The SANS Technology Institute
Contact Stephen Northcutt
FOR IMMEDIATE RELEASE
October 8, 2009

Tel: (808) 823-1375
Email: stephen@sans.edu

SANS Technology Institute announces paper with guidance on mitigating risks to financial loss for small and medium businesses

A new paper has been released from the SANS Technology Institute providing guidance on mitigating risks to financial loss for small and medium businesses. Known as a Joint Written Project, this paper was developed by students as part of the SANS Technology Institute Masters Program. Recently, small and medium businesses have lost millions of dollars from fraudulent electronic financial transactions. This paper reviews the threat and provides guidance for mitigating the threat.

These crimes typically begin with a phishing email targeted at the comptroller or other staff in the finance department. After the comptroller's computer is compromised, sophisticated malware is used to eavesdrop on the comptroller's activity and account credentials for financial systems. Once the attackers have the required information, they begin to steal money with fraudulent transactions in amounts below $10,000. These smaller amounts fly under the laundering detection mechanisms in the US Bank Secrecy Act. In many cases, repeated transactions have added up to hundreds of thousands of dollars lost by individual organizations.

The paper provides a number of possible ways to mitigate these types of attacks. A defense in depth approach is used to provide multiple mitigation recommendations. The number one recommended mitigation is to use Read-Only Bootable Alternative Media (ROBAM) as an isolated environment for financial transactions. The mitigation steps also include protecting the email address of the comptroller, network protection, endpoint protection, virtual machines, awareness training, policy changes and monitoring financial transactions.

To access the paper, please see http://www.sans.edu/resources/student_projects/200910_05.pdf

About SANS and SANS Technology Institute. SANS was established in 1989 as a cooperative research and education organization. Its programs reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, andCIOs who share the lessons they are learning and jointly find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. To develop the technology leaders needed to help strengthen the world-wide defensive information community, the SANS Technology Institute was created as a degree-granting affiliate of SANS. It is one of the nation's leading graduate schools devoted to the study of information security.