CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Compliance and InfoSecurity - Applying the Right Resources

My interactions with credit unions lead me to believe that they have not spent sufficient time regarding compliance and the updated FFIEC Banking in an Internet Environment Guidelines. There are major changes in the guidelines that need to be addressed, and I get the feeling that many credit unions are in a holding pattern. Most want to wait and see the fallout from the first compliance audits which are scheduled in January 2012. Others rely too heavily on their online banking platform providers that offer limited security. Credit unions need to understand that they are responsible for these regulations and that it could take up to 18 months to meet the new guidelines.

Investing in information security is also paramount but lacking. Once again, I think the credit unions are not doing enough. For example, how many credit unions out there are seeking social engineering assessments that educate their employees to thwart attacks? The ones I talk to simply are not interested in such an activity. Investing in the new compliance requirements will help with information security.

Without a doubt, credit unions can implement security measures and systems in ways that actually enhance productivity. A clear example is when a phishing attack and subsequent account takekovers hit members of a credit union. The credit union must then allocate the necessary resources to deal with the attack. Who will answer the phone calls from angry members? Who will shut down the attack and go after the cybercriminal who launched it? All of this must be determined and dealt with, and it shuts down productivity. The good news is that there are easy-to-implement security measures that prevent these attacks and thus enable credit unions to use their resources on activities such as growing their business.

At Easy Solutions, we can help credit unions with both their compliance and security issues by offering them comprehensive and affordable online fraud protection. The new compliance states that credit unions must: 1) detect and effectively respond to suspicious behavior at the member login stage and 2) detect and effectively respond to suspicious transactions. Our key product and service offerings that will help credit unions with these requirements and improve their overall security posture include:

- Detect Monitoring Services: Proactive service that detects and deactivates phishing attacks at the member login stage

- DetectID: Robust authentication solution that detects and stops suspicious behavior at the member login stage

- DetectTA: Software that alerts credit unions of anomalous transactions

David Sylvester
Business Development Manager, North America

EASYSOLUTIONS

David Sylvester is Easy Solutions' Business Development Manager for North America. Easy Solutions provides solutions for identifying and preventing online transaction fraud while helping credit unions comply with existing US domestic and international two factor authentication requirements. Using our advanced transaction fraud prevention solutions, we help protect online businesses and enterprise applications from phishing attacks, online credential theft and Internet fraud threats. By simplifying online transaction security, Easy Solutions provides consumers and online merchants and financial institutions the ability to focus on their business instead of worrying about the safety of their transactions. One of the most important aspects of our solution is that no change in behavior is required on behalf of the users and the implementation is easy for both the credit union and thier members.

Contact Info

www.easysol.net