

Managing Risk and Security Efficiently and Affordably

To really sum up managing risk and security in the most efficient manner, it really comes down to who your friends are. Do you go it alone and blame your end users for downloading malicious applications on Facebook? Or do you have a community of supports that backs you up in tackling risk and improving security?

I met with over 100 bank executives in 2009, and I didn't find a single one talking about their major technology investments in risk management and security. My advice for a first step: complete a risk assessment focused on your digital assets. I'm still shocked to see how many are using spreadsheets or a program that is too elementary when enterprises have been automating risk management and compliance for years. Why? Because they need to reduce TCO, and Gartner reported that compliance for IT Ops will double by 2012. How are rudimentary approaches going to handle double the regulations for managing risk assessments, vendor assessments, and audits? The answer is simple - they're not. Not efficiently and affordably, anyway. Instead, I suggest you shift your thinking. Instead, simply "ask once and comply many" to their compliance and risk programs through low-cost automated systems.

Many of you may know that I served in the U.S. Air Force for eight years providing critical infrastructure protection, including nuclear operations security. I couldn't even imagine if the military used bunch of point solutions and tried to integrate them for a defense system, while changing the technology every three years. How could you ever make critical security decisions with that approach? This is what many banks are still trying to do with their information security when they could simplify with a security "system." Systems over point solutions prove to lower your TCO, consolidate to single dashboards, streamline reports, and improve your security posture.

Here are my recommended security considerations:

- Move perimeter budget to address more vulnerable systems.
- Invest in encryption and HIPS, most common breaches relate to the lack of these.
- Make security fun, e.g., if you keep your PC unlocked, then you're buying donuts or pizza for the whole office.
- Stick to your core competencies as an organization. If your bank's core competency isn't security, then consider using domestic outsourcing.
- Don't test for 500 new vulnerabilities per month - it's not efficient. Some banks accomplish it through strong security communities, and most outsource some or a majority of security.
- Get your employees involved - some of the best security still lies in the bank employees.

At HEIT, you can blame it all on our roots. Like the military, we deliver integrated security systems that improve effectiveness. Our partnership approach with banks provides co-managed security systems, allowing for true service provider oversight. For risk management and compliance automation, we deliver an enterprise GRC platform as a secure SaaS solution to allow banks to take advantage of what the mega banks have at a fraction of the cost. HEIT's PCS-4 Platform is exclusively built for the financial industry, which allows banks to simply plug into the platform and take advantage of as much or as little through our pay as you go hybrid cloud model. As our bank clients like to say, "Think I'll slip on down to the oasis."



Dan Holt
CEO

Dan Holt is co-founder and CEO of HEIT, Inc. Mr. Holt is responsible for all aspects of the corporation including management, company development, strategic partnerships, and overall corporate strategy. Under his leadership, the company continues to expand nationally earning numerous accolades including: Cisco's Financial Services Partner of the Year; ReymannGroup Certified Enabler; and a leading Industry Solutions Provider for Banks and Credit Unions. Additionally, Holt is a leading information technology expert for the financial services industry and specifically delivers thought leadership at Bank seminars, speaking engagements, and provides expertise on the Federal Financial Institutions Examination Council (FFIEC) guidance.

