

## CHOOSING AN INFORMATION SECURITY PARTNER



AN INFORMAL GUIDE TO VENDOR SELECTION



# Table of Contents

Who Can You Trust?	1
Overview	1
Identifying the Short List	1
Narrowing Down the Prospects	2
What to Look For in an Information Security Partner	3
Make Sure You Get Apples to Apples Comparisons	3
Caveat Emptor: “Buyer Beware”	4
Credit Unions are Unique and Deserve to be Treated as Such	5
Summary	6
About MicroSolved, Inc.	7

This document, and its contents, are Copyright 2006 by MicroSolved, Inc.

All rights reserved.

No part of this document may be reproduced or reused without  
the express written permission of MicroSolved, Inc.

# Who Can You Trust?

## Overview

Choosing a company to work with your credit union on information security can be a tough task. The security industry is full of jargon, buzzwords, hype and confusing technologies. To make matters worse, the NCUA and other regulatory bodies have their requirements too. How can you figure out how to make the right choice? How can you pick out who you should trust with these mission critical tasks?

That's the purpose of this guide, to help you understand the process you should use to choose your information security partners and vendors. Along the way, we hope to give you a solid methodology for making your selection, point out some possible problems and catastrophes to avoid and help you come to terms with some of the hype and confusion. Now, obviously, we are an information security company, *but don't let that scare you*. We promise to stay focused on the processes, and give you the tools you need to allow YOU to make YOUR OWN choice. We are confident that given the methodology and the knowledge of other's successes that you will make the right choice for you and your credit union. Even if you don't pick us, we will sleep better at night knowing we helped you make the right decision!

So, let's not delay any further. Let's jump right into how to select your best fit for an information security partner.

## Identifying the Short List

Information security vendors are a wide and varied field of businesses. They range from Fortune 500 accounting and IT companies to small boutiques and single consultants. A simple Google search for "credit union security" returns over 32 million pages. Obviously, we are going to have to narrow this down a bit. Usually, we find the best solution to be to "ask around". Talk to other credit unions in your area, your Corporate credit union and/or your local credit union league. Login to the Credit Union Information Security Professionals Association ([www.cuispa.org](http://www.cuispa.org)) and ask your fellow credit unions about their suggestions. CUISPA also maintains a list of vendors that support their organization, so that may also be a good list to begin with.

However you decide to propagate your list, the next step is to ensure that each of the vendors you have identified actually performs the services you are considering. For example, some security companies do not do penetration testing (the act of simulating attacks by actually attempting to break into systems, networks and applications). If you are seeking a company to do penetration testing (as required by NCUA Section 748 for most credit unions every 18 months), then companies that do not provide that service should be stricken from the list. Another example of this might be removing companies that do not monitor or manage firewalls if you are looking for this service. Simple web site research or a quick email or call to the potential vendor is likely to identify the vendors on your list that do not offer the services you are seeking.

## Narrowing Down the Prospects

Once you have a list of prospective vendors that offer the services you desire, the next step is to establish criteria that is important to your organization. For example, in penetration testing, there are many variables and the process is quite complex. In order to better protect your organization from the possibility of outages or the like, you might establish experience as an important criteria. If you are seeking a partner to help with risk assessment, you might establish that familiarity with credit union financial processes and regulatory guidance might be the most important asset. Perhaps 24x7 contact capabilities are important for your credit union, if so, that would likely be an important criteria.

Now build a matrix of your vendors that shows their names and contact info along an axis, and your criteria along the other axis. A table or spreadsheet in Microsoft Office might look like this:

POTENTIAL VENDOR	EXPERIENCE	NCUA REGULATORY KNOWLEDGE
Company A 555-555-1212		
Company B 555-555-1313		
Etc.		

As you begin to interact with the potential vendors, ask them about their services and focus on getting information about how they meet or work with your criteria. Fill the matrix with your notes as you go, and build out the information for each vendor and criteria. Some people also like to assign a simple scoring system, like 1-10 or high, medium and low to each criteria. In the end, this matrix will greatly help you remember each vendor and sort between their offerings and services. It will also make reporting your decision to management and the board later on much easier.

