

Perimeter, Host and Endpoint Security – Finding the Right Mix

In the past, the perimeter was everything and many organizations simply deployed a firewall and nothing else. Today banks realize that they need many layers of protection from the perimeter to their local area network to the desktop. Intrusion Detection and Prevention Systems should really be mandatory for banks to deploy on their internal networks. While Host Intrusion Prevention Systems also have some value, they can be troublesome to deploy and maintain, especially on the bank's core system platform.

Even with all of these great technologies in place, you cannot ignore the human element. Social engineering tactics were quite popular years ago, and are now making a strong comeback. Attackers have so many ways to go after bank employees – over the telephone, email, websites, etc. Unfortunately, it is not possible to completely lock-down employees' desktops, so once the desktop is compromised, hackers are free to mount their attacks from the inside and completely bypass even state-of-the-art security systems.

At Trace Security, our highly experienced engineers have taught security courses all over the world. We recognize that every bank is different and subsequently we can tailor our courses to each bank's specific needs. The value of a properly implemented Security Awareness Program can be tremendous – for a fairly low investment, the bank can reap big rewards in preventing security breaches and incidents.

Many banks are turning to MSPs (managed security providers) to help them protect their critical assets. In general, we believe that this is a good trend because the vast majority of banks simply do not have the internal IT resources to manage their infrastructure around the clock. As a leading provider of security compliance and risk management solutions to banks across the nation, we do not provide managed security services due to the fact that we believe that you cannot assess what you manage. This type of unbiased and vendor neutral approach to security auditing and compliance enforcement gives our clients peace of mind that their systems are properly configured.

We have spent millions of dollars developing our TraceCompliance Manager which is the first comprehensive solution in the industry to automate regulatory compliance audits, board level reporting, policy management, vulnerability assessment, and employee education and testing. Because it is Web-based, banks can easily implement it and start enjoying the benefits immediately – it provides a real-time view of the bank's environment and provides actionable alerts and remediation recommendations. Our mission is to help banks of all sizes achieve, maintain and demonstrate security compliance, and we accomplish this by covering the three critical areas: people, process and technology.



Jim Stickley
CTO

Jim Stickley is CTO and Vice President of Engineering for TraceSecurity. Jim has been instrumental in directing the TraceSecurity strategy and is responsible for developing and releasing multiple versions of the software used by hundreds of clients today. Jim is in charge of the guiding principles and structure of all TraceSecurity solutions including products and services. Jim has over ten years experience in the high-technology industry. Furthermore, he serves as a speaker at numerous security-related tradeshows, conventions, seminars and forums throughout the U.S., covering topics that range from basic network security to national cyber terrorism. Jim continues to appear on the Today Show at NBC covering topics related to cyber crime and identity theft.

