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

Securing the Credit Union from the Inside to the Outside

When most credit union executives think about security, the focus is on protecting the institution from outside threats. But, even with the latest and greatest firewalls and perimeter security measures in place, vulnerabilities may lurk on the inside. One of the biggest threats to credit unions today is the sheer velocity of money movement. By the time someone follows a paper trail, that money is gone. The bad news is, the speed will only accelerate.

It's important to note that Payment Card Industry (PCI) compliance doesn't equal immunity to risk. In fact, one of the largest security breaches in credit card history occurred not because of lack of compliance, but because one employee did not do his job for one hour. To protect your institution from the inside-out, focus attention on these key areas:

Internal Firewall Configuration: Data access should always be set up on a need-to-know basis. Review what back-office personnel can currently access, and make adjustments as needed.

Encrypt Data Everywhere: Every laptop, as well as PC, should have full disk encryption. Consider using an electronic key for information access. That way, if a laptop is lost or stolen, the data is still protected. If you change out a server, make sure you shred that server - don't just throw it out. Just because you can't access data from it, doesn't mean that criminals can't.

Eliminate Shared Credentials: Every employee should have his or her own code words and logins. If that person leaves the institution, that access can be easily and immediately shut off.

Create and Enforce Written Security Policies: Security breaches can happen because an employee taped her password to the bottom of her keyboard for safe keeping, downloaded an app or left sensitive information up on the screen during a break. Make sure you have a written security policy in place - and then create a physical security "team" who performs periodic evaluations. A clean desk policy, in which every employee locks his or her desk at night, is also a painless, but effective, protective measure.

Combat Social Engineering: Social engineering, or the ability to access critical data through sheer manipulation, is on the rise. Criminals will call in and, with what may seem like a plausible story, convince the credit union employee to disclose sensitive information. People calling in should be subject to the same type of multi-factor authentication as they would with Internet banking. Your employees need to know that just because a person claims to be a specific member that may not be the case. Help your employees get comfortable with asking for additional data to positively identify callers. Then, periodically test the system by calling into the branches, posing as a member, and trying to gain access to this sensitive data.

Watch Micro-deposits: If small amounts of money begin moving from accounts, it's a sign that something is going on. A member could be closing out the account, or criminals could be verifying their ability to transfer funds before stealing a larger amount.

Study Money Movement: If large cash withdrawals are moving out your door, it may be an indication of fraud. Criminals are setting up small shell companies and using online recruiting sites to hire one or two employees, typically to do some sort of short-term research. They set up a small business account, and then the criminals work to electronically move funds from a high-value member account into their new account. Eventually, they'll tell one of the unsuspecting employees to go in and make a withdrawal. They take the money and run.

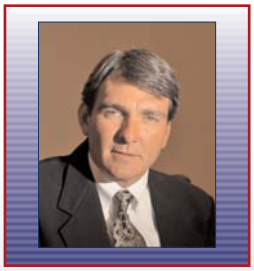
Know Your Vulnerabilities and Take Action Today:
Harland Financial Solutions has a number of solutions to help credit unions stay secure from the inside-out. Our experts can conduct a vulnerability study to pinpoint areas of concern, so you can identify weaknesses before they result in fraud. We also provide intrusion penetration and compliance testing.

A micro-transaction reporting program that works with our UltraData® Enterprise and PhoenixEFE™ enterprise solutions enables credit unions to more easily monitor this activity through real-time, daily reports. Using this tool, credit union security personnel can quickly research suspicious activity and have a better chance of preventing potential fraud.

Many credit unions also opt for our service bureau model for core system delivery. Not only does this model provide outstanding intrusion prevention systems and firewalls, but an event correlation system interprets e-mail data at lightning speed to block threats before they infiltrate the system.

The best advice: Be vigilant. Don't get distracted by the regulations - and don't take your eye off of your business. Because, you can be sure, the bad guys are watching.

Jeff Marshall
Vice President Strategic Technologies



HARLAND FINANCIAL SOLUTIONS

Jeff Marshall identifies and evaluates new technologies, solutions, partnerships and acquisitions that present opportunities for business growth for Harland Financial Solutions. Prior to his current role, Jeff oversaw software development, security and network operations for Harland Financial Solutions' electronic banking business. Before joining Harland Financial Solutions, he developed software for various national industries. He wrote one of the first Internet banking and bill payment systems in the country, as well as one of the first Internet lending systems to include real-time credit decisions. In an ongoing effort to promote the success of community-based financial institutions, he helps hundreds of financial institutions think progressively about the risks and costs related to Internet delivery systems. Jeff is widely recognized in the software industry for his accomplishments, knowledge and vision.

Contact Info

www.harlandfinancialsolutions.com