©2013 CliftonLarsonAllen LLP

Internal and External Fraud

Risks and Protection Strategies for Credit Unions

CliftonLarsonAllen

CLAconnect.com

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-263-6317.**
- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**
- The **PowerPoint presentation, as well as the webinar recoding,** will be sent to you within the next 10 business days.
- If you requested CPE, your certificate will be emailed to you within four weeks.
- Please complete our online survey.

©2013 CliftonLarsonAllen LLP

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
- More than 90 offices nationwide
- Financial Institutions group serves more than 350 credit union clients across the country

©2013 CliftonLarsonAllen LLP

Speaker Introductions

- **Thomas Danielson, CPA**

  Tom is a Partner with CliftonLarsonAllen and specializes in providing services to financial institutions. He has nearly 30 years of experience providing audit, tax, and consulting services for community banks and credit unions and has a wide range of experience with fraud and embezzlement investigations.

- **Randall Romes, CISSP, CRISC, MCP, PCI-QSA**

  Randy is a Principal in the Information Security Services group. He specializes in providing IT audits and security assessments for financial institutions.

- **Peter Storm, CPA, CFE, GCFA**

  Pete is an Information Security Consultant for CliftonLarsonAllen. His experience includes penetration testing, social engineering, general control reviews, IT risk assessments, SSAE16 Type II audits, and internal audit services.

©2013 CliftonLarsonAllen LLP

Learning Objectives

- At the end of this session, you will be able to:
  - Recognize and understand current risks and trends in internal and external fraud.
  - Define and describe key controls to prevent, monitor, and mitigate risks.
  - Implement strategies to combat fraud collaboratively with your employees and members.

©2013 CliftonLarsonAllen LLP

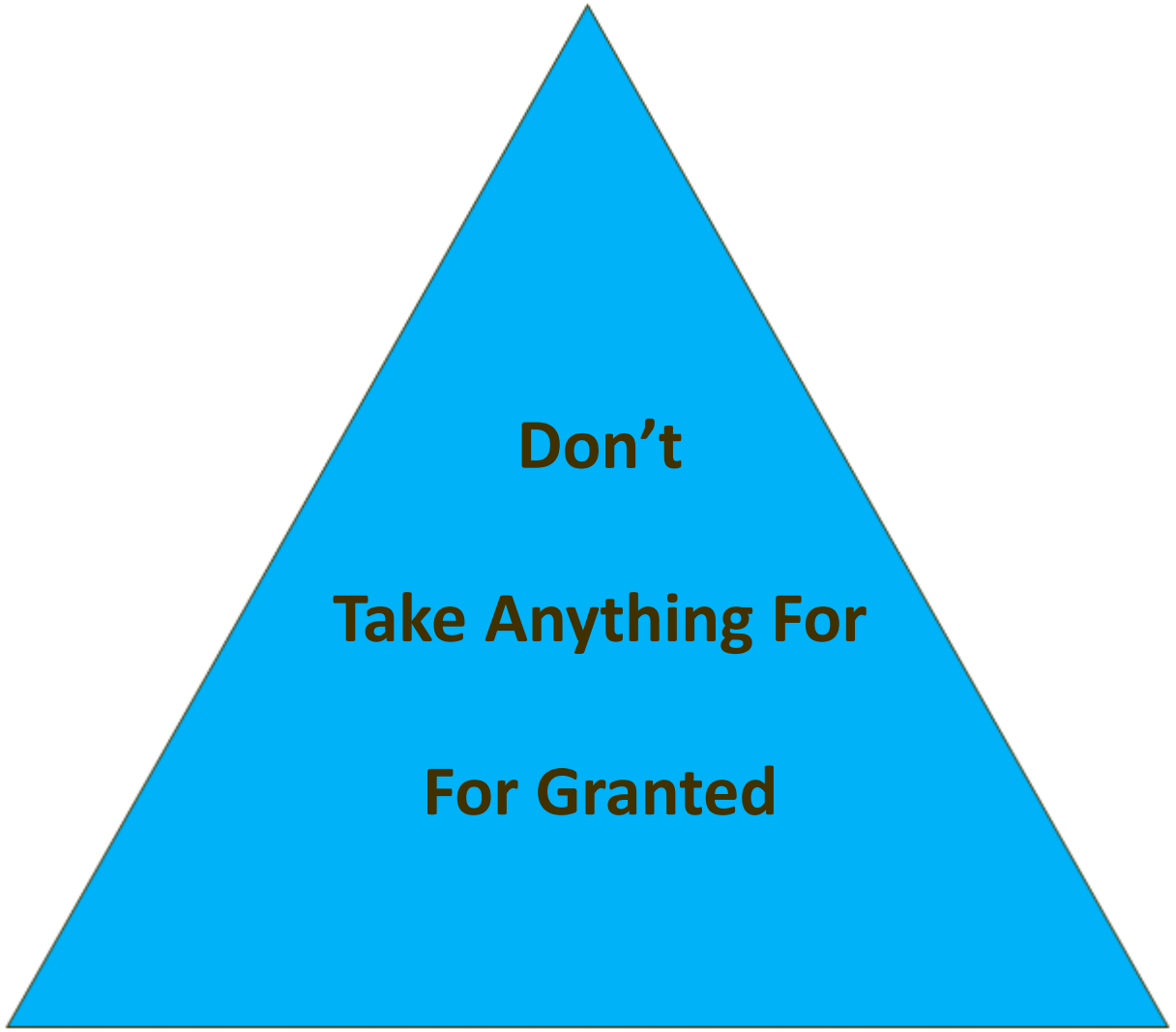
©2013 CliftonLarsonAllen LLP

Internal Fraud Risks and Protection Strategies for Credit Unions and their Members

