IT Governance

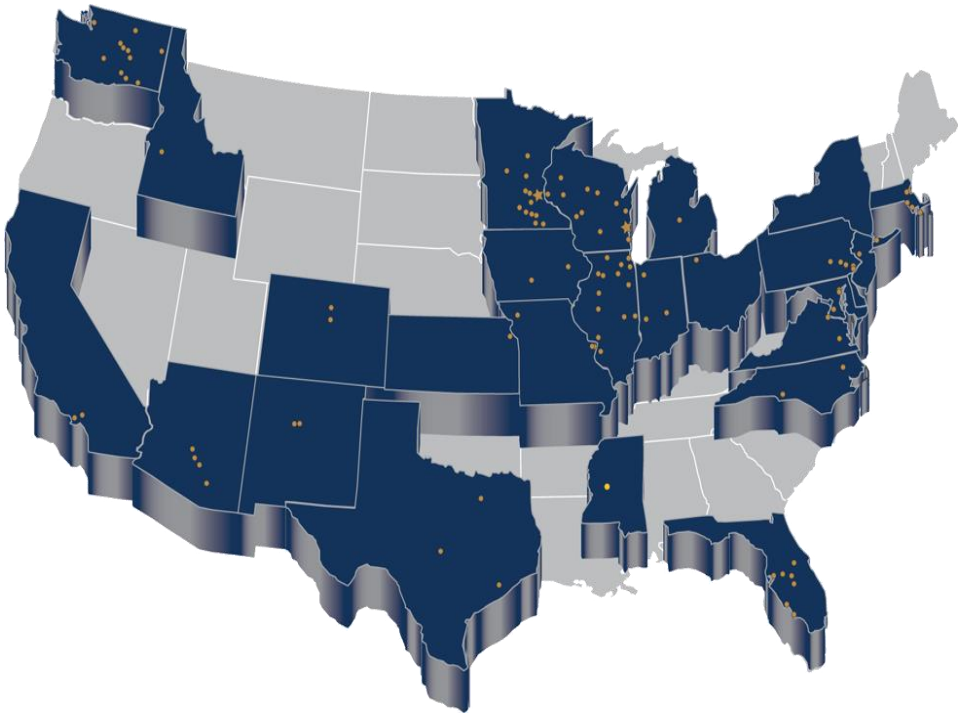
Supervisory Committee's Roles in Information Security

CliftonLarsonAllen

cliftonlarsonallen.com

Our perspective…

- CliftonLarsonAllen
  - Started in 1953 with a goal of total client service
  - Today, industry specialized CPA and Advisory firm ranked in the top 10 in the U.S.
  - Largest Credit Union Service Practice*



*Callahan and Associates 2012 Guide to Credit Union CPA Auditors.

CliftonLarsonAllen's credit union practice has recently grown to over 100 professionals including more than 20 principals. The group focuses on audit, assurance, consulting and advisory, information technology, and human resource management for credit unions across the country.
www.larsonallen.com – news release

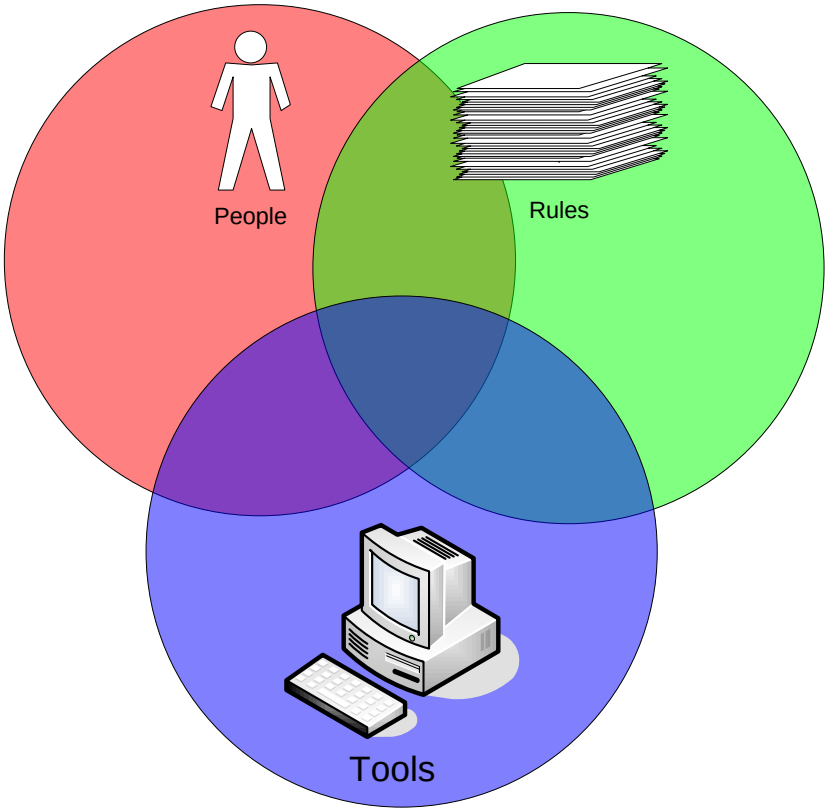
Presentation overview

- Emerging & Continuing Trends
- Social Engineering
- Mobile and Electronic Banking
- The Cloud
- Resources for Strategies and Key Controls

Security is a Business Issue

"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

Trends – SANS Report

- SANS study:

  http://www.sans.org/top-cyber-security-risks/

- Client Side Attacks
  - End user workstation (vulnerabilities)

Unpatched Applications:
- Adobe
- Java
- Apple
- Etc…
- Phishing Attacks

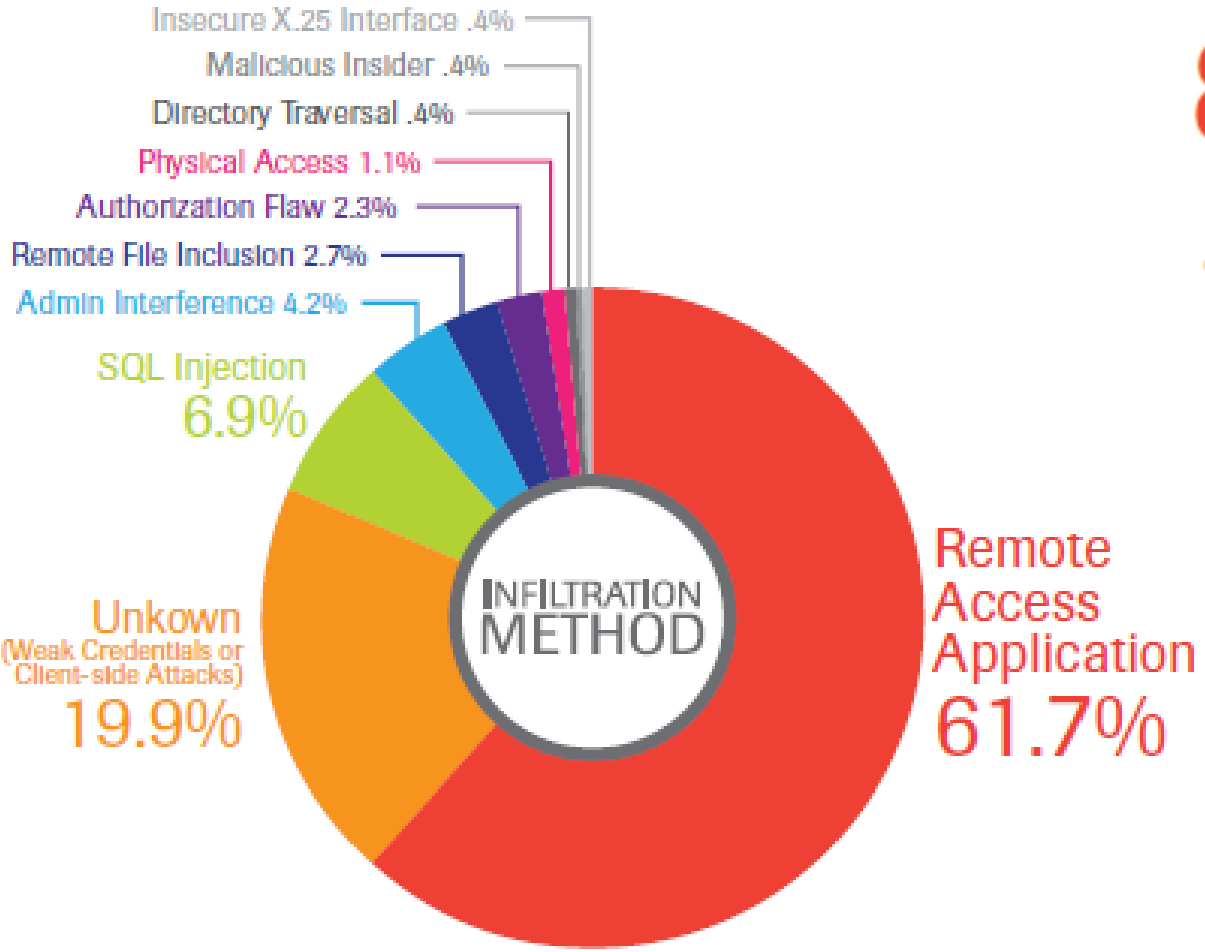
- Website - application vulnerabilities
  - Password guessing
  - Organization's web sites

