

Fraud Scenarios and IT Control Strategies



FGFOA Conference
June 28, 2011

Slides are available here:
[http://www.larsonallen.com/Information_Security/
Presentations](http://www.larsonallen.com/Information_Security/Presentations) link/button on lower left.

Presentation overview

- Cub Scouts, IT Professionals, and Computer Hackers
- Emerging & Continuing Trends
 - Industry Security Reports
- Examples of IT Related Fraud
- Strategies and Key Controls



LarsonAllen – Randy Romes

- Randy Romes
 - Professional Student
 - Pizza Guy
 - High School Science Teacher
 - Hacker
 - Dad



Cub Scouts, IT Professionals, & Hackers

- Cub Scouts
 - Be Prepared
 - Camping Trip
Preparation
 - Road Trip!!!



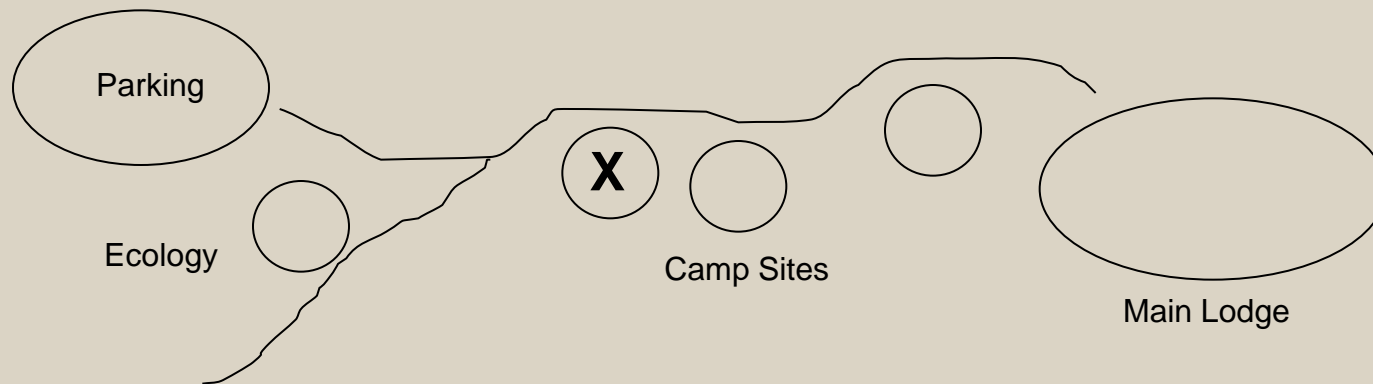
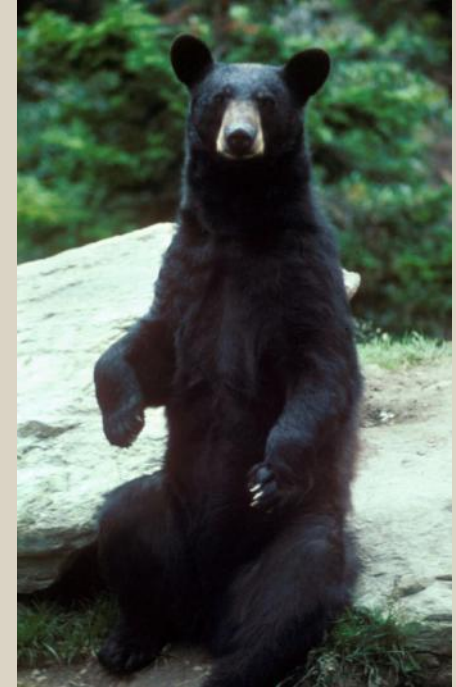
Cub Scouts, IT Professionals, & Hackers

- Cub Scouts
 - Camp Tomahawk
 - Daily Routine
 - Business as Usual...



