



Cybersecurity: Are you gambling with member data?

Tom Schauer – Principal
CISA, CISM, CISSP, CEH, CRISC, CTGA
CliftonLarsonAllen - Information Security Services Group

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor. | ©2015 CliftonLarsonAllen LLP

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



My Background and Experience

- InfoSec Programmer then Manager at \$3.3B Bank
- Ernst & Young then Deloitte - WaMu, BofA, etc
- Started TrustCC in 2000 - Community FI Focus
 - Contracts with NCUA
 - Hundreds of FIs, Thousands of Assessments
 - 2012 Pioneered Breach Simulation Testing at FIs
 - Brought MAJOR ACH Risk to Light
- Couldn't be more delighted to join CLA...

©2015 CliftonLarsonAllen LLP

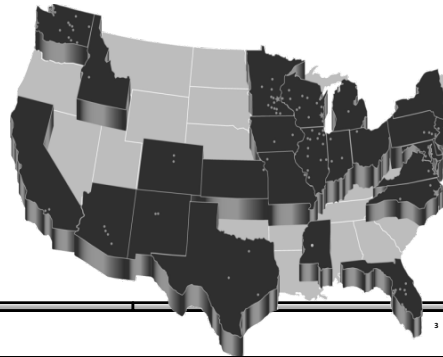


WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Our perspective...

CliftonLarsonAllen

- Started in 1953 with a goal of total client service
- Today, industry specialized CPA and Advisory firm ranked in the top 10 in the U.S.
- Information Security offered as specialized service offering for nearly 20 years
- In Sept 2015 my firm, TrustCC merged with CLA
- Largest Credit Union Service Practice*



*Callahan and Associates 2015 Guide to Credit Union CPA Auditors.

NATIONAL MARKET SHARE RANKING OF AUDIT FIRMS FOR ALL CREDIT UNIONS OVER \$40M IN ASSETS | FINANCIAL DATA AS OF DECEMBER 31, 2014; AUDIT DATE BETWEEN JULY 1, 2014 AND JUNE 30, 2015

RK	CPA FIRM	TOTAL CUS OVER \$40M SERVED	# OF CUS \$40M-\$100M	# OF CUS OVER \$100M	TOTAL ASSETS OF CUS AS OF DEC. 31, 2014
1	CliftonLarsonAllen, LLP	246	48	198	\$192,696,876,479
2	Orth, Chakler, Murmane & Co.	146	22	124	\$98,530,827,285
3	Nearman, Maynard, Vallez, CPAs	122	32	92	\$53,439,563,077
4	Moss Adams	79	8	71	\$99,475,904,632
5	McGladrey LLP	74	16	60	\$55,269,935,953
6	Turner, Warren, Hwang & Conrad	68	19	49	\$35,543,794,334
7	Doeren, Mayhew & Co.	55	8	47	\$31,532,173,712
8	Cindrich, Mahalak & Co.	54	24	30	\$10,551,228,159
9	Financial Standards Group	46	37	9	\$3,989,338,326
10	Richards & Associates	38	20	18	\$8,041,569,170
11	Petersen & Associates	37	17	20	\$5,362,281,413
12	BKD, LLP	33	4	29	\$33,980,398,397
13	Hutto & Carver, P.A.	33	11	23	\$20,017,576,059
14	Wipfli LLP	33	11	22	\$9,188,830,049
15	Lillie & Company	31	13	18	\$4,776,910,255
16	Crowe Horwath	30	0	30	\$43,986,986,285
17	GBQ Partners LLC	30	9	21	\$6,503,860,067
18	Reinsel, Kuntz, Leshner LLP	28	9	20	\$10,257,164,672
19	Wojeski & Co. CPAs, P.C.	24	14	10	\$2,603,780,900
20	J.Tenbrink & Associates	21	13	8	\$3,010,851,954
21	Robert Anderson & Co.	21	8	13	\$2,550,532,599
22	Hiram H. Hollifield	20	15	5	\$1,569,308,195
23	Firley, Moran, Freer, & Eassa	19	4	15	\$6,706,461,220
24	Padden, Guerrini & Associates	19	6	13	\$2,874,118,840
25	Holben Hay Lake Balzer LLC	18	5	13	\$4,351,733,186



2016 Cybersecurity SYMPOSIUM Aug. 1-2, Chicago

REGISTRATION COURSE UPDATE POLICY CONTACT INFO AGENDA

Don't miss the 3rd annual edition of this popular event in 2016!

