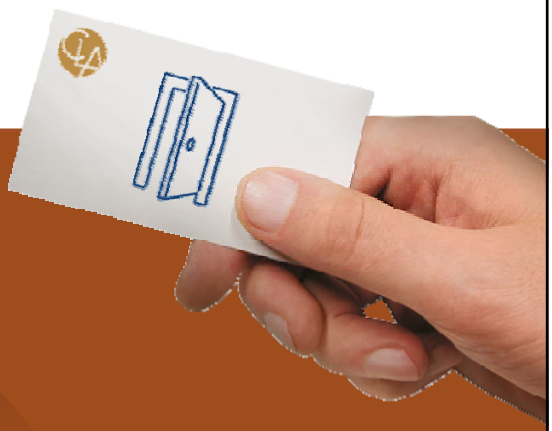
Quarterly Bank Update

Todd Sprang
John Zasada
Mark Eich

CliftonLarsonAllen
cliftonlarsonallen.com



About CliftonLarsonAllen

- One of the nation's top 10 CPA and consulting firms
- Service areas include audit, accounting, tax, consulting, and advisory
- 3,600+ professionals
- 90 offices nationwide

CliftonLarsonAllen

Agenda

- 11 – 11:05 a.m. — Welcome and opening remarks
- 11:05 – 11:20 a.m. — Accounting Update, Todd Sprang
- 11:20-11:35 a.m. – Compliance Hot Topics, John Zasada
- 11:35 – 11:50 a.m. — Strategies for Customer Awareness Training to Combat Payment Fraud, Mark Eich
- 11:50 – 12:00 p.m. — Questions and Closing Remarks

Accounting Update

Todd Sprang

Topics

1. Allowance for Loan Losses – Current Model
2. Allowance for Loan Losses– Expected Loss Model
3. Classification and Measurement Project

Allowance for Loan Losses – Current Model

- Credit quality indicators improving however….
  - Yield and earnings pressure
  - Increasing competition for limited “good” loans results in looser underwriting
  - CRE risk remains elevated
  - Difficult workouts
  - Modifications
  - Asset-based lending, leverage loans, commercial & industrial
  - Farmland/Commodity Prices
  - Home equity risk
  - Reducing ALLL

Allowance for Loan Losses – Current Model

Current issues/topics of discussion include:

1. Use of unallocated and ranges in loss estimates
2. Adjustment of historical loss periods
3. Conversion of loan to OREO
4. Accounting for improving credit quality loans

Allowance for Loan Losses – Current Model

Improving credit quality leads to frequent questions

1. When do I cease reporting as a TDR?
2. When do I return to accrual status?
3. When do I return to the FAS 5 pool?

ALLL – Expected Loss Model

Weaknesses identified following the economic crisis

- Delayed recognition of credit losses under incurred loss model identified as a weakness in existing standards
- Complexity of multiple credit impairment models

ALLL – Expected Loss Model

Financial assets not accounted for at fair value with changes in fair value reflected in net income with exposure to potential credit risk

Examples applicable to financial institutions

- Loans
- Debt securities
- Loan commitments

ALLL – Expected Loss Model

Expected credit loss is an estimate of the present value of cash flows not expected to be collected based on quantitative and qualitative information such as:

1. Past events
2. Historical loss experience
3. Current conditions
4. Borrower credit worthiness
5. Forecasts of expected credit losses*
6. Current point and forecast direction of economic cycle*

Classification and Measurement Project

Proposed Accounting Standards Update – *Recognition and Measurement of Financial Assets and Financial Liabilities*, issued February 14, 2013

The scope of the proposed ASU covers all assets and liabilities meeting the definition of a financial asset or liability with certain exclusions such as:

- Derivative instruments
- Insurance contracts
- Leases
- Pension obligations of employers or plans

Classification and Measurement Project

Classification and measurement of a financial asset is determined at the time of initial recognition based upon

1. Characteristics of the asset
2. Business model for managing the asset

Classification and Measurement Project

Initial measurement

Fair Value

- Financial instruments subsequently measured at fair value with all changes in fair value recognized through the income statement (FV-NI)

