Liability for Security

Security Issues of
Wireless Networks

Vulnerability
Assessments

A Free Publication from Security Horizon, Inc.



Security Horizon

Security Horizon, Inc.

P.O. Box 63741

Colorado Springs, CO

80962-3741

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers

Contributing Authors:

Russ Rogers, CISSP, IAM

Dr. Greg Miles, Phd, CISSP, IAM

Ed Fuller, CISSP, IAM, GSEC

The Security Journal is always on the lookout for quality writers for this publication. If you're interested in submitting an article for inclusion in an upcoming edition of The Security Journal, please contact Russ Rogers at russr@securityhorizon.com.

For more information on Security Horizon, please visit our web site or send us an email at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is based out of Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, and unquestionable integrity.

Table of Contents:

Corporate Officer Liability for Security Likely to Increase

By Greg Miles.....p.2

Security Issues of Wireless Networks

By Russ Rogers.....p.6

NSA IAM Course Schedule

.....p.9

Vulnerability Assessments

By Ed Fuller.....p.11



NSA developed it. Now you can learn it.

(Click [here](#) to find out more)

The INFOSEC Assessment Methodology



Corporate Officer Liability for Security Likely to Increase

By Greg Miles, Phd, CISSP, IAM

Citizen outrage to the apparent lack of corporate responsibility is driving legislation designed to hold corporate officers personally liable for improper company actions. We have seen this trend with the Y2K initiatives and now with the more recent corporate financial reports. People are starting to expect CEOs, CFOs and other corporate officers to act responsibly in relation to information security. One idea being considered by President Bush's Critical Infrastructure Protection Board is to have corporate officers certify their security and remove their personal liability protection for stockholder and consumer lawsuits. Although this may seem a bit radical, the idea is to get the attention of corporate officers so they become accountable for their action/inaction in relation to protecting information and data.

“Many companies are making great efforts to be secure.”

Today, the basic driving principle is ‘due diligence’ in relation to information security. Many companies are making great efforts to be more secure. Some companies are doing a little bit while some companies aren't doing anything.

Whether you are a large or a small company, you must still take into consideration the protection of your, and your customers, information and data. Unfortunately, there is no standard of due care yet and industry ‘best practices’ is a broad undefined term.



Some business areas have even stricter rules and punishments for criminal liability for a security compromise. The Health Insurance Portability and Accountability Act (HIPAA) privacy enforcement regulations carry penalties of up to 10 years in prison and/or a \$250,000 fine. Gramm-Leach-Bliley Act (GLBA) drives security requirements for financial institutions. There are Federal Trade Commission Act (FTCA) provisions that have been used in court during a security incident that included identifying exposure of privacy information as “unfair and deceptive act” under the FTCA. In a recent case with Eli Lilly, the Federal Trade Commission required the company to assess the risks inherent in “the prevention and response to attacks, intrusions, unauthorized access or other information systems failure”. Security is a serious issue.

(Continued from page 3)

So in all the doom and gloom, what can you do?

- ✓ First and foremost, know that information security is a huge issue warranting being addressed by your organization, no matter how big or small you are. Don't forget to address it from an external and internal perspective.
- ✓ Establish and track a security roadmap to show how the organization has or is becoming more secure.
- ✓ Establish and enforce security requirements within your organization that will create the foundation for making security part of your organization's culture.
- ✓ Educate your employees, contractors, subcontractors, third party vendors, and customers on required security.
- ✓ Implement technical security measures such as firewalls, intrusion detection systems (IDS), virtual private networks (VPN), and virus protection to better secure your infrastructure.
- ✓ Assure you implement security patches for operating systems, applications and routers in a timely manner.

- ✓ Hold EVERYONE accountable for the established security standards.
- ✓ Monitor security constantly.
- ✓ Have your security evaluated by a 3rd party on no less than an annual basis.

There is no such thing as 100% protection. Every step you take, however, helps you to eliminate another layer of exposure to security vulnerabilities.