Password Attacks:
FTP, SSH, Remote Access

Application Vulnerabilities:
- SQL injection
- PHP issues

TrustWave – Intrusion Analysis Report

Methods of Entry:



Methods of Propagation:

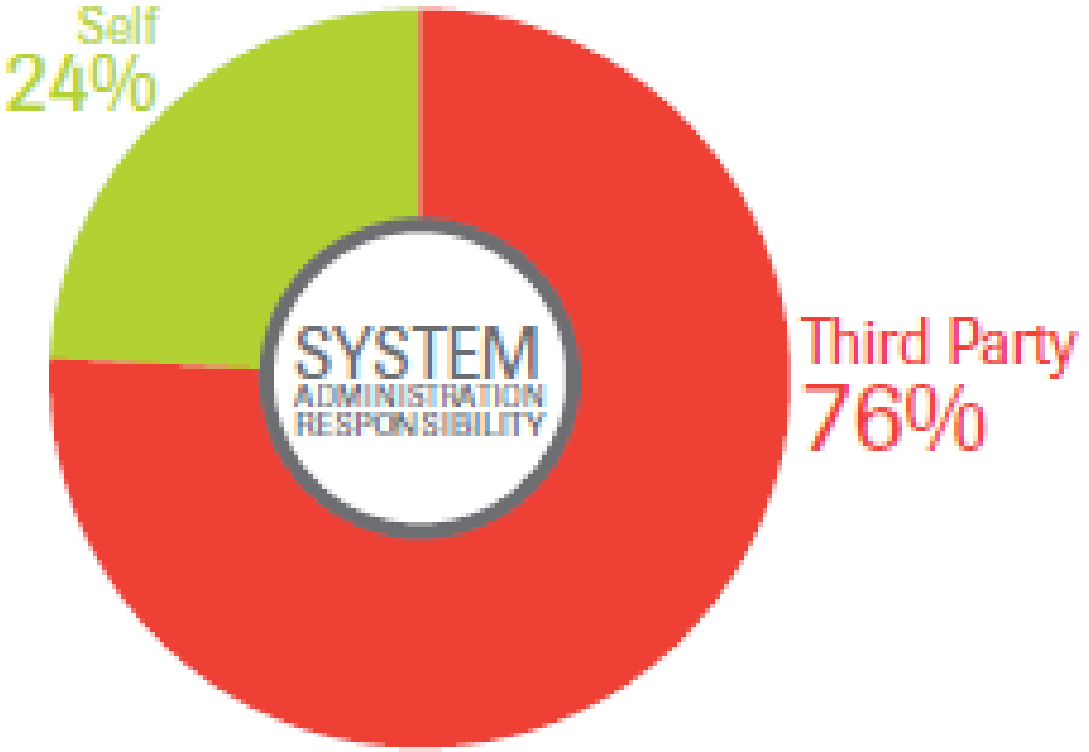
80% Use of weak administrative credentials

15% Default hidden administrative shares

5% Remote access solution credential caching

TrustWave – Intrusion Analysis Report

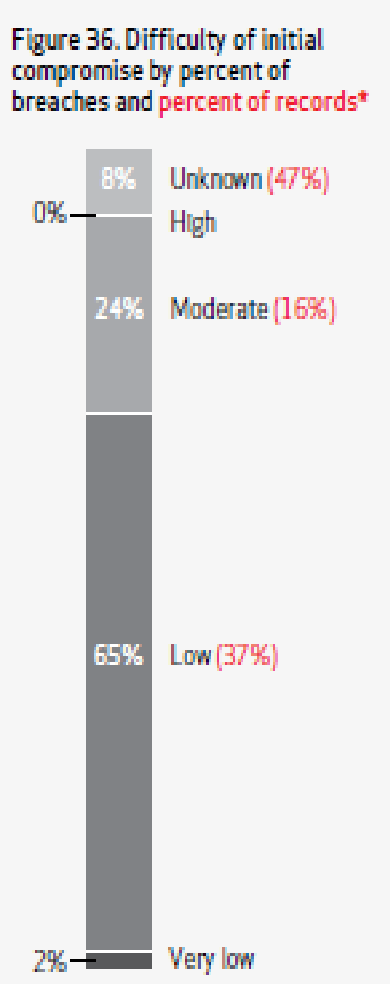
- Most of the compromised systems were managed by a third party…

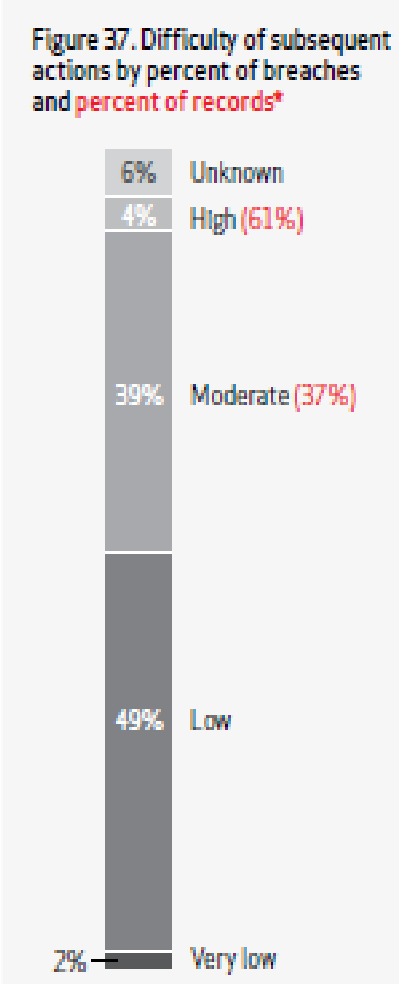


Verizon

- 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.