Transaction Price

- Financial instruments subsequently measured at fair value with all changes in fair value recognized through the Other Comprehensive Income (FV-OCI)
- Financial instruments subsequently measured at amortized cost

Classification and Measurement Project

Subsequent measurement - Assets

1. Amortized cost

2. Changes in fair value recognized through the Other Comprehensive Income (FV-OCI)

3. Changes in fair value recognized through the income statement (FV-NI)

Classification and Measurement Project

SPPI Test

Do the contractual terms give rise on specified dates to cash flows that are solely payments of principal and interest (SPPI) on the principal amount outstanding?

Yes – Perform business model assessment to determine amortized cost or FV-OCI

No – FV-NI

Classification and Measurement Project

Business Model Assessment

- Requires judgment
- Performed at a high level
- Considers matters such as:
  - Performance reporting
  - Management compensation
  - History of sales volume and frequency

Classification and Measurement Project

Business Model Assessment (continued)

Amortized Cost

- Objective is to hold the asset for collection of cash flows

Changes in fair value recognized through the Other Comprehensive Income (FV-OCI)

- Objective is to hold and manage the asset via a combination of collection of cash flows and selling of assets

Classification and Measurement Project

Changes in fair value recognized through the income statement (FV-NI)

1. Assets held for sale
2. Assets failing SPPI test

Todd Sprang
Partner, Financial Institutions
todd.sprang@cliftonlarsonallen.com
630-954-8175

CliftonLarsonAllen
cliftonlarsonallen.com

twitter.com/CLA_CPAs
facebook.com/cliftonlarsonallen
linkedin.com/company/cliftonlarsonallen

22

Compliance Hot Topics

John Zasada

Introducing John Zasada

John Zasada is a principal with the CliftonLarsonAllen LLP (CliftonLarsonAllen) Financial Institutions Group specializing in all aspects of bank compliance. John has over 17 years experience assisting banks nationwide in complying with consumer protection regulations including establishing regulatory compliance programs, conducting compliance assessments, training staff on bank regulations, performing website compliance assessments, and BSA/AML/OFAC independent testing. Prior to joining CliftonLarsonAllen, John was employed by a large audit firm as Managing Director.

John is a frequent speaker on regulatory compliance trends, BSA/AML, compliance management, advertising compliance and website compliance. John has also been the lead instructor for the National bank Administration (NCUA) Regulatory Compliance School and trained over 300 examiners on regulatory compliance.

John attended Utica College of Syracuse University, University of Colorado at Boulder, University of Copenhagen, Denmark, and Vermont Law School.

CliftonLarsonAllen

Compliance Changes

- Remittance Transfers
- TILA/RESPA Mortgage Disclosure Integration
- Reg Z – Requirements for Escrow Accounts
- Reg Z - Mortgage Originator Standards
- Reg Z – Ability to Repay
- Reg Z and Reg X - Mortgage Servicing
- Reg Z - HOEPA – High Cost Mortgage Loans
- Reg B - Appraisal Rules
- Reg Z - High Risk Mortgage Appraisal Rules

Compliance Dates

- Reg Z – Requirements for Escrow Accounts
- Reg Z - Mortgage Originator Standards
- Reg Z – Ability to Repay
- Reg Z and Reg X - Mortgage Servicing
- Reg Z - HOEPA – High Cost Mortgage Loans
- Reg B - Appraisal Rules
- Reg Z - High Risk Mortgage Appraisal Rules

Information overload

- Summaries
- Updated commentary
- Checklists

Compliance Landscape

- Harder to staff
- More enforcement
- Subjective requirements
- Risk-based
- Could be worse?

