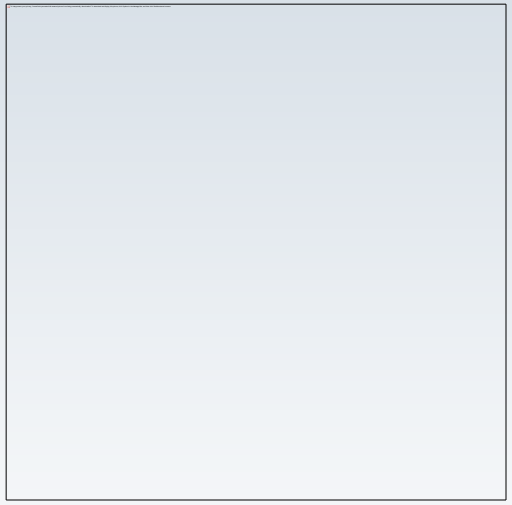
Ensuring Internal Controls in an Electronic Age

"Going Paperless…"

When people hear the phrase "going paperless," they often assume they will no longer be using paper in daily tasks or even have access to it in their office.



This obviously is not true or practical.

Going paperless means using paper wisely and sparingly, and finding effective alternatives.

“Going Paperless…” – Is it Cost Effective?

Switching from a paper-based work environment to electronic sounds like a headache.

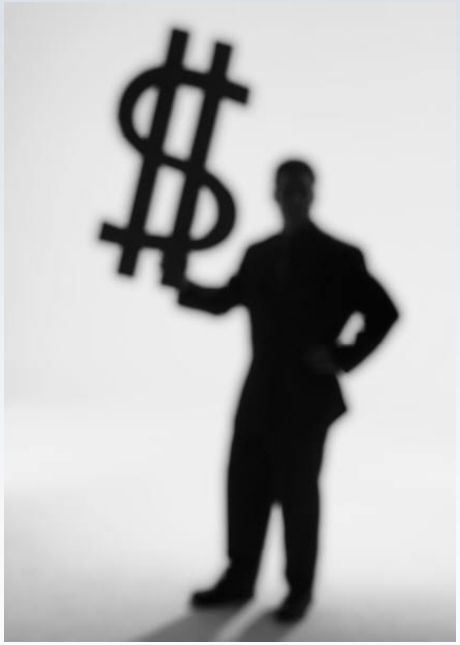
- Maybe you are **comfortable** with the process
- Maybe you **don’t like change**

Have you ever thought about the number of paper invoices that come into your accounts payable dept each month and a like number of paper checks that go out to vendors.

but consider these statistics…

"Going Paperless…" – Statistics

- Organizations spend on avg in labor costs:
  - **$20** to file a document
  - **$120** to find a misfiled document
  - **$220** to reproduce a lost document
- The average cost to process a single invoice manually is $24. *(IOMA)*
- 70% of all accounts payable payments made today are made on paper. It lags most other functional areas in terms of automation.
- Of all documents…
  - **7.5%** get lost
  - **3%** of the remainder get misfiled



Professionals spend 5-15% of their time reading information, but up to 50% looking for it.

(Aberdeen Group)

CliftonLarsonAllen

Fundamentals of Internal Controls

When it comes to going paperless, this can significantly improve efficiency and enhance your internal controls*

1. **Establish prevention procedures**
   - Identify key areas where your organization is most vulnerable and know who is accountable for each. Determine the types of fraud that may occur and how they would likely be concealed. Then establish internal controls to keep these possibilities from becoming realities.
2. **Go paperless**
   - Prevent "lost" bills, invoices, documents and reduce the risk of manipulation and information theft. You'll also get an audit trail so you know exactly who accessed, viewed, or changed a document.
3. **Enforce separation of duties**
   - Clearly define user access to the data, ensuring single users do not authorize, process, and record financial transactions within the organization.
4. **Automate work processes**
   - Enabling different members of your staff to access bills, invoices, documents; workflow is critical to your productivity. By automating reminders and an audit trail, you ensure that nothing falls through the cracks and that people who are not supposed to be part of the process are kept out.

Fundamentals of Internal Controls (cont'd)

When it comes to going paperless, this can significantly improve efficiency enhance your internal controls*

5. **Enforce payment controls**
   - By segmenting role-based controls, you make sure that no one person has access to information and the ability to edit accounting data (vendor addresses, etc.). Separation of the approval process from payment and of data entry from payment processing is key.
6. **Streamline & control check process (incoming and outgoing)**
   - A single check contains every piece of information needed to access your money. By receiving payments electronically you prevent trips to the bank and protect against checks being improperly deposited.
7. **Perform more regular internal audits**
   - Automated systems make regular audits much easier, creating an online audit trail and review of the entry and approval processes.

