

SAVE THE DATE

www.callahan.com/roundtables

Welcome Rebecca Wessler

Account | Logout

MY SUBSCRIPTION

READ & WATCH

SEARCH & ANALYZE

CONNECT

ARCHIVES

ABOUT

Search CreditUnions.com

POWERED BY CALLAHAN & ASSOCIATES

NEWS IN CONTEXT

Spear Phishing Fail A Cautionary Tale

As revealing reports add up, credit union CISO relates a success story in social engineering and the fight against cyber fraud.

BY MARC RAPPORT

1242 VIEWS

2



As we celebrate Independence Day, it might be a good time to think about some of the latest threats from overseas and really, from who knows where else? That would be those cyber thieves seeking to free funds from their rightful owners.

A [new FBI alert](#) and a recent report serve here to illustrate. The FBI’s Internet Crime Complaint Center (IC3) says to be aware of ransomware, particularly the CryptoWall variants that have generated 992 complaints to the IC3 in the past year or so.

Those are not idle threats. That ransomware — in which the victimized institutions have to pay up to retrieve stolen financial records and other valuable data — has netted \$18 million for the thieves in the past year from those 992 complaints alone. (No one knows how much goes unreported.)

The report, meanwhile, is the “[2015 Cost of Breach Study: Global Analysis](#)” from [Larry Ponemon](#) and the Ponemon Institute. That report — Ponemon’s 10<sup>th</sup> on this topic — found that the average total cost of a data breach last year was \$3.79 million, or \$154 per each stolen record.

Credit unions feel those costs, from the [well-documented tab](#) for replacing compromised cards to the daily tasks of thwarting would be fraudsters. And there are also compliance issues. In fact, the FFIEC has just issued a [cybersecurity assessment tool](#). It follows last year’s much-publicized pilot security assessment at more than 500 credit unions and community banks, and includes a section reiterating regulators’ increased expectations of [CEOs and boards of directors](#).

**Also read:** [FFIEC “Recommends” Cyber Self Knowledge](#)

Through all this, people continue to be the weakest link, industry experts say, and here’s a cautionary tale:

**Dodging The Spear Phishing Point**

ADVERTISEMENT



SEARCH & ANALYZE

Find A Credit Union

Find An Executive | Build A Peer Group

ADVERTISEMENT

SAVE THE DATE

www.callahan.com/roundtables

ALSO RECOMMENDED

Most Commented

Most Viewed

1. [“The Big Short” Is Required Watching For Credit Union Leaders, Or Should Be](#)
2. [6 Things To Know About Credit Union Lending Trends](#)
3. [Hispanic “Together We Advance” Credit Union Seal Goes National](#)
4. [The Quest For A Simplified Lending Experience](#)

The chief information security officer at a West Coast credit union says the FBI ransomware report prompted him to ask to present on the topic at an all-team meeting on phishing. The next day, one of the credit union's vice presidents got an email with a resume attached.

"She recalled my briefing and reached out to IT before opening the attachment," the credit union CISO says. "Yes, it was malware and she pointed right to the briefing as the reason for her not clicking on the attachment.

"You can't catch them all, but if we can create a culture of healthy awareness, we can take some of the risk away."

However, the very nature of credit unions might make that a bit harder. "We train our employees to go over the top to increase member satisfaction. This can open us up to giving up too much or being too trusting towards people looking to take advantage of our culture," says Chris McGee, vice president of IT at [Del Norte Credit Union](#) (\$494.3M, Los Alamos, NM).

"Unfortunately, it only takes one person to click on the wrong thing or someone passing out sensitive information for your member data to be compromised," McGee observes.

### Phish In A Barrel

That's what happened at a client credit union of Security Compliance Associates. "Several users opened an email attachment that infected workstations with a particular Trojan associated with abilities to collect credentials and to 'call out' and download financial malware," says Brian Fischer, business development manager at the Florida-based provider of security and compliance services.

His company's CTO is now working with that credit union to clean up the mess, Fischer says, adding that a multi-layered approach that includes social engineering education and regular security assessments is key. For instance, "financial malware often times uses automated processes for ACH or balance transfers," Fischer says. "Dual controls of these transactions is an effective way to combat this, since two employees are harder to fool than one."