Cub Scouts, IT Professionals, & Hackers

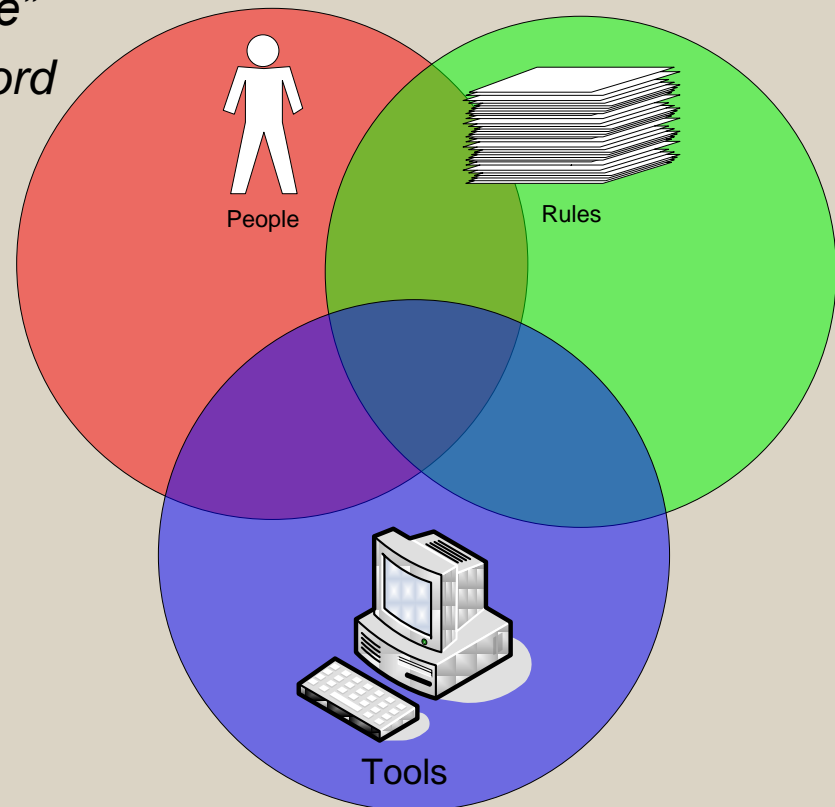
- Cub Scouts
 - Monday Morning...
 - NOT Business as usual...



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
 - <http://www.sans.org/top-cyber-security-risks/>
- Intrusion Analysis: TrustWave (2010)
 - <https://www.trustwave.com/whitePapers.php>
- Intrusion Analysis: Verizon Business Services
 - 2010 report
 - http://www.verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf
 - 2011 report
 - http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf



SANS – Client Side Vulnerabilities

- Client side vulnerabilities
 - Missing operating system patches
 - Missing application patches
 - Objective is to get the users to “Open the door”
- Vulnerable Web sites
 - Password guessing
 - Attacks on application interfaces with “input fields”



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%]



TrustWave – Intrusion Analysis Report

- Most of the compromised systems were managed by a third party...
- Third Party 88%
- Self managed 12%



TrustWave – Intrusion Analysis Report

- Incident Response – Investigative Conclusions
- Data exposure
 - Time from initial intrusion attempts, to successful theft of data
- Window of Data Exposure
 - Data “In Transit” 110.5 days
 - Data “Stored” 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!



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 for > 60%.
 - **Log files contained evidence** of the intrusion attempt, success, and removal of data.
 - Most successful intrusions were not considered highly difficult
 - ◇ > 40% difficulty was Low or NONE
 - ◇ > 50% moderate difficulty



Hackers, Fraudsters, and Victims

- Opportunistic Attacks 12%
- Targeted Attacks 83%



Securing The System

- “Default Open”
 - Everything On
 - Maximum permissions
- Hardening the systems
 - Turn off unneeded services
 - Change default password
 - “Minimize the attack surface”



Phone Fraud

- Pre-text phone calls



Phone Fraud

- Pre-text phone calls
- Validation
 - What to do for name dropping
 - Can't rely on caller ID
 - Procedures for "IT service calls"



Phone Fraud

- HELOC
- Begins with publicly available information
- Series of phone calls
- Puts pressure on service rep
- Gathers information
- Requests wire transfer
- The final “trick”



