CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

If you look at the major security breaches that have occurred, Target et al, you will find one common denominator among all of them and that is the people who have the oversight responsibility for security. This can be further refined by roles and responsibilities both internal and external.

Unfortunately too many organizations (and credit unions) take the easy way out and outsource everything thinking this will give them the protections they need because they hire the experts. The reality is, that you may be outsourcing but do you really know the employees or personnel who are running the operations in the background.

Think about Target for example, this was a classic case of a criminal organization compromising an employee to gain access to the programs that ran the card readers. Target had all sorts of safeguards in place that sounded all kinds of bells and whistles alerting to possible breaches but they were ignored, so in fact there were two major failures, one on the vendor and one on the staff.

So, did the technology fail or did the people? We both know the answer to that and it was the people.

In a former life I dealt with Corporate Network Security working for a well know Global 100 firm that specialized in this very market and the same concerns and issues that were problems then still hold true today and that is;

People are your weakest link. Harsh you say? You bet but it doesn't alter the facts.

Case in point, how many credit unions actually have skilled IT staff that are both certified and current in those certifications relevant to their job function whether is it networking, security, programming, etc. Taken a step further what do you know about your vendors' staff? From my experience, very few companies across the board can meet that benchmark.

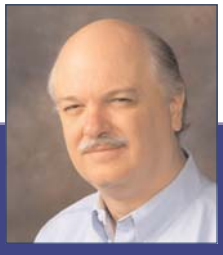
That is not to say these folks are not competent, many in fact are, but are they keeping their skill sets up, maintaining the highest standards in their organizations? Unfortunately, no! There are a variety of reasons for this, money, time the unwillingness of management to support ongoing education and the list goes on. However, if you really want to address the security problem, it begins in-house with your staff and your employees being empowered to act, to be properly vetted and to be skilled in maintaining their responsibilities. Taken a step farther, it also requires doing extreme due diligence on your business partners, vendors, suppliers etc.

Criminal organizations have the luxury of time, money, trial and error to perfect their attacks. Social engineering is still the starting point for many of these attacks because the door needs to be opened and a way in to the organization established. The front door as it were could be something as simple as an email address, a phone number, an account number etc. If a criminal can deduce any or multiple items of this nature, it is very easy to construct profiles that will work against your CU.

With that one little bit of information they can then go online and find out all sorts of things about people, customers, vendors, employees, etc, that can then be used to exploit people into kicking in the front door for them.

The key is training your staff to be vigilant against these probes and diligent with information. For example, I might go in as a vendor and drop off some freebies at the front desk, they may include product literature, t-shirts and thumb drives with my logo on them. How many staff would simply just plug one of these little guys into an open USB slot? In reality, almost all would, even if there are policies in place that forbid it. So what is the solution then? How about this - epoxy all the USB ports, remove the CD\DVD drives and make it impossible to allow employee access to your work computers.

continued on Page 2



Scott Cowan
Vice President

MVi
Capture the Future

Contact Info
www.mviusa.com
Phone: 888-684-6684

Scott Cowan is the Vice President of Marketing for Millennial Vision, Inc., a Laserfiche reseller that specializes in providing Document Solutions tailored to the Financial Services Industry. Mr. Cowan has an MBA in IT along with 25 years of industry experience working with Financial Institutions including Several Fortune 100 companies in the Financial Software as well as Telecomm and Data Security Fields. MVi was founded in 1996 with a mission to provide quality products and services. Our vision is to help customers Go Paperless with MVi, and our commitment is to deliver technologies that empower people to create efficient document workflows. MVi offers More than Imaging with a product suite that enables credit unions of all sizes to replace paper-based processes with digital document management.

CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

And speaking of devices, the biggest risk to businesses and financial institutions today? Smart phones! Think about it, you are allowing employees to bring a covert camera, listening device, and mass storage disc disk right past your safeguards each day. They use them outside the work environment, download apps, etc and then bring them in and plug into your network unopposed. Bad idea! Solution? Lock up cellphones at the work place. Yeah I know good luck with that, but you want to keep things as safe as possible, remove the obvious simplest threats. Over and above these highly unpopular safeguards, make sure you spend the money, time and resources on keeping your technology current.

I still see companies that are using Windows XP machines in their environment. Really? To me that is completely criminal and negligent and should anything happen in those environments I would hold those responsible to a higher standard of accountability and punishment for their complete disregard of fiduciary responsibility.

The purpose of this article was simple, how do you mitigate risk? The answers are tough, but then again so is the cost of being breached. How many millions of dollars in card re-issue fees and fraud losses were due to the improper procedures and incompetent employees. Now magnify that down the food chain and you begin to understand why the recommendations for such extreme measures. The biggest problem again is people, they are your weakest link, but also have the capability of being your strongest defense. Proper Vetting, training and education are far less costly than the fraud that can occur because of them

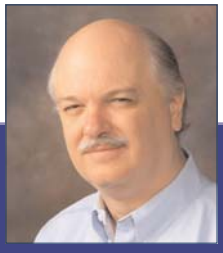
MVi provides Enterprise Content Solutions that are DOD 5015.2 compliant. Meeting that requirement means having the strongest security and safeguard measures in place to ensure documents are safe, secure and accessible only by those who have the proper credentials. Since most sensitive information is stored in databases as well as the documents generated as part of the business process, it becomes imperative that this information is maintained as securely as possible. The bottom line is It still comes down to your people and making sure they have appropriate security rights, are properly trained, vetted and given the best tools for the job.

Unfortunately, NCUA has not seen the light when it comes to Document Imaging systems. This is one area that really does need to be looked at due to vast amount of information that exists within these systems. Most organizations simply think that once documents are scanned and imaged that is enough, but in reality, security rights, compliance and oversight also need to be addressed.

The US Government and specifically the Department of Defense have done a very good job in outlining a set of standards required within their domain. The standard that is followed is called DOD 5015.2 and it relates specifically to records management. NCUA would be wise to adopt many of these guidelines as they relate to imaging systems and at the very least demand that any vendors providing these kinds of solutions become certified to this standard and maintain this standard.

This will of course take time, but it becomes too easy to simply print out information from these non-compliant systems and pass them on for sale in today's environment. Couple this with the fact that cell phones can take pictures of these records and you begin to understand why such standards of compliance need to take place.

There is no magic pill that will address all the security issues and woes in the marketplace. But, sound operating principals, enforceable security policies, ongoing training and better employee and vendor screening will, at the very least, give the perception that your CU takes security seriously and that in turn will give you the trust of your members and employees alike.



Scott Cowan
Vice President

MVi
Capture the Future

Contact Info

www.mviusa.com
Phone: 888-684-6684

Scott Cowan is the Vice President of Marketing for Millennial Vision, Inc., a Laserfiche reseller that specializes in providing Document Solutions tailored to the Financial Services Industry. Mr. Cowan has an MBA in IT along with 25 years of industry experience working with Financial Institutions including Several Fortune 100 companies in the Financial Software as well as Telecomm and Data Security Fields. MVi was founded in 1996 with a mission to provide quality products and services. Our vision is to help customers Go Paperless with MVi, and our commitment is to deliver technologies that empower people to create efficient document workflows. MVi offers More than Imaging with a product suite that enables credit unions of all sizes to replace paper-based processes with digital document management.