



**Pivot Point Security**

957 Route 33

Suite 111

Hamilton Square, NJ 08690

(609) 890-1131

[www.pivotpointsecurity.com](http://www.pivotpointsecurity.com)



## Final step in security audit process

by [John Verry](#) | [More from John Verry](#) | Published: 9/12/02

**Category:** Wireless Networking | **Audience:** IT Consultant

**Rating:** 4.4 (out of 5) [Rate it](#) **Comments:** 9 | **0 NEW** | [View all](#)

**Takeaway:**

Best practices in sharing audit results, solutions with client enterprise

---

Following the theft of its key customer contact lists, NCTPTI, Inc. (Name Changed To Protect The Innocent) hired our company to perform a security assessment. We found the client's wireless local area network (WLAN) unsecured and accessible from any area within 500-plus feet of its office building. Undetected, we successfully "hacked" its network and retrieved a copy of key customer contact lists.

Our next task was to take this information to the client and tell the client what was wrong and how to fix it.

---

### Last in a series

This is the final installment of a series that details a security assessment on a business whose computer systems had been violated via a wireless LAN. Previous articles detail the [vulnerabilities found in the client's network](#) and describe the [penetration testing](#) used by consultant John Verry and his firm, CQUR IT.

---

## Hack and tell

Once we identified the WLAN vulnerabilities, we immediately alerted the senior management team (SMT) to their significance. The following day, five of the six members of the SMT held a meeting at their facility to discuss the security assessment. The CEO excluded the CIO to ensure that the findings could be discussed openly.

After introductions, we pulled a notebook PC from a briefcase, opened it on the conference room table, and posed the rhetorical question, "Would you allow any individual with a notebook to walk in off the street and plug it into your network?"

The SMT sat around the conference table with amused faces, until the CEO smiled knowingly and replied, "Of course not, but I don't suspect you would have kicked off the presentation with that question without a reason."

We smiled back and rotated the notebook to demonstrate our ability to access the client's content, including the customer contact lists that had been exploited. We sat through several seconds of silence until the director of business operations said, "Somehow, I think this meeting is going to get worse before it gets better."

The halfhearted laughs and serious faces indicated that we had accomplished our initial goal of getting their attention and relaying our concerns regarding their current network security.

The balance of the meeting with the SMT focused on "reasonable and appropriate" uses for WLAN technology. The SMT agreed that there were compelling business reasons—cost and mobility—to continue using WLAN technology in their facility, but they would only do so if they could secure their data. To address the vulnerability as quickly as possible, we were asked to work with the information technology group to properly secure the WLAN.

## **Building bridges**

As is often the case when conducting a senior management-initiated security assessment, the review was as much about the key members of the IT team as it was about network security. In this case, the CIO, an SMT member, was kept distant by the CEO to ensure that the proper level of separation and control was applied. While this was in the best interest of the client, it made the situation potentially difficult for us as consultants.

According to members of the IT staff, the severity of the findings, coupled with the CIO's exclusion, resulted in an unpleasant meeting between the CIO and the CEO. In the wake of that clash, we met with the CIO and his staff to initiate the WLAN vulnerability remediation. The meeting proved to be painful for both parties, but was surprisingly productive. Without building trust, however, that productivity wasn't guaranteed to last.

After the meeting, we requested a one-on-one with the CIO to discuss the assessment, with the intent of transforming our relationship from antagonistic to advantageous. (Having led a software development organization in the past that was often the subject of FDA audits, I have a significant appreciation for the "violated and exposed" feelings one can experience during an audit review with senior management.)

The CIO was pleased to learn that a considerable amount of my discussion with the SMT positioned the WLAN problem as indicative of broader organizational issues, including insufficient IT governance by the SMT and the lack of a formal IT steering committee. Because he had recently raised the same issues, the CIO felt validated in his opinion: His IT organization wasn't consistently being put in a position to succeed.

Over time, we continued to build our relationship with the CIO and established our team as a key asset and regular contributor to the client's information security efforts. Had we not taken steps to help bring the CIO along, it's doubtful that the client would have adopted most of our recommended changes.

## **WLAN security 101**

The actual remediation efforts necessary to correct the WLAN vulnerabilities were fairly straightforward. We provided the client with some very basic guidelines for optimal WLAN deployment.

### **Reposition the access point or use a directional antenna**

The access point (AP) had been placed toward the southeast corner of the building, where it broadcast a quality signal to the local interstate and a neighboring office building. Depending on the building's physical structure, additional walls can significantly reduce the distance the AP broadcasts beyond the building. Directional antennae can also be used on the AP to further restrict broadcasting.