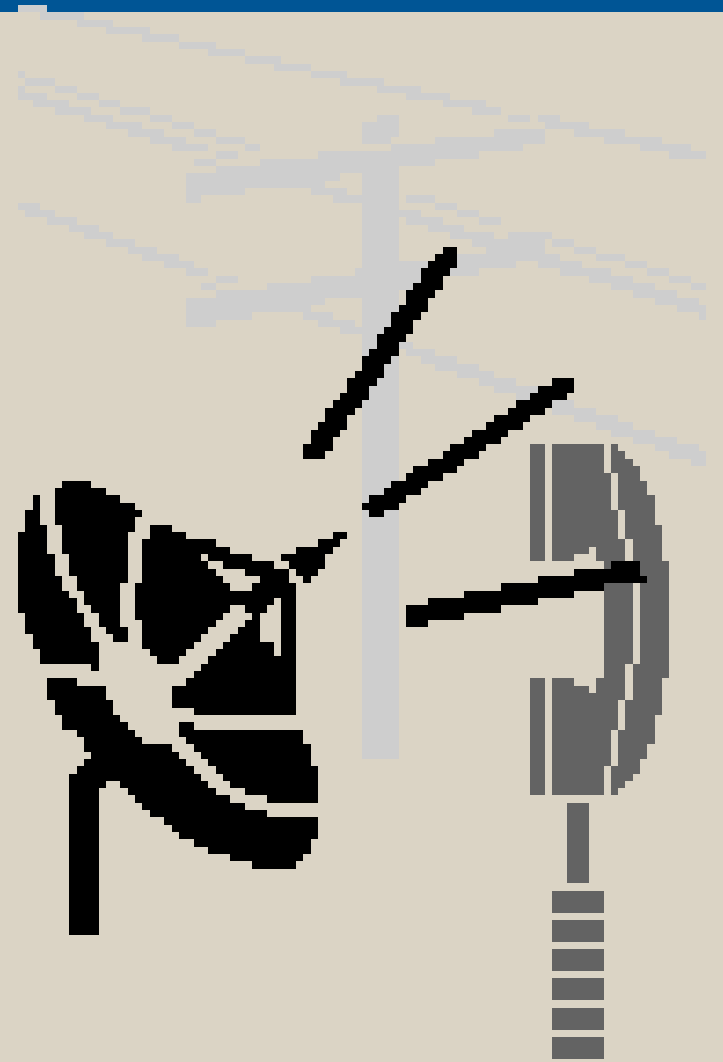
Phone Fraud

- HELOC
- Validation
 - Structured procedures
 - Specific questions to be asked and correctly answered
 - Clear escalation scenarios
- “Public documents”



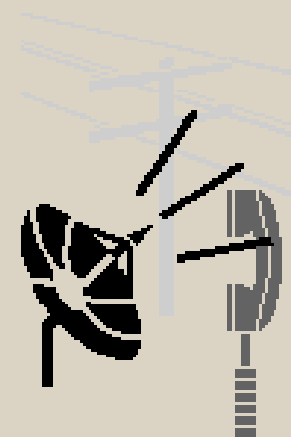
Phone Fraud

- War dialer
- Default credentials
- Default configurations (NOT hardened)
- \$\$\$



Phone Fraud

- War dialer
- Harden the phone system
 - Change default credentials
 - Implement stronger password controls
 - Disable un-needed services
 - ◇ Call forwarding
 - ◇ International calls
- Issues to consider during upgrades*



Our Website Has Been Hacked...

- Saturday morning at 8:30 AM...
- Is there “data” ... Is there “data” ... Is there “data”
 - 4th time is the charm...
- Can we get access to investigate
- Root cause(s)
- Default credentials
- Default “additional features”