Greg Miles, Ph.D, CISSP is the CIO and Executive Vice President of Security Horizon.

gmiles@securityhorizon.com,

www.securityhorizon.com

719-488-4500.



The workers of Security Horizon proudly salute our men and women in uniform around the globe.

We appreciate you all!



Black Hat

Windows Security 2003 call for papers

Sheraton Seattle Hotel & Towers

Training: February 24-25, 2003

Briefings: February 26-27, 2003

WWW.BLACKHAT.COM

Security Issues of Wireless Networks

By Russ Rogers, CISSP, IAM

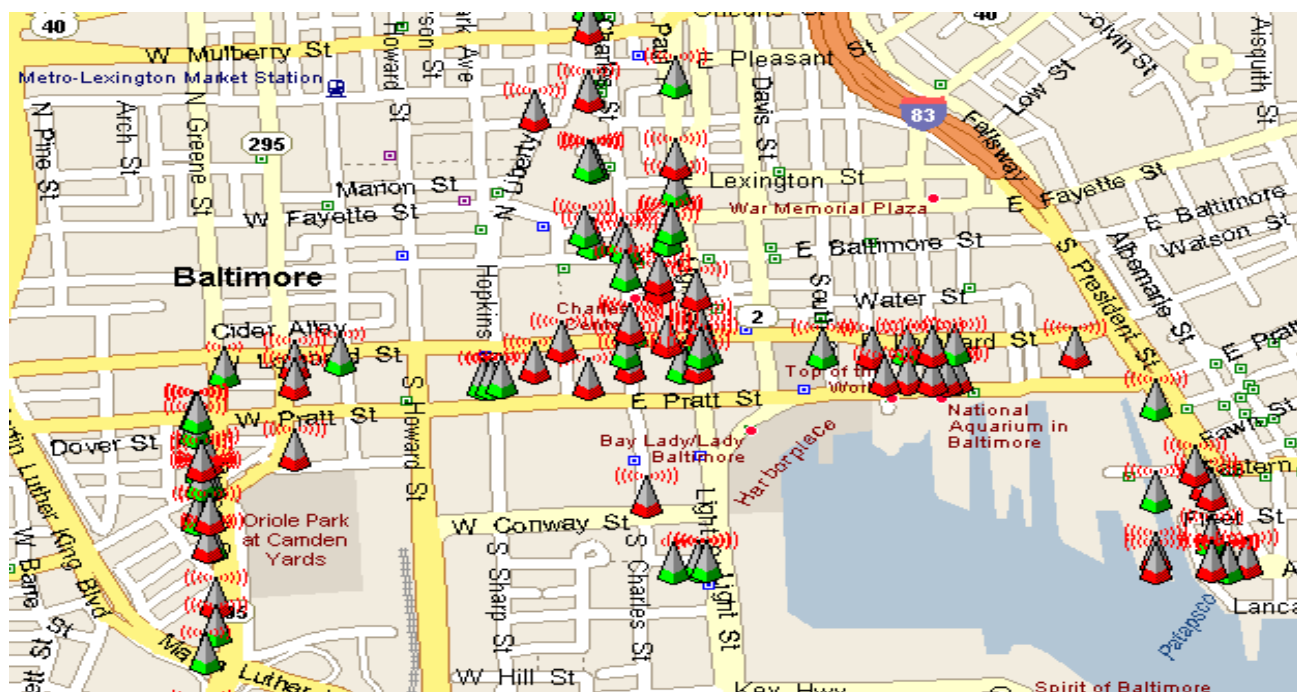
Wireless 802.11b networks are taking off around the globe. Their convenience and the lack of those confining network cables are causing even home users to seriously consider a wireless alternative. And who can blame them? After all, the world is hurdling towards a globally connected and mobile society where location doesn't matter anymore.