CliftonLarsonAllen

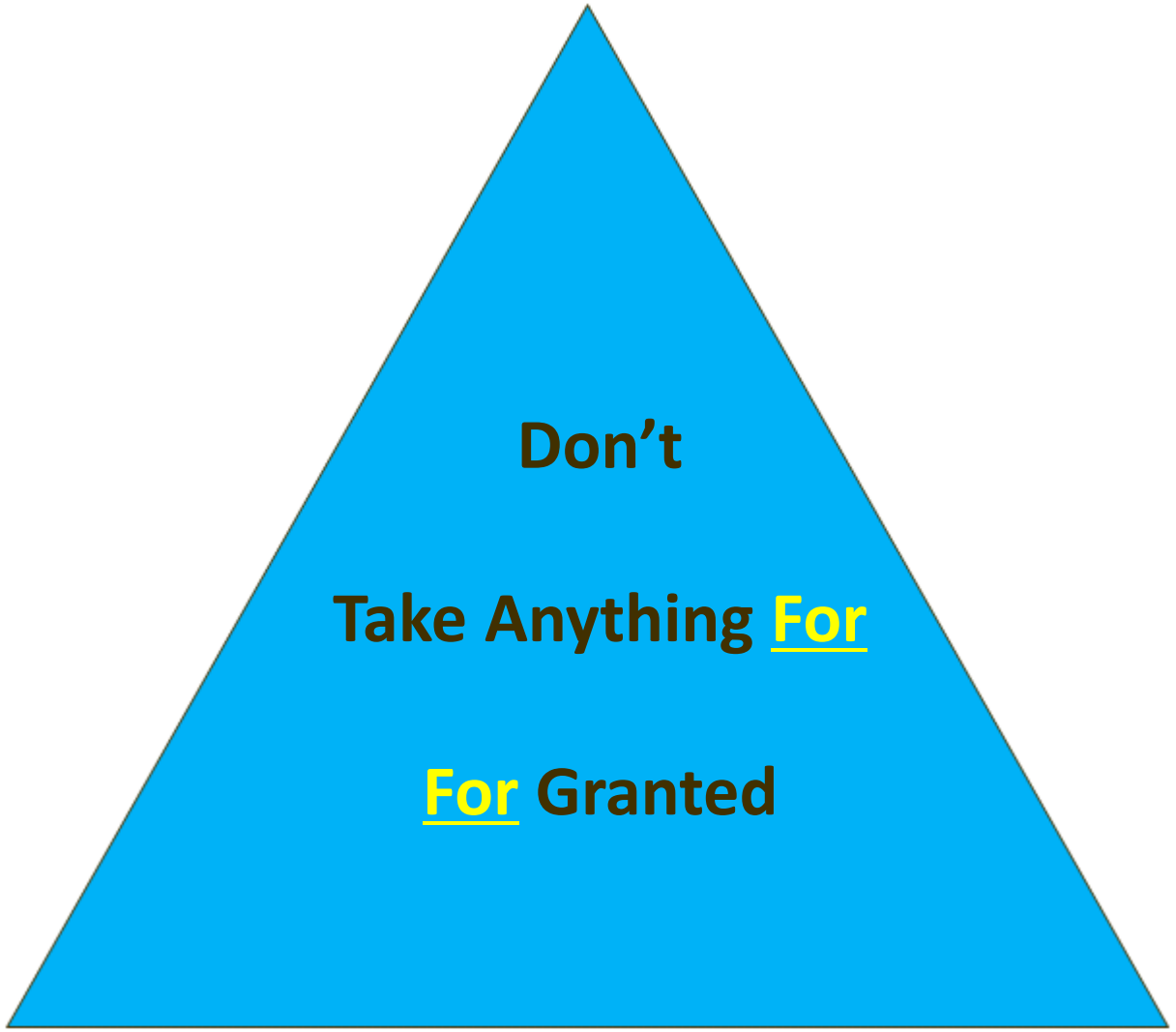
CLAconnect.com

Fraud – Be Alert



©2013 CliftonLarsonAllen LLP

Fraud – Be Skeptical



©2013 CliftonLarsonAllen LLP

ACFE 2012 Report to the Nations

- Banking and financial services is the most victimized industry
- Median losses of $232,000
- Good anti-fraud controls tend to reduce average incurred losses by ⅓ to ½
- Frauds get detected twice as quickly if good anti-fraud controls are in place

©2013 CliftonLarsonAllen LLP

ACFE 2012 Report to the Nations

- Control weaknesses that contributed to fraud
- The 'Big 3'
  - Lack of internal controls 35.5%
  - Override of existing controls 19.4%
  - Lack of management review 18.7%
- Preventing fraud is about caring about tedious matters
- Blocking and tackling issues

©2013 CliftonLarsonAllen LLP

ACFE 2012 Report to the Nations

- Position of perpetrator
  - Employee 43.0%
  - Manager 34.3%
  - Owner/Executive 18.5%
  - Other 4.2%
- Median amount of loss
  - Employee $50,000
  - Manager $150,000
  - Owner/Executive $373,000
  - Other $86,000

©2013 CliftonLarsonAllen LLP

Fraud is More Common Than You Think

- The next slides illustrate how common fraud is for community-based financial institutions
- Fraud impacts community banks, thrifts and credit unions especially hard
  - Fewer resources to combat fraud
  - Greater impact if it occurs
  - More likely to occur
- Pay attention to:
  - Title of perpetrator
  - Amount
  - Scheme used

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Deborah Shaw**, believed to be 51, of Marshall County, Mississippi, has been charged with three federal counts of embezzlement for allegedly misappropriating more than $108,000 from a special benefit account for a child shot and left for dead in 2006, held at **Merchants and Farmers Bank** in Holly Springs, where Shaw had been a bank executive. Court records revealed that Shaw is accused of transferring funds from the benefit account to other accounts that she owned or controlled.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Ignacio "Nacho" Morales**, 40, of North Philadelphia, PA, was charged with embezzling more than $2.3 million from the **Borinquen Federal Credit Union**, where he was employed as a manager. Morales reportedly used the ill-gotten gains to purchase 15 kilograms of cocaine and real estate. Specifically, Morales has been charged with conspiracy to defraud the government with respect to claims, misapplication and embezzlement, making false reports on federal credit institution entries, engaging in monetary transaction in property derived from specified unlawful activity, filing false federal income tax returns, and attempted possession with intent to distribute more than five kilograms of cocaine.

