

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

Credit union network administrators have a difficult balancing act to follow in that they need to keep their network up and running, while trying to be as secure as possible. Unfortunately, sometimes security takes a back seat to day to day operational issues. Both the credit union's IT staff and senior management need to see security as a business driver and devote the necessary resources to staying secure.

Another problem that we often see is that financial institutions don't always have the right priorities and really know the most important things to protect. We recommend that they perform an overall risk assessment by creating a matrix of their systems and determining the criticality and risks of each. Only after going through this exercise can they prioritize their efforts, apply appropriate controls, and establish a security program that is based on a continuous risk-based approach.

The traditional view of security was one of the castle wall and moat, but that no longer serves us well. What is needed now is a 'city view' of door to door security at each and every house. That is because there are so many ways to access a credit union's network: virtual private networks, vendors and other third parties. It is important to move to this layered approach to security as the regulators are getting more knowledgeable and up to speed on security issues. We work with and train many government employees so we are quite familiar with the ways that they approach security and compliance audits.

Because Ambiron is an independent information security advisory firm, our clients always receive unbiased security advice. Many organizations are not familiar with all of the latest security technologies and how to apply them. We employ a four stage - plan, implement, verify, and monitor - methodology that takes into account each of our client's unique situations. Having worked with hundreds of financial institutions across the United States, we can safely say that each one handles their operations, paperwork and workflow differently. That is why our advisors work closely with their in-house staff to deploy the latest in information security policies and technologies that are specific to their business goals.

We offer a whole gambit of security services including network security review, internal and external penetration tests, Internet vulnerability scans and social engineering. Our vision and expertise in working with both public and private security groups is recognized by our work with the NCUA, credit union administrative staff, and financial institution industry consortiums. We are also proud of the fact that Ambiron is the only approved security assessor and forensics reviewer for all of the card associations including Visa, MasterCard, Discover and American Express. These are the types of relationships that set us apart from other firms and make us the enterprise information security solutions experts.



Michael Dahn is a Security Consultant with Ambiron, LLC, specializing in security implementation, network auditing, and penetration testing. He has implemented effective information security solutions for both Fortune 500 and other smaller companies. Michael has industry experience in the management, design, systems integration and implementation of information security technologies for Financial Institutions, Commercial and International Clients. Michael has been published and quoted in several news articles on information security, both technical and targeted to the general public. He has given presentations to a variety of industry associations including financial institutions, payment services, and government regulatory groups on topics including compliance, information security programs, auditing, and network security.