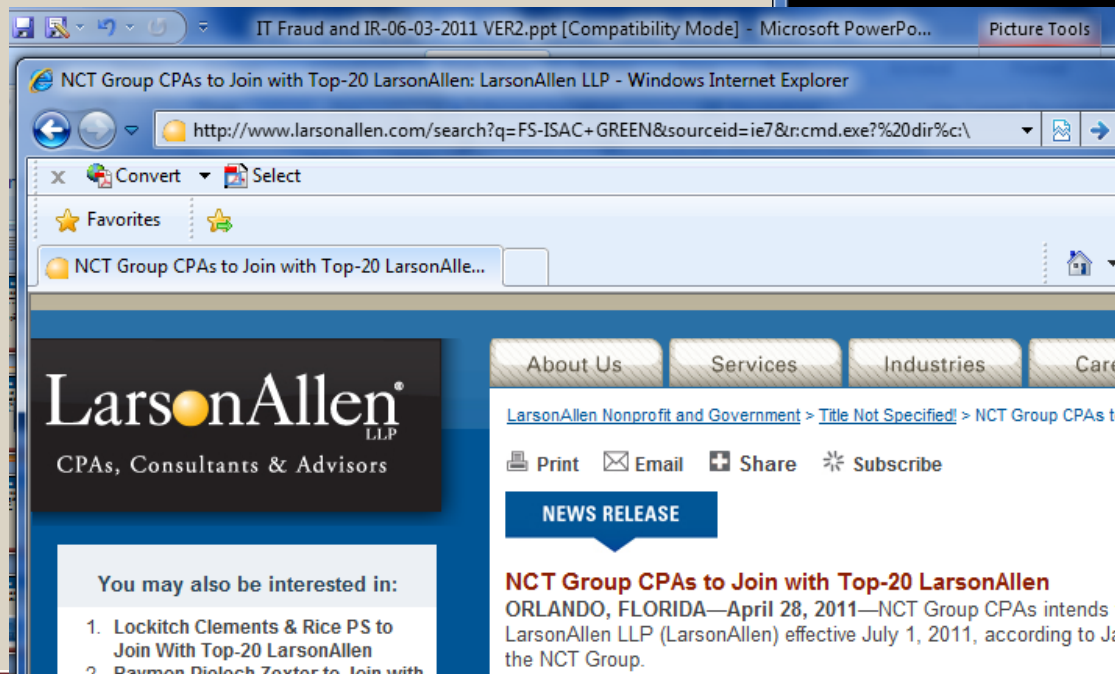
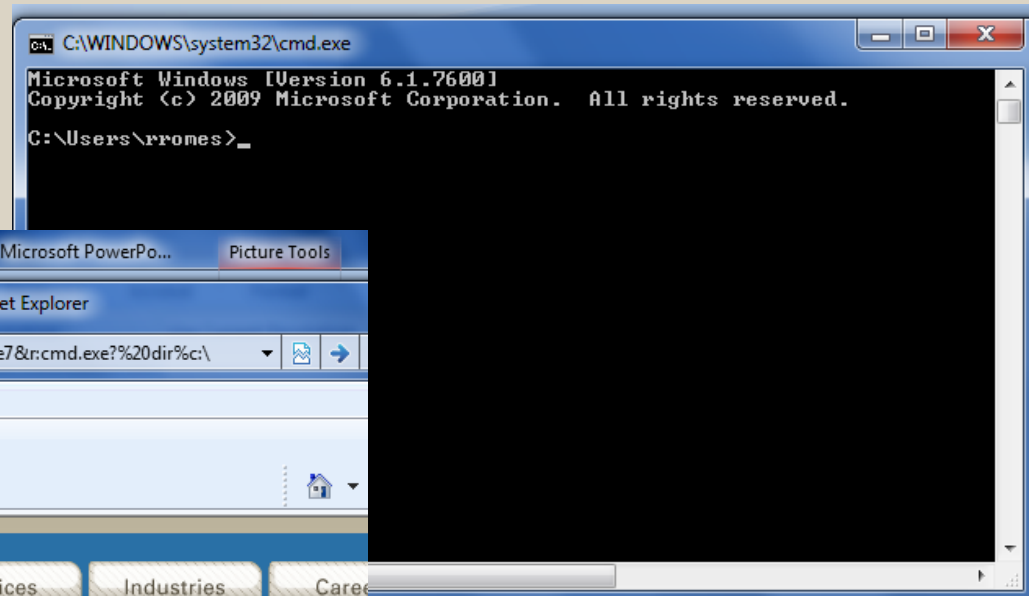
Our Website Has Been Hacked...

- Harden the web server AND applications
 - Change default credentials
 - Periodically review processes to identify high risk activities
 - Who is responsible for website? “Marketing”?
- Understand implications of lower cost solutions
- Contracts
 - Right to audit
 - Right to investigate



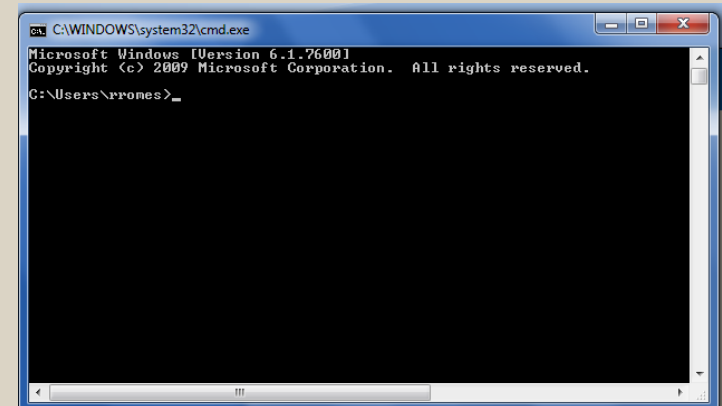
YOUR Website Has Been Hacked...

- Penetration test finds...
- Cmd.exe accessible via URL
- 18 months ago
- 8 months ago...



YOUR Website Has Been Hacked...