  Note: This credit union failed due to the loss.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Heather Laake**, 21, of Winifrede, West Virginia, has been charged with embezzling more than $101,000 from the **South Charleston Employees Federal Credit Union** where she had been employed. According to authorities, Laake took funds from customer accounts and changed the account information in an effort to conceal the thefts. Laake's boyfriend at the time, **Dewayne Spaulding**, is also facing similar charges. The misappropriations reportedly spanned a 4 month period.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Mirza H. Baig**, 49, of Marlborough, Massachusetts was sentenced to 51 months in federal prison for embezzling more than $2 million from **New England Cash Dispensing Systems, Inc.** which was contracted to manage ATMs for the **Domestic Bank of Cranston**, Rhode Island. Baig and other NECDS employees reportedly ordered excess cash for ATM refills and pocketed the difference.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Jamie Askew**, 36, of Troy, Illinois, has been indicted on charges she embezzled $104,755 between July 2009 and May 2012 from **St. Louis Community Credit Union** in St. Louis, Missouri, where she had been employed.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Barbara Kaye Rechtzigel**, 47, of Belview, Minnesota, has been charged with embezzling about $1 million from customer CD accounts at **Minnwest Bank** in Marshall where she had been employed. According to prosecutors, Rechtzigel misappropriated funds for personal use over a period of 14 years, beginning in 1998. She has been charged with one count of embezzlement by a bank officer. Rechtzigel and her husband, **Ken Rechtzigel**, are reported to be the owners of **The Bauhaus** in Lucan, Minnesota, which they purchased in October 2008.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Sarah Ann Kwasinskas**, 30, of Naugatuck, Connecticut is facing trial for allegedly embezzling $254,000 from **Naugatuck Valley Savings & Loan**, where she had been employed as a teller. Authorities allege that Kwasinskas transferred funds from 17 bank customer CD accounts into her teller drawer “to cover the thefts and balance her drawer.”

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Jennifer Hughes-Boyles**, 40, of Topeka, Kansas, has been ordered to pay $712,145 in restitution to **Heritage Bank**, for which she had been employed as a vice president. Hughes-Boyles pleaded guilty to bank fraud in connection with her misappropriation of the funds from the bank through a fraudulent loan scheme.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Aubrey Lee Price**, 46, of Southern Georgia, has been charged with embezzling about $17 million from a bank where he had served as a director. Price, who is being sought by authorities since he disappeared in June, had been entrusted by the bank to invest the funds on their behalf. He has been charged with wire fraud in absentia. Authorities are concerned that he may have fled to South America, where he has done mission work and built churches.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Brenda K. Smith**, 37, of Lincoln, Alabama, was sentenced to 21 months in prison for embezzling nearly $129,000 from two customer accounts at **Regions Bank** in Lincoln where she had been employed as a branch manager. Smith reportedly misappropriated the funds over a two year period.

©2013 CliftonLarsonAllen LLP

Fraud Talk Blog Excerpts

- **Mary M. Sheedy**, 49, of Morrisonville, Illinois, pleaded guilty to embezzling more than $60,000 from the **Morrisonville State Bank**, where she had been employed as a branch manager. Sheedy reportedly embezzled a total of $235,000 from 14 customer accounts. She paid back over $172,000. Sheedy admitted that some of the methods she used to illegally obtain money was to forge checks, alter amounts on legitimate withdraw slips and keep the difference, and run checks through a "proof" machine a second time after tearing off the check number. She admitted that she concealed the embezzlement by altering customer bank statements and deliberately removing other statements from the mail.

©2013 CliftonLarsonAllen LLP

Our Experience over the past 18 months

- Vault cash
- Employees acting improperly to support struggling family businesses
- Clearing accounts, especially ATM clearing accounts
- Employees manipulating ACH transactions on their own accounts
- Improper use of the bank's debit card
- Improper expense reports
- Loans to family members

©2013 CliftonLarsonAllen LLP

Why did the Thefts Occur?

- Lack of internal controls
- Override of existing controls
- Lack of management review
- People knew about it and didn't say anything
  - Fear of retribution
  - No one to tell

©2013 CliftonLarsonAllen LLP

Where Did the Money Go?

- Support struggling family businesses
- Buy personal goods
- Support lifestyle
- Gambling/alcohol addictions
- Medical expenses
- Support grown children

©2013 CliftonLarsonAllen LLP

ACFE 2012 Report to the Nations

- How are frauds detected?

1.	Tip	42%
2.	Management review	15%
3.	Internal audit	14%
4.	By accident	7.4%
5.	Account reconciliation	5.3%
6.	External audit	3.3%
7.	Notified by police	2.6%

©2013 CliftonLarsonAllen LLP

Action Plans - Awareness

- Be aware of possibility of fraud
  - Employee fraud
  - Customer fraud
  - Financial reporting fraud

©2013 CliftonLarsonAllen LLP

Action Plans - Deterrence

- Internal controls matter
- Implement and follow standard operating policies and procedures
- Set appropriate Tone at the Top
- Listen to the concerns of your external and internal auditors

©2013 CliftonLarsonAllen LLP

Action Plans - Detection

- Create a Tip Hotline
  - May be the most important, cost effective anti-fraud procedure that you can do
- No retribution policy for whistleblowers
- Management review
  - Take it seriously
  - Do not simply sign-off without review
- Strong internal audit
  - Good technical and communication skills
  - Supported by Board

©2013 CliftonLarsonAllen LLP

©2013 CliftonLarsonAllen LLP

Payment Fraud: External Fraud Risks and Protection Strategies for Credit Unions and their Members

CliftonLarsonAllen

CLAconnect.com

What do the following have in common?

