White Paper

September 2006

SOX-Compliant Data Security for Business Travelers:

Protect against data theft over the unsecured wired and wireless networks employees access on the road

"...Just because you choose to ignore a risk, doesn't mean the risk is going to ignore you."

- Alan Brill
Senior Managing Director,
Technology Services
Kroll Inc.

Statement of Purpose

C-level executives charged with managing risk understand that Sarbanes-Oxley (SOX) mandates control of corporate and financial data to safeguard assets and protect against abuse. That mandate extends beyond the secure firewalls protecting internal information systems to the data that travels on laptops and across public networks. At greatest risk are the files traveling employees carry with them on the road, where the use of unsecured wired and wireless networks can expose data to theft and abuse.

According to the Privacy Rights Clearinghouse, a non-profit consumer information and advocacy organization, security breaches reported since ChoicePoint's Feb. 15, 2005, announcement have involved nearly 91 million records containing sensitive personal information.[i] These breaches resulted from unwelcome intrusions, lost laptops, hacked databases and inadvertent Internet postings, among other lapses. The reported breaches are only those cases involving consumer data. The total exposure to corporate financial data loss may be far greater.

The cost of data loss to companies, consumers, employees and patients remains to be tallied. InformationWeek Magazine reports breach-related lawsuits costing upwards of $13 million per individual case, including the cost of litigation, fines and penalties, as well as reimbursement of expenses related to fraudulent credit card charges and credit monitoring and restoration services.[ii] Costs not calculated: Tarnished reputations and lost business.

By informing employees about the risks associated with unsecured Internet access and providing guidance on securing laptops and other mobile devices, companies can take proactive measures to protect sensitive data wherever it resides. This white paper reviews the SOX compliance mandate and proposes steps for protecting the confidential financial data and personal information transported by business travelers.

Not Just a Public-company Challenge

The Sarbanes-Oxley Act became law on July 30, 2002, and is designed to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to security laws." SOX Section 404 is intended to build strong internal financial control programs, including information technology processes and controls.

Appropriate practices to comply with SOX Section 404 include the development and enforcement of corporate-wide information security policies that cover all employees. While these policies are broad in nature, the requirements for data integrity and security for traveling business people are crucial. Because SOX requires data security irrespective of physical location, corporate officers are obliged to ensure traveling employees are aware of and practice appropriate security measures.

At the same time, the rapid deployment and nearly ubiquitous availability of wired and wireless Internet access is making it more difficult to monitor and maintain the security of critical corporate data. Compounding the problem is the widespread misconception that firewalls and virtual private networks (VPNs) are sufficient protection against the theft of confidential information such as contracts, financial spreadsheets and customer lists—information that resides on the hard drives of most business people's laptops.

There is an attitude prevalent among executives that the risk of data loss is insufficient to merit high-level attention. According to Alan Brill, Senior Managing Director of Technology Services at Kroll Inc., a leading global risk consulting company:

> *"Data in the possession of your company which requires protection—for personal privacy reasons or because the information is proprietary—needs it wherever it is. It doesn't matter whether it is in the office, in an employee's home, or left on a laptop in a hotel room. Because if confidential information*

is lost or compromised, it's going to be a problem, wherever it is.

"Our experience shows us that many companies choose to ignore this risk, which is short sighted, because there are a lot of ways to manage the problem. But 40 years of looking at information security management issues has taught me one important lesson: Just because you choose to ignore a risk, doesn't mean the risk is going to ignore you."

SOX pushes public companies to take immediate and appropriate action, the very real threat of data theft should motivate every business enterprise to secure the confidential and personally identifiable information that resides on employees' mobile computing systems. As noted attorney and legal advisor to the hotel and hospitality industry Joshua Grimes said, "The Sarbanes-Oxley Act has created a duty of care for anyone with access to data to take measures to keep it confidential."[iii]

Ease of Internet Information Theft

The use of connectivity options has grown explosively—for example, 80 percent of all laptops are now wireless-enabled at purchase[iv]—creating a dangerous situation for traveling employees, whether road warriors or the occasional business traveler. According to Jupiter Research, frequent business travelers depend on Internet access on the road, with 98 percent of them checking e-mail while traveling.[v] When they check e-mail over an unsecured connection, they're exposing the corporation to undue risk.