Ability-to-Repay Final Rule

- Issued January 2013
- Compliance required by January 10, 2014
- CFPB and the housing collapse
- Not verifying debt and income
- No-doc, low-doc
- Analyzing payments based on teaser rate

Underwriting Standards

Obtain and Verify:

(1) Income or assets;

(2) Employment status;

(3) Monthly payment for the loan;

(4) Monthly payment on any simultaneous loan;

(5) Monthly payment for mortgage-related obligations;

(6) Current debt obligations, alimony, and child support;

(7) Monthly debt-to-income ratio or residual income the borrower would take on with the mortgage; and

(8) Credit history

Qualified Mortgages

- Qualified mortgages have a “presumption” of compliance
- No risky loan features
- “No-doc” loans prohibited
- Points and fees less than 3% of the total loan amount
- Monthly payments based on highest payment
- Debt-to-income ratios 43 percent or less

Temporary Category

- Some lenders will be hesitant
- More flexible underwriting criteria
- Loan eligible to be guaranteed, purchased or insured by
  - Fannie/Freddie
  - HUD, VA, Ag, or Rural Housing Service.
- Phased out within 7 years

Presumptions of Compliance

- Intent is to prevent unnecessary litigation
- Prime vs. subprime
- Subprime – rebuttable presumption
- Prime – safe harbor as qualified mortgage

Rural Balloon-Payment Qualified Mortgages

- Small lenders in rural areas
- Treat as qualified mortgages
- 5 year term or more, fixed rate, set underwriting standards
- Hold loan in portfolio for 3 years

Miscellaneous Requirements and Penalties

- Prepayment penalties generally prohibited
- Evidence of compliance for 3 years
- Structure as open-end loan to evade requirements prohibited
- Penalties for noncompliance

Ability-to-Repay Proposal

- More exemptions from rule
- Create new category of qualified mortgages for small lenders not in rural areas making non-balloon payment loans
- Less than $2b in assets, fund less than 500 a year, hold for at least 3 years
- If approved also effective January 10, 2014

John Zasada
Principal, Regulatory Compliance Services
john.zasada@cliftonlarsonallen.com
218-790-1086

CliftonLarsonAllen
cliftonlarsonallen.com

twitter.com/CLA_CPAs

facebook.com/cliftonlarsonallen

linkedin.com/company/cliftonlarsonallen

38

Strategies for Customer Awareness Training To Combat Payment Fraud

Mark Eich

Network Security – Doing Business Safely

- Emerging & Continuing Trends
  - Three Security Reports
- Common attack vectors
- Tips for training program

CliftonLarsonAllen

Three Reasons Why We Should Care

- Organized Crime
  - Wholesale theft of personal financial information
- Payment Fraud
  - Use of online credentials for ACH, CC and wire fraud
- Hackers are targeting your customers!
  - WSJ front page 7/15/2011

Banks vs. Customers – In the Courts

Bank Sues Customer

- **$800,000** fraudulent ACH transfer - Bank retrieves $600,000 = $200,000 lost
- Both bank and customer have responsibilities, who is at fault?

Customer Sues Bank

- **$560,000** fraudulent ACH transfer
- **Funds wired to accounts in Russia, Estonia, Scotland, Finland, China** and the US and were withdrawn soon after deposits were made.
- Multiple wires = unusual activity so bank notifies client, but how quickly and what actions were taken to prevent additional fraud?
- What are the bank's obligations versus the client's?
- Updated regulatory guidance should improve consistency of controls.

Court Cases Will Eventually Set Standard - Both parties accountable for risks

Norton/Symantec Corp – The Cost

- **Norton/Symantec Corp.**
- Cost of global cybercrime: $114 billion annually.
- Time lost due to cybercrime an additional $274 billion.
- Cybercrime costs the world significantly more than the global black market in marijuana, cocaine and heroin combined ($288 billion).