Hackers, Fraudsters, and Victims

- Opportunistic Attacks
- Targeted Attacks

Figure 38. Attack targeting by percent of breaches and percent of records*

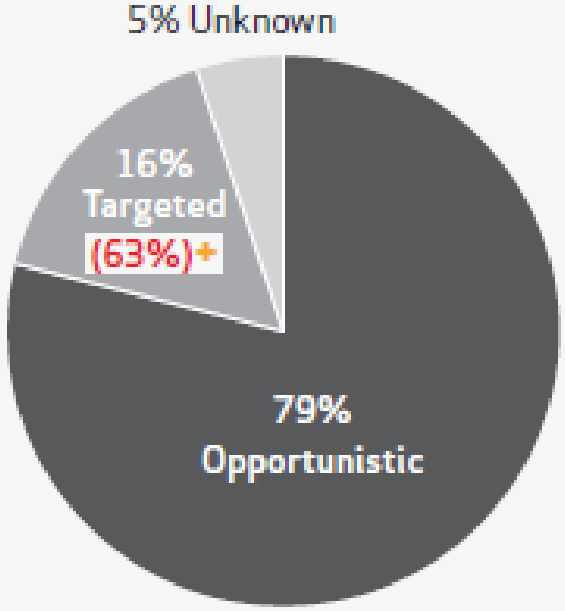


Table 5. Varieties of external agents by percent of breaches within External and percent of records

	All Orgs	
Organized criminal group	83%	35%-
Unknown	10%	1%
Unaffiliated person(s)	4%	0%
Activist group	2%	58%+
Former employee (no longer had access)	1%	0%
Relative or acquaintance of employee	0%	0%

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…**

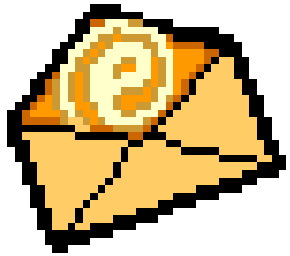
Pre-text Phone Calls

- "Hi, this is Randy from Comcast. I am working with Dave, 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

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

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

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

Strategies to Combat Social Engineering

- (Ongoing) user awareness training
- SANS "First Five"
  - Secure/Standard Configurations (hardening)
  - Critical Patches – Operating Systems
  - Critical Patches – Applications
  - Application White Listing
  - **Minimized user access rights**
- Logging and Monitoring capabilities (SIEM and DLP)
  - "The 3 R's": Recognize, React, Respond
- VALIDATION → Periodic testing
  - ➢ People, Rules, Tools, and Spaces

Mobile Devices

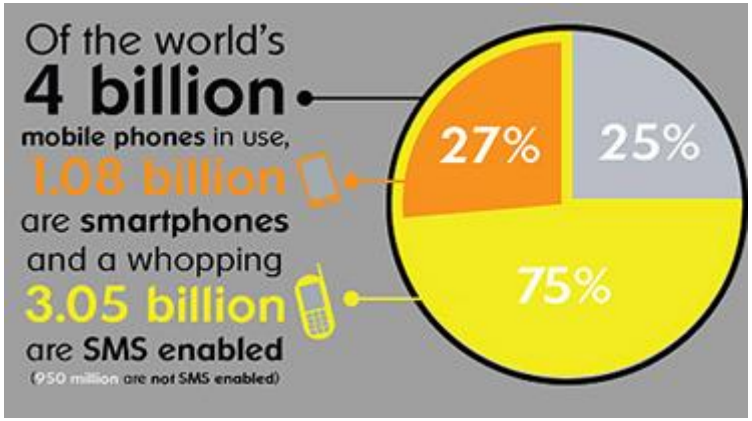
Understanding the Risks

CliftonLarsonAllen

cliftonlarsonallen.com

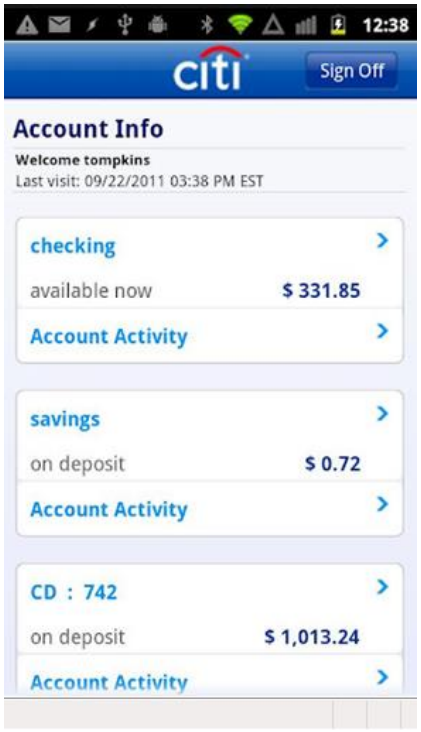
Mobile Computing Basics

- Mobile Devices are here to stay…
- More people have (smart) phones than computers
- Mobile payments are here
  - Topic for another time



Mobile Banking Basics

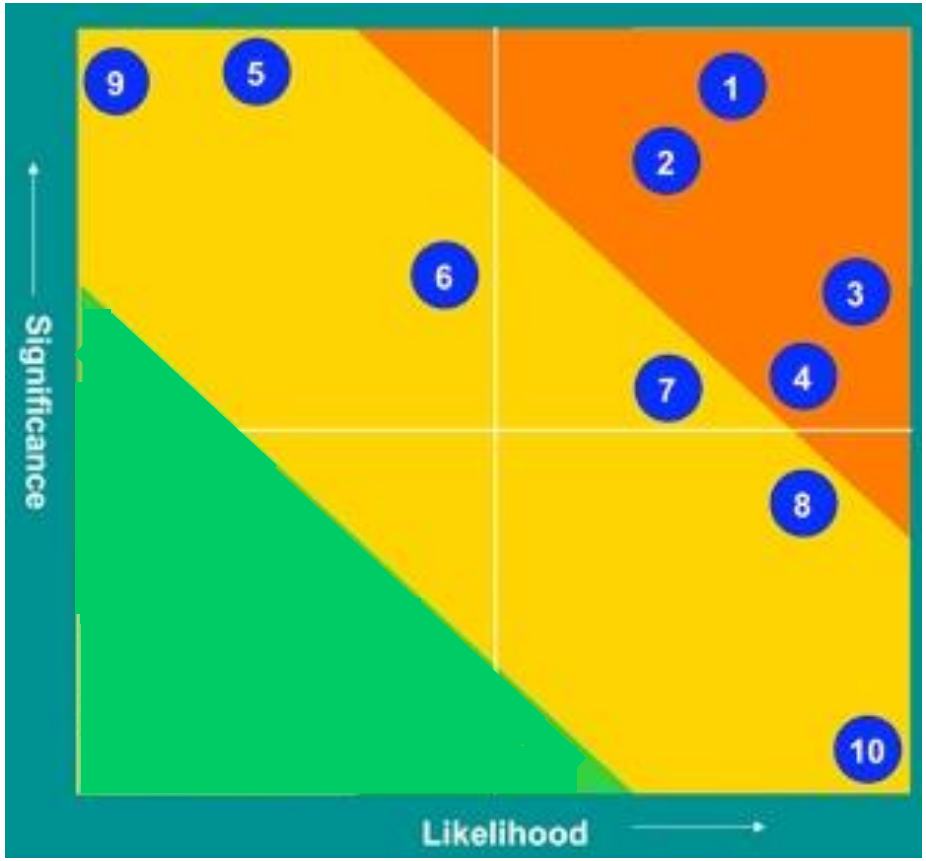
- Different types of mobile banking
  - SMS mobile banking
  - Mobile web
  - Mobile applications