But along with this newfound freedom comes the responsibility to protect those networks, especially corporate networks, from intruders, both accidental and intentional. A new "hobby" has sprung up around the advent of wireless networks, called war driving. War driving basically consists of driving, walking, or riding a bike around town with a laptop, wireless network card, and a piece of software that allows the network card to detect wireless

networks en route. The serious war drivers utilize a GPS device to specifically determine locations of each wireless access point along the way.

As an example, visit the WiGLE website at <http://www.wigle.net>. The map below is one example of the information collected from these wardrives in the downtown Baltimore, Maryland area. What they've found is that approximately 30% of all wireless access points use encryption. The inverse of that is the other 70% of wireless networks that sit out there completely vulnerable and with factory default SSID (access point names).

Okay, now we know they're out there watching us. And we REALLY like our wireless network. So what can we do to protect our network from attack and still



(Continued from page 4)

retain the freedom that wireless gives us?

While is no foolproof method to keep yourself completely safe, there are reasonable steps that you can take to mitigate the risks.

- ✓ Choose a quality SSID (name) for your access point. Many companies simply name the access point after the company they work for or the address they work at. Unfortunately, this makes it incredibly easy to associate wireless networks with the company that owns them. Pick a name that you understand, but won't give any hints to outsiders of who owns the network.
- ✓ Turn off the SSID broadcast feature. A lot of wireless appliances come from the factory ready to tell the world that they exist by broadcasting the network SSID publicly. Find the feature within the access point configuration that turns this off. This will also negate one of the most popular war driving applications called NetStumbler (see <http://www.netstumbler.com>).
- ✓ Some wireless manufacturers, such as the Cisco Aironet series, have the ability to further deceive potential intruders by constantly changing the MAC address of the access point. This makes war driving tools see multiple access points when there may actually only be one. The

MAC address is, in the simplest sense, the network identity of the wireless access point.

- ✓ Turn on the Wireless Encryption Protocol (WEP). WEP isn't perfect, but it will definitely slow determined intruders down. The longer the WEP key, the better. Mix the characters in the key much as you would with a good administrator password. Tools such as AirSnort (available at <http://airsnort.shmoo.com>), that runs under Linux, can be used to sniff wireless networks; constantly collecting packets that can be used to crack the WEP key. 'H4ckM3n0T!' is an example of a high quality password/key that will be difficult to crack. And although there are still known weaknesses in the WEP protection, you can mitigate that risk with longer and more complex keys.
- ✓ Restrict access to the wireless network only to those machines that are specifically configured to communicate on your network. This is called a "Closed Network". Turning WEP on is good, but if you leave it open to people who don't know the key, you're still leaving yourself wide open to misuse.
- ✓ Consider changing the WEP key on a scheduled basis. This creates more work for the administrators of the network, but helps limit the time

that potential intruders have to crack the old key before a new key kicks in. We recommend changing the key every 30-60 days. As an example, during one of our wireless assessments we discovered only 11 useful packets in a 3 hours period. Since most cracking tools take at least 1500 useful packets to crack a WEP key, it would take over a month in 8 hours a day increments to crack the key. Consider who might want into your network when designating how often the key much change.

- ✓ Don't use DHCP to assign addresses to new clients on the wireless network. And although these network ranges can be discovered through various freeware war driving tools, such as Kismet (<http://www.kismetwireless.net>), letting clients connect with DHCP is just asking for trouble because it will give the client all the necessary

information to utilize your network, such as an IP address, a default gateway, netmask, and DNS servers.

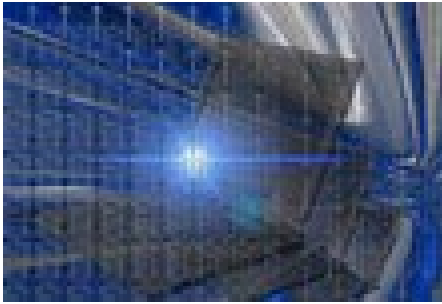
- ✓ Lastly, consider how far your wireless access points are broadcasting. How much power are they using to communicate with peers and clients on the network? Walk around the outside of your office building with your laptop and wireless card to see where the wireless network is strongest and where it is weakest. Consider moving the access point to minimize potential public access. As a side note, some wireless manufacturers give you the ability to change the transmission power values within the configuration. Consider changing that to a value that gives you the amount of coverage you need without going too far outside your needed space.

