AL 2003-10

OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Risk Management of Wireless Networks

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel.

PURPOSE

This advisory letter highlights risks associated with wireless networks and provides guidance for managing those risks. National banks can use this guidance to help in protecting company assets and confidential customer information, achieving service level requirements, maintaining safe and sound practices, and ensuring compliance with regulatory security expectations.

BACKGROUND

The emergence of wireless networking standards and products that rely upon unlicensed radio frequencies is causing an increasing number of national banks to consider how they might benefit from the technology advancements. National banks can use wireless technologies to build local-area-networks and personal-area-networks with low-cost devices and easy installations. The basic technology components include:

- Systems and devices sharing information (e.g., computers, workstations, networks);
- Access points and network interface cards sending and receiving data;
- Radio waves providing the conduit for data transmissions between access points; and,
- Authentication techniques establishing wireless connections.

The Institute of Electrical and Electronics Engineers, Inc. (IEEE) has been instrumental in expanding wireless network capabilities by developing standards that rely on unlicensed radio frequencies. The IEEE standards address varying capacity levels, transmission speeds, and functionality. In addition, the Wi-Fi Alliance, originally known as the Wireless Ethernet Compatibility Alliance (WECA), was formed to promote wireless devices interoperability through a formal certification process. Certified devices are considered to have certain minimum interoperability and performance standards that may reduce the user's need to test product performance individually.

Potential Risks Associated with Wireless Networks

Wireless networks can affect a bank's risk profile in a variety of ways, depending upon how the technology is used. Because wireless network standards continue to emerge and evolve, potential users face the challenging questions of how to obtain the necessary technical expertise and whether to be an early adopter or wait for proven standards. Failure to keep abreast of changing standards can expose a bank to strategic and reputation risks.

A bank's ability to mitigate these risks will depend upon:

- Effectiveness of board and management oversight;
- Effectiveness of management's policies and procedures to implement and manage wireless networking projects;
- Ability to keep up with technological changes;
- Network reliability and capacity;
- Adequacy of business continuity plans;
- Effectiveness of the bank's security program; and,
- Actions to monitor adverse events and take additional risk reduction steps.

There are two particular security challenges worth mentioning: the broadcast nature of wireless networks and an initial weak encryption standard. Wireless networks transmit data to anyone in the broadcast area that has the right equipment to tune-in reception. This is a unique difference from wired networks and poses security challenges that can expose a bank to significant transaction and reputation risks. Managing the broadcast area involves controlling radio transmissions that can travel through walls, windows, and doors. In addition, the initial encryption standard to protect data transmissions, named "Wired Equivalent Privacy" (WEP), has well-known weaknesses and vulnerabilities. Experts have cracked the WEP security standard, and tools are available to exploit WEP vulnerabilities. The combination of uncontrolled broadcast areas and use of a weak encryption standard creates an environment in which unauthorized access to systems and information can occur. This combination increases the importance of an effective security program and the quality of risk management.

RISK MANAGEMENT CONSIDERATIONS

The OCC wants to ensure that board and management oversight of wireless networks is effective and that the level of risk taken by using such networks is responsibly managed and controlled.[1] The following discussion focuses on security, project management, and performance considerations that are important in mitigating and controlling risks associated with the use of wireless networks. In addition, the appendix to this Advisory Letter highlights National Institute of Standards and Technology (NIST) risk management suggestions relating to effective management of wireless networks.

Key Steps

- Security risk assessments, appropriate policies, and adequate internal controls should be in place before wireless networks are used.

[1] See OCC Bulletin 98-3, "Technology Risk Management."

- Security measures should protect bank networks and wireless-enabled devices from unauthorized access, intercepted transmissions, and disclosure of confidential customer information, and other vulnerability threats.
- Security test plans should address wireless networks.
- Performance levels of service level agreements should be monitored to ensure that wireless solutions are effective.
- Total cost of ownership or return on investment objectives to implement and maintain the network, including incremental security costs (e.g., authentication, monitoring, updating, testing), should be considered as a component in determining project success.

Wireless Network Security

The OCC expects banks to have effective controls to maintain system security and protect customer information while it is stored or transmitted. The Federal Financial Institutions Examination Council's *IT Examination Handbook – Information Security Booklet* (December 2002) outlines a process to manage security-related risks as part of a bank's security program. The process identifies the following key steps: risk assessment, strategies, controls, testing, and monitoring and updating. It is important that the board and management update the bank's security program before activating new systems, such as wireless networks, since the use of new technologies may render an existing security program ineffective. Failure to update the program may violate regulatory requirements to safeguard customer information.[2]

Implementing User Policies and Procedures. Implementing effective policies and procedures for wireless network installations and their usage reinforces the importance of system security. Wireless policies usually restrict employees from establishing their own wireless networks without prior approval, since wireless access points are relatively easy to install. Unauthorized wireless networks may present high and potentially large risks to the security and integrity of bank networks. In addition, effective policies and procedures should encourage employees using approved wireless networks to report unusual activities.

