MIS Quarterly

SPECIAL ISSUE

MARKET VALUE OF VOLUNTARY DISCLOSURES CONCERNING INFORMATION SECURITY

By: **Lawrence A. Gordon**
Robert H. Smith School of Business
University of Maryland
4332F Van Munching Hall
College Park, MD 20742-1815
U.S.A.
lgordon@rhsmith.umd.edu

Martin P. Loeb
Robert H. Smith School of Business
University of Maryland
4333L Van Munching Hall
College Park, MD 20742-1815
U.S.A.
mloeb@rhsmith.umd.edu

Tashfeen Sohail
IE Business School, Madrid
Calle Pinar 15 - 1B
28006 Madrid
SPAIN
Tashfeen.Sohail@ie.edu

Appendix A

Coding Instrument for Information Security Disclosure

Proactive security activities encompass voluntary disclosure concerning information security that firms are taking to improve the security of their information and information systems. Examples of voluntary disclosures falling into this category include discussions about a firm's use of encryption, secure socket layers data transmission, implementation of network security measures, or disclosure of computer security policy. The disclosure is coded as 1 if the firm provides any information, 0 otherwise.

Potential security vulnerabilities includes voluntary disclosures that discuss a firm's vulnerability in infrastructure (i.e., a susceptibility of their computer systems), or report that the firm's infrastructure is at risk of being disrupted by computer viruses or hacking. The disclosure is coded as 1 if the firm discusses any vulnerability, 0 otherwise.

The third category is comprised of voluntary disclosures that report an actual information security breach (i.e., these disclosures explicitly consist of reports that detail "denial-of-service" attacks or hacker penetration of the information system infrastructure). The disclosure is coded as 1 if the firm specifically lists a security breach, 0 otherwise.

Appendix B

Examples of Disclosures of Security Activities

Proactive Security Activites

"…disclose nonpublic personal information to nonaffiliated third parties and affiliates; annual notices of their privacy policies to current customers; and a reasonable method for customers to opt out of disclosures to nonaffiliated third parties. Compliance with these rules was mandatory after July 1, 2001. San Rafael Bancorp and Tamalpais Bank were in full compliance with the rules as of or prior to their respective effective dates. SAFEGUARDING CONFIDENTIAL CUSTOMER INFORMATION. Under Title V, federal banking regulators are required to adopt rules requiring financial institutions to implement a program to protect confidential customer information. In January 2000, the federal banking agencies adopted guidelines requiring financial institutions to establish an information security program. Tamalpais Bank implemented a security program appropriate to its size and complexity and the nature and scope of its operations prior to the July 1, 2001 effective date of the regulatory guidelines, and since initial implementation has, as necessary, updated and improved that program. (PAGE: 27)

Filer: *EPIC BANCORP* *Date Filed: 3/30/2004*
Report: 10-KSB *Period: 12/31/2003*

Potential Security Vulnerabilities Disclosure

Many of our competitors have substantially greater resources to invest in technological improvements. We cannot assure you that we will be able to effectively implement new technology-driven products and services, which could reduce our ability to effectively compete. Our hardware and software systems are vulnerable to damage that could harm our business. We rely upon our existing information systems for operating and monitoring all major aspects of our business, including deposit and loan information, as well as various internal management functions. These systems and our operations are vulnerable to damage or interruption from natural disasters, power loss, network failure, improper operation by our employees, security breaches, computer viruses or intentional attacks by third parties. Any disruption in the operation of our information systems could adversely impact our operations, which may affect our results of operations and financial condition. (PAGE: 9)

Filer: YARDVILLE NATIONAL BANCORP Date Filed: 3/31/2003
Report: 10-K Period: 12/31/2002

Actual Security Breaches

For example, approximately four percent of our customers experienced a brief delay in delivery of services on June 15, 2004 as a result of a denial of service resulting from an attack by hackers on our network. We believe this attack targeted several well-known websites that are customers of Akamai. Although we have taken steps to enhance our ability to prevent the recurrence of such an incident, there can be no assurance that similar attacks will not be attempted in the future, that our enhanced security measures will be effective or that a successful attack would not be more damaging. Any widespread loss or interruption of our network or services would reduce our revenues and could harm our business, financial results and reputation. (PAGE: 10)

Filer: AKAMAI TECHNOLOGIES INC Date Filed: 3/16/2005
Report: 10-K Period: 12/31/2004