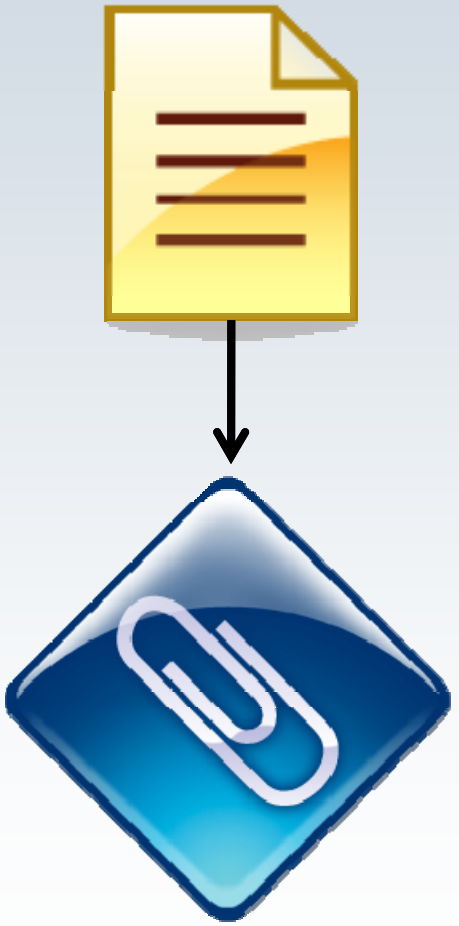
The “Paperless Plan”

Overcoming the hurdles & Get Buy In

- **Tossing out paper requires cooperation** not just from your team, but the organization, and ultimately to go completely paperless need to have buy in from customers, vendors, 3rd parties

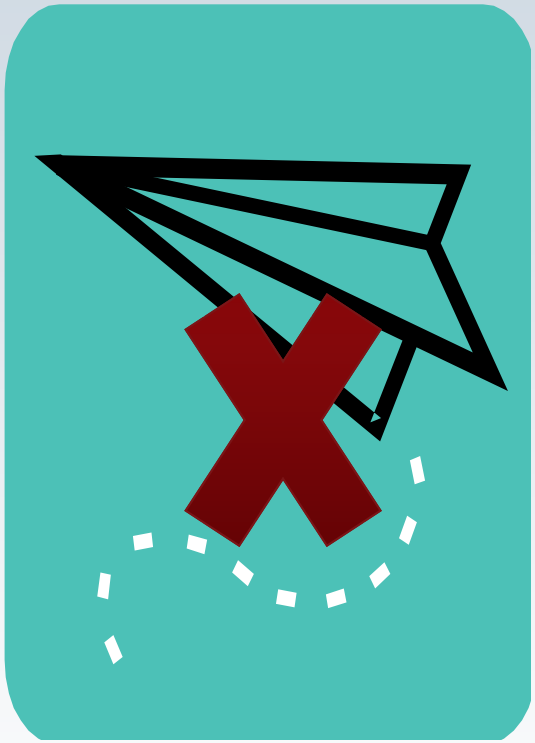
Start Small

- which areas do you have the buy in and try a specific process (maybe banking since easy to get online statements, maybe billing if your software can attach billing detail to it…)
- While vast segments of the finance function have gone electronic, accounts payable remains one of the last to convert. Per IOMA, they call this the “paper tsunami.” (Don’t do AP first, do something small and you can get your arms around)
- **It can be as simple as taking the paperless concepts you already embrace in your personal life** (e.g. online bank statements, credit card statements) and employing that same mindset to your office.
- Maybe you like the idea of adding a second computer monitor to help cut down the number of documents you print.



The "Paperless Plan" (cont'd)

- **Document the Process**
  - Document the workflow processes from beginning to end so you know how you want it to look and be done (this will be great for laying out the internal controls)
  - Include Records Retention Policy & Clean up the hard copies for each area as you go through the process
- **Go Gradual**
  - devise a timeline, include meetings, followup, pros, cons on each process
- **Perform Annual Audits on each Paperless Process**
  - Review to make sure documentation is in line with actual process, savings, costs, efficiencies, inefficiencies



Best Practices around Financial Areas

- ***Clinging to paper, inflates invoice processing costs, ups payment errors and increases the chances of payment fraud. You may miss opportunities to take early payment discounts, miss payment deadlines completely, incurring late fees. All this ties up cash when it could be put to better use growing the organization or spending on program expense.***

- **Accounts Payable**
  - scan invoices, attach to check requests, ability to route check requests for approval electronically…
  - Dual check signers don't need to be in the same building or even same city to approve checks…
- **Accounts Receivable**
  - scan invoices, backup; send documents via email instead of snail mail…
- **Banking**
  - Online access, EFTs, ACHs, check scanners instead of running to the bank…
- **Payroll**
  - Online timesheets & approval system…

