

AuditOne Advisory

From Bud Genovese, Chairman

Not All Network Penetration Testing Is Created Equal

As banks continue to provide increasing percentages of their services online (with hackers and technical bugs hopefully more than a few steps behind), regulators are paying closer attention to internal and external network penetration testing. Once considered a subset of the annual IT examination, penetration testing has risen to a prominent role in the risk management programs of most financial institutions.

But there are key differences in the quality and scope of penetration testing vendors out there. The sobering truth is that over 90% of the time we try, AuditOne is able to successfully hack or compromise critical systems and obtain secure confidential data from systems of banks that have not engaged AuditOne for penetration testing in the past. Here are a few tips to help you in your selection of penetration testing vendors.

First of all, be certain that the firm offering penetration testing is technically qualified. Regulators are requiring more complex technical analysis in penetration testing, so the staff providing the service should hold technology certifications such as CISSP and CISA, the highest technical standards in the information security industry.

Secondly, Federal guidelines recommend independent diagnostic testing. To be considered independent, the testing firm should not be responsible for the design, installation, maintenance, or operation of the system being tested. Likewise, firms performing the tests must not have a financial or reputational interest in the systems being tested.

Thirdly, social engineering testing (assessment of vulnerability to telephonic and other non-network threats) is now a critical element of penetration testing. Penetration testing without this important component overlooks the very significant threat of identification theft.

Fourthly, penetration testing reports must be clear, free of technical jargon, and easily understandable to bank boards and directors as well as providing specific technical analysis for the bank IT staff.

And finally, the beneficial results of penetration testing are best realized within the context of other critical Information Technology reviews such as Information Security/GLBA Compliance and Business Continuity/Disaster Recovery. The most effective approach is a coordinated, multi-faceted view of the entire IT operation, not just a snapshot that can ignore full insight.

Our AuditOne team of technology experts hold CISSP certifications, and have real world, hands-on IT/network systems operational experience inside billion-dollar banking and financial institutions. We have developed an internal knowledgebase over the past decade to keep our staff up-to-date on the latest banking application security flaws. In addition, we have a large enough staff to rotate the individual penetration testers to ensure a fresh approach every time we perform these tests. Our network penetration testing and IT audits are based upon the latest FFIEC Information Security Exam Guidelines and other standards recommended within those guidelines such as ISO17799-2005.

AuditOne penetration testing includes social engineering testing, and we're constantly refining and updating our work programs and protocols to provide the latest technology and non-technology analysis required. Our reports are written in both general language for bank executives to understand and deeper, specific technical analysis upon which for the bank IT staff can act.

AuditOne's full range of technology services include External and Internal Network Penetration Testing with Social Engineering Analysis, Information Technology (IT) Audits, Electronic Banking (with Cash Management, Remote Capture) Audits, and consulting for specific aspects of Information Security Risk Assessment (methodologies), Business Continuity Planning (Business Impact Assessments), and other Information Security policies and procedures.

We'd be honored to discuss your current and future needs for network penetration testing and IT auditing. We have the right expertise at the right price. Please contact me or AuditOne CEO Kevin Watson (kevin.watson@audit-one.com) or AuditOne President Jeremy Taylor (jeremy.taylor@audit-one.com). Thank you.--Bud

*Bud Genovese is Chairman of AuditOne LLC, a California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit and credit review services by gathering wide-ranging, extraordinary expertise within one firm. AuditOne now serves over 160 clients throughout the Western United States, and **nationally**. Contact Bud Genovese at 408-980-8099 or bud.genovese@audit-one.com*