- Mining company
- Electrical contractor
- Catholic church parish
- Rural hospital
- Health care trade association
- Collection agency
- Main Street newspaper stand
- Hospice
- On and on and on and on…….

©2013 CliftonLarsonAllen LLP

Three Reasons Why We Should Care

- Organized Crime
  - Wholesale theft of personal financial information
- Payment Fraud – Corporate Account Takeover
  - Use of online credentials for ACH, CC and wire fraud
- Hackers are targeting (very) small businesses!
  - WSJ front page 7/15/2011

©2013 CliftonLarsonAllen LLP

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”
- ➢ Credit union members are much easier targets than the credit unions themselves

©2013 CliftonLarsonAllen LLP

Ponemon Study(s) – The Cost

- Ave per capita cost of data breach has declined from $214 to $194
- Business Banking Trust Trends:
  - Small businesses not changing their technologies or processes to keep up.
  - Small businesses are holding banks accountable for the security of their banking transactions.
  - Seventy-four percent of respondents say their businesses have experienced online banking fraud.
  - Often businesses learn about fraud before the bank notifies them.
  - In many cases, if funds are stolen banks are not reimbursing the business that was a victim of an attack.

➢ These findings indicate that businesses are vulnerable to various forms of online fraud and, as a result, banks are at risk of losing their customers if they do not improve their fraud prevention practices.

©2013 CliftonLarsonAllen LLP

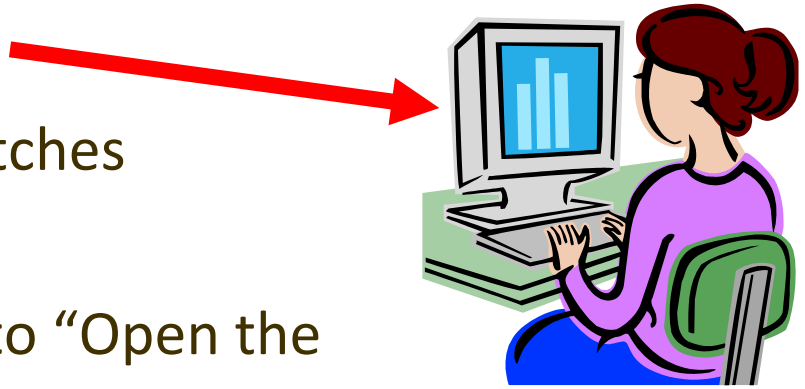
“Three” Security Reports

- Trends: Sans Top Cyber Security Threats
  - http://www.sans.org/top-cyber-security-risks/
- Intrusion Analysis: TrustWave
  - https://www.trustwave.com/global-security-report/
- Intrusion Analysis: Verizon Business Services
  - 2011 report
  - http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
  - 2012 report
  - http://www.verizonbusiness.com/about/events/2012dbir/

©2013 CliftonLarsonAllen LLP

SANS – Client Side Vulnerabilities

- Client side vulnerabilities
  - Missing operating system patches
  - Missing application patches
  - Objective is to get the users to “Open the door”
  - ➢ Phishing attacks and drive-by downloads



- Vulnerable Web sites
  - **Password guessing**
  - Attacks on application interfaces with “input fields”

©2013 CliftonLarsonAllen LLP

TrustWave – Intrusion Analysis Report

Methods of Entry:

- Remote Access Application – 61.7%
- Unknown – 19.9%
- SQL Injection – 6.9%
- Admin Interference – 4.2%
- Remote File Inclusion – 2.7%
- Authorization Flaw – 2.3%
- Physical Access – 1.1%
- Directory Traversal - .4%
- Malicious Insider - .4%
- Insecure X .25 Interface - .4%

Methods of Propagation:

- 80% - Use of weak administrative credentials
- 15% - Default hidden administrative shares
- 5% - Remote access solution credential caching

©2013 CliftonLarsonAllen LLP

TrustWave – Intrusion Analysis Report

- Incident Response – Investigative Conclusions
- Window of Data Exposure
  - In Transit: Widow of Exposure = 110.5 Days
  - Stored Data: Window of Exposure = 557.5 Days
- Once inside, attackers have very little reason to think they will be detected…

The bad guys are inside for 1 ½ YEARS before anyone knows!

©2013 CliftonLarsonAllen LLP

Verizon

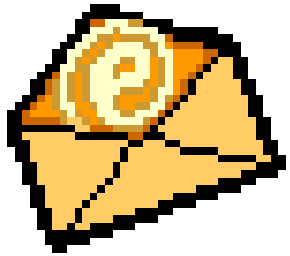
- Report is analysis of intrusions investigated by Verizon and US Secret Service.

- KEY POINTS:
  - Time from successful intrusion to compromise of data was days to weeks.
  - **Log files contained evidence** of the intrusion attempt, success, and removal of data.
  - Most successful intrusions were not considered highly difficult.

©2013 CliftonLarsonAllen LLP

Email Attacks - Spoofing and Phishing

- Impersonate someone in authority and:
  - Ask them to visit a web-site
  - Ask them to open an attachment or run update



- Examples
  - Better Business Bureau complaint
  - http://www.millersmiles.co.uk/email/visa-usabetter-business-bureaucall-for-action-visa
  - Microsoft Security Patch Download
  - Example on following pages…

©2013 CliftonLarsonAllen LLP

FW: Microsoft Security Update - Message (HTML)

File Edit View Insert Format PGP Tools Actions Help

Reply | Reply to All | Forward

From: **Randall J. Romes [Randall.Romes@CLAconnect.com]**
To: 'rromes'
Cc:
Subject: FW: Microsoft Security Update

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

Two or Three tell-tale signs

Can you find them?