Current Trends

- **Implementing Software**
  - Cloud-Based Accounting System
    - ◊ Attach supporting documentation for Journal Entries, Accounts Payable, Accounts Receivable, Banking
    - ◊ Typically web-based systems are hosted at top tier data warehouses with IT infrastructure comparable to Fortune 100 companies. Many of these companies provide everything from onsite back-ups to disaster recovery plans. This is a much more effective storage facility than rooms full of filing cabinets with no backup.
  - Writing, Editing and Office Work
    - ◊ Leverage Adobe and Microsoft Software, users can mark up doucments and add notes just like you would on paper.
  - 3rd Party Storage Sites VS Document Management Systems VS Network Tree/Folder Structure (and everything in between)

- **Multiple Computer Monitors**
  - makes research, drafting, and review much more efficient

- **Office Floor Copier/Scanner vs Individual Desktop Scanners**

Current Trends (cont'd)

- **Due Diligence**
  - Use a 3rd Party, talk to your Auditor or another Consultant, get references from Organizations your size… Do the Research
  - Does the software have the appropriate documentation to provide to the auditor that the process has the appropriate internal controls, backup, security

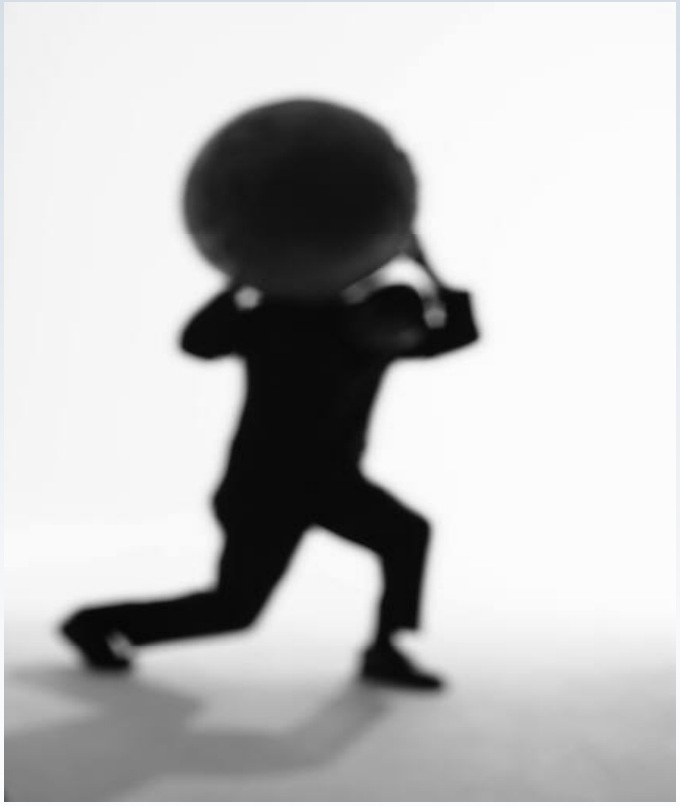
- **Costs**
  - Fixed or variable costs, upgrades, man hours…
  - Many web-based software companies spread out the cost among many clients, offering pricing and features that small to midsize businesses normally couldn't afford.
  - Learning how to markup and share a word document costs nothing but a few minutes of time through a self-directed tutorial.

“Going Paperless” - Pitfalls

- What if your boss is not about **changing** something if it isn’t broken
- Planning & spending **upfront time** to make sure things go as planned
- **Network & Software capabilities**
- **Hard costs** related to going paperless

“Going Paperless” – is this for you…

We are all creatures of habit and this can seem like an overwhelming process. Just remember, going paperless doesn’t have to mean a complete overhaul of your world.



Network Security – Doing Business Safely

- Emerging & Continuing Trends
  - Three Security Reports
  - 10 Years of Information Security Audit, Assurance, and Incident Response
- Solutions to Common Problems