The process here is simple: contact each vendor, via email or phone, and let them describe their solutions and how they meet your criteria. Let them answer as they will, but don't expose your criteria directly to them. Ask broad, but leading questions and let them talk about how they do things. Pay careful attention to make sure they are offering the same services you are expecting, and be wary of attempts to bundle or cross sell services if you did not ask for them or do not need them. Sometimes, bundling is fine, but don't be persuaded by attempts to bundle items you don't need or "free" tools and the like. As the old saying goes, "there is no free lunch".

Once you have completed your matrix, assign your scores if you have not done that already. This should make it easy to identify one to three truly leading vendors that will be a good fit for your organization. To go the rest of the way, and pick the one to work with, read through the rest of this process.

## **What to Look For in an Information Security Partner**

The first criteria we hear the most about from credit unions is trust. The regulatory and legal environments that surround potential loss of member identity or financial data today are simply brutal. Items like board member personal responsibility, fines and potentially losing the charter of the credit union seem harsh, but they have become needed mechanisms given the public's hypersensitivity to the information security issue. The fact of the matter is, organizations that lose member's data are usually out of business within five years. As such, picking the right vendor is a critical piece of the puzzle. You will have little room for error. Trust, however, is a hard thing to quantify, but you have taken some of the initial steps already by asking your fellow credit unions about their vendor choices. To further identify trustworthiness, ask the vendor for other credit union references you can talk to. Then, actually make contact with the references and find out about their experiences. Ask about potential issues, problems or the like. Again, ask leading but open-ended questions. The answers you get may surprise you.

The second most common criteria is experience. Has the vendor done these services before? Have they done them for someone your size? Are they aware of any nuances that might be associated with your organization? How would they handle such and such event if it occurred? These are all proper questions for qualifying your selection. Make sure you talk to, not just their sales team, but some of the actual folks that will be doing or managing the work. Be wary of any vendor that won't let you have conversations with their work teams. The bait and switch is very common in the security industry. Again, use references, and this time, some good old fashioned Internet research to verify their claims. Now that you know company and principal names, you should have an easy go of doing some Internet searches to verify their experience, knowledge and skills.

No matter what criteria you value, make sure you get complete and certain answers from the vendors. If you have doubts, identify them and either get answers or notate them in the scores. It may seem like a hassle, but completely work through the matrix you built above, and make sure you feel completely comfortable with the answers that you get from each of the vendors. That is the critical difference that will prevent you from getting sold on the hype, and will keep you on the track to find the best fit for your credit union.

## **Make Sure You Get Apples to Apples Comparisons**

In order to understand the services you are asking for and the components that are critical to each piece, make sure you spend some time reviewing the terminology. Sources like Google and Wikipedia are often good resources for getting the basics of a topic and identifying the "need to know" pieces of the puzzle. Be wary of buzzwords, and don't be afraid to ask vendors to explain their services in "plain English". You will have to make sure you know what you are getting anyway, since eventually you will have to ensure the Board of Directors approves of the purchases and the security program (as required by NCUA Section 748). If the vendors use terms you aren't familiar with, either look them up or ask them to define them.

Make sure that you identify components of larger tasks. For example, a risk assessment may or may not include items like vulnerability assessment or review of your Business Impact Analysis documents. Make sure you know the difference between vulnerability assessment (running scanning tools, and hopefully, verifying the results), risk assessment (an enterprise wide or IT focused look at risk around the credit union - more programmatic than technical) and something like penetration testing (ethical hacking, actually exploiting identifying vulnerabilities like an attacker would). This is essential to make sure you really get what your credit union needs to improve security and regulatory compliance.

If you're interested, and it seems like a good fit, you can also identify other potentially useful ways the vendor may be able to assist you. Look for items like awareness, document and policy creation and other resource intensive tasks that your credit union may need. If it makes sense, now is the time to think about bundling these services or to find out about possible discounts now or down the road should your partnership grow.