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 vulne

Instructions:

1. Click on this link https://microsoft.issgs.net/msupdate.php?id=bWphY2tzb25AbGFyc29uYWxsZW4uY29tCg==

2. On the resulting web page, click the "Download" button.

3. A dialog box will pop up (you may need pop-ups enabled). Start the installation immediately by clicking the "Run" button. The i

FW: Microsoft Security Update - Message (HTML)

File Edit View Insert Format PGP Tools Actions Help

Fr: **Randall J. Romes [rromes@larsonallen.com]**

To: 'rromes'

Co:

Su:

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

Two or Three tell-tale signs

Can you find them?

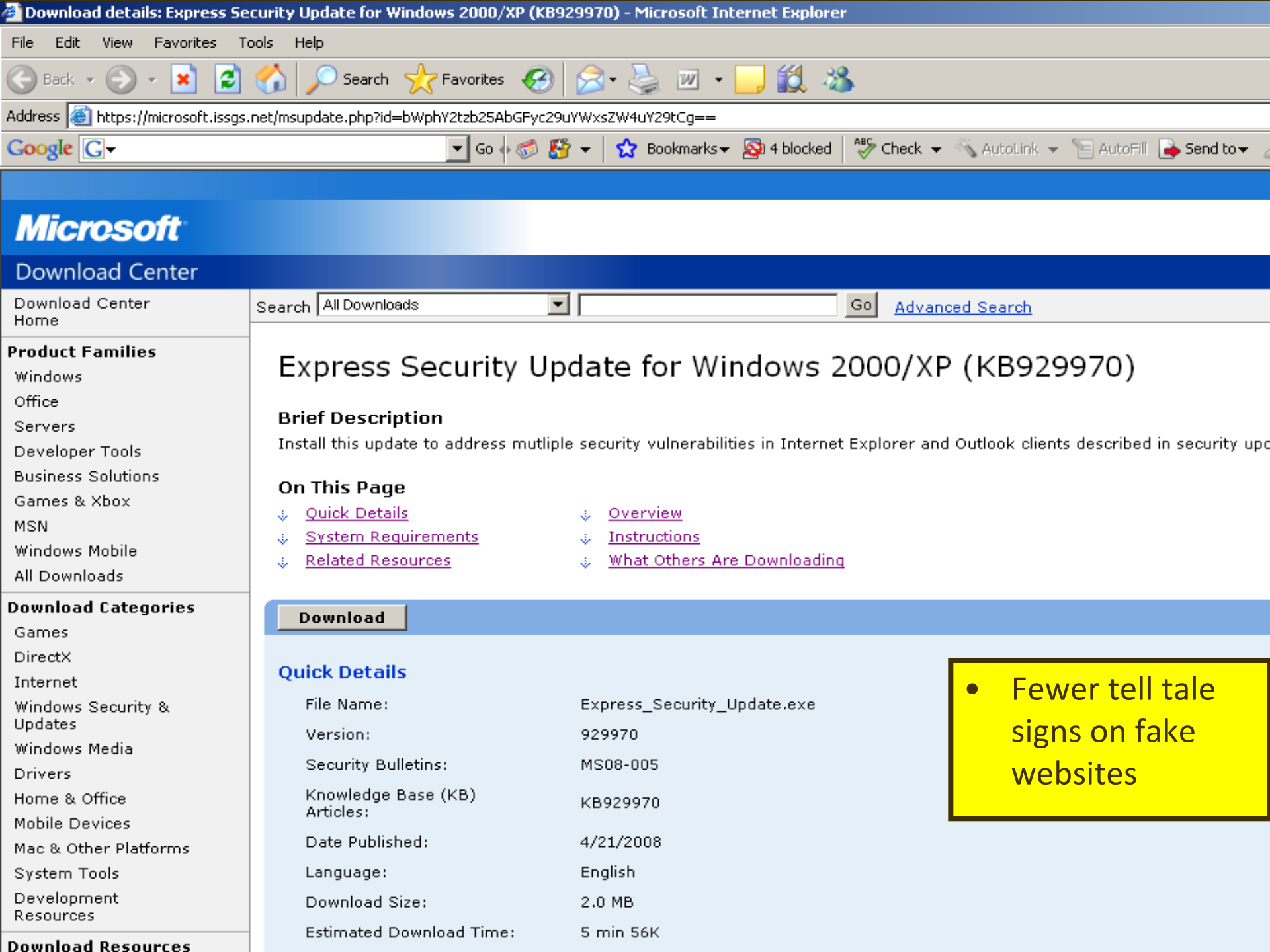
Greetings,

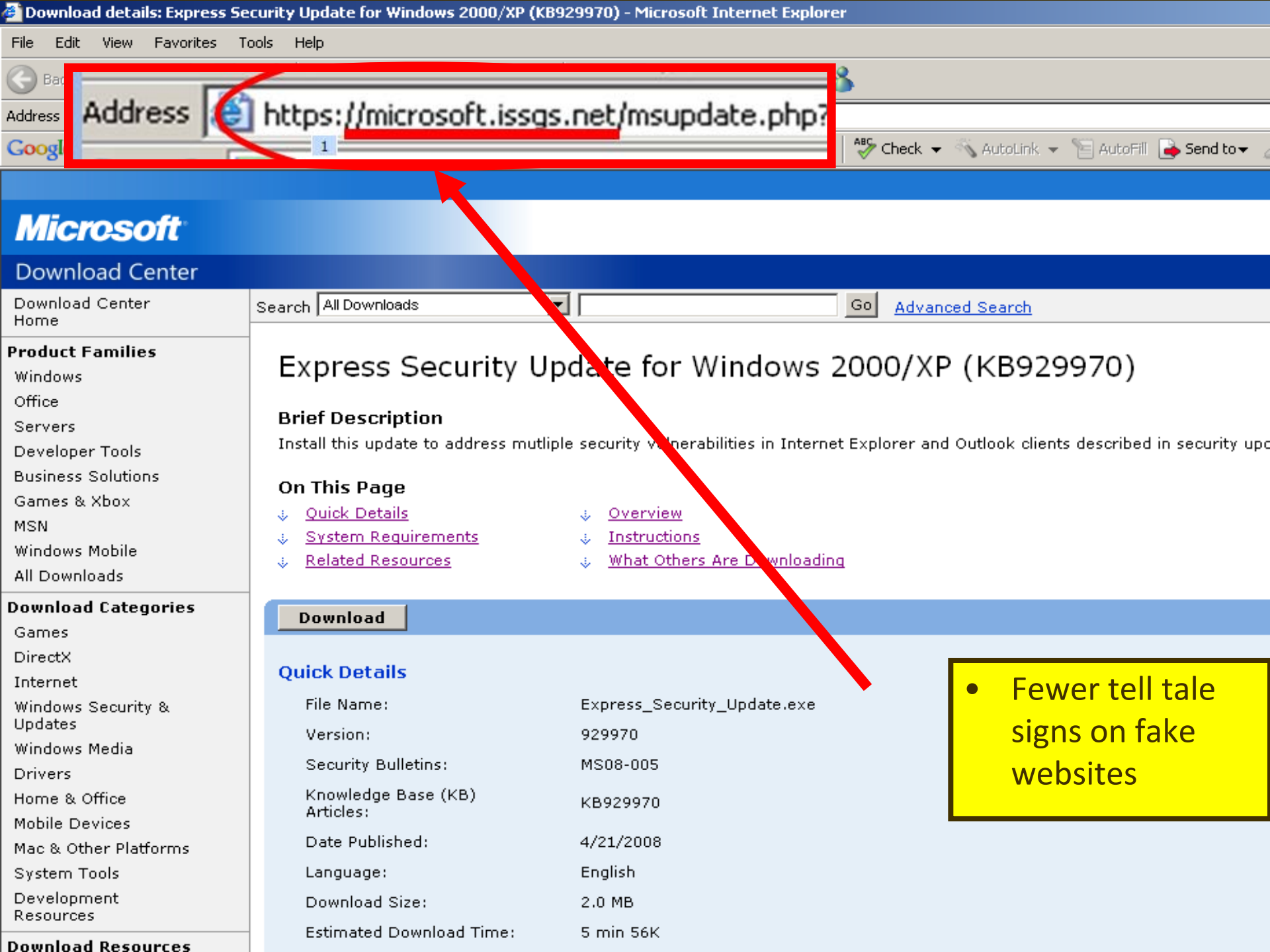
A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Internet Explorer an personal information. The viruses targeting Microsoft Outlook are particularly dangerous because they only require the recipient to

Anyone running Microsoft Windows 2000 or XP should download the following patch and install it immediately, to patch the vulne

1. Click on this link https://microsoft.isgs.net/msu 4uY29tCg==

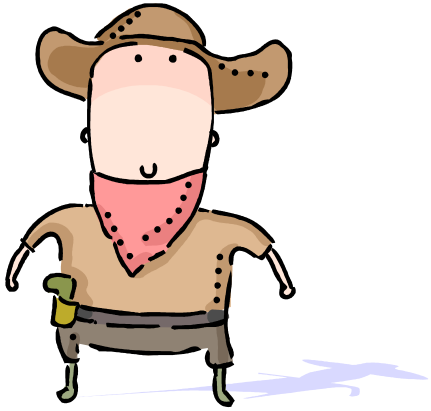
3. A dialog box will pop up (you may need pop-ups enabled). Start the installation immediately by clicking the "Run" button. The i


Download details: Express Security Update for Windows 2000/XP (KB929970) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://microsoft.issgs.net/msupdate.php?id=bWphY2tzb25AbGFyc29uYWxsZW4uY29tCg==
Google Go Bookmarks 4 blocked Check AutoLink AutoFill Send to
Microsoft
Download Center
Download Center Home
Product Families
Windows
Office
Servers
Developer Tools
Business Solutions
Games & Xbox
MSN
Windows Mobile
All Downloads
Download Categories
Games
DirectX
Internet
Windows Security & Updates
Windows Media
Drivers
Home & Office
Mobile Devices
Mac & Other Platforms
System Tools