Vulnerabilities, Risks, & Controls

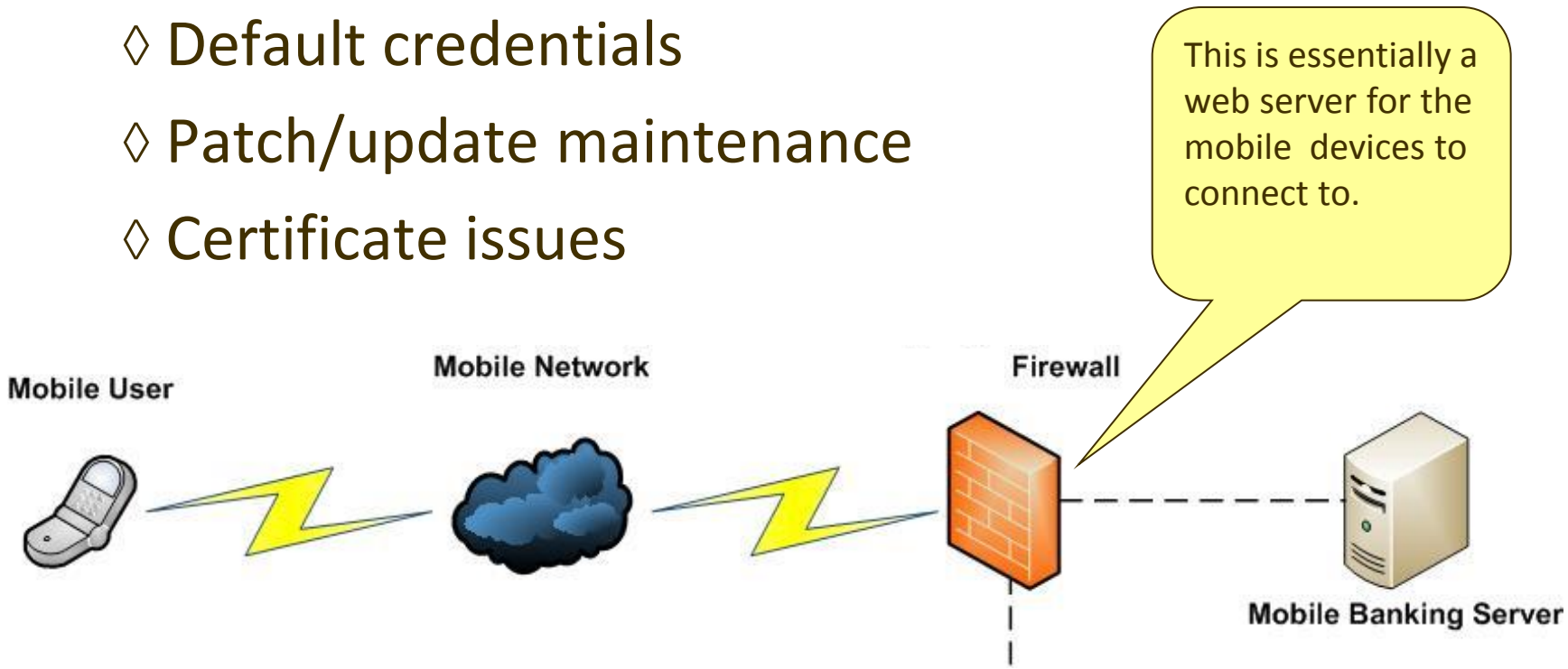
- Vulnerabilities and risks at each component
- Perform a risk assessment
  - Server Side Risks
  - (Vendor Risks)
  - Transmission Risks
  - Mobile Device Risks
  - Mobile App Risks
  - End User Risks

Risk Assessment Heat map



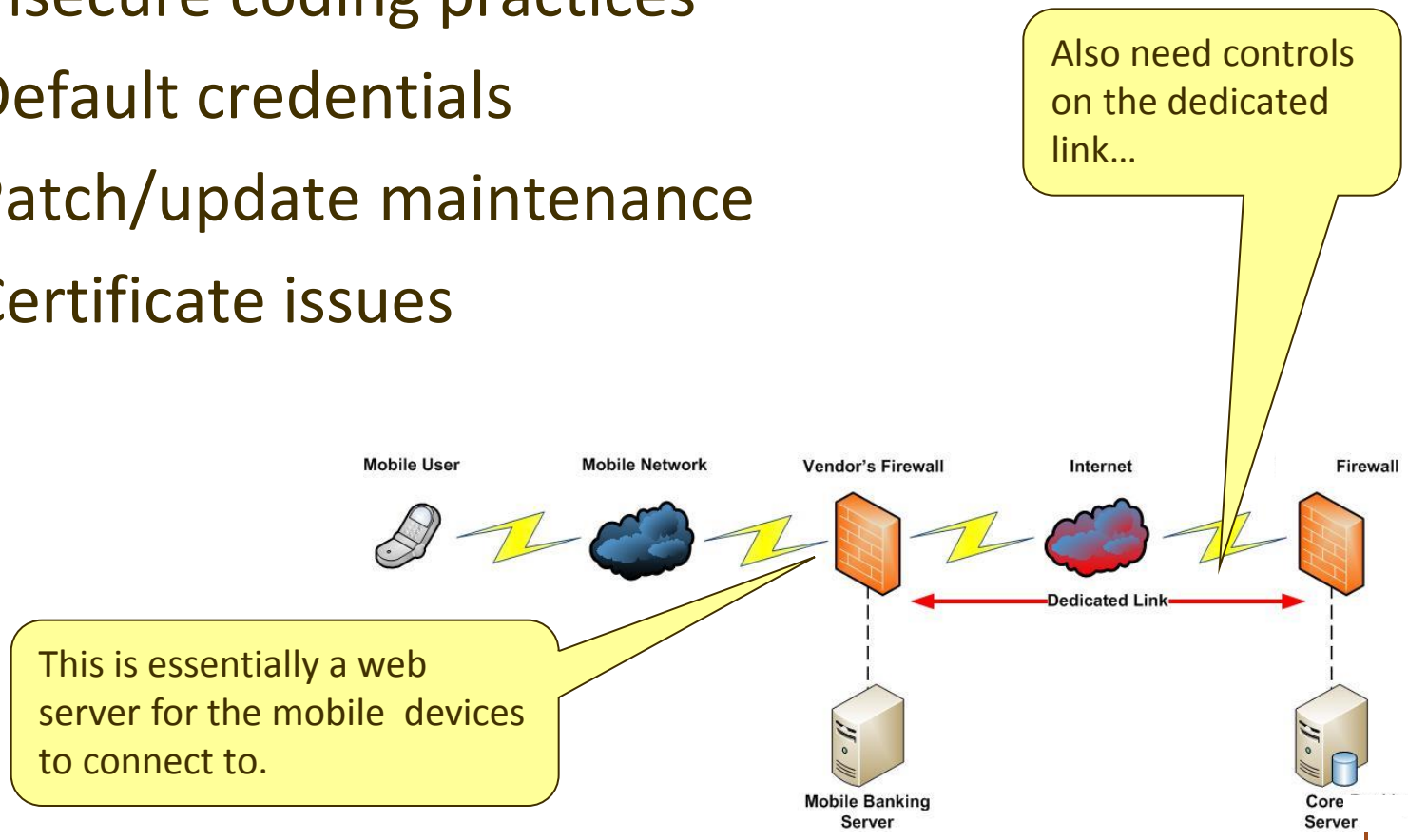
Vulnerabilities, Risks, & Controls

- **Server Side Risks** – Essentially the same as traditional Internet banking website risks
  - ◊ Insecure coding practices
  - ◊ Default credentials
  - ◊ Patch/update maintenance
  - ◊ Certificate issues