### **Caveat Emptor: "Buyer Beware"**

Here is a quick bullet list of danger signs from vendors. These are items to remain wary of, and to help you identify and avoid major issues down the road. They are in no particular order:

- Beware of claims that vendors or products will "make you secure". Security is a journey, not a destination. There are no "silver bullets" for information security. Deep defenses that are complex and focused on your assets are the best solutions.
- Be very careful about potential conflicts of interest. The same company that monitors your network and/or systems should not also be the company that audits how secure you are. Companies that act as auditors should not be retained to perform IT consulting and such. These are disparate functions and they require independence from each other.
- Pay attention to single points of failure, as this represents a logical and regulatory risk to the credit union. No matter if this is a piece of hardware, software or a person - the credit union must have options to continue business without it. This is especially important if you are deploying technologies like firewalls, IPS tools or employing network management from a vendor. Make sure they have a plan for ensuring the credit union stays operational, even if hardware malfunctions, employees leave or they, themselves, are out of service.
- Beware of hype. The information security field is full of overblown technologies, overly touted certifications and grandiose claims. This is where your criteria and looking for items like experience and trust come into play again. The antidote to hype is trust.
- Make sure that you review details like sample reports, sample contracts and resumes of the individuals performing the work. Make sure you understand who will be doing the work, what the timelines for completion will be, how travel costs will be handled and what steps the vendor is taking to ensure that both your services and their organization comply with NCUA Section 748 guidance.
- Lastly, be very careful about potential vendor's company ethics. The NCUA and the public are paying close attention to IT and management ethics these days, and you should too. Ask the company about their policies pertaining to hiring "hackers". Ask them about their firm's security research teams, and how they may handle new vulnerabilities. Do they report them to the vendor? Do they announce them to the public? You will find that some vendors not only identify new vulnerabilities, but actually help attackers by releasing "exploits" and other tools that attackers use to break into systems. Pay careful attention to the answers to these questions. Don't be afraid to ask what, if anything, the vendor is doing to help prevent future attacks, or to "give back" to their customers and others.

## **Credit Unions are Unique and Deserve to be Treated as Such**

All organizations are not created equal. Those of us that have worked in the credit union field for many years often forget how very special working for a member-driven organization is. Quite frankly, it is very different from almost any other type of organization out there. As such, make sure your potential vendors understand how credit unions work. Verify that they have a grasp of the structure, role and processes that take place at a credit union. Without this basic understanding and knowledge, how could they assist in securing your environment?

Further, the relevant regulatory requirements for a credit union are significantly different from other types of organizations. Gramm-Leach-Bliley might be a commonality between banks and credit unions, but the similarities mostly stop there. NCUA requirements are complex, sometimes vague and require experience to understand and communicate. As such, the more experience a firm has with credit unions and these requirements, the better off they are to help you, your management and your Board understand and respond to issues. Ideally, identify a vendor that can refer to regulations like these and FFIEC when selecting your partner. The deeper the knowledge they have, the greater the value they bring to your organization.

## **Why Price is Often a Poor Indicator of Performance**

Be very careful of using price as a differentiator between vendors. If possible, completely avoid using price as a criteria in the matrix. Over the years, we have seen some serious disasters at credit unions when they made decisions based largely on price. Now, that is not to say that price is not important. It is. We all have budgets and we all have limits to the resources we can expend. That is a given, just be very careful of making decisions based largely on price. Choosing an information security partner is a mission critical decision, and you don't want to cost the organization tens of thousands to save a few hundred dollars.

Also be aware that many times information security is used as a loss leader by companies looking to get their foot in the door. They will often underbid engagements, just to begin working with your credit union. This is very dangerous for all parties, as they often sacrifice diligence and quality to meet their prices. They may not perform deeper steps like validation of results, quality control or other highly important, but less visible functions. The tell-tale sign of this type of approach is that they often begin the engagement with follow on work in mind. They may even tell you at the time of the sale that they can fix the issues they identify. Be very careful of this, as it clearly can quickly become a conflict of interest.