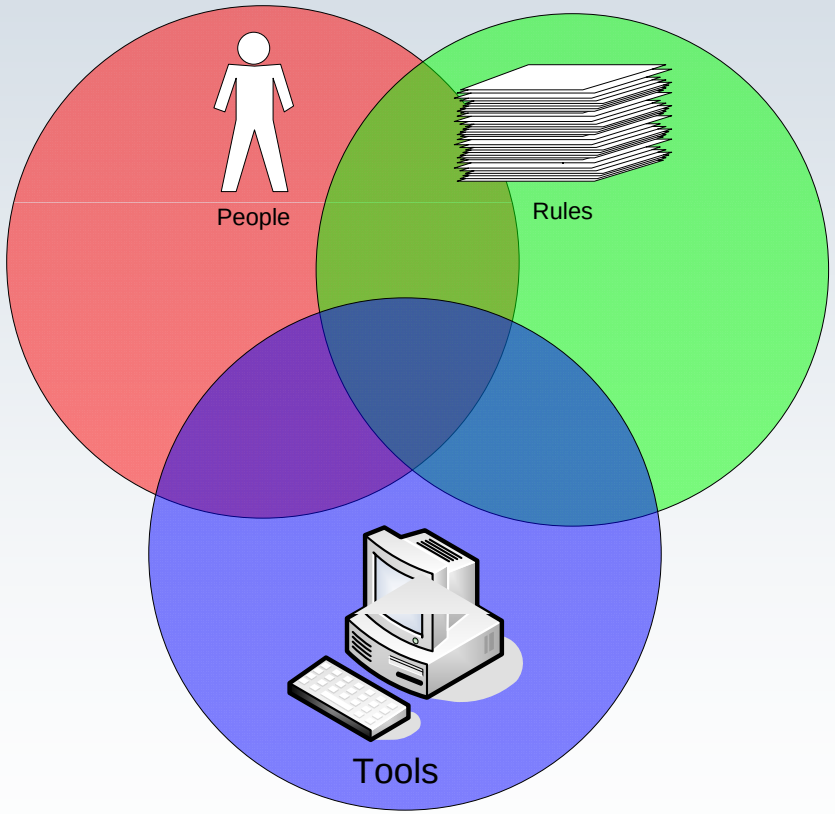
Three Reasons Why We Should Care

- Organized Crime
  - Wholesale theft of personal financial information
- Payment Fraud
  - Use of online credentials for ACH and wire fraud
- Regulatory and industry requirements:
  - PCI, HIPAA/HITECH, FFIEC, GLBA, State Laws, ISO (this list is not getting smaller…)
  - http://net.educause.edu/ir/library/pdf/CSD5876.pdf

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



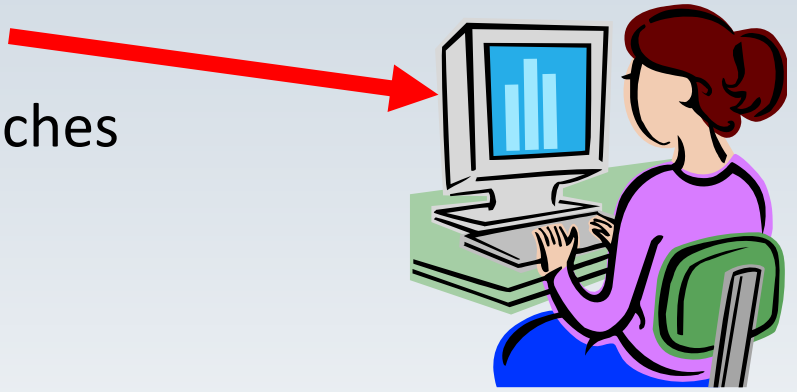
- Confidentiality
- Integrity
- Availability

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

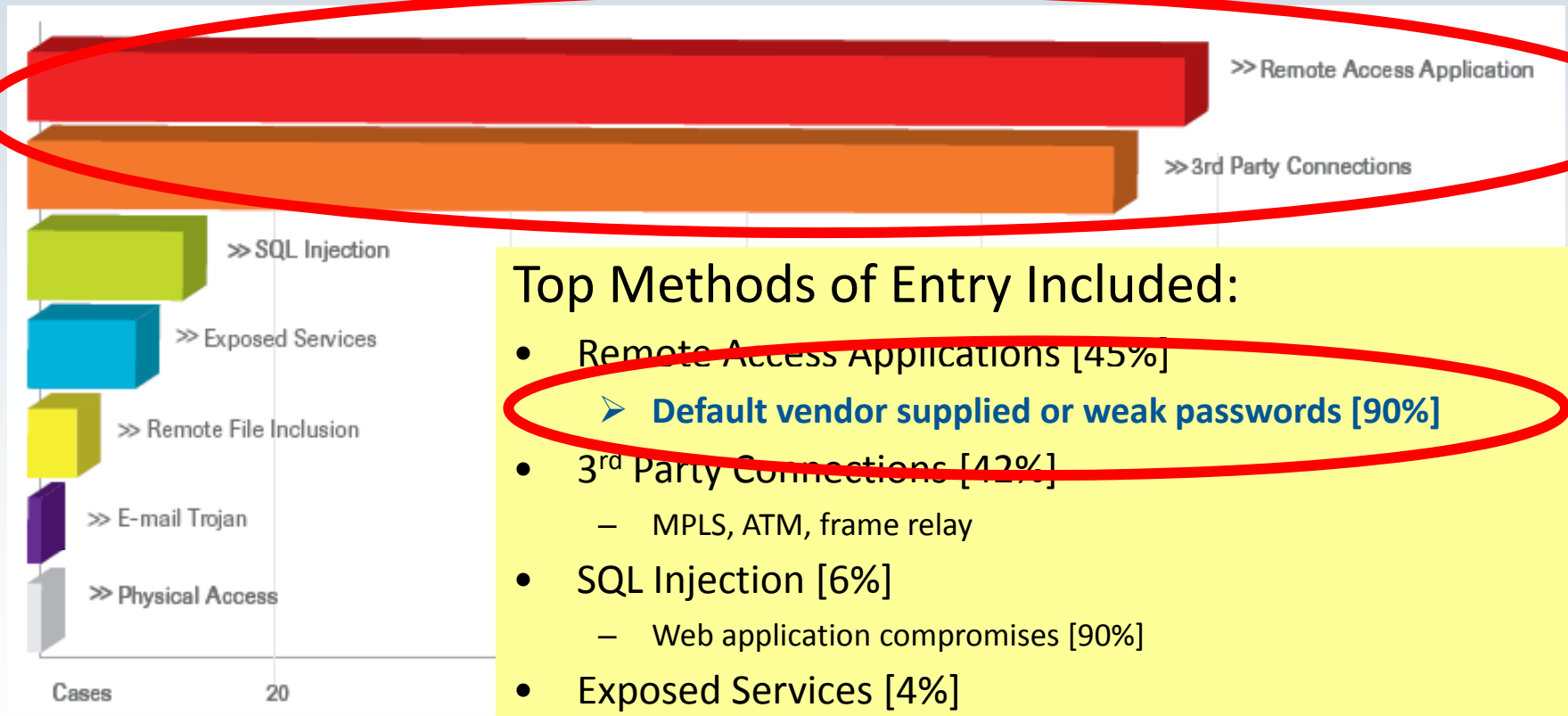
- Client side vulnerabilities
  - Missing operating system patches
  - Missing application patches
    - ◊ Apple QuickTime
    - ◊ Java Vulnerabilities
    - ◊ MS Office Applications
    - ◊ Adobe Vulnerabilities (PDF, Flash, etc…)



