



Pivot Point Security

957 Route 33

Suite 111

Hamilton Square, NJ 08690

(609) 890-1131

www.pivotpointsecurity.com



Lock IT Down: How to conduct a wireless security audit

by [John Verry](#) | [More from John Verry](#) | Published: 7/15/02

Category: System Intrusions | **Audience:** IT Consultant

Rating: 4.5 (out of 5) [Rate it](#) **Comments:** 6 | **0 NEW** | [View all](#)

The senior management team of NCTPTI, Inc. (Name Changed To Protect The Innocent) concluded that an external investigation of their network security was required after a series of security incidents culminated with the theft of key customer contact lists.

My company, [COUR.IT](#), was selected to perform a security assessment. We proposed to address the review as a comprehensive audit rather than as an investigation of the contact list theft incident. Our hope was that this approach would identify not only the source of the incident but other vulnerabilities that would leave NCTPTI susceptible to future security breaches.

I think that focusing on one security-related incident often gives an organization a false sense of security and removes it from a heightened state of awareness. Because a significant percentage of security incidents are internal, we were also concerned that the perpetrator might in fact be a member of the IT staff who was also involved in the mitigation. A thorough network security audit significantly reduces the risk associated with this "fox guarding the chicken house" scenario by identifying necessary improvements to controls (log review, vulnerability assessments, independent review) for key systems, processes, and applications. This type of audit ensures that any future incidents will be readily detected and minimizes any opportunity for internal incident cover-up.

Here's a look at our audit and what we found.

First in a series

This is the first in a series of articles that explores the results of a consultant's security audit for a client. The next article will detail more of the consultant's work and focus on remedies he used to secure the client's network.

Scope of the engagement

The audit's scope was considerable in light of the company's size, market position, value of its IT-secured assets, and the previously documented security incidents. The \$165 million company has more than 1,000 employees in three offices. Because of the nature of the security breach—stolen customer information—we identified the direct mail database as the critical issue. We also estimated the length of the engagement to be about 10 days.

The interview

During the initial phase of our network security audit, we met with executive management, major business unit leaders, key application/system/data "owners," and many members of the IT organization. This interview process is

strictly an information gathering mechanism. Generally, we do not challenge individuals to prove or document their assertions ("yes, we have a documented Disaster Recovery & Business Continuity Plan"), although we will often ask for a certain level of detail. ("In the event of a disaster, does it include a mechanism to communicate the company's current posture to all employees in a manner that would allow them to know the company's status and their responsibility?")

We look for a general awareness of IT security and industry best practices, a sense of the organization's commitment to strong controls over business critical systems—a measure of the degree of IT governance exercised by senior management—and a proper understanding of the individual's role in the development, enforcement, and maintenance of the organization's IT security.

These more qualitative measurements, coupled with the quantitative data gathered during the interviews, helped us establish the direction and focus of the investigative phase of the audit and formed the foundation for the formal recommendations that we presented to senior management.

The investigation

During the interview phase we noted that several significant issues were affecting the confidentiality and integrity of the network and the client's direct mail database. The first issue we investigated was the recent implementation of a wireless local area network (WLAN). We focused on this because of the inherent insecurity of WLANs, the high incidence of improperly secured WLAN deployment, and the correlation of the timing of the most significant security incident with the installation of the WLAN.

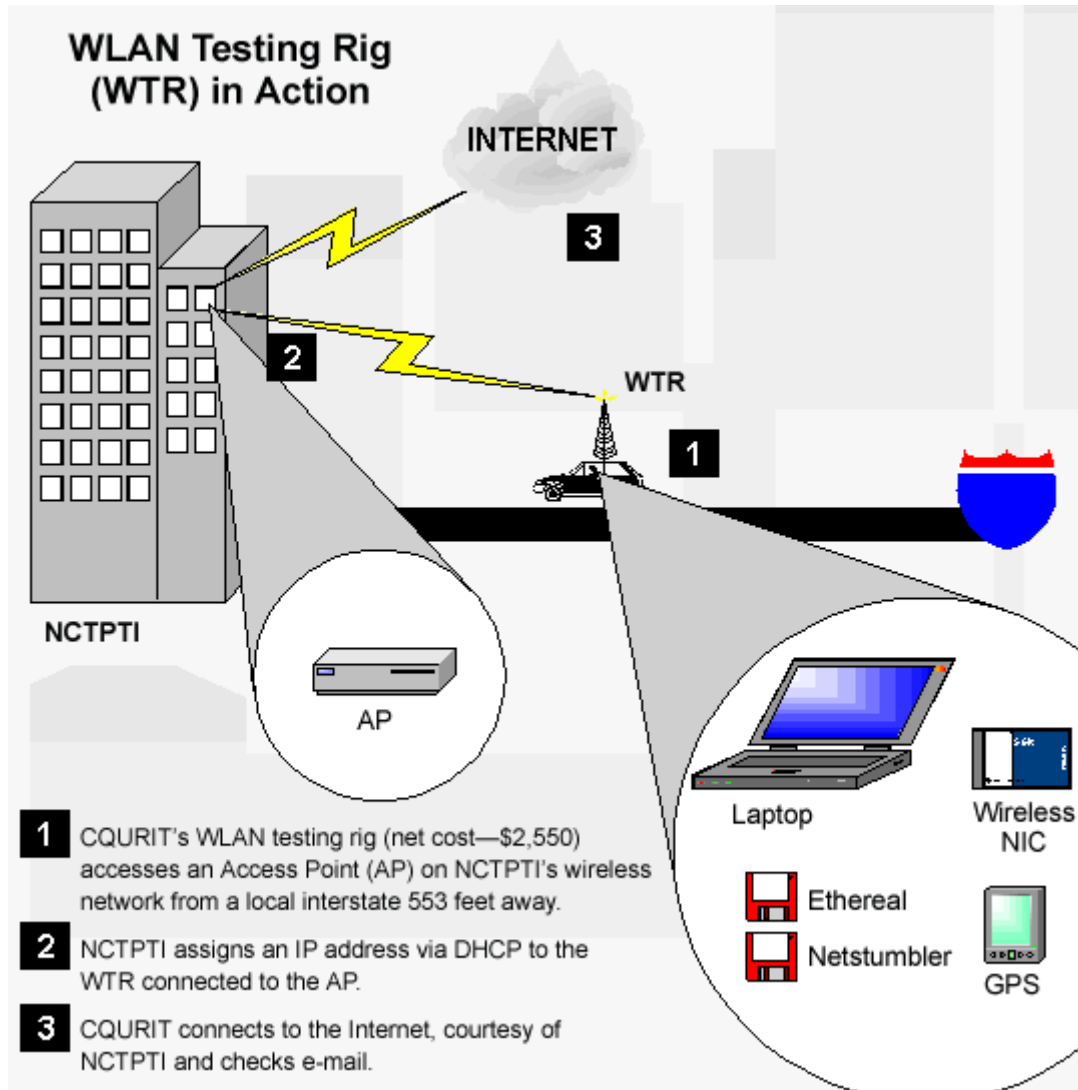
Recent surveys in publications and Web sites like Information Security and PC Magazine suggest that 60 to 90 percent of WLANs are deployed without even the most basic security mechanisms (changing default names, enabling encryption, optimized placement of AP).