Our third annual cybersecurity symposium picks up where our first two, wildly popular programs left off. Hear and see cutting-edge techniques, best practices and procedures that protect your organization from the latest threats. Among the highlights of the 2015 event:

Highlights of the 2015 Cybersecurity Symposium included:

- Live illustration of a computer/network hacking;
- A presentation by law enforcement of its view of cybercrime;
- An review of what a credit union's directors should know about cybersecurity;
- An examination of vulnerabilities in the payments system, including those associated with Apple Pay and "chip and pin" credit and debit card security techniques;
- A panel discussion on what a cybersecurity exam should look like;
- 13 hours of educational presentations, panel discussions, demonstrations and group discussions;
- Presentations and group discussion led by more than 10 experts in cybersecurity.

REGISTER NOW

**2016 NASCUS/CUNA
CYBERSECURITY
SYMPOSIUM**


Monday and Tuesday
Aug. 1-2, 2016
Chicago, Ill.

Location:
Westin Chicago River North
320 North Dearborn Street
Chicago, IL, 60654
312-744-1900

 WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING 5

©2015 Citicorp Securities, LLP

"In the world of networked computers every sociopath is your neighbor" . . . Dan Geer

 WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING 6

What about financial institutions?

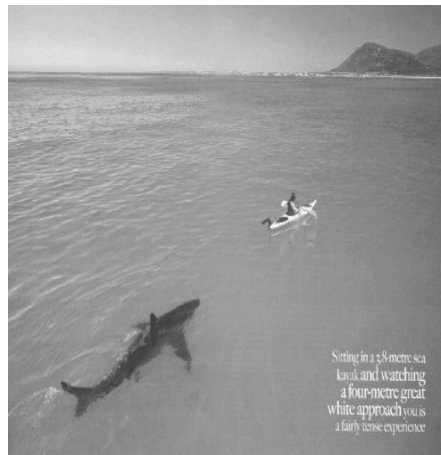
©2015 CliftonLarsonAllen LLP

- Less than 5% of all attacks directly target financial institutions.
- Most FI breach loss occurs through online banking account takeover, wire transfer fraud and PIN transaction skimming.
- Why? Do not know how to monetize.

“Corporate Account Takeover” - CATO

©2015 CliftonLarsonAllen LLP

- Catholic church parish
- Hospice
- Finance company
- Main Street newspaper stand
- Electrical contractor
- Utility company
- Industry trade association
- Rural hospital
- Mining company
- Credit Union (board members)
- On and on and on and on.....



Ransomware

©2015 CliftonLarsonAllen LLP

The FBI wants companies to know that the Bureau is there for them if they are hacked. But if that hack involves Cryptolocker, Cryptowall or other forms of ransomware, the nation’s top law enforcement agency is warning companies that they may not be able to get their data back without paying a ransom.

“The ransomware is that good,” said Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI’s CYBER and Counterintelligence Program in its Boston office. “To be honest, we often advise people just to pay the ransom.”

Example:

