

CU SECURITY - ESTABLISHING A PROACTIVE APPROACH

The first thing that should be recognized in establishing a proactive security stance is that security programs must be planned for, designed and executed within the context of business risk and not focused solely on technology risk; it's about pervasive risk management. Too often energy, time and money are focused on the wrong things for what appears to be the right reasons. Security is about common sense, actionable intelligence, and focused core competencies.

It is important to communicate and collaborate with your business units to find out what is important to them, categorize the assets and draft a framework that establishes clearly what you seek to protect, what the impact would be to the business should something bad occur, and how you intend to manage and recover from the risk when it happens - and it will happen. Articulate your plans clearly and as non-technically as possible and recognize that all the best written policies and procedures in the world are useless without a way of appropriately enforcing them, so get management's buy-in by educating them.

A real need exists to respectfully treat the approach to securing data in the CU environment as one would in a more traditional financial services company - too often the roots of the Credit Union movement cloud the fact that literally billions of dollars in business are at risk. Non-profit or not, it is a Credit Union's duty to its Members to provide appropriate levels of security and governance. Credit Unions face the same threats as everyone else, but the relaxed atmosphere and easy-going nature of the movement also raises the potential for risk as internally-focused vigilance is sometimes sacrificed in the name of culture.

It is important to realize this and balance an effective internal security posture against the ability to conduct business. Again, it's about common sense. Security awareness is key and making sure everyone recognizes that security is everyone's problem provides the capability to recognize and manage risk that much easier.

Focus on what squeaks first, but only if it has business impact. Don't be afraid to be tactical and worry about overall strategy when prudent and possible. Recognize that the old guard model based on perimeter security is dead - there are no Maginot lines and no silver bullet that will cure all your security ills.

In terms of cost avoidance, defending and scratching for budget, and establishing ROI, focus less on trying to quantify what security you get for your money and more on what you'll lose if you don't have it. Instead of ROI, think RROI - Reduction of Risk on Investment.



Christofer Hoff serves as WesCorp Federal Credit Union's Director of Enterprise Security Services. WesCorp is the country's largest corporate Federal Credit Union with assets totaling \$24 Billion. Hoff is responsible for WesCorp's Enterprise Security initiatives focused on providing internal business units and credit union members with rational risk management services and a consultative approach to information security. Hoff is tasked with the overall responsibility to provide and support a secure computing environment for WesCorp. This includes the creation and security life-cycle management of policies, procedures and information security governance efforts including regulatory compliance requirements. Hoff currently holds several security credentials including CISSP, CISA, CISM, IAM, CCSE+ and is an accomplished and accredited technical instructor.