According to David Garrison, President and CEO of iBAHN, a leading global provider of secure wired and wireless Internet service to the hospitality industry, most laptop users don't realize how easily hackers can obtain private information stored on their hard drives, and how detrimental that data loss can be. In a 2006 survey report issued by the Enterprise Strategy Group, 68 percent of corporate information security professionals surveyed said that confidential data is most at risk on laptops, and one-fourth of these professionals admitted that their organizations are vulnerable or very vulnerable to experiencing security breaches.[vi]

The reality of unsecured networking is that unless every hard drive file has its own password, information on a laptop can easily be viewed by others connected to the same unsecured network. In addition, potential hackers don't need special software to steal hard drive information. Most PCs with Windows Explorer come factory-equipped with the necessary tools for information theft, and hackers are only three clicks away from effortlessly obtaining another person's confidential information:

1. Open Windows Explorer and click once on the "My Network Places."
2. Click again to select "Entire Network."
3. Click a third time on "Microsoft Windows Network" to reveal all possible domains on the network.

If the network is secure, the user will be unable to view or access these domains. If the network is unsecured, as are a significant number of wired and wireless networks, the user will be able to surreptitiously view and download the files on any available computer hard drive in the domain range.

In an apparent nod to this weakness, Microsoft has issued beta test software for a Wi-Fi management utility called Windows Live Connection Center Wi-Fi. The service, which is not scheduled for full release until in 2007, will provide facilities for connecting to secure and non-secure Wi-Fi hotspots using encryption, enabling users to establish a VPN from an unsecured hotspot.[vii] Given the slow adoption rate of new utilities, this fix can not be relied upon to staunch the flow of corporate data from unsecured networks.

Prevalence of Unsecured Wireless Networks

As of May 2006, there were 113,596 global wireless hotspots functioning in 127 countries around the world —up 111 percent from January 2005, when there were 53,779 Wi-Fi hotspots in 93 countries. Hotels and resorts top the list of the most popular Wi-Fi hotspot locations with more than 30,000 hotspots around the world, making laptop security a prime issue for business travelers.

According to a global survey conducted by iBAHN in April 2006, 68 percent of respondents claimed to own a Wi-Fi enabled device, and an additional 21 percent said they do not own one but plan to purchase a Wi-Fi enabled device within the next year. Given easy access to Wi-Fi hotspots in places such as airports, hotels, railway stations and coffee bars, 55 percent of iBAHN's survey respondents said they still have concerns about data security in these public areas. A sizeable 30 percent admitted that it was the "hotspot" element that troubled them, while another 20 percent claimed they were nervous about using an unfamiliar Wi-Fi provider.

Their concerns are not without merit. Consider this scenario: At a recent information security conference in London, 62 percent of the 200 wireless access points at the conference were found to be unsecured. Outside the exhibition hall, 40 percent of the 250 public Wi-Fi networks were open. In all, 49 percent of the public wireless Internet access sites around the city had no encryption whatsoever.[viii] These were just the public areas. Though encryption of business networks is increasing, RSA Security reports that in major cities worldwide, about one quarter of wireless business networks are unsecured.[ix]

With 95 percent of 135.4 million American workers doing business away from their offices at some point during 2005,[x] protecting corporate information wherever it resides is crucial. As the wireless sector continues to grow, and cities like New Orleans, San Francisco and Philadelphia implement unsecured municipal area networks, the potential for exposure to intrusion is only increasing. For road warriors, occasional business travelers and remote workers alike, the implications are grim. Accessing the Internet away from the office can be a risky proposition.

Mandate to Mitigate Risk

Imagine the chagrin of a corporate officer who learns that the company's annual sales meeting has been infiltrated by a competitor, and proprietary product information has been stolen from an as-yet undelivered laptop presentation. In addition to exposing companies to the business risks associated with revealing product specifications, pricing information and earnings reports, loss of confidential data can violate employee, customer and patient privacy rights. For example, imagine a healthcare organization's despair upon learning that a patient list has been downloaded from an employee's laptop while attending a medical conference.