©2015 CliftonLarsonAllen LLP

June 11, 2014 [Redacted] BSF DISC 18,000
Palo Alto, California

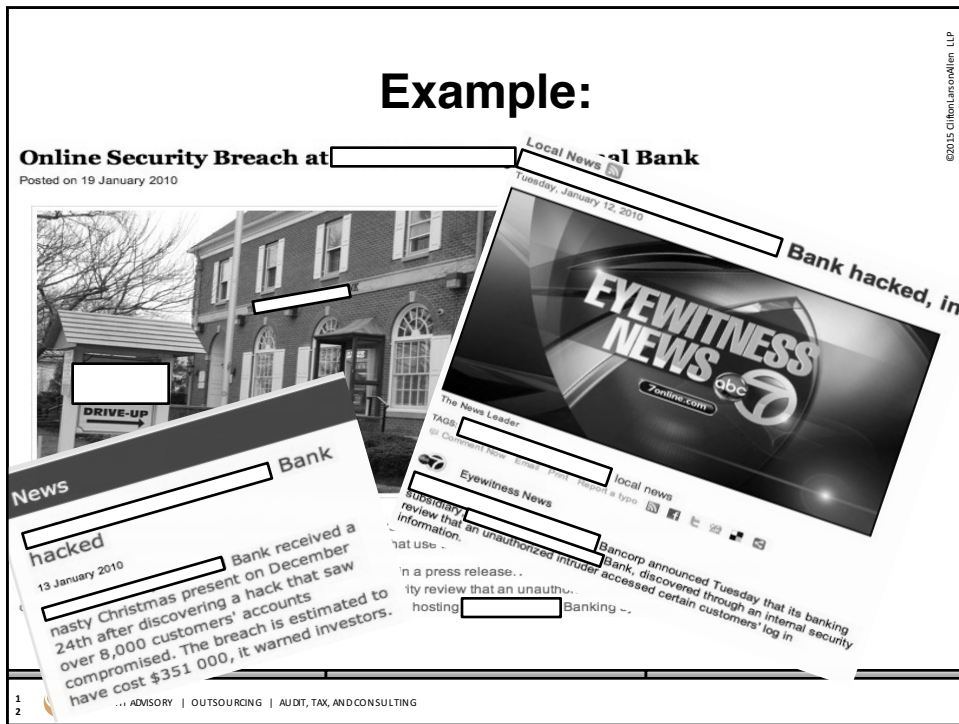
[Redacted] informed 18,000 [Redacted] that their personal information was sent to another [Redacted] accidentally. According to the letter [Redacted] employees recognized the error immediately and the data was destroyed without it being read to the recipient. The data sent was a list of [Redacted] who were pre-approved for loans. The [Redacted] employee who sent the list inadvertently sent it to a [Redacted] who had the same first name as the staff member it was meant for.

According to the [Redacted] the [Redacted] had not yet read the mail and worked with the staff of the [Redacted] to properly destroy it.

Information Source:
California Attorney General *records from this breach used in our total: 18,000*



©2015 CliftonLarsonAllen, LLP



©2015 CliftonLarsonAllen, LLP

Recent Calls to CLA

©2015 CliftonLarsonAllen LLP

- “We have a VPN connection for a vendor to manage one of our applications. The vendor just told us they were hacked into. What should we do?”
- “An ACH payment for \$120,000 was just sent to Romania, what do we do now?”
- “We think someone is reading the CFO’s email – how do we know for sure?”



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Recent Vulnerabilities

©2015 CliftonLarsonAllen LLP







Juniper Networks to rip out NSA-developed code amid new backdoor security concerns

Fortinet tries to explain weird SSH 'backdoor' discovered in firewalls


Update your firmware or suffer the consequences



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

2014 United States	2015 United States	2016 United States
  	 	

©2015 CliftonLarsonAllen, LLP

 WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

15

Is the past a good predictor of the future?

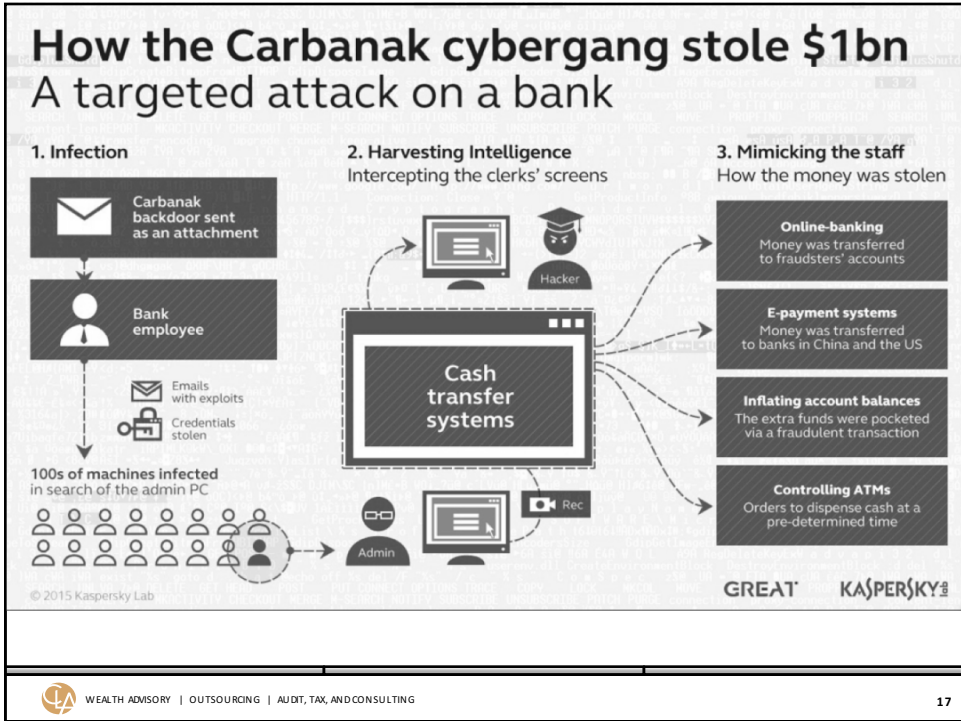
**To predict the future lets look at
elsewhere... Russia!**

