CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing Insider Threats, Cyber Attacks & Data Security

Without a doubt Employees are the greatest risk\asset a Credit Union has. That being said there are several things credit unions can\need to do if there are serious about security.

1 Make the Internet For Official use only. Get rid of ubiquitous employee access to the Net.

2 Set up restricted access to Approved sites only and then only by employees with need for access.

3 Restrict email access because to many times employees are breached by email phishing schemes. Set limits to who has access to contacts in the CU. This is a very broad discussion but this is a high level recommendation.

4 Require that all cell phones, personal electronics be locked up at work. Only exceptions would be those employees required for mobile access. Cellphones are mass storage devices and cameras defeat all security measures. They don't belong in the credit union.

5 Do not ever allow wireless access in the Credit Union period. Guest access is fine as long as it is physically separated from all other lines. In other words, separate ingress but best option is simply don't allow it. I know not realistic but you asked.

6 Cement shut all external access points on terminals. USB ports, etc. - never allow any 3rd party device to be plugged into the machine ever. Test in an isolated sandbox only.

7 Set up secure and monitored access with trusted vendors and make sure all activity requires human authentication. Make sure all access rights are only set for those applications they need access to.

a Require proof of security protocols with trusted vendors. Allowing them to log into your network may be the entry point for a host of nasty things.

b Log all activity and review it periodically to make sure there are no incongruities with what is being done.

c If possible, set up sandboxes where programs\fixes can be tested before deployments or hotfixes are implemented.

d Make sure to assign key contacts per vendor so that the familiarity with each company's personnel is known.

e Constantly test, review and revise security programs\parameters to make sure they keep pace with ever-changing environments

f Require secure password protocols and enforce regular password resets and keep access limited to key personnel only.

8 Choose vendors (Such as MVi\Laserfiche) that meet defined industry standards.

In our case, Laserfiche meets the DoD 5015.2 and VERS standards for Records Retention and Document Management. Not every vendor will be able to always provide that layer of compliance, but in those cases, make sure the vendors follow good internal security\development\personnel practices. In other words, aside from the product make sure you have strong vendor due diligence policies in place as well to insure compliance on the fringe.

I recently read a report that said that the vast majority of large US as well as global companies have been hacked. The question is that for those that have been hacked what are they doing about it, but worse, for those that have been hacked and don't know about it, what can be done? *(continued on Page 2)*

Scott Cowan
Vice President

MVi
Capture the Future

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 more than twenty five 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.

Contact Info

www.mviusa.com

CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing Insider Threats, Cyber Attacks & Data Security

That statement in and of itself says it all, everyone everywhere is subject to vulnerabilities whether it is the malicious viruses that pervade our own PCs or the human factors issues facing every organization, there is always the risk of breach. I was asked several years ago my thoughts right after the Target breach what I thought happened. I speculated that in time, the investigation would find that employees were to blame. In that sense I was correct, but it was the third party vendor's employees that were at the root cause of their problems.

So the question of 'are breaches inevitable' is very valid and the answer will always be yes. EMV is a perfect example. We print the card number on the card along with the CVV code, expiration date, etc. So in-person purchases are made more difficult but online purchases are still possible if you have that information. Search sites such as zabbaserach, intelius, etc. can be used to verify personal information along with a myriad of other sites that I won't mention where you can find out pretty much anything you need to know in order to reconstruct someone's profile. As long as people are in the loop, they will always be the weakest link. Therefore the best action one can take is risk management and trying to mitigate risk to the best extent possible and then make sure you have contingency plans in place so when it does happen, there is a plan of action to deal with it.

Finally, diligent employee education, training and awareness coupled with proper vetting will go a long way to overcoming the simple threats, but the more complex ones requires constant training, evaluation and preparation and unfortunately I think there are a lot of credit unions that fall short in this area due to resource limitations, educational issues and lack of a top down emphasis on the serious nature of security issues.

Until security really takes the front stage from the management team, then we will continue to have these types of breaches, security issues, etc., in every aspect of our digital lives, and credit unions are no exception. In fact they may be more susceptible due to the trusting nature and culture they are well known for.

MVi and our Laserfiche Enterprise Content Management (ECM) solutions provide layers of secure access, which if utilized correctly, will help protect critical documents and electronic files in a secure repository environment. Additionally, knowing that DoD 5015.2 compliance is being maintained also means that development is constantly making sure that new secure programs and protocols are being implemented based on the constant updating, which in turn is required in order to combat both current and anticipated threats to these environments.

Documents can be secured via encrypted access which completely eliminates the ability of the end user to see anything but those documents which have been determined necessary for their job functions. In this way, out of sight - out of mind means end users don't know what is there, can't see or access them and if by some miracle they were to try and open them, their attempted access will be logged and the documents are still made unreadable due to the encryption that can be placed on these files.

Finally, setting up an infrastructure that provides a secure repository for these files along with the software tools helps our customers maintain the integrity and security across their ECM enterprise.

Scott Cowan
Vice President

MVi
Capture the Future

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 more than twenty five 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.

Contact Info

www.mviusa.com