

CU SECURITY - ESTABLISHING A PROACTIVE APPROACH

As with any financial risk management program, in security risk management, the first security step any credit union needs to take is to assess their present status or posture vs. where they need to be. Meaning, first assess the current security status of their network and their applications, the engines that drive the financial services they provide - and control the privacy of their members' data.

For example, a quick survey shows us that ten out of one thousand credit unions surveyed - for only one type of security hole - can most likely and most easily be "hacked" into. Once they have closed current security holes such as this, CUs can move on to hardening their environment and creating a solid security and risk management baseline. This simply means being diligent in staying on top of security issues and compliance regulations and ensuring that security education is a priority throughout the credit union. The CEO is not immune - they must own this issue of security and be hands-on.

While regulators do force credit unions to be actively involved in security, CUs need to be proactive in self-regulating themselves. A lot of it, again, boils down to risk management: what is the CU's tolerance for risk? No one can be one hundred percent secure, so it is a matter of prioritizing the CU's risks and assets. We don't believe in security for security's sake, we think that security must always be approached from an ROI angle. Credit unions must understand, prioritize, and manage their one-time security costs, as well as their ongoing security costs. They must also force their technology suppliers to provide them with out-of-the-box secure applications and products. In addition to that worry, recently an employee at a major financial CU credit card processor obtained and sold its credit card numbers to another company for profit. On the positive side, that company is trying to make its CU customers whole. But the CUs had to re-issue cards at great cost and member dissatisfaction. The point is that wherever your data goes, you are responsible for its protection.

We take a holistic and preventative approach to security that includes looking at both the technical side and the human side of a CU's operations, including those with whom you do business. On the technical side, firewalls, servers, applications, and websites must be thoroughly assessed, properly configured and continually monitored. On the personal side, employees must transform into "human firewalls" to help mitigate the many threats CUs face. Our clients receive a customized approach to their organization's specific situation; and because we are not allied with only one security hardware or software supplier, we deliver unbiased assistance in picking and choosing the best-of-breed solutions that fit their needs and their budget.

Another area where we are uniquely qualified to assist credit unions is with MasterCard's new Site Data Protection program. This important, new, and little known program is a key part of MasterCard's effort to battle credit/debit card fraud. Secure20 is a certified MasterCard SDP Security Provider, one of only ten in the world today. This prestigious designation provides us with the opportunity to assist MasterCard's issuing and acquiring members with a certification program that ensures that they are adequately protected against hacker intrusions and account data compromises.



SECURE 20

Michael Harris is the founder of Secure20 and has over twenty-five years of experience in information technology. Michael is internationally recognized as a security professional, speaker, and writer. He and his team have been working with Internet security since 1992. As an AVP in the IT Security Consulting Division at Wells Fargo Bank, he helped to develop the security controls for the first online banking program back in 1994. Along with their business partners such as Cisco, Secure Computing, and Sabertooth, Secure20 truly understands the high security needs of financial institutions. Secure20 has assembled a staff of leading security professionals and Security Partners to meet the complex challenges of implementing secure e-commerce solutions. Secure20 consultants have extensive experience in risk management and the selection and implementation of information security methods and technologies.