**Carbanak: An Attack on Russian Banks in
2014**

©2015 CliftonLarsonAllen, LLP

 WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

16



Carbanak showed attackers how to monetize a bank breach.

©2015 Citibank, a Citigroup Company. LLP

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Cyber Fraud Risk Themes

- Hackers have “monetized” their activity
 - More sophisticated hacking
 - More “hands-on” effort
 - Smaller organizations targeted
 - Blackmarket economy

- Hackers targeting financial institution, consumers and businesses



©2015 CliffordLasswell LLP



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

19

Opportunity

- **Why do so many hacks originate in Eastern Europe**
 - 28% of all attacks in the US originate from Romania
 - “Living Wage is tough to find
 - “You’ve been Klug’ed”
 - Limited Consequences

©2015 CliffordLasswell LLP



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Perspective

©2015 CliftonLarsonAllen, LLP

- **Putin's Rules For Russian Cyber Criminals**

- Rule No. 1: Russians must not hack Russians, or anyone else in a nation that formerly was part of the Soviet Union.
- Rule No. 2: If a Russian intelligence service asks for your help, you provide it.
- Rule No. 3: Watch where you vacation.



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

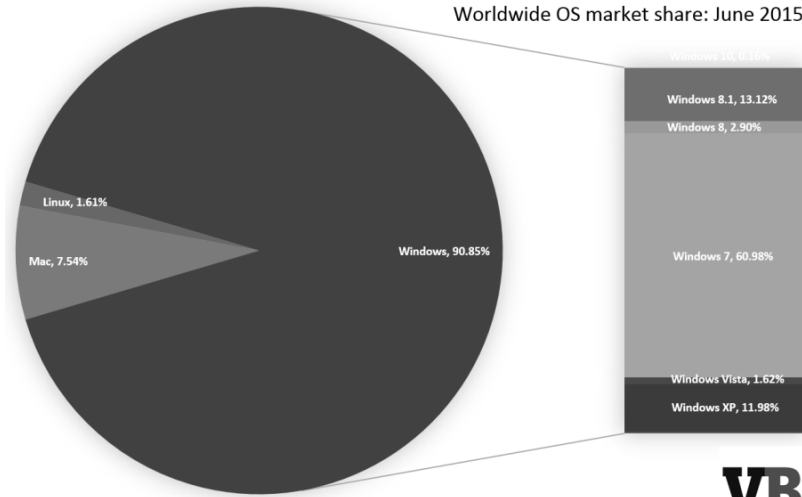
**If I wanted to steal
money from a FI, how
would I do it?**