Vulnerabilities, Risks, & Controls

- **Vendor Risks** – Same risks as credit unions – now outside of your direct control.
  - ◊ Insecure coding practices
  - ◊ Default credentials
  - ◊ Patch/update maintenance
  - ◊ Certificate issues



Vulnerabilities, Risks, & Controls

- **Transmission Risks**
  - Most mobile devices have always on Internet connection
    - ◊ Cellular (cell phone service provider)
    - ◊ Wifi (802.11 – home, corporate, “public”)
  - Need encryption
  - Common end user practices

Vulnerabilities, Risks, & Controls

- **Mobile Device Risks**
  - Multiple hardware platforms & multiple operating systems

Vulnerabilities, Risks, & Controls

- **Mobile App Risks**
  - Secure coding issues
  - Installation of App
  - Use and protection of credentials
  - Storage of data
  - Transmission of data

```
1  <!DOCTYPE html PUBLIC "-//W3C//DTD
   XHTML 1.0 Transitional//EN"
2  "http://www.w3.org/TR/xhtml1/DTD/
   xhtml1-transitional.dtd">
3
4  <html xmlns="http://www.w3.org/1999/
   xhtml">
5      <head>
6          <meta http-equiv="Content-
   Type" content=
7          "text/html; charset=us-
   ascii" />
8          <script type="text/
   javascript">
9              function reDo() {top.
   location.reload();}
10             if (navigator.appName ==
   'Netscape') {top.onresize = reDo;}
11             dom=document.
   getElementById;
12         </script>
13     </head>
14     <body>
15     </body>
16 </html>
```

Vulnerabilities, Risks, & Controls

- **End User Risks**
  - Lose the device
  - Don’t use passwords, or use “easy to guess passwords”
  - Store passwords on the device
  - Jail break the device
  - Don’t use security software
  - Use/don’t recognize insecure wireless networks
  - Let their kids “use” the device

Vendor Due Diligence and Management

- All of the above – applies to your vendor(s)
  - Mobile banking application provider
  - Mobile banking hosting provider

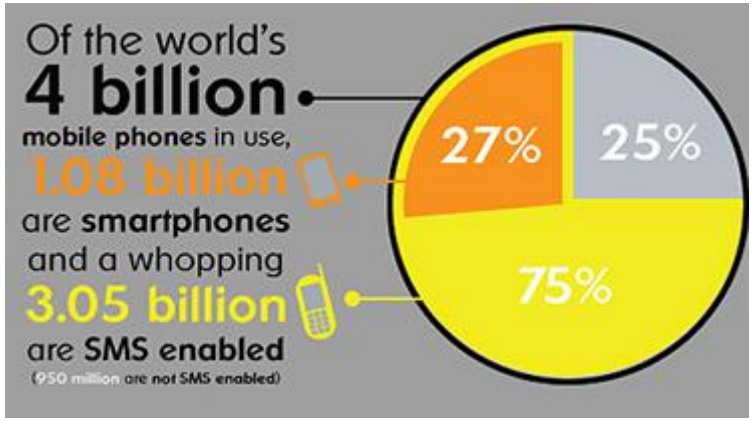
- Contracts with SLA's
- SSAE16 reviews
- Independent code review and testing

Mobile Devices

Bring Your Own Device (BYOD)

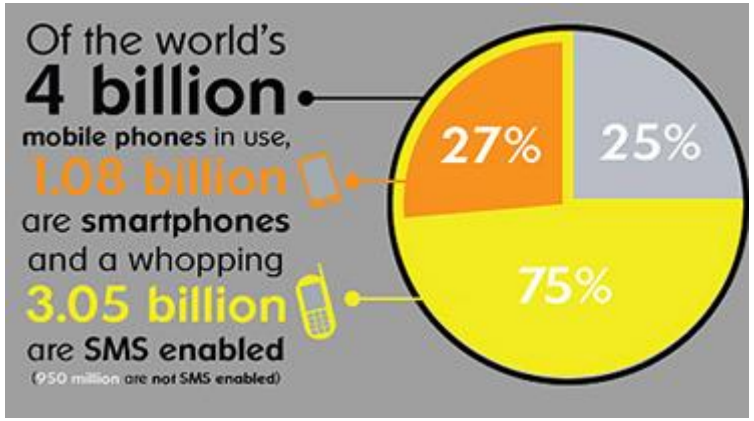
BYOD

- People, Rules, and Tools:
  - Standards
  - Data Classification
  - Acceptable Use
  - Incident Response
  - Litigation Preparedness



BYOD

- Controls and Enterprise management of:
  - Credentials
  - Login/Screen Saver
  - Encryption
  - Monitoring
  - Data Loss Prevention (DLP)
  - Remote Locate and Wipe
  - Segregation...



Risks and Controls for Electronic Banking

Phishing and ACH – In the News

Customer Sues Bank

- **$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.

Phishing and ACH – Examples

- 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
- This one was just “resolved”…

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 member base
- **Changes in the member functionality**
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

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 member**
- Technical (IT/systems) controls

Controls for Layered Security

- Control of administrative functions
- **Enhanced controls around payment authorization and verification**
  - "Positive Pay" features
  - Dual authorization
  - "Call back" verification
- **Detection and response to suspicious activity**

Controls for Layered Security (2)

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

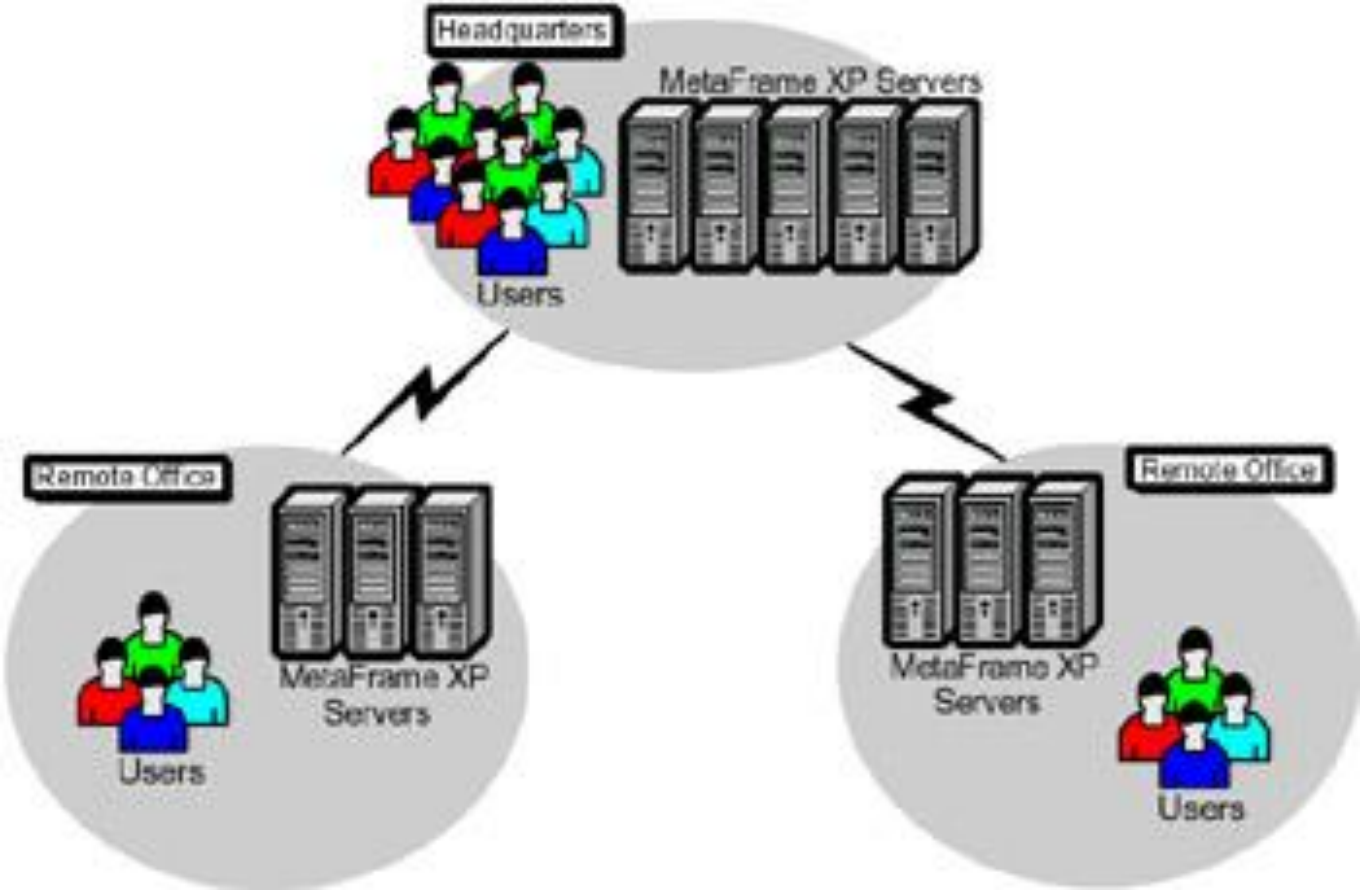
Risks and Controls for "The Cloud"