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

TrustWave – Intrusion Analysis Report

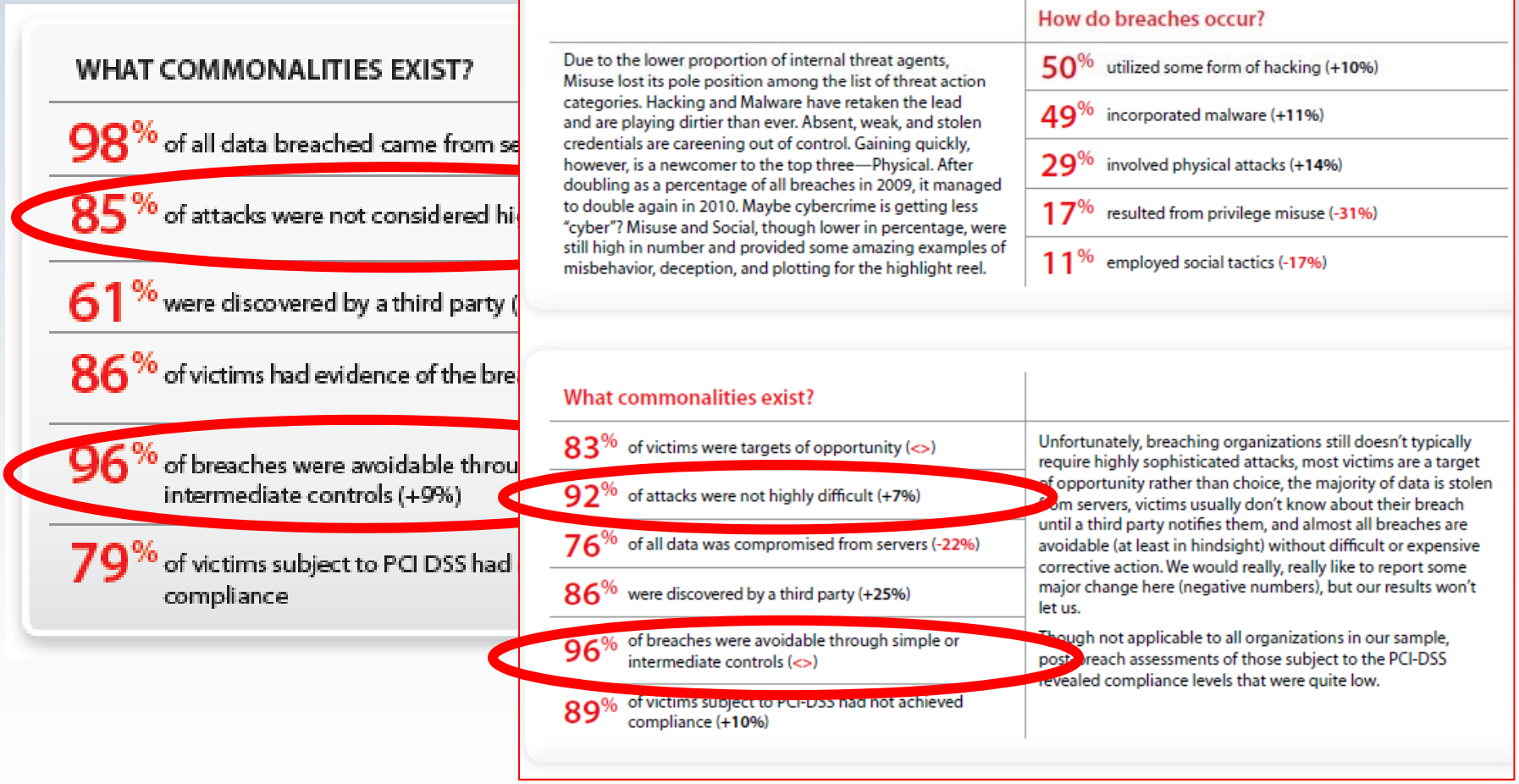
Top Methods of Entry Included:



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%]

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

How do breaches occur?

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.

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

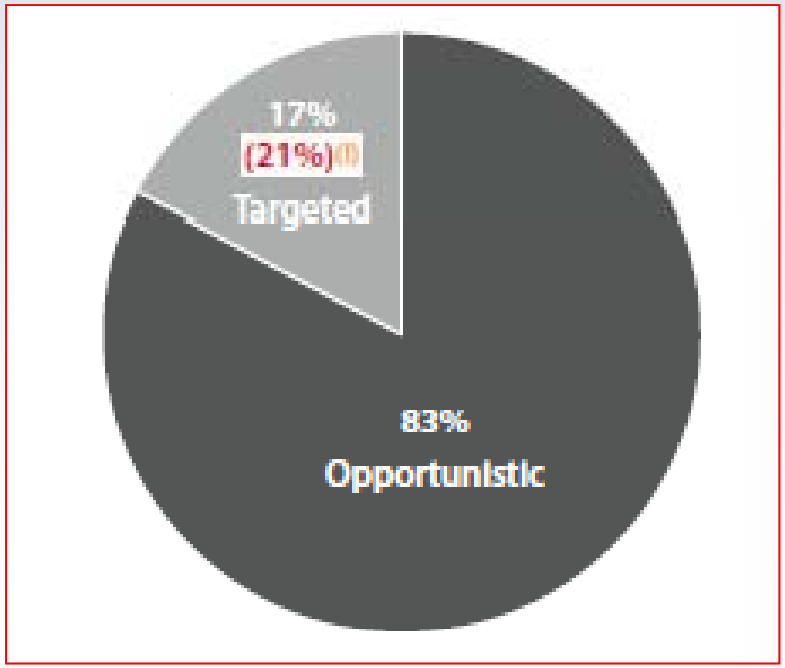


Table 6. Types of external agents by percent of breaches within External

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

How do hackers and fraudsters break in?

- Social Engineering
- Email Phishing
  - "Spear Phishing"
- On-line banking trojans

The fine art of “People Hacking”

- Social Engineering
  - What is it?

- Social Engineering uses non-technical attacks to gain information or access to technical systems
  - Examples abound in the following movies:
    - ◊ Catch Me If You Can
    - ◊ Oceans 11

Pre-text Phone Calls

- "Hi, this is Randy from Comcast. I am working with Mike, and I need your help…"
  - Name dropping
  - Establish a rapport
  - Ask for help
  - Inject some techno-babble
  - Think telemarketers script

- Home Equity Line of Credit (HELOC) fraud calls
- Recent string of high-profile ACH frauds

How do hackers and fraudsters break in?

Social Engineering relies on the following:

- People want to help
- People want to trust
- The appearance of “authority”
- **People want to avoid inconvenience**
- **Timing, timing, timing…**

Physical (Facility) Security

Compromise the site:

- "Hi, Joe said he would let you know I was coming to fix the printers…"

Plant devices:

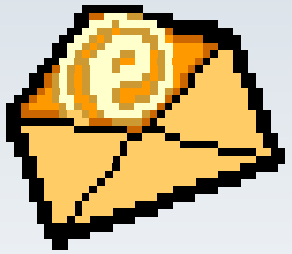
- Keystroke loggers
- Wireless access point
- Thumb drives ("Switch Blade")

Examples…
Steal hardware (laptops)