©2015 CliftonLarsonAllen, LLP



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

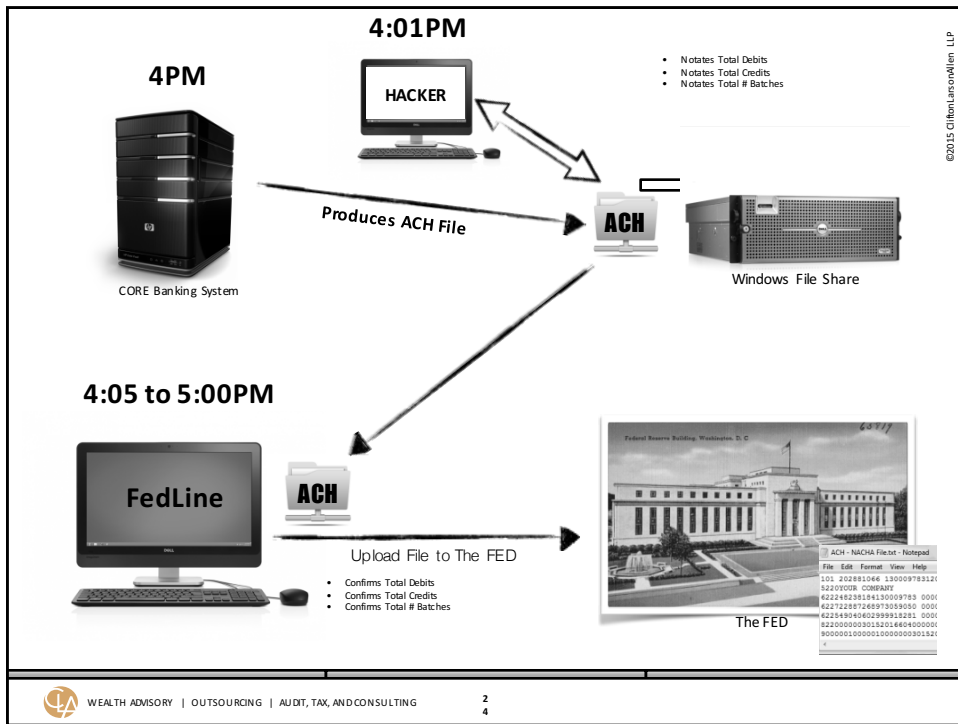
What systems are hackers most proficient at hacking?



©2015 Citifinancial.com, LLC

VB

- Information protected by native Windows security is more susceptible to compromise.



©2015 Citifinancial.com, LLC

ALTERING THE ACH FILE

Routing # Check Digit Account #

```

SWIFTSOURCE
ACH File Manipulator 20140920 by brando

* Directions: Run this file from the same
folder as the .ach file. A new .ach file
will be created using your account info.

Altering ACH File:
~ Routing and Account Numbers Have Been Changed
~ Batch Entry Hashes Have Been Updated
~ File Entry Hash Has Been Updated

New ACH File Has Been Created:
ACH File Debits/Credits Written to New File
Total File Debits: $412,679.50
Total File Credits: $3,553,847.42

File Hash Has Been Recalculated and Written to New File
Old File Hash: 1029136428
New File Hash: 5584091669

File Control Record Has been Updated
Old 9 Record: 9 18261364280000041267950000355384742
New 9 Record: 9 55840916690000041267950000355384742

~~~~~ DONE! ~~~~~
Your file has been saved in your current directory.
Routing/Account #'s have been updated on 3,099 items
~~~~~ $3,553,847.42 will be collected. ~~~~~

[Finished in 0.1s]
  
```

```

ACH - NACHA File.txt - Notepad
File Edit Format View Help
101 20288106613000978812071310532094101BANK OF ANY TOWN YOUR COMPANY
5220YOUR COMPANY 1657777777PPDAUTOPAY 120716120716
622248238184130009783 0000725152 AROUND THE HORN 020288106000019
622722887268973059050 0000555986 SEVEN SEAS IMPORTS 020288106000019
622549040602999918281 0000231437 BOTTOM-DOLLAR MARKETS 020288106000019
82200000030152016604000000000000000000015125751657777777
90000010000010000000030152016604000000000000000001512575
  
```

- This file format was developed in 1974 and has no “built in” security.
- N**** acting irresponsibly
- Regulators notified
- Reported to Congress

2
5

Imagine..

- You’ve determined that your ACH origination file has been manipulated for fraud. Now what?