### **Add an additional low-end firewall between the AP and the network**

Using a firewall can provide basic authentication to WLAN users.

### **Test the perimeter**

Identify locations, and their distances from the AP, where someone can connect to the network. Five hundred feet away in the middle of a cornfield is preferable to 100 feet away in a neighboring office building. In the case of NCTPTI, moving the AP successfully eliminated the ability to access the network from a neighboring building, but only minimally reduced the distance from which someone could connect on the interstate

### **Enable Wired Equivalent Privacy**

Wired Equivalent Privacy (WEP) is a mechanism that encrypts WLAN traffic to prevent unauthorized users from reading data captured in transit. WEP can be cracked, but it requires a more knowledgeable and determined individual than your average war driver to crack it. Most WEP-cracking tools, like Aircrack-ng, run on Linux and require the user to gather approximately 4,000 packets with weak keys (keys being the secret keys used to generate the ciphertext) from packets of network traffic, which is usually enough of a deterrent to select another target (of which there are many).

### **Change AP's default settings**

Default AP configurations—Service Set ID (SSID), SNMP Community String, Administrative Password—are widely known by war drivers, and it's relatively easy for a knowledgeable war driver to connect to the network and commandeer control of an AP with default passwords. (Sadly, default passwords aren't uncommon.)

### **Restrict access to key systems/data**

Block WLAN access to the intranet server and other key data.

### **Disable SSID broadcasting**

To prevent the AP from broadcasting the network name and associating with nodes that aren't configured with the WLAN's unique SSID, disable SSID broadcasting. While this will protect the network from rogue users, it will make WLAN deployment a more hands-on experience because WLAN clients will require that the network name be manually configured.

### **Additional recommendations**

Several additional recommendations, which were not possible to implement for our client, include:

#### **Use MAC address filtering at the AP**

Many APs can be set to use MAC address filtering to restrict AP usage to specific machines.

#### **Implement out-of-band user authentication**

Should the security policy demand a stronger authentication scheme, two-factor authentication can be employed using a separate authentication server on a wired segment adjacent to the AP. This measure ensures that only authorized users are granted access to both wired and wireless resources.

#### **Disable AP Dynamic Host Configuration Protocol (DHCP)**

By default, most APs are set as DHCP servers and will automatically grant a WLAN IP address to any machine that requests one. This makes it very easy for war drivers to gather information and connect to your network. Disabling AP DHCP prevents this action.

#### **Utilize IPsec or VPN**

In cases where confidential data must traverse a WLAN, the data can be protected by VPN or IPsec-based encryption to provide the level of confidentiality required.

### **Don't shoot the messenger**

The WLAN was only one element of the security vulnerabilities that resulted in the theft of NCTPTI's key customer contact lists. Poor security practices and an improperly hardened IIS server were equally at fault. Additional recommendations were made regarding network architecture, system hardening policies and procedures, and authentication and access control to provide the level of security required for key corporate data.

Within 10 days of the penetration testing that revealed the WLAN vulnerabilities, the client had fully addressed the vulnerability and met the business requirements that dictated WLAN usage while maintaining an appropriate and reasonable level of security.

### **Final thoughts**

Essential to the successful deployment of a WLAN is the proper consideration by senior management of the business requirements and risks associated with their usage. Only after senior management has fully identified the requirements and acceptable levels of risk can an IT organization deploy a WLAN appropriately.

Due to the sheer number of targets available to the casual war driver, even the most basic WLAN precautions are generally sufficient to dissuade a potential hacker. Organizations that believe they could potentially be the targets of a more sophisticated attack (e.g., industrial espionage) should fully consider the risks associated with a WLAN before deployment.

Remember, because WLANs are inherently insecure, you must consider a number of important factors before their deployment:

- Why are we deploying a WLAN?
- Who will be allowed to use the WLAN?

- Where will we allow the WLAN to be deployed?
- Where are we going to position the access points in our infrastructure?
- What data will not be accessible via the WLAN?
- What additional technologies can we use to further secure the WLAN?
- How can we harden the WLAN to make it as difficult as possible to compromise?

It is generally most beneficial to look at this technology decision from a business perspective. For example, if the sole reason for the WLAN is to provide mobile access to the Internet, the risk is minimal.

The worst-case risk scenario with an exploit of a properly segmented network is the unauthorized use of the client's bandwidth for Internet access. Unfortunately, things are generally not that easy. By properly considering the client's organizational assets and the risk relating to their compromise, our policies for the WLAN provided reasonable and appropriate levels of security while allowing NCTPTI to reap a significant percentage of wireless technologies' business benefits.