Development Resources
Download Resources
Search All Downloads Go Advanced Search
Express Security Update for Windows 2000/XP (KB929970)
Brief Description
Install this update to address mutliple security vulnerabilities in Internet Explorer and Outlook clients described in security upd
On This Page
Quick Details
System Requirements
Related Resources
Overview
Instructions
What Others Are Downloading
Download
Quick Details
File Name: Express_Security_Update.exe
Version: 929970
Security Bulletins: MS08-005
Knowledge Base (KB) Articles: KB929970
Date Published: 4/21/2008
Language: English
Download Size: 2.0 MB
Estimated Download Time: 5 min 56K
• Fewer tell tale signs on fake websites


Download details: Express Security Update for Windows 2000/XP (KB929970) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
https://microsoft.issqs.net/msupdate.php?
Check AutoLink AutoFill Send to
Microsoft
Download Center
Download Center Home
Product Families
Windows
Office
Servers
Developer Tools
Business Solutions
Games & Xbox
MSN
Windows Mobile
All Downloads
Download Categories
Games
DirectX
Internet
Windows Security & Updates
Windows Media
Drivers
Home & Office
Mobile Devices
Mac & Other Platforms
System Tools
Development Resources
Download Resources
Search All Downloads Go Advanced Search
Express Security Update for Windows 2000/XP (KB929970)
Brief Description
Install this update to address mutliple security vulnerabilities in Internet Explorer and Outlook clients described in security upd
On This Page
Quick Details
System Requirements
Related Resources
Overview
Instructions
What Others Are Downloading
Download
Quick Details
File Name: Express_Security_Update.exe
Version: 929970
Security Bulletins: MS08-005
Knowledge Base (KB) Articles: KB929970
Date Published: 4/21/2008
Language: English
Download Size: 2.0 MB
Estimated Download Time: 5 min 56K
• Fewer tell tale signs on fake websites