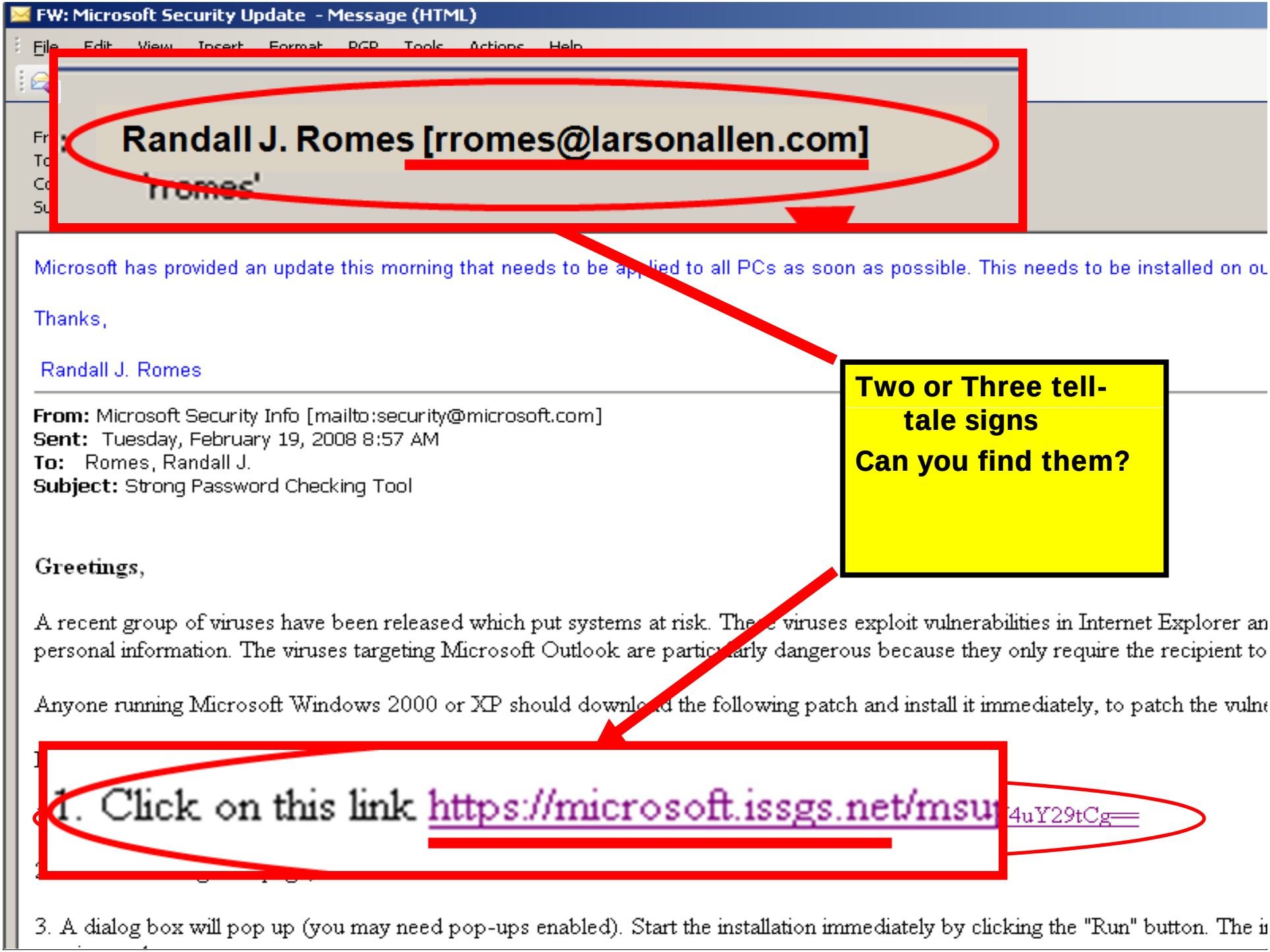
http://www.sptimes.com/2007/10/28/Business/Here_s_how_a_slick_la.shtml
http://www.privacyrights.org/ar/ChronDataBreaches.htm