What is the Cloud?

- The original “cloud computing”: Mainframes

What is the Cloud?

- The next generation: Thin Clients (Citrix, RDP, etc…)



What is the Cloud?

- Today's cloud: Hosted service or process all the way to hosted infrastructure.

Standards Have Been In Place…

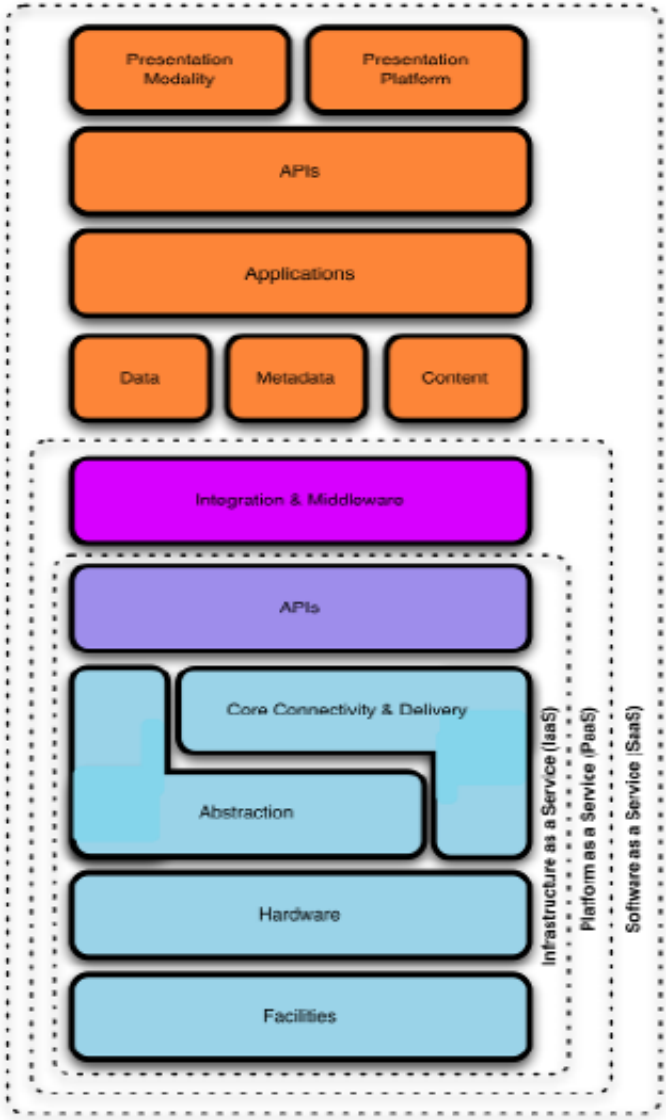
- National Institute of Standards and Technology (NIST) definition of cloud computing published October 7, 2009:

  "Cloud computing is a model for enabling convenient, on-demand network access to **a shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Three Cloud Computing Service Models

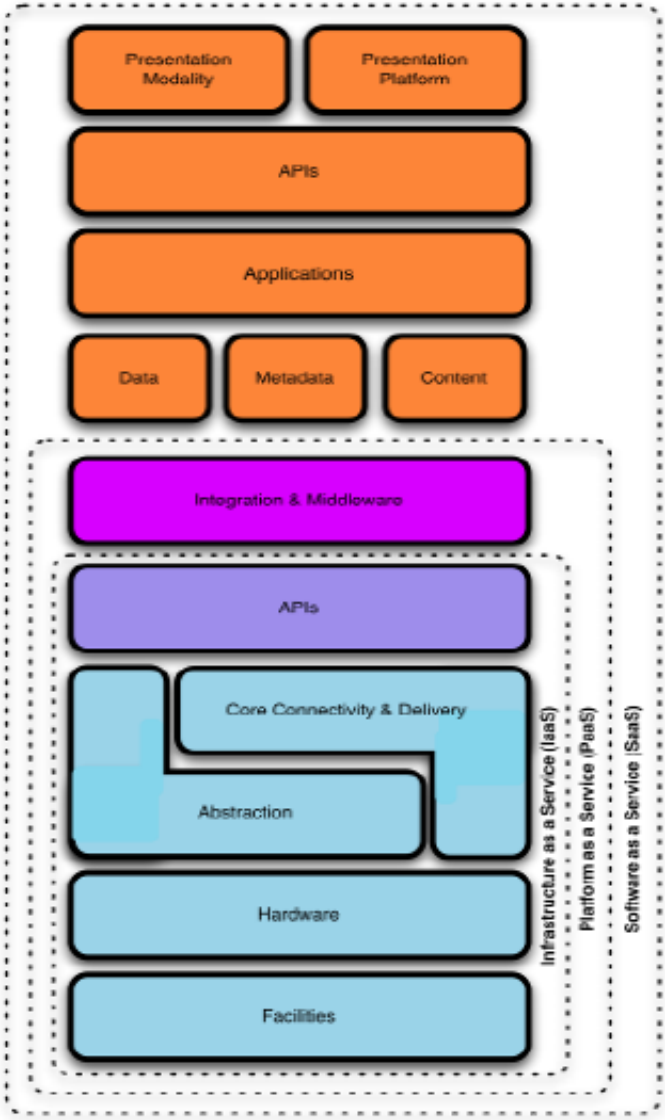
- Software as a Service (SaaS)
  - Capability to **use the provider's applications** that run on the cloud infrastructure.
- Platform as a Service (PaaS)
  - Capability to deploy onto the cloud infrastructure **customer-created or acquired applications** created using programming languages and tools supported by the provider
- Infrastructure as a Service (IaaS)
  - Capability to provision **processing, storage, networks and other fundamental computing resources** that offer the customer the ability to deploy and run arbitrary software, which can include operating systems and applications

Cloud Computing Service Models



- Cloud Computing is about "Multi-Tenancy"
  - Multi-Tenancy implies the use of the same resources or application by multiple businesses/user communities/consumers that may belong to the same organization or different organizations.