This diagram shows an access point (colored blue) in a hospital and the range of that access point (cream colored). As you can see, the range of the AP intersects with other local areas that should be considered by the administrators.



(Continued from page 6)

If those other local areas also contain wireless networks, there could be overlap where unintentional access to your network occurs.



So enjoy the freedom that wireless gives your company. There's nothing better than taking your laptop to a meeting in the boardroom while you're still on the network so you can address questions immediately. But ensure you use this new tool responsibly. And if you feel you might be in over your head, contact someone who knows about wireless networks and the associated security measures. It doesn't take much time to secure a wireless network and it's worth the trouble to help avoid the trouble later.

Russ Rogers, CISSP is the President of Security Horizon and also the editor of this publication

Questions or comments can be sent to the following locations:

russr@securityhorizon.com, or
info@securityhorizon.com
or please visit our website at:
www.securityhorizon.com
719-488-4500.



Schedule of Courses

Oct. 9-10, 2002	Clearwater, FL
Oct. 23-24, 2002	Columbus, OH
Oct. 24-25, 2002	Colorado Springs, CO
Nov. 7-8, 2002	Washington DC
Nov. 14-15, 2002	San Jose, CA
Dec. 4-5, 2002	Monterey, CA
Jan. 23-24, 2003	Clearwater, FL
Feb 24-25, 2003	Seattle, WA
April 25-26, 2003	Myrtle Beach, SC

Tentative Course Locations

January, 2003	Albany, NY
March, 2003	San Diego, CA
Spring, 2003	London, UK

Now Publicly Available!

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting INFOSEC assessments of U.S. Government information systems. The course teaches NSA's INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

To register for one of these courses or to get further information on the IAM methodology, please contact us at:

Security Horizon, Inc.
(719) 488-4500
info@securityhorizon.com
<http://www.securityhorizon.com>



L E W A N

Technical Services

Becoming your trusted partner in *Anything* IT.



It's rarely a slam-dunk launching the right information technologies. Successful technology innovation takes business insight - *pure people power*. New installations and system upgrades require technical experience and know how. That's why people call Lewan.

Innovation, problem solving, accountability.

That's the Lewan way.

IT consulting *services*

For more information visit www.lewan.com

Since 1986, Lewan has helped thousands of customers meet their businesses objectives through *leading-edge technical consulting services*. Our Consulting Services Team has multidisciplinary expertise to solve your *local and wide area network* challenges.

Lewan's resume includes success with some of the region's most respected large corporations. And we've helped transform hundreds of small and mid-size companies as they embrace enabling technologies.



Vulnerability Assessments

By Ed Fuller, CISSP, GSEC, IAM

How do you know what the actual state of your security posture is? How can your organization evaluate the current state of their security? How can management be assured that all the facets of their security are alive and well? One suggestion that I have heard has been addressed in the book by Lance Spitzer, "Know Your Enemy", July 2000. Through the analysis of 'bad guy' activities we can learn how to better defend ourselves against what are known threats and vulnerabilities. Armed with the knowledge of the tools and techniques that are used to attack we can build better defensive systems and protect what is important, our 'critical information.'

It is a given that in an ideal world, security should be designed and correctly implemented from the top down. A layered defense strategy is developed that properly prevents attackers from gaining access to sensitive information or systems. At the very least the perimeter defenses should slow them down long enough to be detected. Logging and active monitoring should alert us when something improper such as misuse, abuse or an intrusion may have occurred. However, out in real world networks this doesn't seem to occur as often as it should. The larger the network, the more the tendency for it to develop undocumented or unmonitored parts and pieces, all of this is done for a particular reason that hopefully somebody remembers. Security concerns give way to functionality and performance.