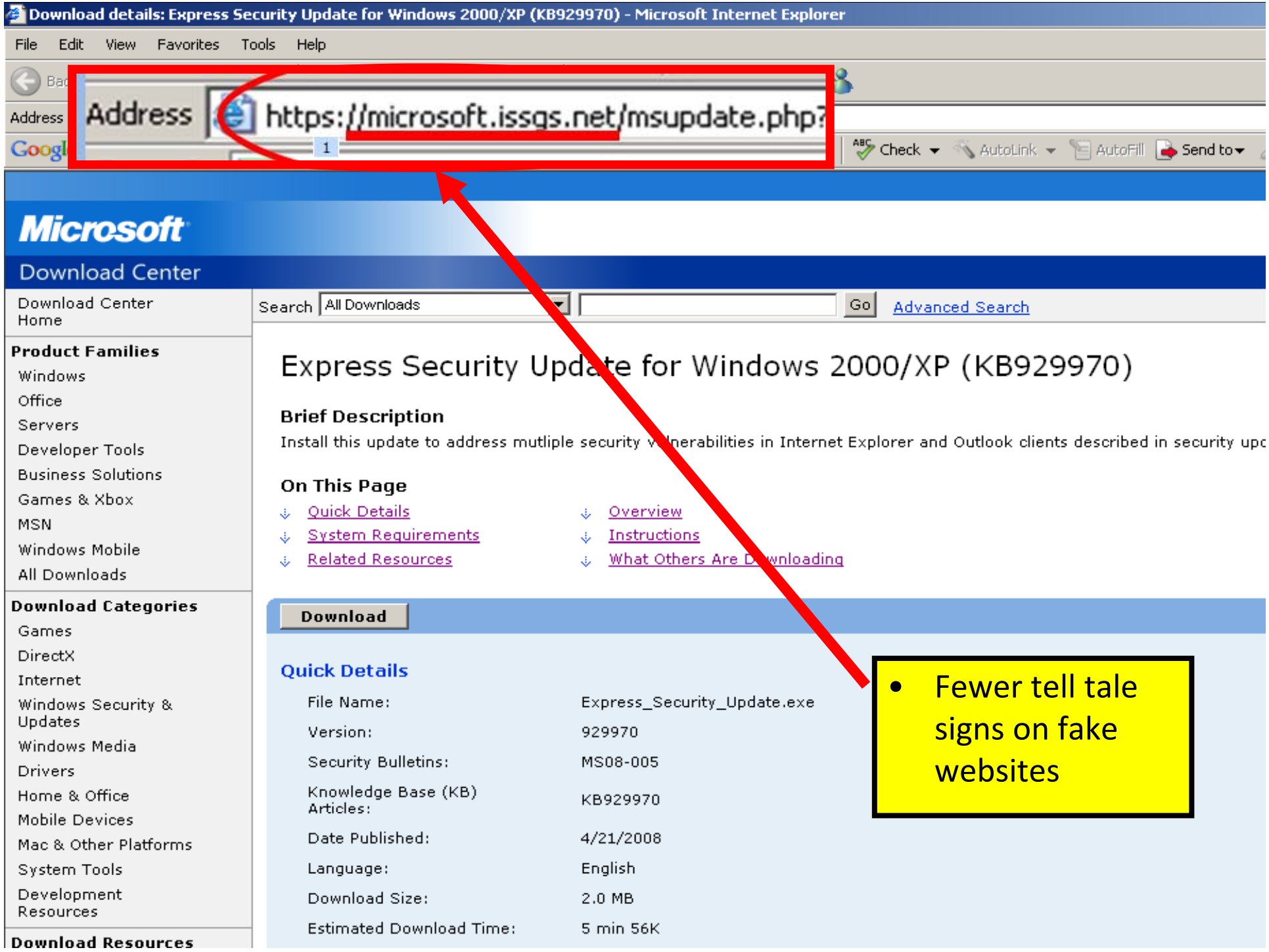
Email Attacks - Spoofing and Phishing

- 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://scmagazine.com/us/news/article/660941/better-business-bureau-target-phishing-scam/
  - Microsoft Security Patch Download
  - http://www.scmagazine.com/us/news/article/667467/researchers-warn-bogus-microsoft-patch-spam/


FW: Microsoft Security Update - Message (HTML)
File Edit View Insert Format PGP Tools Actions Help
Randall J. Romes [rromes@larsonallen.com]
rromes'
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
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

Online Banking Trojans

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

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

Nine Things Every Organization Should Have

1. **Strong Policies – Define what is expected**
   - Foundation for all that follows…
   - http://wickapedia.net/ or www.google.com ….
2. Defined user access roles and permissions
   - Principal of minimum access and least privilege
   - **Users should NOT have system administrator rights**
   - Why this is important…
   - Don't forget your vendors

Nine Things Every Organization Should Have

3. Hardened internal systems (end points)
   - Hardening checklists
   - Turn off unneeded services
   - **Change default password**
4. Encryption strategy
   - Email
   - Laptops and desktops
   - Thumb drives
   - **Email enabled cell phones**
   - Mobile media

Nine Things Every Organization Should Have

5. Vulnerability management process
    - Operating system patches
    - **Application patches**
    - Testing to validate effectiveness

Nine Things Every Organization Should Have

6. Well defined perimeter security layers:
   - **Network segments**
   - Email gateway/filter
   - Firewall – “Proxy” integration for traffic in AND out
   - Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)
7. **Centralized audit logging, analysis, and automated alerting capabilities**
   - Routing infrastructure
   - Network authentication
   - Servers
   - Applications

Nine Things Every Organization Should Have

8. Defined incident response plan and procedures
   - **Be prepared**
   - Including data leakage prevention and monitoring
   - Forensic preparedness
9. **Validation that it all works the way you expect (remember the definition?)**
   - IT Audits
   - Vulnerability Assessments
   - Penetration Testing
   - A combination of internal and external resources

Questions?

Go Paperless, Go Green

CliftonLarsonAllen

Thank you!

Mark Eich, Partner

Information Security Services Group

mark.eich@cliftonlarsonallen.com

***

Kelly Kienholz, Manager

Nonprofit Outsourcing Solutions

kelly.kienholz@cliftonlarsonallen.com