Email from N****

On Oct 17, 2014, at 9:40 AM, Cindy [redacted] <C.[redacted]@N[redacted].ORG> wrote:

©2015 Citibank, a Citigroup Company, LLP

Hi Tom,

Thank you for providing the PDF. We appreciated the opportunity to sit on the call and hear about the issues you've been discussing with the Atlanta Fed relative to concerns with your bank clients' handling of ACH files. At this point, with the information we have collected, we cannot validate that the issue you have described is in fact a network issue, but instead appears to be a bank system level problem reflective of weak internal data security practices and a failure to comply with the applicable policies set forth in the N[redacted] Rules.

We will continue to work to gain an understanding of financial institution practices - and work to educate on the need for strong data security. We thank you for bringing this issue to our attention, however, at this time, we would request that you remove all reference to working with N[redacted] from the document, as that would not be accurate given the current facts.

Email to N****

©2015 Citibank, a Citigroup Company, LLP

Your email clearly supports a position that strong internal data security practices should be sufficient to protect the ACH file. In order to illustrate our position that Windows networks with strong internal data security practices are susceptible to breach, we are hereby offering to perform a security test of N[redacted]'s networks for a contingent fee. We offer to test N[redacted]'s security over a 60 day period in early 2015. If we are unable to obtain access to your internal network than our assessment is free. If we are able to access your internal network than you agree to pay us a greatly discounted assessment fee of \$10,000.

Sometimes Vendors don't "get it"?

©2015 CliftonLarsonAllen, LLP

- Lacking Independence: Cannot see how/why their system could be the problem.
- Lacking Incentive: More incentive to make systems work than to make systems secure.
- Lacking Accountability: Often too dominant to be held accountable OR unwilling to take contractual responsibility.
- Vendor Management programs attempt to overcome these challenges.

Any remarks related to N** are my own personal opinion and are not necessarily representative of any past, current or future employer.**

©2015 CliftonLarsonAllen, LLP

Now what?

©2015 CliffordLassmanAllen LLP

- If cardholder breach has slowed...
- Ransomware doesn't generate BIG \$.
- Have attackers retired?
- What is next for U.S. Financial Institutions?
- **Lets Hope it is not Carbanak.**



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Breach Cost

©2015 CliffordLassmanAllen LLP

- A breach need not result in fraud to be costly.
- 46+ States have breach disclosure laws.
- Notify if potential breach of unencrypted data.
- Cost, according to research, > \$200 per record.



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Where is your data?

©2015 CliffordLassmanAllen LLP

- Where is the sensitive information at your organization?
- Who can access it?
- What tools are you using to know where your data has proliferated?