Ideally, look for the most value for your expenditure. Look for partners who can help improve your security posture, your compliance and your team's knowledge throughout the engagement. Those are the partners that we have found to be the best fit for credit unions over the last fifteen years. They are out there, you just have to "ask around" to find them.

## **What the NCUA Says About Picking a Vendor**

The NCUA has some definite requirements for vendors to a credit union. These requirements are universal, in that they don't specifically apply to security vendors, but any vendor working with a credit union. The problem is, given the potential exposure that information security services bring to the credit union, there is much more risk to the credit union if security vendors do not meet these requirements.

First, you should keep in mind that you are ultimately responsible for the protection of member information. If a breach occurs, even if that breach is caused by a vendor or located at a vendor facility, it is the credit union and not the vendor that the NCUA will hold responsible. That means that unless specifically contractually protected, your credit union could be fined or face other regulatory issues as a result of problems on the part of the vendor. This is a significant risk and must be managed by choosing to partner only with vendors who meet NCUA guidance and who you are confident are taking the needed steps to protect your member and other confidential data.

Secondly, the NCUA requires that credit unions perform “due diligence” on their potential partners prior to starting a contractual relationship. This is the time to ask them about their security mechanisms, their financial status, their processes and such for ensuring the compliance we discussed earlier. Ask the questions; document the answers and make sure you get results that you feel comfortable with.

Lastly, there are specific reporting requirements set out by the NCUA for information security providers. These requirements include specifics like the creation of “heat maps” and other steps to accurately and concisely communicate the risks of issues identified in the credit union. The NCUA clarifies requirements for report delivery, report contents and other vital regulatory guidance in their Letter to Credit Unions released in 2002. Vendors should, at the least, be familiar with these requirements and ensure that they are meeting these guidelines.

### **Ensuring Board Oversight and Approval**

Finally, once you have identified the right security partner and have arrived at the contract stage, there is one final requirement. The Board of Directors, or their appropriately tasked sub-committee, must approve of the information security program as a whole, and must be made aware of the specifics of the engagement and process, as a minimum. The NCUA Section 748 regulations gives oversight of the information security program to the Board, and requires that they be updated on any significant events or changes. It also requires yearly, at a minimum, updates of the board about the status of the information security program.

In the past, several credit unions have done well by ensuring that the board is aware of new security vendors, their selection criteria and the engagements they are undertaking. We urge all credit unions, regardless of their size or vendor choice, to inform the board of these decisions. Ensuring their oversight will go a long way toward maintaining complete compliance.

### **Summary**

We hope this guide has helped you identify a process for picking information security vendors that are an excellent fit for your organization. Using this methodology is likely to make the process easier, less time consuming and make you more confident in your selection. Hopefully, it will also lead to better security for credit unions and more widespread compliance with regulatory and legal requirements. If you have any questions, concerning this guide, our services or our insights into how to pick between potential vendors, please do not hesitate to contact us. Thanks for reading!

### **About MicroSolved, Inc.**

Founded in 1992 by Brent Huston, MicroSolved, Inc. is one of the key information security service providers to credit unions around the world. With more than a decade of experience with financial institutions; having worked with more than half of the US corporate credit unions and hundreds of natural persons credit unions, our experience is unrivaled. Our staff members regularly teach security topics and present to various CU groups around the world, establishing safer credit unions on a global scale. From risk assessment and policy development to vulnerability management and penetration testing, our experts are world renown and passionate about the credit union movement. We routinely receive accolades from various clients, the NCUA, technical working groups and the public. Our work with WOCCU has even included pro-bono work to help them establish the first corporate credit union in South America. If your looking for a true information security partner for your credit union, give us a call and experience the difference that a truly professional, knowledgeable and credit union focused partner can make!

For more information, please contact us at [info@microsolved.com](mailto:info@microsolved.com) or via phone at (614) 351-1237 x 206. We look forward to assisting you!