- Need independent investigation
- Need for independent review of IT systems
 - Book keepers don't get to choose their auditors, yet time and time again we see that IT chooses who audits them...



Credit Card Fraud

- We just received call from Visa...
- Charges in Toronto, Mexico City, and Alabama



Credit Card Fraud

- Unsecured Wireless
- Wireless on same network as POS
- Default open internal systems
 - Missing patches
 - Excessive services
 - Staff passwords
- Vendor defaults
 - Vendor passwords



ACH Fraud – In the News

Bank Sues Customer

- **\$800,000** fraudulent ACH transfer
- Bank retrieves \$600,000
- What happens to the other \$200,000?



ACH Fraud – In the News

Customer Sues Bank

- **\$560,000** fraudulent ACH transfer
- The transactions **wired funds to bank accounts in Russia, Estonia**, Scotland, Finland, China and the US and were withdrawn soon after the deposits were made.
- Also alleges that the bank failed to notice unusual activity. **Until the fraudulent transactions were made, EMI had made just two wire transfers ever; in just a three-hour period, 47 wire transfers and 12 transfer of fund requests were made.**
- In addition, after EMI 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.



ACH fraud

- Dual controls
 - Initiate wires
 - Approve wires
 - **DO NOT allow one person to perform both**
- Dedicated PCs for wire transfers
 - **DO NOT do wire transfers from home**
- Two factor authentication
- ACH positive pay
 - White list
 - Daily authorizations



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/>



From: 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

Greetings,

A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Internet Explorer and 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 vulner

1. Click on this link <https://microsoft.issgs.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 in

**Two or Three tell-tale signs
Can you find them?**

Address <https://microsoft.issgs.net/msupdate.php?>

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 [Advanced Search](#)

Express Security Update for Windows 2000/XP (KB929970)

Brief Description

Install this update to address multiple security vulnerabilities in Internet Explorer and Outlook clients described in security update...

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

Solutions

- User awareness training
- Network perimeter security layers
 - Mail filter, mail gateway, hardened workstations
 - Antivirus software (3 places) and anti-malware software
 - Minimized user access rights
 - Internet browser proxies and filtering
- Application white listing
- **VALIDATION** → Periodic testing
 - The systems
 - The people
 - The rules



Mobile media

- Recent conference



- Recent Social Engineering – night deposit box



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>



IT Procurement

- We spent several \$\$\$...
 - Hardware
 - Software
 - Services
- What do we have to show for it?
- Two examples



Incident Response

Incident Response Policy and Procedures
The Boy Scouts Motto: Be Prepared...

- **Documentation is readily available BEFORE hand**
- High Level Defined Processes
- **Well Defined and Structured Procedures**
- **Defined communication**
- Chain of command
- Escalation procedures



Ten Things Every Organization Should Have

1. Strong Policies – Define what is expected

- Foundation for all that follows...
- www.google.com

2. Defined user access roles and permissions

- Principal of minimum access and least privilege
- **Most users should NOT have system administrator rights**
- Don't forget your vendors



Ten Things Every Organization Should Have

3. Hardened internal systems (end points)
 - Hardening checklists
 - Turn off unneeded services (minimize attack surface)
 - **Change (vendor) default password**

4. **Encryption strategy (variety of state laws...)**
 - Email
 - Laptops, desktops, email enabled cell phones
 - Thumb drives/Mobile media
 - Data at Rest?



Ten Things Every Organization Should Have

5. Vulnerability management process

- Operating system patches
- **Application patches**
 - SMS and Shavlik
- Testing to validate effectiveness



Ten Things Every Organization Should Have

6. Well defined perimeter security layers:
 - **Network segments**
 - Email gateway/filter, firewall, and “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 (SIEM)**
 - Routing infrastructure
 - Network authentication
 - Servers
 - Applications



Ten 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



Ten Things Every Organization Should Have

10. Dual Controls, Segregation of Duties, ACH controls

- **Listen to those financial auditors!!!**
- Separate initiation and authorization
- Use available authentication controls and security measures
- Monitor accounts



Questions?



Thank you!

Randy Romes, CISSP, CRISC, MCP, PCI- QSA
Principal
Information Security Services
rromes@larsonallen.com
888.529.264



Slides are available here:

[http://www.larsonallen.com/Information_Security/
Presentations](http://www.larsonallen.com/Information_Security/Presentations) link/button on lower left.

Upcoming seminars:

<http://www.larsonallen.com/Calendar.aspx?TaxId=160&sort=ascending>