The result is, we need some measure of security; but how do you increase security with the least amount of pain to your organization or your customer? The answer, that I perceive, is to know what you are protecting and why. This requires that you know what your current security posture is and developing a plan, or road map, to improve the security posture. Security over the years has evolved from the concept of protecting components or networks to protecting information. Sometimes addressed as Information Security (INFOSEC) or Information Assurance (IA). A popular method of doing this is to hire a consultant or third party to conduct an organizational assessment to determine the weaknesses in the security posture. A repeatable and measurable method that has been developed to address this is the National Security Agency's (NSA's) INFOSEC Assessment Methodology (IAM).



The key to security is, of course, always top down support. Senior management are the system/information owners that set the security policy for protecting critical information. Without a coherent set of policies it is not really possible to ever be truly secure. You might be fooled into feeling secure because you have installed the latest and greatest firewall and intrusion detection suite, however technical controls are only part of a properly developed security program. The security process is all about applying the appropriate policies through proper

procedures and management practices, to protect the critical information that the organization needs. For example, how can you secure all of the entry points to your network if modems are allowed without a policy prohibiting or controlling their use? The simple answer is that you can't. Assume that security is not a static achievable state, but a moving target that should be continually tracked and programmed for over time. There is no magical silver bullet to solve all security problems, however assessments are a key element in an overall security program for any organization. To quote George Kurtz and Chris Prosis from the September 2000, Information Security Magazine article 'Penetration Testing: Myth vs. Reality'; "There is a significant issue with assessments in that they are a 'snapshot in time' of a Organization, system, or network's security posture. As such, assessment analysis is limited to known vulnerabilities and the current configuration of the network."

There currently isn't a broad consensus as to the precise meanings and definitions of the term 'vulnerability assessment' as used here. This activity is sometimes also referred to as security testing, which seems to imply using a specific quality assurance type of methodology. Other terms can include security auditing, threat or risk assessments, ethical hacking, penetration testing, white-hat security testing and security diagnostics. The lines between the various terms and their practical applications are also not always clear. For example they may all use similar methodologies, people and tools.

For purposes of this article I will use the definition that Ira Winkler used in "Audits, Assessments & Tests (Oh, My)" July 2000, Information Security Magazine, for an assessment as "an overt study to locate security vulnerabilities." The NSA Glossary of Terms Used in Security and Intrusion Detection defines penetration testing as "the portion of security testing in which the evaluators attempt to circumvent the security features of a system." This definition normally implies emulating the activities of hackers, crackers, and script kiddies. A security audit is defined as a comparison of the security implementation of systems against a given set of standards to measure compliance. The way I view it all is, penetration testing is done from the outside poking inwards to see what happens and how far you can get. Vulnerability assessments are something you do from the inside to understand what vulnerabilities exist. Auditors, either corporate or otherwise, do audits to check for compliance.

In my view, I always try to associate increasing the security posture with reducing organizational risk. The trick is to discover as many vulnerabilities to the critical information as possible, make an informed risk management decision as to how much risk each presents to the environment, and then reduce the risks from high to low. The NSA IAM is one method of helping you find and plug the holes. It is not possible to eliminate all risk, only to mitigate the risk to an acceptable level of pain. As long as you remain aware of how much



risk there is to the critical information, that the organization is willing to accept, you are improving the security posture. We must consider that for a given exploit, there must be a threat to have a vulnerability and increasing the mitigation techniques can reduce the risk of loss.

So, where do you start?

So, where do you start? Start at the top. It's that simple. Work with the senior management to determine the critical information that the organization needs to achieve the organizational mission. Once you have the critical information topics, what would the impact be to the organization if you lose confidentiality, integrity, or availability? This is one of the least identified items of any vulnerability assessment. What is the critical information and what is the value to the organization? This can only be done with the senior management, without their views, opinions and information the assessment team will not be able to adequately evaluate the correct systems without wasting time and effort.