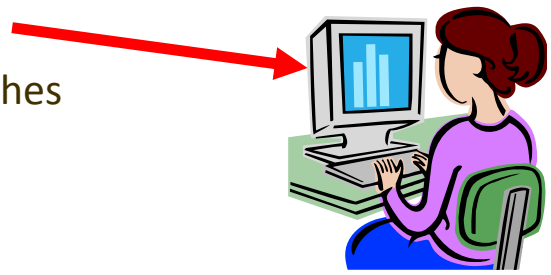
- Hackers go for the “easy money”
- Bank customers are much easier targets than the banks themselves

Three Security Reports

- Trends: Sans 2009 Top Cyber Security Threats
  - September 2009
  - http://www.sans.org/top-cyber-security-risks/
- Intrusion Analysis: TrustWave
  - January 2010 and April 2011
  - https://www.trustwave.com/GSR
- Intrusion Analysis: Verizon Business Services
  - July 2010 and April 2011
  - http://securityblog.verizonbusiness.com/2011/04/19/2011-data-breach-investigations-report-released/

SANS – Client Side Vulnerabilities

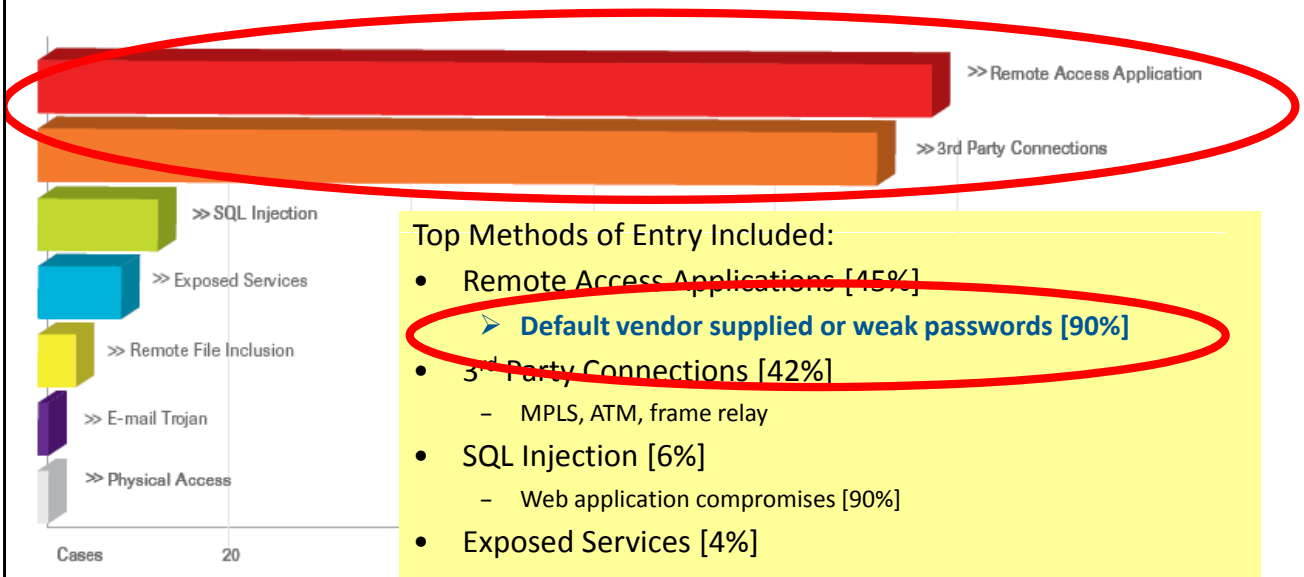
- Client side vulnerabilities
  - Missing operating system patches
  - Missing application patches
    - Apple QuickTime
    - Java Vulnerabilities
    - MS Office Applications
    - Adobe Vulnerabilities (PDF, Flash, etc…)



- Objective is to get the users to “Open the door”

TrustWave – Intrusion Analysis Report

Top Methods of Entry Included:

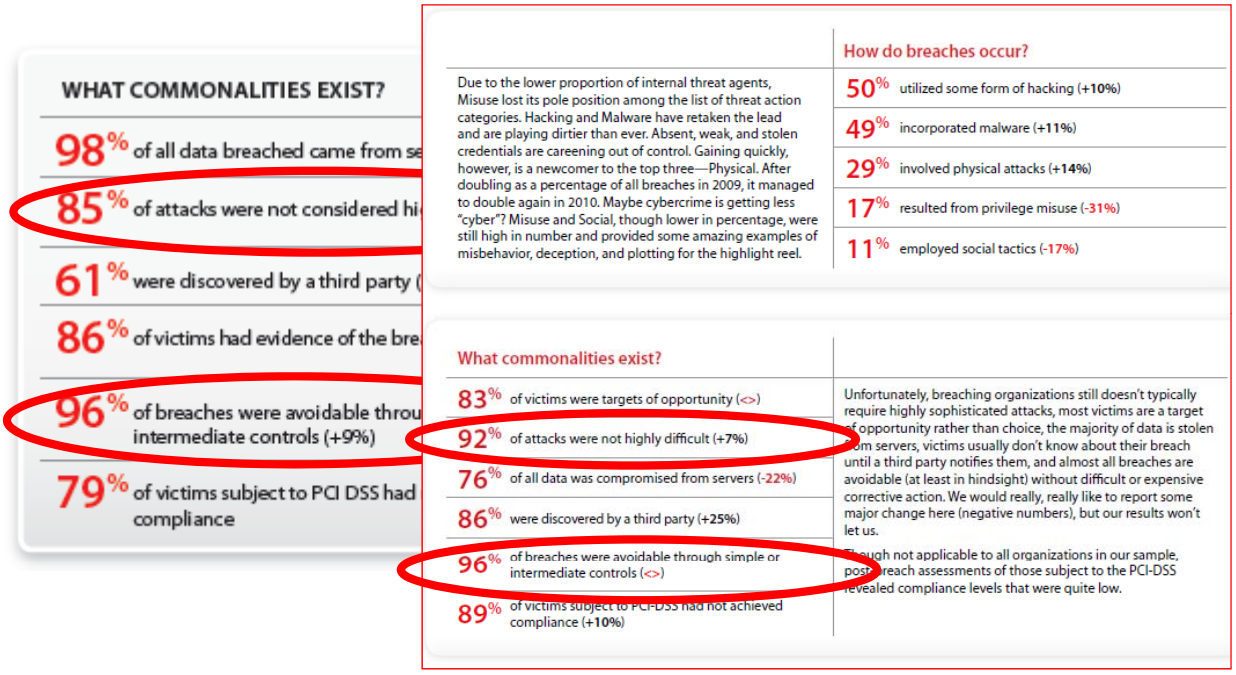


Top Methods of Entry Included:

- Remote Access Applications [45%]
  - **Default vendor supplied or weak passwords [90%]**
- 3rd Party Connections [42%]
  - MPLS, ATM, frame relay
- SQL Injection [6%]
  - Web application compromises [90%]
- Exposed Services [4%]

CliftonLarsonAllen

Verizon 2010 and 2011



WHAT COMMONALITIES EXIST?

- 98% of all data breached came from se
- 85% of attacks were not considered hi
- 61% were discovered by a third party (
- 86% of victims had evidence of the bre
- 96% of breaches were avoidable throu intermediate controls (+9%)
- 79% of victims subject to PCI DSS had compliance

Due to the lower proportion of internal threat agents, Misuse lost its pole position among the list of threat action categories. Hacking and Malware have retaken the lead and are playing dirtier than ever. Absent, weak, and stolen credentials are careening out of control. Gaining quickly, however, is a newcomer to the top three—Physical. After doubling as a percentage of all breaches in 2009, it managed to double again in 2010. Maybe cybercrime is getting less "cyber"? Misuse and Social, though lower in percentage, were still high in number and provided some amazing examples of misbehavior, deception, and plotting for the highlight reel.

How do breaches occur?

- 50% utilized some form of hacking (+10%)
- 49% incorporated malware (+11%)
- 29% involved physical attacks (+14%)
- 17% resulted from privilege misuse (-31%)
- 11% employed social tactics (-17%)

What commonalities exist?