But fact is stranger than fiction. Among the more alarming data loss incidents reported by Privacy Rights Clearinghouse are these events that occurred in the month of August 2006 alone:[xi]

- 24,000 patients may have had their names, addresses, social security numbers and insurance information stolen from a home health care nurse's laptop
- 59,000 employees may have had their SSNs and sensitive information related to health and disability plans stolen from a company auditor's laptop
- 132,470 commercial drivers, pilots and motorists may have had their license numbers, birth dates and social security numbers stolen from a DOT agent's laptop
- 650,000 subscribers may have had their Internet searches posted on a public web site, where query records exposed SSNs, credit card numbers and other sensitive data

- An unknown number of customers had money stolen from their bank accounts when data was intercepted using a wireless laptop computer

Company executives negligent in protecting consumers' private information are exposing their organizations to expensive lawsuits, fines and penalties. These incidents, and the hundreds of incidents like them, potentially violate Sarbanes-Oxley requirements and, in the case of patient data, the patient privacy protections required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Failure to report such incidents would also violate the data protection laws of more than 20 states. And the laws protecting privacy and data security are only getting tougher.[xii]

In light of the outbreak of security breaches at dozens of U.S. companies—at least 284 reported since ChoicePoint's 2005 incident—Congress is stepping up to address the situation through newly proposed legislation. Now in the House is the Data Accountability and Trust Act (DATA), which requires companies to protect consumers "by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach."[xiii] Rep. John Dingell (D-Michigan), Chairman of the Committee, said the Bill's message on secure information is clear: "If you can't protect it, don't collect it."[xiv]

Data Protection for Business Travelers

With workers using an ever-increasing number of mobile wireless devices, companies need to maintain productivity while protecting the security and integrity of the enterprise's critical business data. This means ensuring that all appropriate steps have been taken to protect against data theft when employees leave the secure enterprise network.

The threat to mobile data security can be summed up as "the transmission and capture of unencrypted data on unsecured wired and wireless networks." While tools are available to alert users that they have accessed an unsecured network, it should not be assumed that business travelers use and respond to these alerts. Developing a clearly stated policy for out-of-enterprise use of Internet connectivity is the critical first step to protect against data loss and mitigate risk. These policies cost little yet offer a broad range of protection.

The recent string of data loss incidents at federal agencies—beginning May 22, 2006, when the Department of Veterans Affairs disclosed the theft of a laptop and external hard drive with unencrypted names, Social Security numbers and birth dates for about 26.5 million veterans—prompted the White House Office of Management and Budget to recommend measures to protect the security of personal information that federal civilian agencies hold on millions of employees and citizens.[xv] The June 23rd OMB memo includes a checklist for protection of remote information prepared by the National Institute of Standards and Technology (NIST). These are recommendations that any organization would do well to follow.[xvi]

A risk-management policy for traveling employees should provide these safeguards for personally identifiable information and other sensitive or confidential data:

- Ensure that all laptops are equipped with a firewall
- Ensure that file-sharing and peer-to-peer communications are disabled
- Ensure that all vulnerable ports on laptops are closed
- Define requirements for setting strong passwords and securing laptops and handhelds when left unattended
- Identify rules for determining whether the downloading of sensitive data onto laptops and handhelds is allowed
- Require documentation of sensitive information downloaded to laptops or handhelds, and verification that those records are deleted within 90 days unless their use is still required

- Require sensitive data stored on laptops and handhelds to be encrypted
- Require two-factor authentication—a password plus a physical device such as a key card—to reach a work database through a remote connection
- Require remote connections to be automatically severed after 30 minutes of inactivity
- Develop scheduled, annual security training for traveling employees
- Require employees to seek secure lodging and work environments
- Require laptops and handhelds to be locked in a safe when left in a hotel room
- Require laptops used in hotel conference rooms that are at times unoccupied to be locked to a table via cable
- Require corporate travel departments to identify lodging with secure Internet access
- Post hotel and conference sites approved for secure access on your corporate Intranet

When identifying lodgings, business centers and conference facilities with secure Internet access, business travelers and corporate travel departments should look for these characteristics:

- **Guest Rooms:** Wired (via an always-on hardware connection) or wireless Internet access secured against hacking, spyware, viruses and spam. For access to the corporate VPN, each connection must have an individual public IP address.
- **Conference and Meeting Rooms:** Secure, high-speed always-on connectivity supports multi-user connections, video conference sessions and webcasting. Private meeting networks are segregated into virtual local area networks (VLANs).
- **Business Center:** Secure, high-speed Internet access enables users to download files, send and receive e-mail, connect to the corporate VPN and print material.
- **Public Areas:** A fully deployed Wi-Fi Protected Access (WPA) network affords the highest level of security for wireless networks.
- **Back Office:** Internet-connected Property Management Systems (PMS) provides layered security and encrypts Internet data communications.