Identifying Available Information. The types of information available through wireless network access (i.e., transmitted and network-accessible data) should be identified to ensure that the risk assessment is accurate, and the security plan is reasonable.

Identifying Wireless Access Points. Maintaining an inventory of all approved and deployed wireless network solutions and access points is important for effective project management. This improves management's ability to manage and update device settings and configurations, apply upgrades and patches, and manage network and device security. Clearly identifying wireless networks and devices on system architecture diagrams is also beneficial for ongoing risk assessments and security testing.

Controlling Broadcast Areas. The broadcast nature of wireless network signals means that anyone with the right equipment can tune-in and receive the signal, increasing the potential for unauthorized access to systems and information. This threat can be reduced through various techniques, such as strategic placement of wireless access points (e.g., center of building), reducing the broadcast signal strength to the minimum necessary, or turning devices off when

[2] See OCC Bulletin 2001-8, "Guidelines Establishing Standards to Safeguard Customer Information." The guidelines mandate that banks protect certain customer information and amend its information security program before implementing systems. This requirement would apply to a bank adopting wireless network technology.

not in use. Directional antennas, signal shielding, and physically securing wireless access points also improve control of the broadcast area and protect against unauthorized access.

Encrypting Information and Data. Encrypting wireless transmissions protects against unauthorized systems, devices, and information access. While WEP encryption is considered a weak security measure, it provides a security layer that acts as a deterrent. A better solution is to consider end-to-end encryption to maintain data integrity and protect confidential information transmissions. In general, end-to-end security measures protect data from inception to the end destination point regardless of the transportation method (i.e., wired, wireless). For example, using a virtual private network (VPN) adds another protective layer to enhance security. Emerging IEEE standards strive to provide stronger encryption alternatives to mitigate existing wireless encryption protocol weaknesses. Overall, the type of security used should be consistent with management's conclusions drawn from their security risk assessment.

Maintaining Authentication Controls. Authentication controls for users and devices need to protect the system's confidentiality and integrity, and mitigate risks associated with wireless environments. User password-only authentication may allow unauthorized systems access through password guessing or radio wave eavesdropping. The potential risk may warrant enhanced techniques such as token-based or certificate-based solutions because of uncertainty regarding the user's physical location, vulnerabilities in wireless network standards, and the broadcast nature of wireless communications.[3] Also, efforts to authenticate wireless devices accessing systems can mitigate threats from unauthorized wireless devices. Emerging IEEE standards also support new techniques for device authentication that can improve security (e.g., Wi-Fi Protected Access or WPA).

Protecting Against Logical and Physical Attacks. Wireless networks and devices are subject to intentional attacks (e.g., denial of service, man-in-middle, theft of data). Firewalls, intrusion detection systems, and anti-virus tools can protect systems and devices from attack. Also, disabling wireless connectivity during off-hours provides another protective measure. It is important that physical access restriction to wireless access points prevent intentional or accidental system configuration changes. Employee training that encourages reporting unusual workstation activities can also help identify problems.

Monitoring System Vulnerabilities. Emerging wireless network hardware and software standards and technologies have not been widely tested for vulnerabilities. Effective project management practices should include ongoing network security vulnerability monitoring, identification, and software patch processes.[4] Actively monitoring systems for unusual activities can ensure that these activities are identified and damage is minimized.

Banks that use Internet banking applications have learned that monitoring and updating network security should be a regular, ongoing process.[5] Additionally, when system changes are made, it is important to carefully review and assess the effect on other systems to be assured that previous vulnerabilities are not reintroduced into the network.

[3] See OCC Advisory Letter 2001-8, which transmits FFIEC guidance on "Authentication in an Electronic Banking Environment."

[4] See OCC Alert 2001-4, "Network Security Vulnerabilities."

[5] See FFIEC IT Handbook, Information Security booklet (December 2002); OCC Alert 2001-4, "Network Security Vulnerabilities;" and OCC Bulletin 2000-14, "Infrastructure Threats – Intrusion Risks."

Completing Security Tests. Wireless network systems should be included in the overall security testing program. Security testing can help ensure that only known wireless systems and devices are operating, controls are functioning properly, and vulnerabilities are mitigated. The security testing results can be used to update the risk assessment and ensure that policies, procedures, and controls remain appropriate.

Project Management Practices

In addition to the effective project management considerations mentioned in the previous “Wireless Network Security” section, the technology project management process needs to consider the rapidly evolving nature of wireless network technologies and standards. As new standards and products develop, early adopters need to obtain the necessary technical expertise and should consider and evaluate cost-benefit scenarios for staying with legacy, and perhaps more stable, standards or migrating to newer standards to gain more efficiency and benefits.