- 83% of victims were targets of opportunity (<>)
- 92% of attacks were not highly difficult (+7%)
- 76% of all data was compromised from servers (-22%)
- 86% were discovered by a third party (+25%)
- 96% of breaches were avoidable through simple or intermediate controls (<>)
- 89% of victims subject to PCI-DSS had not achieved compliance (+10%)

Unfortunately, breaching organizations still doesn't typically require highly sophisticated attacks, most victims are a target of opportunity rather than choice, the majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hindsight) without difficult or expensive corrective action. We would really, really like to report some major change here (negative numbers), but our results won't let us.

Though not applicable to all organizations in our sample, post-breach assessments of those subject to the PCI-DSS revealed compliance levels that were quite low.

CliftonLarsonAllen

Hackers, Fraudsters, and Victims

- Opportunistic Attacks
- Targeted Attacks

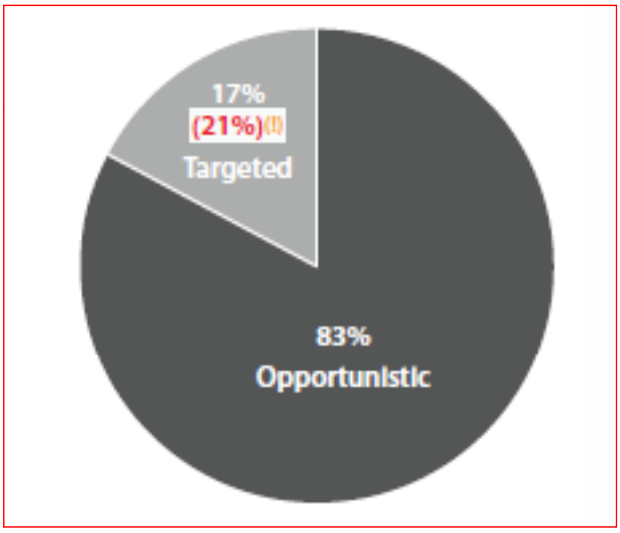
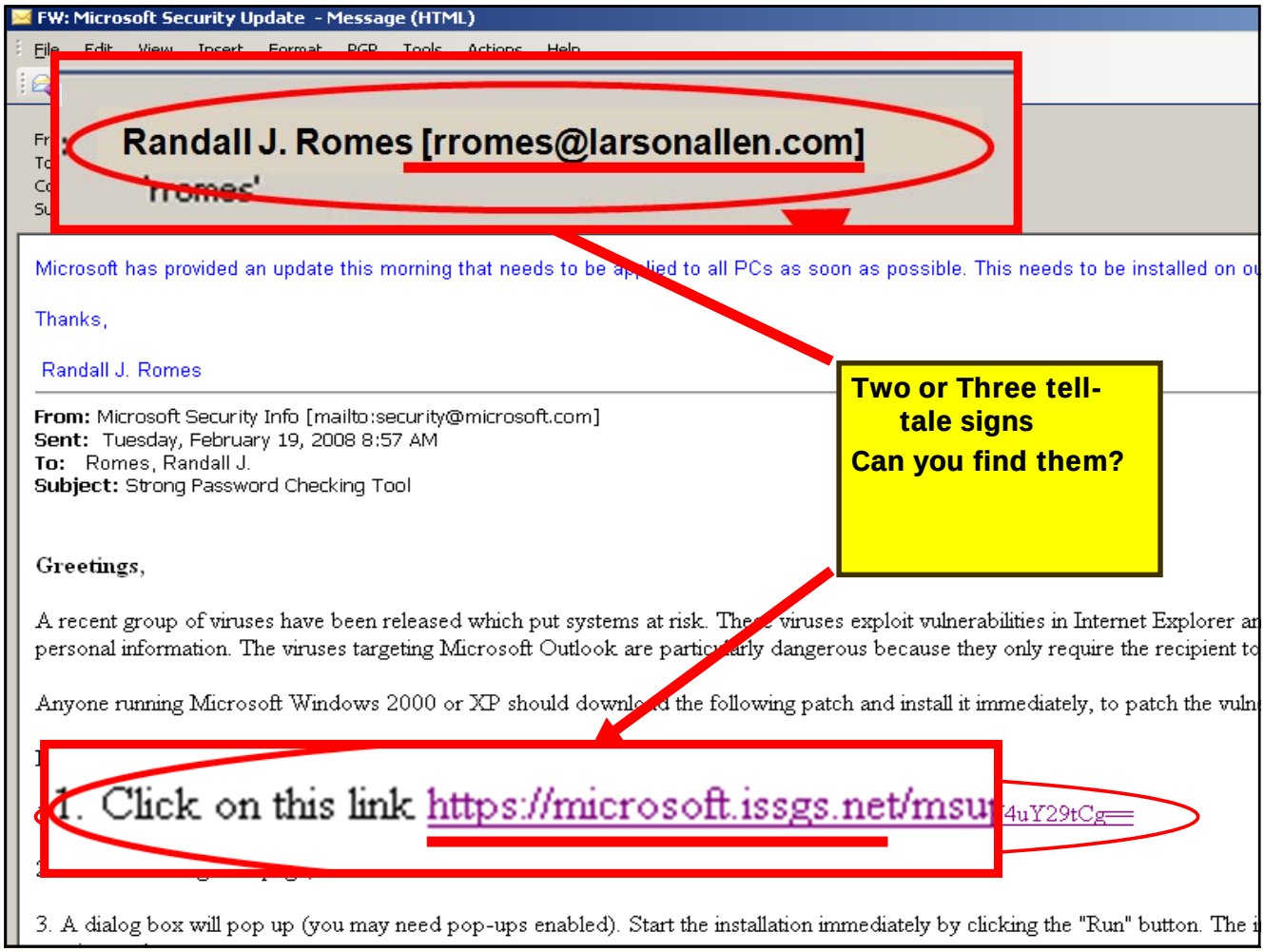


