

Finding a Balance between Security and Convenience

The tradeoff between security and convenience revolves around the value and criticality of information assets involved versus the cost of securing those assets. For example, you don't spend \$10 to protect a \$1 asset. It is important when evaluating the value of assets to consider both hard and soft costs and the ability to quantify each. In terms of soft costs, credit unions must always consider the value of their reputation.

So, how does one quantify the value of an event where 100 member records are compromised or accounts are pilaged? Perhaps the capital cost to recover from the event is only \$2500 – stolen funds and the cost of notification, call center costs, and free credit reports for a year. But what about the damage to the credit union's reputation? What are the opportunity costs from new members that never join because the event was reported in the local newspaper? What are the costs in terms of lost membership (and their account balances)? How can those issues be quantified so that a budget can be applied to mitigate those risks?

Internally, credit unions struggle to find the right balance of security and convenience for their employees. For instance, what is the cost/benefit ratio of providing Internet access to employees? Is the risk adequately mitigated through the controls in place? Can you mitigate \$50,000 in quantified risk via a \$20,000 series of security controls? Another consideration: Are you locking down the USB ports on those new PCs you are buying? If not, how can you be sure that credit union data is not walking out the door?

The only way to accurately answer these questions is to perform a thorough risk assessment, preferably using a robust, quantitative methodology such as NIST 800-30 (rather than a qualitative methodology such as ISO 17799). Such a risk assessment provides an accurate measurement of the risk in several control areas such as Management, Operational and Technical security. The results of such an assessment provide the credit union a roadmap outlining where to achieve the most risk mitigation for their limited security budget.

At Integrated Computer Solutions, we maintain a staff of heavily credentialed security experts who perform NIST 800-30 audits on government agencies, financial institutions, and many other types of businesses. In addition to NIST 800-30 audits, penetration tests and network security assessments, we offer credit unions our NetworkArmor Managed Services: Intrusion Detection Services, Managed Firewall Services, Virus Management Service and others. With a deep background in risk management, policy development and technical implementation services, credit unions can trust ICS to help them implement strategic solutions to difficult IT and security problems; develop cost effective and proactive solutions to an ever-changing threat landscape; and provide world class security services that are optimized for their environment.



Stephen Goldsby
CEO

Stephen Goldsby is President and CEO of Integrated Computer Solutions, Inc. (ICS), an Information Security Consulting firm founded in 1997 and headquartered in Montgomery, AL. A Certified Information Systems Security Professional (CISSP), Goldsby has been an information security professional since 1991. In 2003 the National Small Business Administration honored Goldsby as the Alabama Small Businessman of the Year. Additionally, he was recognized and received an award as a finalist for IT Executive of the Year by the Alabama Information Technology Association in 2006. Mr. Goldsby is a popular featured speaker at national and state conferences as an Information Security subject matter expert. His Information Security articles and papers have been featured in national trade magazines and journals. In October 2004, ICS was honored as a CNN Champion of Industry and showcased in a segment of the CNN News narrated by Pat Summerall.