Executives at top hotel chains acknowledge their systems are routinely probed by hackers, making security a priority for the hospitality industry.[xvii] Hotel properties and meeting facilities with up-to-date data security procedures not only protect the personal and confidential information of their guests but also provide business travelers with a secure environment to conduct their business.

iBAHN's Role in Data Security for Travelers

As a leading global provider of secure wired and wireless Internet service to the hospitality industry, iBAHN works with hotels and conference centers to ensure their networks are secure. An iBAHN-enabled hotel property provides these security services and precautions:

- A layered network design that insulates each layer—the guest, the hotel, and the Internet
- A VPN certification program that ensures corporate travelers have a secure "tunnel" to their companies' VPNs
- Wi-Fi Protected Access (WPA) implemented throughout the network that locks the connection between a wireless access point and guests' laptops, eliminating the possibility of user-to-user communication or hacker intrusion

- Continuous pro-active monitoring of the network to identify infected traffic before it can bring down the hotel network
- Bandwidth on demand to enable high-speed access for bandwidth-intensive applications such as video streaming
- Non-stop availability through peak usage times and, when outages are detected, traffic redistribution within milliseconds so guests experience no loss of connectivity
- 24/7 phone support to answer guest questions and on-site technical support for conferences

Serving more than 2,100 hotels and meeting and conference venues in 18 countries worldwide, iBAHN's secure, broadband high-speed Internet access allows business travelers to work safely and efficiently from public access locations. iBAHN is unique in providing secure wireless access (WPA) throughout its entire network, allowing travelers to rely on iBAHN to protect themselves outside of their corporate environments.

Unlike other system providers, the iBAHN network is "locked," eliminating the ability for hackers to intercept a signal before it reaches the security gateway, protecting users from phishing, worms, spyware, and other attacks threatening their hard drives, passwords, and VPN connections. Additionally, the secure and continually monitored wired backbone delivers the industry's most practical and safest available wired or wireless connection, allowing business travelers to conduct business away from the office with confidence that their private information will be protected and easily accessible.

For more information on the contents of this paper or how iBAHN-enabled hotels and conference centers can assist in protecting business travelers against data theft, please contact:

Shannon R. Michael
Director, Corporate Communications
iBAHN Corporate Headquarters
10757 S. River Front Parkway, Suite 300
Salt Lake City, Utah 84095
801.563.2000
pr@ibahn.com
www.ibahn.com

Disclaimer: The contents of this white paper are meant for informational purposes only and are not meant to take the place of professional legal counsel. For specific advice related to individual case studies and issues pertaining to SOX compliance, it is recommended that you seek informed legal advice.

---

i www.privacyrights.org/ar/ChronDataBreaches.htm#Total
ii www.informationweek.com/story/showArticle.jhtml?articleID=183700367
iii http://meetingsnet.com/corporatemeetingsincentives/mag/meetings_data_secure/
iv www.gartner.com/press_releases/pr23sept2003a.html
v www.jupiterresearch.com/bin/item.pl/research:concept/625/id=97153/
vi www.the-dma.org/cgi/dispnewsstand?article=4692+++++
vii www.vnunet.com/vnunet/news/2162996/windows-live-wifi-hotspot
viii www.internetnews.com/security/article.php/3608876
ix www.rsasecurity.com/press_release.asp?doc_id=6870&id=1034
x www.workingfromanywhere.org/news/pr100405.htm
xi www.privacyrights.org/ar/ChronDataBreaches.htm
xii www.informationweek.com/story/showArticle.jhtml?articleID=183700367&pgno=6
xiii www.infoworld.com/products/print_friendly.jsp?link=/article/06/03/29/76930_HNhouseondata_1.html
xiv http://energycommerce.house.gov/108/News/03292006_1830.htm
xv www.washingtonpost.com/wp-dyn/content/article/2006/06/27/AR2006062700540.html
xvi www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf
xvii www.hotel-online.com/News/PR2005_3rd/Sep05_NorthwindSafeguards.html