Table 6. Types of external agents by percent of breaches within External

Organized criminal group	58% (I)
Unaffiliated person(s)	40% (I)
Former employee (no longer had access)	2%
Competitor	1%
Unknown	14%
Other	<1%

CliftonLarsonAllen


FW: Microsoft Security Update - Message (HTML)
Randall J. Romes [rromes@larsonallen.com]
Microsoft has provided an update this morning that needs to be applied to all PCs as soon as possible. This needs to be installed on ou
Thanks,
Randall J. Romes
From: Microsoft Security Info [mailto:security@microsoft.com]
Sent: Tuesday, February 19, 2008 8:57 AM
To: Romes, Randall J.
Subject: Strong Password Checking Tool
Greetings,
A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Internet Explorer an
personal information. The viruses targeting Microsoft Outlook are particularly dangerous because they only require the recipient to
Anyone running Microsoft Windows 2000 or XP should download the following patch and install it immediately, to patch the vuln
1. Click on this link https://microsoft.issgs.net/msu
3. A dialog box will pop up (you may need pop-ups enabled). Start the installation immediately by clicking the "Run" button. The i
Two or Three tell-tale signs
Can you find them?

Zues, Odd-Job, Spyeye, Sinowal…

- **$72 million** stolen by international cybercrime gang
- Install back doors or use "Man-in-the-Browser" attack
- Bypass tokens and secret questions
- Display expected info to user – conduct fraud in background
- Intelligent malware and criminals avoid triggering detection

Money Mules

- "Work at Home"
- Re-shipper, insurance settlements processing, etc.
- Sometimes mule is co-conspirator, sometimes victim
- Move money out of the country without triggering alerts

Multi-Factor Authentication Solutions

- Authentication guidance calls for stronger authentication
  - Authentication factors
  - Multi-factor authentication
  - Silver bullet?