Phishing and ACH

- “Mr. Jessie James, why do you rob credit unions???”
- Online banking convenience …
- Global economy…
- On-line availability of ACH
- “Corporate account take over”
- Targeting small and medium sized commercial customers



- Google: “ACH fraud suit”

©2013 CliftonLarsonAllen LLP

Phishing and ACH – In the News

Customer Sues Financial Instituion

- **$560,000** in fraudulent ACH transfers **to bank accounts in Russia, Estonia**, Scotland, Finland, China and the US; withdrawn soon after the deposits were made.
- Alleges that the bank failed to notice unusual activity.
- **Until the fraudulent transactions were made customer had made just two wire transfers ever**
- **In just a three-hour period, 47 wire transfers requests were made**.
- In addition, after customer became aware of the situation and asked the bank to halt transactions, the bank allegedly failed to do so until 38 more had been initiated.

©2013 CliftonLarsonAllen LLP

Updated Authentication Guidance

- Risk Assessment, Risk Assessment, Risk Assessment…
- At least annually or after "changes"

- Changes in the internal and external threat environment,
  - including those discussed in the Appendix of the Supplement
- Changes in the customer base
- **Changes in the customer functionality**
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

©2013 CliftonLarsonAllen LLP

Updated Authentication Guidance

- **Do not rely on single control**
  - Controls need to increase as risk increases
  - Multi-layer
  - Additional controls at different points in transaction/interaction with customer

©2013 CliftonLarsonAllen LLP

Updated Authentication Guidance

- Specific authentication guidance
  - Device identification
  - **Multifactor and two factor authentication**
  - **Challenge questions (“out of wallet…”)**
  - **“Out of band” authentication**

©2013 CliftonLarsonAllen LLP

Controls for Layered Security

- Control of administrative functions
- **Enhanced controls around payment authorization and verification**
  - ➢ "Positive Pay" features
  - ➢ Dual authorization
  - ➢ "Out of Band" verification
- Detection and response of suspicious activity

©2013 CliftonLarsonAllen LLP

Controls for Layered Security

- Customer awareness and education
  - Explanation of protections provided and not provided
  - How the financial institution may contact a customer on an unsolicited basis
  - **A suggestion that commercial online banking customers perform assessment and controls evaluation periodically**
  - A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk
  - A listing of financial institution contacts for customers discretionary use to report suspected fraud

©2013 CliftonLarsonAllen LLP

Phishing and ACH – Case Study Two

- December 2011 - Finance person receives "2000 spam messages"
- Later in the day, fraudsters make three ACH transfers all within 30 minutes:
  - $8,000 to Houston
  - Two transfers for $540,000 each **to Romania**
- In this case, business insists the following controls were not followed:
  - Dollar limit/thresholds were exceeded
  - Call back verification did not occur
- Lessons learned…

©2013 CliftonLarsonAllen LLP

Phishing and ACH – Case Study Four

- October 2012 → January 2013
- Credit Union member (hospital) gets hacked/phished…
- Two ACH payroll files totaling > $150,000.00
- Lessons learned…

©2013 CliftonLarsonAllen LLP

Vendor Due Diligence and Management

- All of the above – applies to your vendor(s)
  - Hosted Internet banking and online cash management
  - Mobile banking application provider
  - Mobile banking hosting provider

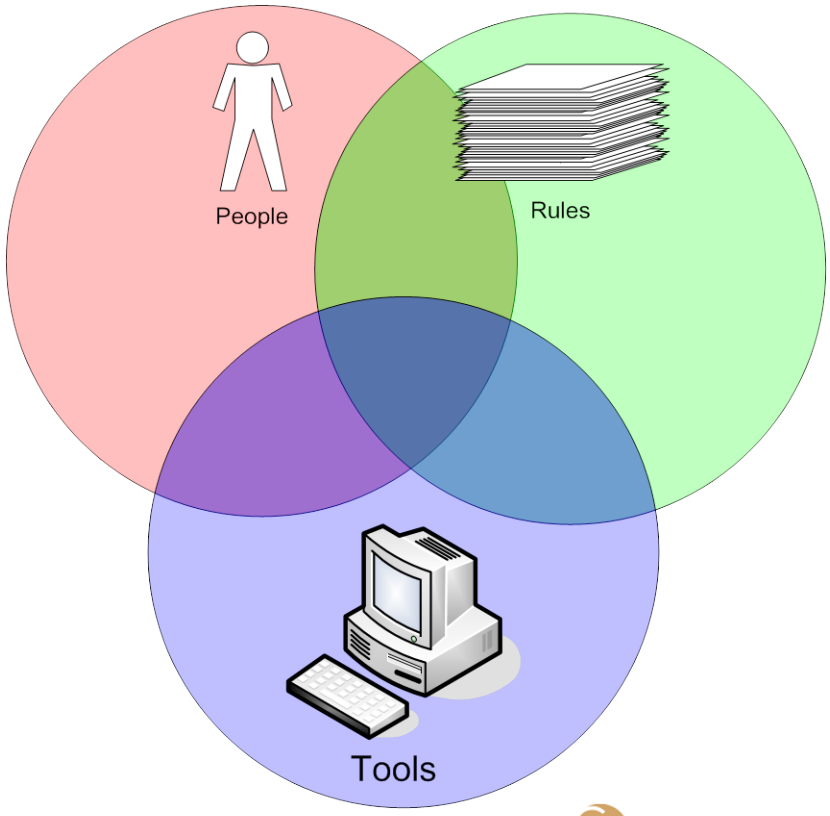
- Contracts with SLA's
- SSAE16 reviews
- Independent code review and testing