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

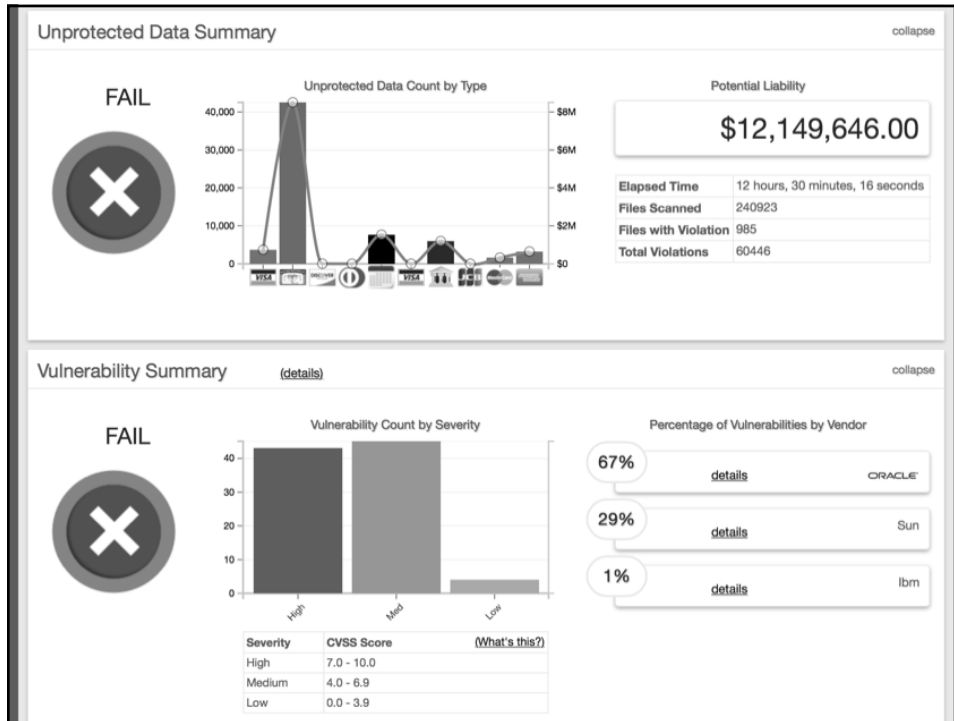
Other Targets Rarely Considered

©2015 CliffordLassmanAllen LLP

- NCUA AIREX FILES
 - Data dump provides ID theft opportunity for all members. (Windows Security)
 - Attacker must sell data at \$5 per identity
- Letter: We've changed our Banking Relationship



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



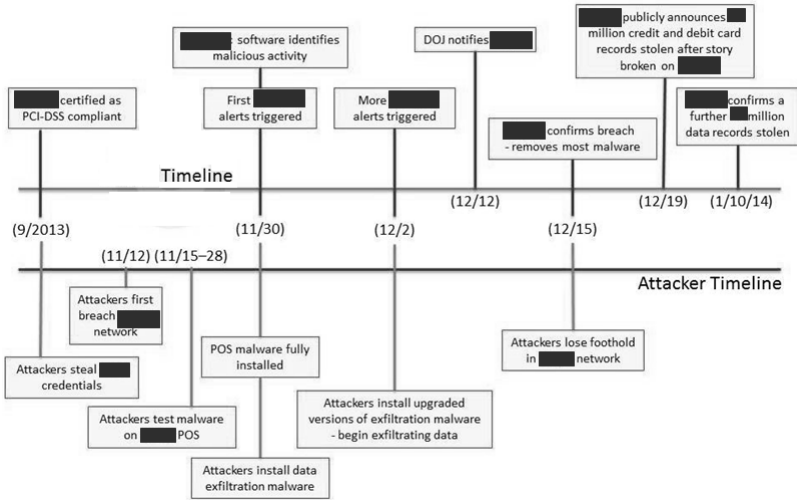
Breach Facts

"Amateurs hack systems, professionals hack people."

Bruce Schneier

- The majority of attacks begin from Social Engineering
- Most organizations do not detect their own breach

Anatomy of a Breach



©2015 Citibank, a Citigroup Company. All rights reserved.

Threat: Social Engineering



©2015 Citibank, a Citigroup Company. All rights reserved.

From SE to DA...

©2015 CliffordLassmanAllen LLP

- SE gives control of a trusted computer and a trusted account.
- Pivot to machine with a local admin logged in.
- Set traps to capture domain admin credentials.
 - Mimikatz
 - Password Guessing
 - SMB Relay



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Top Defensive Techniques

©2015 CliffordLassmanAllen LLP

1. Set the Tone from the Top
2. Risk Assess to Identify Risks and Controls
3. Facilitate Stronger Passwords
4. Prepare Personnel for Social Engineering
5. Change the IT Group's Paradigm
6. Dedicate Resources to Systems Patching
7. Audit for Configuration Compliance
8. Scan for and Remediate Vulnerabilities
9. Contract for Independent Testing of Key Controls
10. Perform True Breach Simulation



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Key Takeaway

©2015 CliffordLassmanAllen LLP

- Regularly revisit these questions...
 - If I wanted to steal money from the CU, how would I do it and what can prevent this attack?
 - If I wanted to negatively impact the reputation of the CU, how would I do it and what can prevent this attack?



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

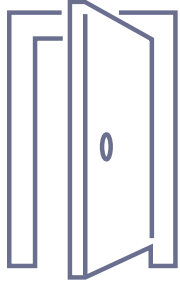
Stay tuned for later...

©2015 CliffordLassmanAllen LLP

- FFIEC CyberSecurity Risk Assessment
- Breach Preparedness
- And if time permits...
 - Top Ten IT Audit/Exam Findings



WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



Tom Schauer, Principal
CliftonLarsonAllen
Information Security Services Group
tom.schauer@CLAconnect.com
253-468-9750

©2015 CliftonLarsonAllen, LLP

CLAconnect.com