Cloud Computing Service Models



- The **KEY** takeaway for cloud architecture is that:
  - The lower down the stack the cloud service provider stops --
  - The more capabilities and management the users are responsible for implementing and managing themselves

Cloud Computing Deployment Models

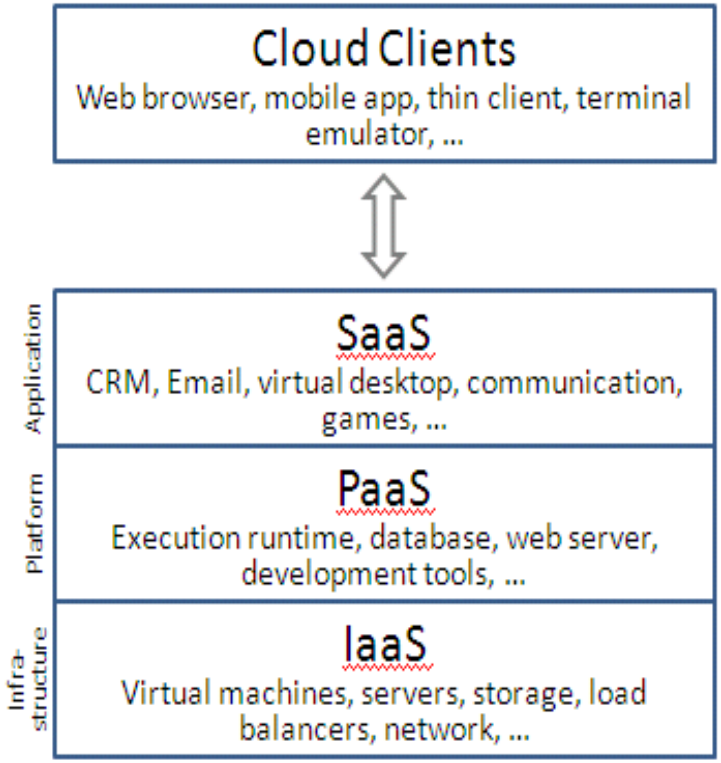
- **Private cloud:**
  - Operated solely for an organization
  - May be managed by the organization or a third party
  - May exist on or off premise
- **Community cloud:**
  - Shared by several organizations
  - Supports a specific community that has a shared mission or interest
  - May be managed by the organizations or a third party
  - May reside on or off premise

Cloud Computing Deployment Models cont.

- **Public cloud:**
  - Made available to the general public or a large industry group
  - Owned by an organization that sells cloud services
- **Hybrid cloud:**
  - Composed of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Examples of Cloud Services

- Hosted Email: Hosted Exchange, Gmail
- Hosted applications
  - Google Apps
- On-line/cloud back up services
- Hosted infrastructure
- Private Clouds



Benefits and Risks

- Cost
- Administration
- DR/BCP
- Compliance

- Vendor Risks
- Governance Risks
- Data Risks

- Who has your data?
- Where is your data?
- Who has access to your data?

Examples closer to home…

- Recent conference
  - Between sessions vendors describe their service offerings…
  - Company X offers online, secure back up to the cloud
  - Company X has grown “over 300%” in the last year
  - Best of all, Company X now provides online, secure, cloud based back up for Company Y – one of the larger Core hosting company providers

  - Where does the outsourcing chain end?
  - How many FI’s using Company Y know where their data is

What does that mean?

- Cloud computing means:
  - An increased need for good polices
  - Clear communication between the provider and the consumer of the services
  - Ownership and governance of the relationship with the provider.

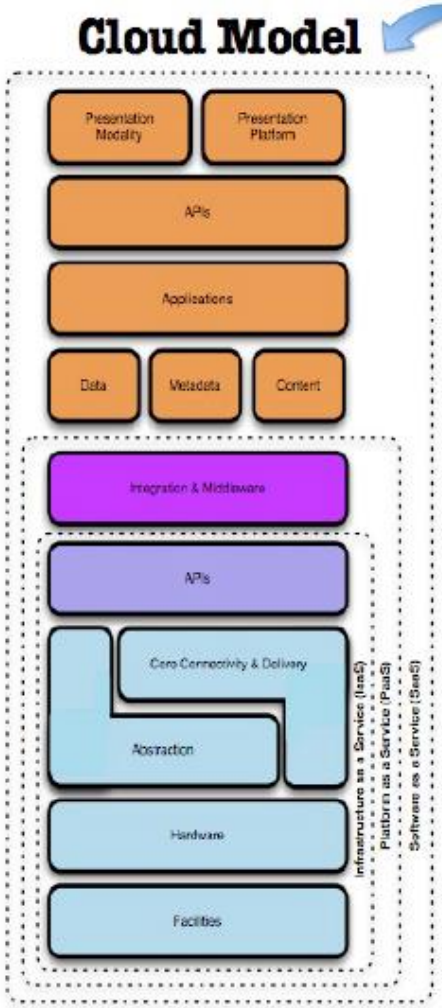
Cloud Computing Controls

- The overall control domain is the same as an in house IT environment, the challenge is to figure out who is doing what.

- Controls in the cloud computing environment may be provided by the consumer/company, the cloud service provider, or a separate 3rd party.

- SSAE 16 SOC2 report from service providers

Evaluate the Control Environment



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- Firewalls
- Code Review
- WAF
- Encryption
- Unique User IDs
- Anti-Virus
- Monitoring/IDS/IPS
- Patch/Vulnerability Management
- Physical Access Control
- Two-Factor Authentication...

HIPAA

GLBA

SOX

Risk Assessment: A Quick Approach

How does Confidentiality, Integrity, Availability change if all or part of an asset is handled in the cloud?

- Identify the Asset in the cloud
  - Data
  - Applications/Functions/Processes
- Evaluate the Asset - **How would the business be harmed or impacted if**:
  - ◊ The data became widely public and distributed
  - ◊ The provider accessed the data
  - ◊ The data or function was manipulated by an outsider
  - ◊ The function failed to provide expected results
  - ◊ The data was unexpectedly changed
  - ◊ The data or function were unavailable

Risk Assessment: A Quick Approach cont.

- Determine the Cloud Deployment Model
  - Public
  - Private, Internal / External
  - Community
  - Hybrid
- Map out the Data Flow
  - Public
  - Private, Internal
  - Private, External
  - Community
  - Hybrid

Other Considerations

- Legal issues
  - Where is the data?
  - Is it “here”? Another State? Country?
  - eDiscovery:
    - ◊ How do you identify all documents that pertain to a case?
    - ◊ Possession, Custody and Control: How do you control and make available data that is not in your own systems yet is your data?

Things to do…

- Risk Assessment
- Cost benefit analysis
- Vendor due diligence
- Scrutinize contracts
- Ongoing vendor management
- Be rigorous about where your data is
- Understand vendors responsibility and YOURS
- Remember basic security tenants

Questions?

