

COMPLIANCE CORNER

January 2005

Laptop Security

The burden of maintaining information confidentiality falls directly upon the employee in possession of such information. According to the California Senate Bill 1386, FFIEC Information Security Compliance Standards and Guidelines, and the Gramm-Leach-Bliley Act requirements, enormous responsibility is mandated regarding information security and risk response. Serious ramifications face an institution if any non-public information is lost or stolen. The Board of Directors is ultimately responsible for all institution activities and compliance; however, all employees have a duty to ensure information security at all times.

Laptop computers pose a unique information security risk to financial institutions as data can be stored entirely on a remote and portable system and operated independently from the parent location.

The 2004 CSI/FBI Computer Crime Survey establishes losses by U.S. companies from laptop theft at \$6.8 million; this does not include the value of the data lost, penalties to the institutions due to legal ramifications, damage to reputation, and regulatory sanctions. Additionally, the FBI links 57% of all computer crimes (identity theft, fraud, etc.) to stolen computers, 49% of all stolen computers are laptops.

Another issue for all laptop users to recognize is the ever increasing complexity of scams and theft strategies. The Federal Aviation Administration recently issued a warning regarding the theft of laptops from the conveyor belts of X-ray machines at airport security checkpoints. It's a simple yet effective scam involving two thieves in the security line. The first one passes through the metal detector quickly. The second stalls the process, delaying the entire line with loose change, keys, and other items that trigger the alarm. Meanwhile,

the people behind these potential thieves have already placed their luggage, including laptops, on the conveyor belt. As the line is at a stand still, the first thief casually picks up the laptop as if it was his or her own and calmly walks away while the other accomplice continues to the line, ensuring a clean getaway.

To augment existing information and asset security efforts, institutions should implement concise policies and procedures regarding the use and restrictions of laptops. These policies should enforce security standards and expectations regarding the handling, storage, processing, or dissemination of sensitive data and the technology required to ensure confidentiality, integrity, and availability of that data. Encryption methods should be implemented to increase security and control, either by applying encryption to the entire device or creating an encrypted "vault" where sensitive information is stored.

The amount of sensitive information stored on a laptop should be limited to only what is immediately required. All local laptop data should be uploaded to a secure network drive as soon as possible for redundancy and security purposes. Periodic wiping of all sensitive information from the laptop and requiring the employee to keep only sensitive information required for immediate tasks should be enforced.

By keeping only necessary confidential information and maintaining a log of what sensitive information is maintained locally, liability is limited to only that information stored on the laptop. If sensitive data on a laptop is stolen or lost, the institution may be required to disclose the loss/theft to the institution's entire customer list, potentially causing severe damage to its reputation, revenue loss, and regulatory penalization.