Completing Due Diligence. Outsourcing can provide technical expertise to install, maintain, and test wireless networks. Proper due diligence is critical when outsourcing wireless network activities because of the potential security threats. It is important that adequate due diligence be completed to ensure that the third-party provider is technically capable of implementing a solution that supports the bank’s needs (as identified during the risk assessments).[6]

Analyzing Costs versus Benefits. Evaluating cost and benefit assumptions related to wireless networks using a total cost of ownership (TCO) or return on investment (ROI) approach enhances overall project management. These analyses consider the anticipated benefits such as lower installation costs, improved employee productivity, expanded product and service offerings and better customer service. Costs include those incurred while deploying and maintaining the wireless network, acquiring the hardware and software, enhancing authentication requirements, data transmission security, routine maintenance, missing service level agreement requirements, potentially short product life cycles and upgrade periods, and access to technical expertise. This type of financial analysis provides a reference benchmark for determining whether products and services are achieving expectations.

Wireless Network Performance

Estimating Network Capacity. Data transmission rates and network capacity are dependent upon the standard chosen. A standard reporting high transmission rates does not mean that the network can handle the capacity necessary for timely transmissions. The performance requirements for wireless networks are important to identify during the development process. A good understanding of the types and volume of data transmitted allows effective planning to meet business objectives and service level agreements.

Understanding Network Availability. Network availability that is dependent upon unlicensed frequency means that it may be available now but may not be available in the future.[7] If a bank’s wireless networks experience unacceptable interference from other area networks,

[6] See OCC Bulletin 2002-16, “Bank Use of Foreign-Based Third-Party Providers;” OCC Bulletin 2001-47, “Third-Party Relationships;” and OCC Advisory Letter 2000-12, “Risk Management of Outsourcing Technology Services.”

[7] The Federal Communications Commission (FCC) allocates and licenses radio wave spectrum in the United States. The public, including banks, can own and establish networks that use unlicensed radio frequencies without direct ownership and licensing of the frequencies by the FCC.

devices, or appliances (e.g., microwave ovens, wireless phones), the bank is responsible for identifying the issues and taking the appropriate actions to support its business objectives.

Developing Business Continuity Plans. Business continuity plans need to consider the criticality of the businesses and systems supported, with alternative solutions developed as appropriate to achieve business needs and service level requirements.[8]

SUMMARY

Wireless network solutions provide national banks with an alternative for systems development that requires effective board and management oversight. Effective wireless network management includes maintaining adequate security, ensuring appropriate project management, and achieving performance goals. The OCC requires the board and management to update the bank's security program before implementing wireless networks and monitor the security program to ensure that effective risk management practices are in place. The guidance provided in this Advisory Letter, along with other OCC and FFIEC guidance can help national banks use wireless networks in a safe and sound manner.

RESPONSIBLE OFFICE

Questions regarding this advisory letter can be directed to the director for Bank Information Technology unit at (202) 874-5920.

Ralph E. Sharpe
Deputy Comptroller for Technology

[8] FFIEC IT Handbook, Business Continuity Planning booklet (May 2003). Wireless network solutions also may play an important role in business continuity plans.

APPENDIX

The National Institute of Standards and Technology (NIST) has produced a special publication (800-48) on *Wireless Network Security* that includes suggestions on policy, procedures, and controls to effectively manage wireless networking issues. This Appendix lists considerations that NIST discusses that are specific to wireless local area network (WLAN) security policies and access point configuration.

The OCC encourages banks that are interested in implementing wireless networks to review the NIST paper, particularly the tables titled “Wireless LAN Security Checklist” and “Summary of Wireless LAN Security” and narrative discussions on mitigating WEP encryption weaknesses.

A WLAN security policy should consider the need to:

- Identify who may use WLAN technology;
- Identify whether Internet access is required;
- Describe who can install access points and other wireless equipment;
- Provide limitations on the location of and physical security for access points;
- Describe the type of information that may be sent over wireless links;
- Describe conditions under which wireless devices are allowed;
- Define standard security settings for access points;
- Describe limitations on how the wireless device may be used, such as location;
- Describe the hardware and software configuration for any access device;
- Provide guidelines on reporting losses of wireless devices and security incidents;
- Provide guidelines on the use of encryption and other security software; and,
- Define the frequency and scope of security assessments.

Access Point Configuration should consider the need to:

- Update default passwords;
- Establish proper encryption settings;
- Control the reset function;
- Use Medium Access Control (MAC) Access Control Lists (ACL) functionality;
- Change the Service Set Identifier (SSID);
- Change default cryptographic keys;
- Change default Simple Network Management Protocol (SNMP) Parameter;
- Change default channel; and,
- Use Dynamic Host Control Protocol (DHCP).