

Pay Now or Pay Later: Obtaining ROI from Security Solutions

The demands to show an ROI on Security reflect the changing role of CIOs. In the past, credit union CIOs were simply expected to run an efficient IT shop. Now they are expected to bring a businessman's perspective to the boardroom table, to communicate the strategic value of today's and tomorrow's technologies and the impact on the credit union and its members.

It used to be acceptable to rely on fear, uncertainty and doubt to sell security. The thinking was, if you scare them, they will spend. The Gramm, Leach, Bliley bill of 2000, which holds directors personally responsible for safeguarding their members' personal information, is a prime example of forcing appropriate behavior by the threat of punitive sanctions.

But today's CIOs are moving from a tactical to a strategic perspective. CIOs will be both more valuable and effective by presenting a business case for security, not a technical case. The CIO should answer the following questions in order to start developing an effective IT strategy. What happens if the member data is at risk? What are the risks of a compromised backup strategy? What is the business impact of the IT system? How much security can we afford?

Then, to start a vital strategic dialog with fellow executives and directors, the CIO should have the group consider the answers to these questions:

1. Do we understand the financial, competitive, reputational, regulatory and business risks?
2. Do we understand the risks of non-compliance with privacy and security laws and regulations?
3. Have we balanced all the various issues to devise a viable solution?
4. Do we have a strong leader who will take ownership?
5. Have we created priorities and can we measure success?
6. Can we afford the solution? Can we afford not to have the proposed security in place?

At Accume Partners, we have 300 professionals who work with financial institutions across the country. We begin each engagement with a top down approach to managing risk. Once we gain agreement to our risk approach at the strategic level the tactics to achieving the goal quickly fall in place.



Every credit union we work with is different in their operations and risk tolerances, but the constant is that by beginning with a top down business risk assessment, the credit union's needs will be addressed strategically first and tactically second. In this fashion, the credit union can best assure itself of realizing a sound ROI on its IT security investment.

For those CIOs who aren't strategic or don't have the luxury of spending time on strategy, we have 60 professionals who are IT auditors and who understand both the intricacies of technology and our top-down risk assessment methodology. We have worked with numerous institutions to bridge the strategic/tactical gap through co-sourcing, outsourcing, training and education. In fact, knowledge transfer is a big part of what we do – we prepare our credit union clients to continually improve their security posture after our auditors finish their immediate assignment.



Frank Padavano is managing director of information technology at Accume Partners. He has more than 17 years of experience in information technology auditing services, including information security, system acquisition development and maintenance, computer operations and information systems support and business recovery planning. Previously, Frank was a senior manager at a Big Four firm in the Philadelphia market focusing on risk management and delivering internal and external information technology audits. Currently, Frank is the director of the Philadelphia Chapter of Information Systems Audit and Control Association (ISACA) and a certified information systems auditor (CISA). He is a graduate of Rutgers University.