©2013 CliftonLarsonAllen LLP

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford

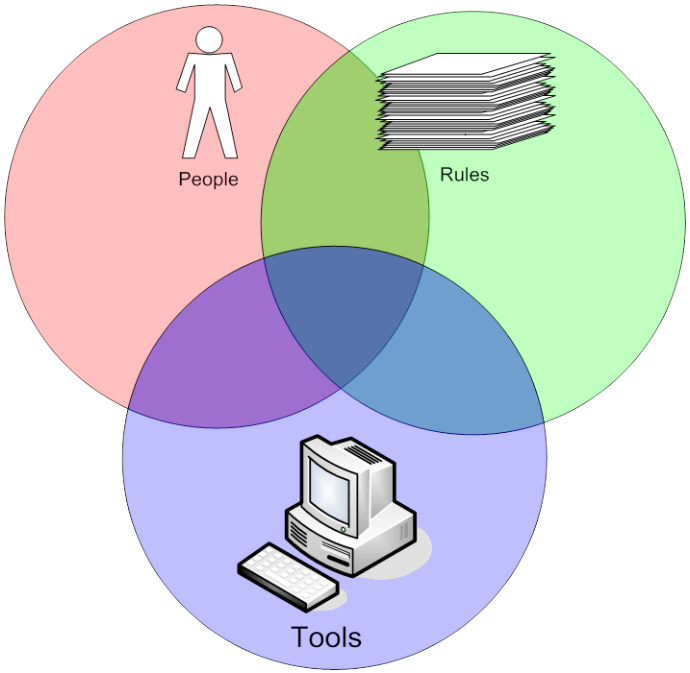


- Confidentiality
- Integrity
- Availability

©2013 CliftonLarsonAllen LLP

Summary

- Hacker Trends
- Education – communicate with your customers
- Risk Assessment
- Technical Controls
- Authentication
- Administrative Controls
- Monitoring and Anomaly Detection
- Hosted Solutions and Vendor Management
- Communicate with your customers



©2013 CliftonLarsonAllen LLP

Questions?

©2013 CliftonLarsonAllen LLP

©2013 CliftonLarsonAllen LLP

Thomas Danielson, Partner
Financial Institutions
Thomas.Danielson@CLAconnect.com
612-376-4795

Randy Romes, CISSP, CRISC, MCP, PCI-QSA, Principal
Information Security / Financial Institutions
Randy.Romes@CLAconnect.com
612-397-3114

Peter Storm, CPA, CFE, GCFE, Senior
Information Security / Financial Institutions
Peter.Storm@CLAconnect.com
612-397-3070

CliftonLarsonAllen

CLAconnect.com

twitter.com/CLAconnect

facebook.com/cliftonlarsonallen

linkedin.com/company/cliftonlarsonallen

Risk Mitigation for Online Banking

- Review and understand bank supplied/required controls for electronic banking

- Review and understand the differences between wire transfer, ACH, and other methods of payment

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Limit administrative control on banking acct
- Do NOT use master account to perform standard banking activities
- Create segregation of duties and delegate responsibilities
  1. Initiation/request
  2. Authorization
  3. Review (might be part of authorization – might be independent review later)

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Meet with insurance agent to understand what if any cyber liability coverage is in place or can be acquired
  - Understand limitations and exclusions

- Perform risk analysis of (electronic) banking function at least annually - review the following:
  - AV and anti-malware software function
  - Patch/update management
  - How do other roles/ responsibilities /activities of staff interact/intersect with banking responsibilities

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Consider having systems tested to ensure they are configured to operate securely (behave as expected)
  - Firewall
  - Wireless
  - Servers
  - Workstations/laptops/tablets
- Strongly consider the use of dedicated PC(s) for banking activities
  - Stand alone pc
  - NOT used for internet browsing, email, or any other functions

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Manually scrutinize payment activities on/around high volume times (i.e. payroll, month-end accounts payable activities, etc…)

- Implement “positive pay” features/functionality if available

    ◊ Pay for it if available

- Monitor/review your account(s) as frequently as possible (i.e. at least daily)

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Follow good password practices

➢ DO NOT use the same password for banking that you use anywhere else

➢ Make banking password as long as the system will support and you can remember (think pass phrases)

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Computer/system controls to implement:
  - Enable automatic updating for operating systems and applications
  - Ensure that Antivirus/Antimalware software is automatically updating every day
  - Employ email spam filtering service

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Configure email client software so that it does NOT automatically open/render/display imbedded graphics or pictures in email messages

- Consider using person/dedicated cellular MIFI cards for “wireless” internet access if banking must be done from laptops/portable devices

- Turn on system auditing and retain log files (consider hiring a consultant to ensure this is occurring properly)

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- Do NOT…

➢ DO NOT Perform banking activities from home/personally owned PCs

➢ DO NOT Perform banking activities from public use PCs/kiosks

©2013 CliftonLarsonAllen LLP

Risk Mitigation for Online Banking

- DO NOT Open attachments or links from unsolicited/unexpected email messages claiming “there is a problem with your account” or “there is a problem with your payment”

- DO NOT provide information proving who you are (i.e. password, SSN, account numbers) to unsolicited callers or unsolicited email

- The bank will NOT contact you in this manner…

©2013 CliftonLarsonAllen LLP

©2013 CliftonLarsonAllen LLP

Reference Materials

CliftonLarsonAllen

CLAconnect.com

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

©2013 CliftonLarsonAllen LLP

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

©2013 CliftonLarsonAllen LLP

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

©2013 CliftonLarsonAllen LLP

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

©2013 CliftonLarsonAllen LLP

References to Specific State Laws

©2013 CliftonLarsonAllen LLP

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