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
Information Security Services
randy.romes@cliftonlarsonallen.com
888.529.2648

Ten Things Every Organization Should Have

1. Strong Policies – Define what is expected

- Foundation for all that follows…

Section	Control Domain
Section 1	Organization Administration
Section 2	Vendor Administration
Section 3	Technical Infrastructure Administration
Section 4	Data Administration
Section 5	Software Administration
Section 6	Application Administration
Section 7	User Account Administration
Section 8	IT Operations & Support Administration
Section 9	Physical Environment Administration
Section 10	Incident Response – Business Continuity – Disaster Recovery

Ten Things Every Organization Should Have

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

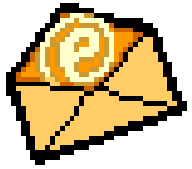
3. Hardened internal systems (end points)

- Hardening checklists
- Turn off unneeded services (minimize attack surface)
  - Turn off Telnet
  - Turn off FTP
  - Turn off SMTP…
- **Change (vendor) default password**

Ten Things Every Organization Should Have

4. Encryption strategy (variety of state laws…)

- Email



- Laptops, desktops, **email enabled cell phones**

- Thumb drives/Mobile media
- **Data at rest**

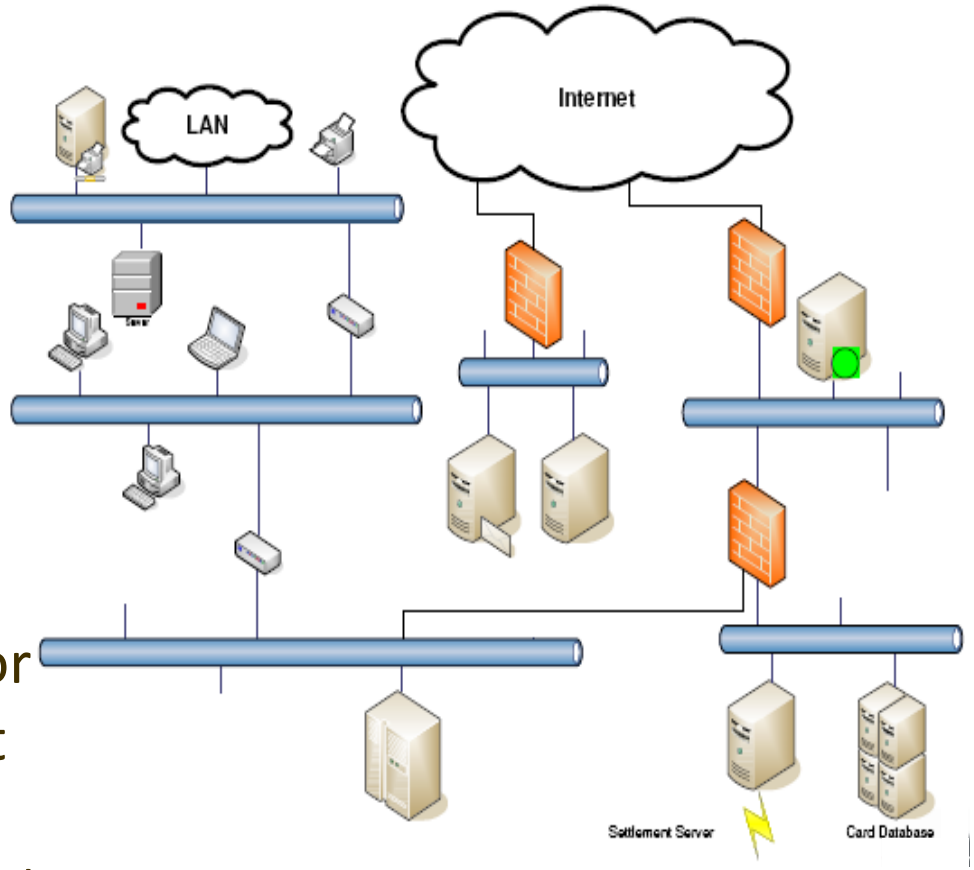
Ten Things Every Organization Should Have

5. Vulnerability management process

- Operating system patches
- **Application patches**
  - SMS and Shavlik (now owned by VMWare)
- Testing to validate effectiveness – find and address the exceptions

Ten Things Every Organization Should Have

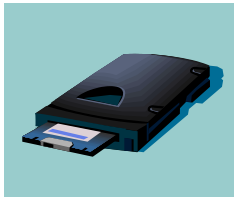
6. Well defined perimeter security layers:
   - **Network segments**
   - Email gateway/filter, firewall, and “Proxy” integration for traffic in AND out
   - Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)



Ten Things Every Organization Should Have

7. Centralized audit logging, analysis, and automated alerting capabilities (SIEM)

- Routing infrastructure
- Network authentication
- Servers
- Applications
- Archiving vs. Reviewing



Ten Things Every Organization Should Have

8. Defined incident response plan and procedures

- Be prepared
- **Documentation and procedures**
- Including data leakage prevention and monitoring
- **Incident Response testing, just like DR testing**
- Forensic preparedness

Ten Things Every Organization Should Have

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
- Pre-implementation and post-implementation

Ten Things Every Organization Should Have

10. Vendor Management

- The previous 9 topics should all be applied to your vendors/business partners
  - Require vendor systems be at least as secure as your own…
- For managed services, require vendors to agree to operate up to your standards
  - Vulnerability management
  - Secure communication protocols
  - Incident response capabilities
  - Right to audit
  - Understand your contracts and SLAs

➢ Do we have time to talk about the cloud?

“Three” Security Reports

- Trends: Sans 2009 Top Cyber Security Threats
  - http://www.sans.org/top-cyber-security-risks/
- Intrusion Analysis: TrustWave (Annual)
  - https://www.trustwave.com/whitePapers.php
- Intrusion Analysis: Verizon Business Services (Annual)
  - 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

Solutions – From SANS Report

20 Critical Controls:

- http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. **Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers**
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. **Boundary Defense**
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. **Controlled Use of Administrative Privileges**
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. **Malware Defenses**
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

Additional Critical Controls (not directly supported by automated measurement and validation):

16. Secure Network Engineering
17. **Penetration Tests and Red Team Exercises**
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Common Compliance Requirements

- Compliance Matrix Resources:

- http://net.educause.edu/ir/library/pdf/CSD5876.pdf

- http://www.infosec.co.uk/ExhibitorLibrary/277/Cross_Compliance_wp_20.pdf

Resources – Hardening Checklists

Hardening checklists from vendors

- CIS offers vendor-neutral hardening resources

  http://www.cisecurity.org/

- Microsoft Security Checklists

  http://www.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true

  http://technet.microsoft.com/en-us/library/dd366061.aspx

Most of these will be from the “BIG” software and hardware providers

Resources – In the News

- Privacy Rights <dot> org

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

- Resource for State Laws

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

References

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

- 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

- 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

- 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

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

References

- Juniper Networks Malicious Mobile Threats Report:
- http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

- Sybase Mobile Commerce Guide 2012:
- http://www.sybase.com/mobilecommerceguide

References

Juniper Networks Malicious Mobile Threats Report:

http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

Safeguards of enterprises:

- On-device anti-malware
- On-device firewall
- Centralized remote locate, track, lock, wipe, backup and restore facilities for
- Centralized administration to enforce and report on security policies across the entire mobile device population
- SSL VPN clients to effortlessly protect data in transit, and to ensure secure and appropriate network access and authorization
- Device monitor and control, such as the monitoring of messaging and control of installed applications
- A solution that integrates with network-based technologies, such as network access control (NAC), to ensure the security
- posture of mobile devices and determine appropriate access rights prior to allowing access to corporate resources
- Management capabilities to enforce security policies, such as mandating the use of PINs/passcodes
- Ability for an administrator to monitor device activity for data leakage and inappropriate use

References

Juniper Networks Malicious Mobile Threats Report:

http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

Safeguards of consumers:

- On-device anti-malware
- On-device personal firewall
- Password protection for device access
- Remote locate, track, lock, wipe, backup and restore software
- Antispam software to protect against unwanted voice and SMS/MMS communications

For parents - device usage monitoring software to monitor and control pre-adult mobile device usage and protect against

- cyberbullying, cyberstalking, inappropriate use, and other online threats, including automated alerting for:
- SMS message content
- Email message content
- Insight into pictures taken, sent, and received by the device, as well as those stored on the device
- Installed applications
- Address book and contact lists

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