Meanwhile, It's that ability to target multiple recipients at once that worries Gene Frederiksen, a longtime IT security expert who now serves as CISO at PSCU. "Given the sophistication of the criminals and their methods, we will begin to see more incidents of what I refer to as the 'distributed breach,'" Frederiksen says.

The idea there is that if the message is slick enough, enough members or employees will fall for the bait to create the same net effect as a general breach at a credit union. "Unless that credit union has subscribed to a service that specifically monitors traffic to known crime servers, the credit union will not have early warning that the event is taking place," the PSCU CISO warns.

### Some Timely Tips

At the risk of preaching to the choir, here are some tips from Frederiksen at PSCU about how to address the breach risk at your credit union.

- Educate members and employees. "Let them know you'll never ask for account numbers and passwords," Frederiksen says. "Encourage them to take an active role in prevention by calling the institution if there is any question. You can never educate too much. Keep at it until you see a culture change."
- Execute a phishing test with employees. It's inexpensive and will let managers know just how big of a risk may indeed exist.
- Consider subscribing to services that monitor crime server traffic for instances of the credit union's domain name. "It will alert you to potential problems early," Frederiksen says.
- Tell the FBI if something happens. Criminals count on the fact that most people will not report. In fact, reach out before something happens. "Your local FBI office can help with awareness training and materials, as well as helping the credit union develop a list of

### 5. How Attentive Listening Makes For Stronger Lending





contacts in case you have an issue,” Frederiksen says.

VIEW ALL POSTS IN NEWS IN CONTEXT

Jul 02, 2015

MORE: [Fraud](#), [New Mexico](#), [News In Context](#), [Operations & Technology](#), [Security](#), [Technology](#),



JOIN THE CONVERSATION

Comment

ABC✓

2000 characters left

Your Name (optional)

Enter Name

Your Email Address (optional)

Enter Email Address

SUBMIT

COMMENTS

Mike  
Angelinovich  
7/2/2015 11:29 PM

Marc, I'm sure you remember our OHVA, Inc. OnhandID sound wave Authentication Smartcard solution that provided extremely strong Login security that plugged directly into the microphone jack. I'm also sure you remember that most folks did not want to carry around a card and a reader. When we presented OnhandID to ABECU they agreed it provided very strong MFA security but back in 2005 carrying around hardware was not in the picture. ABECU asked if we could duplicate OnhandID as a software solution and we did with SoundPass. We all realize that any credential entered by a user(Human)can be stolen by a Trojan Keylogger or Phished out of the user. Since SoundPass generates, encrypts and automatically transmits a dynamic virtual credential every time a user elects to Login to their online account, prevents a Trojan Keylogger from stealing it because it is not entered by a human on the Login page and the user never knows what it is so you cannot Phish it out of someone who doesn't know what it is and it changes every time you Login. ABECU is in their 9th year operating under the protection of SoundPass across the nation and they have never been breached. My point is to explain that the strongest Authentication solution must remove the user from the total Login equation, which also provides the most convenient solution as it can be implemented on any Login page and be invisible to the user.

[Reply](#)  
Anonymous

7/3/2015 12:29:51 PM

Thank you, Mike, always good to hear from you.

PLATINUM SUPPLIERS | [GET LISTED](#)



READ & WATCH

Cooperative Strategy  
Deposits & Payments  
Financial Performance  
Lending  
Marketing  
Operations & Technology

SEARCH & ANALYZE

Industry Overview  
Find A Credit Union  
Find An Executive  
Build A Peer Group

CONNECT

Buyer's Guide  
Career Center  
Industry Calendar  
Press Center

ARCHIVES

Callahan Report  
Research  
CUSP  
Credit Union Directory  
Market Share Guides

ABOUT

Advertise  
Contact Us  
Privacy Policy  
FAQ  
Sitemap



P: 800-446-7453 | F: 800-878-4712

1001 Connecticut Ave. NW Suite 1001  
Washington, DC 20036