

Securing the Bank from the Inside to the Outside

We take for granted the Internet's ubiquity today with its myriad of applications and services. Was it really only 15 or so years ago that we first permanently connected our community banks to the Net and began to offer the first, nascent iterations of home banking? Back then, we did what the vendors and consultants told us; we bought their firewalls, shored up our anti-virus, then slapped in an Intrusion Detection Sensor (IDS) to look for craftier attacks. The IDS morphed into Intrusion Prevention Systems (IPS), claiming superiority because it could stop "bad" traffic in its tracks rather than merely detect. When the preponderance of external threats vastly outweighed - at least in volume - any threats posed from the inside, this model was sufficient.

As our security standards evolved, criminals and miscreants matured alongside, developing bypasses through and around these perimeter defenses. Yet many of our IT departments lag in updating controls and security definitions due to cost, lack of knowledge, or minimal audit enforcement. The ever-present challenge is really about the evolution of the threats themselves. What was right to prevent attacks in 1995 is laughable today. What is right today will be a joke in five years. Many institutions don't have any reference to understand their security posture as it pertains to right now.

Vulnerability scans or penetration tests establish a baseline posture, but what happens after the scanner is turned off and the \$15 per-hour-teller turns on? When your employee unwittingly visits a compromised website and the bank's PC is subjected to a cross-site scripting attack, how do you stop it? Or, when the teller finds out they can earn up to \$10 for every stolen account record, are you sure that your perimeter security is up to the task to see, stop and report the activity? The threat today is as equally internal as it is external. Meanwhile the regulatory environment is constantly evolving and becoming increasingly stringent.

Security is, to reuse a familiar phrase, an effort in risk mitigation and avoidance, not of absolutism. For many community banks, it isn't cost effective to maintain a staff of security experts steeped in the ever changing world of security threats, much less one that's clocked in 24x7x365. With cloud-based managed security offerings like HEIT's, community banks have the opportunity to achieve enterprise-level security through cost and knowledge sharing across peer institutions, without having to develop and maintain your own platforms. In this model, regulatory considerations and reporting requirements are built into the foundation of the security program, making it easier to manage and enabling a stronger compliance posture for the community bank. All of these factors add up to allowing you more time to focus on the business of running your bank, with the assurance that your bank is secure against today's threats - both external and internal.

Should your bank still employ a firewall, IPS and anti-virus? Sure. But we also need to isolate systems into areas of business relevance. If we are going to encrypt email communications, we should also implement policies, procedures and controls to ensure that outbound emails don't contain proprietary or customer-sensitive information. Our desktop and server patch management programs need to address all of our local applications, not just those from Microsoft. We ought to deploy host-based intrusion prevention software that doesn't depend on just signatures, but is intelligent to the role, function and behavior of the system and users accessing the system. Finally, threats to security don't clock out at 5 PM and neither should your defenses. Security must be monitored and maintained 24x7x365, which usually involves outsourcing a portion of it to a trusted partner to keep costs from spiraling out of control.

The end result to seek: A strong defense architecture that can proactively position your bank against real-time internal and external threats, while maintaining the agility to respond to future threats. The challenge lies in ensuring a comprehensive and effective security program while keeping time, resource and cost burdens under control. Working with a managed services provider enables you to leverage a whole army of defense in the security war, rather than relying on a few internal soldiers to win the battle.



Jeff Simpler
Chief Business Development Officer

Jeff Simpler is Chief Business Development Officer for HEIT. Jeff's responsibilities include strengthening HEIT relations with industry partners, associations, vendors and clients, as well as conducting strategic and industry analysis to support client technology investments. In 1993, Jeff co-founded Simpler-Webb, an Austin, Texas-based information technology consulting and managed services provider to the financial industry. Simpler-Webb merged with HEIT in 2010. Jeff continues to energize the HEIT team and holds each individual performer to the highest standards of excellence in his key leadership position. Prior to HEIT and Simpler-Webb, Jeff instructed astronauts in space shuttle communications and instrumentation at NASA's Johnson Space Center. Jeff is an engaging and insightful speaker, and provides editorial content and subject matter expertise for a number of highly circulated financial publications.