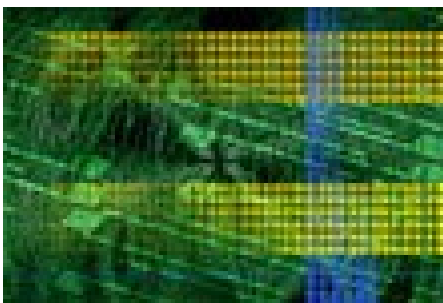
Once you have set the boundaries of the vulnerability assessment and agreed on the level of effort, move on to a thorough evaluation of the policies, plans and practices that set the tone of security for the organization. Examine the current state of the infrastructure; compare that with how the infrastructure should be based on security best practices and policy. What are the differences?

It is important to understand that there are multiple steps to Vulnerability Discovery. Too often providers give a "laundry list" of vulnerabilities and their countermeasures. An often overlooked step is the identification of the Security Goals and Objectives, or where the organization wants/needs to be. This step provides the very important information that puts that "laundry list" in context so the customer can make informed decision on spending limited resources. Then the INFOSEC posture analysis can be performed and countermeasures can be identified to reduce the security gap.

The vulnerability assessment is useful for discovering potential problems, and it is also a great method of testing the intrusion detection systems. External penetration testing should set off the 'alarms' on the perimeter devices. An Intrusion Detection System, either network or host based, should detect any scanning. In fact, normal security duties such as examining log files on systems that have been tested should give you an idea of what to look for in looking for actual intrusions. It should be mentioned that it is a good practice to ensure that all the system administrators should be forewarned of the vulnerability assessment that is occurring.

Implementing changes based on the INFOSEC posture analysis should still be subject to the change management process and configuration management approval process. There is a simple test to be applied; will this change actually improve protection based on what the organization considers valuable? Does the expense or

effort required to make the change outweigh the benefit of reducing that particular vulnerability risk? Does this sound like simple risk management? In a way, a vulnerability assessment can be an extension of systems configuration analysis. It can detect unauthorized changes to systems. Vulnerability assessments can also help demonstrate that you have applied due diligence by applying known best practices for IT security.



A thorough vulnerability assessment would have to include all of the areas where you could be attacked, which is not accomplished through just running scanning software. It is normal to use scanners to help in narrowing down specific technical areas for further analysis. But don't forget the personnel that have access to the equipment or the physical environment that houses the equipment. This brings about another interesting point, how far should you go? Is it enough to believe there may be an exploitable vulnerability or do you actually have to run the exploit to prove it is there? Downloaded exploits are fine, in isolated test labs, but may have unexpected consequences on production environments.

There is no single answer here. To a significant extent, the client expectations of the results and their desire not to impact production servers will likely influence

this decision. In fact, these points should all be clarified and negotiated in advance with full knowledge of the risks.

Keep archived logs of all the activities accomplished and include them in the final

"...how far do you go?"

report to the customer or management. A good practice to follow would be to perform an initial assessment on a specific set of targets. Develop a plan to implement recommended changes to address the problem areas. Make the changes and then do a second assessment that quantifies that the work accomplished achieves the security goals intended. You should be able to clearly see improvements. Decide on a reasonable interval to perform periodic vulnerability assessments on both the internal and external systems. I believe that there should be periodic vulnerability assessments annually or if there is a significant change in the physical or network environment. This process will give you an opportunity to evaluate the security of your infrastructure on an ongoing basis and engage in continuous improvement. The bottom line is that vulnerability assessments play an important role in a coherent security program.

Edward Fuller, CISSP, GSEC is a Vice-President and the lead instructor of the NSA IAM for Security Horizon, Inc.

efuller@securityhorizon.com