Our own surveys mirror these numbers for both residential and corporate WLANs. Of the 139 residential WLANs we identified in May, only 11 had Wired Equivalent Privacy (WEP) encryption enabled, and 98 were left in the default factory configuration. Because a significant number of these installations are used to connect to corporate networks via virtual private networks (VPNs), a malicious external user who exploits the WLAN can use the existing VPN connection to access and exploit the corporate network.

War Driving

One tactic that we often use to test the security of a wireless network is War Driving, which involves using a laptop's wireless network interface card (NIC) and other equipment to locate wireless LANs. This is usually done while driving in areas where one may expect to encounter an unsecured WLAN (see **Figure A**).

Figure A



Depending on the investigation, we employ several different WLAN Testing Rigs (WTRs). These WTRs are identical to rigs employed by War Driving enthusiasts and hackers. The WTR we used for this engagement included a Compaq Armada M700 notebook computer running Windows 2000, an Orinoco Gold wireless 802.11b NIC, a Fab-Corp 5 dBi Magnetic Mount Omni external magnetic mount antenna, a Garmin eTrex Global Positioning System, a NetStumbler Wireless Access Point Mapping Application, an Ethernet Wireless Sniffer, and an ACAnywhere mobile power converter to power the notebook.

When testing, we generally drive to the client location with the WTR listening for Wireless Access Points (APs), the transmitters/receivers that are connected to the wired network to allow wireless access. In this case, even before we pulled into the client's parking lot, we heard a familiar series of broonnnnggggs from our WTR, indicating the locations of multiple Wireless Access Points.

In addition to four access points, which we presumed belonged to the client, we detected an additional access point from another company in the same office park. Immediately, our level of concern grew. Could someone sitting at his or her desk in the neighboring company currently be connected to our client's network? To determine the answer, we needed to identify which APs belonged to the client. Because both our client and the neighboring company had left their AP configuration in factory default settings, and were using APs from different vendors, we were easily able to differentiate the APs.

Once we had identified the client's APs, we used NetStumbler to establish the perimeter of its wireless network, which provided us with the distance from which it was possible to connect to the client's network. To connect to the network, we requested an IP address via DHCP. After IP receipt, we further verified connectivity by accessing the Web via the client's

network.

Our perimeter testing determined that we could access the WLAN from any area within 100 feet of the building, and two alarming locations—the neighboring company and the interstate several hundred feet behind the building. Vendor claims regarding an AP's range can be greatly altered by deployment location, weather conditions, and the antennas being used on the AP and access card.

Although our client's AP vendor only claimed a 400-foot range, we experienced great signal strength and conducted much of our testing on the shoulder of a local interstate 553 feet from the client's building, beyond the reach of any physical security measures. In testing, I have confirmed the ability to access a remote network from up to 695 feet, using a GPS to determine the distance. (Oddly enough, this is the distance from my home's driveway to the home of a neighbor who, as a vice president of a Fortune 500 organization, regularly uses a VPN to access his corporate network. The WTR determined that factory default settings were maintained and WEP wasn't enabled, leaving the AP unsecured. I advised my neighbor and secured the AP, and he notified his company of the issue.)

The client's WLAN is public knowledge

After checking our e-mail from the highway, we found the AP MAC addresses and physical location (GPS) had been posted to a database on the Web that details accessible APs (public or unsecured). The database is sometimes used by individuals to gain free Internet access but is also frequented by less scrupulous individuals who use it for hacking. We immediately requested that the APs be removed from the database and confirmed the removal later in the week.

Final thoughts

This client engagement further validated our belief that addressing security incidents with a broader security audit is more beneficial to both the client and consulting firm than an investigation that is focused on a discrete incident. It results in a more secure solution for the client and an improved understanding of how they can prevent, detect, and address security incidents. From the consulting firm's perspective, this type of audit results in significantly improved client satisfaction and additional consulting opportunities stemming from the initial security audit.