CliftonLarsonAllen

Training Tips to Consider

- Components of Education Program
  - Elements of adult learning styles
    - ◊ In person
    - ◊ Video
    - ◊ Email
    - ◊ etc
  - Repetition, repetition, repetition…

- Incentives (positive and negative)
  - ➢ To attend training"
  - ➢ To use bank tools (see point #9 below)
  - ➢ To have security assessment performed periodically

Keys to Teach Your Customers

- **Know / use Bank Tools**
  - Multi-factor authentication
  - Verification / call back thresholds
  - ACH positive pay
  - ACH blocks and filters
  - **Isolate the PC used for wires/ACH**
- **Strong Passwords**
- **InfoSec 101**

CliftonLarsonAllen

What is a strong password?

Tip: Build a password from a phrase.

I like to eat Oreo cookies at night.

ilteocan

or

Il2eOc@n

Questions?

Hang on, it's going to be a wild ride!!

Mark Eich, Partner

Information Security Services Group

mark.eich@cliftonlarsonallen.com

***

(612)397-3128

CliftonLarsonAllen

References

- FFIEC Authentication Guidance
- http://ffiec.bankinfosecurity.com/
- http://www.ffiec.gov/pdf/pr080801.pdf (2001)
- http://www.ffiec.gov/pdf/authentication_guidance.pdf (2005)
- http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf (2011)

- Bank Info Security:
- http://ffiec.bankinfosecurity.com/

- FDIC ACH Advisories:
- http://www.fdic.gov/news/news/SpecialAlert/2011/index.html

References

- FDIC ACH Advisories:
- http://www.fdic.gov/news/news/SpecialAlert/2011/index.html

- SANS report (2009)
- http://www.sans.org/top-cyber-security-risks/summary.php

References

Fraud Detection and Monitoring Solutions

- Guardian Analytics - FraudDesk
- http://www.guardiananalytics.com/products/FraudDESK/fraud-analyst.php
- Guardian Analytics - FraudMAP
- http://www.guardiananalytics.com/products/fraudMAP-overview/transaction-monitoring.php
- Easy Solutions – Detect Safe Browsing
- http://www.easysol.net/newweb/Products/Detect-Safe-Browsing
- Easy Solutions – Detect Monitoring Service
- http://www.easysol.net/newweb/Services/detect-monitoring-service
- Jack Henry Banking – Gladiator NetTeller ESM
- http://www.jackhenrybanking.com/products/risk/NetTellerESM
- ICT Solutions – Smart Fraud Monitoring
- https://sites.google.com/a/ictedu.info/ict-solutions/smart-application-suite/smart-fraud-monitoring
- ACH Positive Pay
- http://www.achalert.com/index.php?page=ach-cops

Resources and References

- Privacy Rights <dot> org

  http://www.privacyrights.org/ar/ChronDataBreaches.htm

- Resource for State Laws

  https://www.privacyrights.org/data-breach-FAQ#10

- Michigan Company sues bank

  http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000_?taxonomyId=17

  http://www.krebsonsecurity.com/2010/02/comerica-phish-foiled-2-factor-protection/#more-973

- Bank sues Texas company

  http://www.bankinfosecurity.com/articles.php?art_id=2132

References to Specific State Laws

Are there state-specific breach listings?
Some states have state laws that require breaches to be reported to a centralized data base. These states include Maine, Maryland, New York, New Hampshire, North Carolina, Vermont and Virginia (Virginia's notification law only applies to electronic breaches affecting more than 1,000 residents).

However, a number of other states have some level of notification that has been made publicly available, primarily through Freedom of Information requests. These states include California, Colorado, Florida, Illinois, Massachusetts, Michigan, Nebraska, Hawaii and Wisconsin.

State laws:
http://www.privacyrights.org/data-breach#10

For details, see the Open Security Foundation Datalossdb website:
http://datalossdb.org/primary_sources

http://www.privacyrights.org/ar/ChronDataBreaches.htm

CliftonLarsonAllen

Mark Eich
Partner, Information Security
mark.eich@cliftonlarsonallen.com
612-397-3128

CliftonLarsonAllen
cliftonlarsonallen.com

twitter.com/CLA_CPAs

facebook.com/cliftonlarsonallen

linkedin.com/company/cliftonlarsonallen

62