Vendor Management and Security Awareness

Is Your Financial Institution on the Right Track?

CliftonLarsonAllen

CLAconnect.com

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623.**

- **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 recording,** will be sent to you within the next 10 business days.

- Please complete our online survey.

CPE Requirements

- Answer the polling questions

- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact sada.kempf@CLAconnect.com

- Allow four weeks for receipt of your certificate; it will be sent to you via email

* *This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Accounting and Consulting
  - Outsourcing
  - Wealth Advisory
- 3,600 employees
- Offices coast to coast
- Serve more than 1,100 financial institutions

Speaker Introductions

- **Joshua Juergensen**

  Josh is a manager in CLA's financial institutions practice and has more than 7 years of experience providing audit, internal audit, and consulting services.

- **Laura Espeseth**

  Laura is a manager in CLA's financial institutions practice and has more than 10 years of experience providing audit, internal audit, and consulting services.

- **Randy Romes**

  Randy is a principal in the information security services and financial institutions practices at CLA. He has more than 15 years of experience providing IT audits and security assessments specifically for financial institutions.

Learning Objectives

- At the end of this session, you will be able to:
  - Recognize the importance of vendor controls for SSAE 16 reporting
  - Understand the significance of proper SSAE 16 report reviews
  - Define and describe key controls to detect, monitor, and mitigate security risks

Vendor Controls Assessment for SSAE 16 Reporting

Josh Juergensen and Laura Espeseth

Service Organization Controls (SOC) Overview

- Service Organization Controls (SOC) assurance engagements are intended to provide client user organizations reasonable assurance that controls within the service organization have been accurately described and are suitably designed based on services provided, types of data processed/maintained and the overall operating environment….*referred to as a Type 1*.
- Assurance (reasonable) can also provided that the controls implemented were operating effectively for a specified reporting period which is typically either 6 or 12 months….*referred to as a Type 2*

Vendor Risk Management Objective

- Ensure that the oversight of service providers utilized by the organization are properly managed are selected based on the result of a risk assessment process and structured due diligence procedures.
- Services obtained from a third-party that involves significant operations must be supported by a written agreement that outlines specific responsibilities
- In addition, service providers must be monitored on an ongoing and periodic basis for quality and service delivery with an emphasis on the internal control environment within the service provider organization.

Who is Responsible?

- Identify a key liaison who has adequate knowledge of risks associated with outsourcing to perform the following:
  - Establishing and maintaining a centralized list of all third-party vendors
  - Verify signed contract and/or service level agreements exist
  - Evaluating prospective service providers based on requirements
    - ◊ Sensitivity of data accessed, processed or maintained by the service provider
    - ◊ Volume of transactions
    - ◊ Criticality of the service to the organization's product offering(s)
  - Obtaining and reviewing SSAE 16 reports

What Should be Assessed?

- In addition, the organization will evaluate the service providers:
  - Financial position
  - Marketplace position
  - Dependency on key personnel
  - Use of subcontractors
  - Location of applications/data (off shore*)
  - Dependency on subcontractors
  - Availability/security of systems
  - Redundancy/reliability of communications
  - Disaster recovery/business continuity

What to Assess for SSAE 16 Reports

- When assessing the SSAE 16 look for the following governance level controls:
  - Report type
  - Appropriateness of coverage of the report
  - Time period of coverage
  - IT applications and/or transaction flow
  - Specific controls tested and whether the control objective listed meets your control objective
  - The service auditor's opinion on the operating effectiveness of the controls

What to Assess for SSAE 16 Reports

- The following SSAE 16 controls should be tested on an annual basis (or term of the SSAE16 report):
  - Appropriateness of controls included in testing
  - Quality of the firm executing
  - Variance in time resulting in additional procedures needed to be completed
  - Any changes in the current control structure since the last report
  - **Evaluation and completion of User Consideration Controls**
    - ◊ **Identify controls and test procedures**
    - ◊ **Execute testing**
    - ◊ **Document results**

Examples of Critical Vendors

- Core Processor
- Payroll Provider
- Bond Accountant
- Online or mobile banking
- Bill Pay
- External Statement Processor
- Other (off-site storage, credit card, electronic BOD, etc.)

Regulatory Pressures

- Banking guidance expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures.
- Banks expected to have a more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities – significant bank functions or significant shared services.

Vendor Management Process

- Planning
- Due diligence and third-party selection
- Contract Negotiation
- Ongoing Monitoring
- Termination
- Oversight and Accountability
- Documentation and Reporting
- Independent Reviews

Outsourcing Solutions

Outsourcing solutions can assist with ongoing monitoring and documentation, most commonly in the following situations:

- Lack of internal resources
- Lack of internal expertise
- Regulatory criticisms related to the process

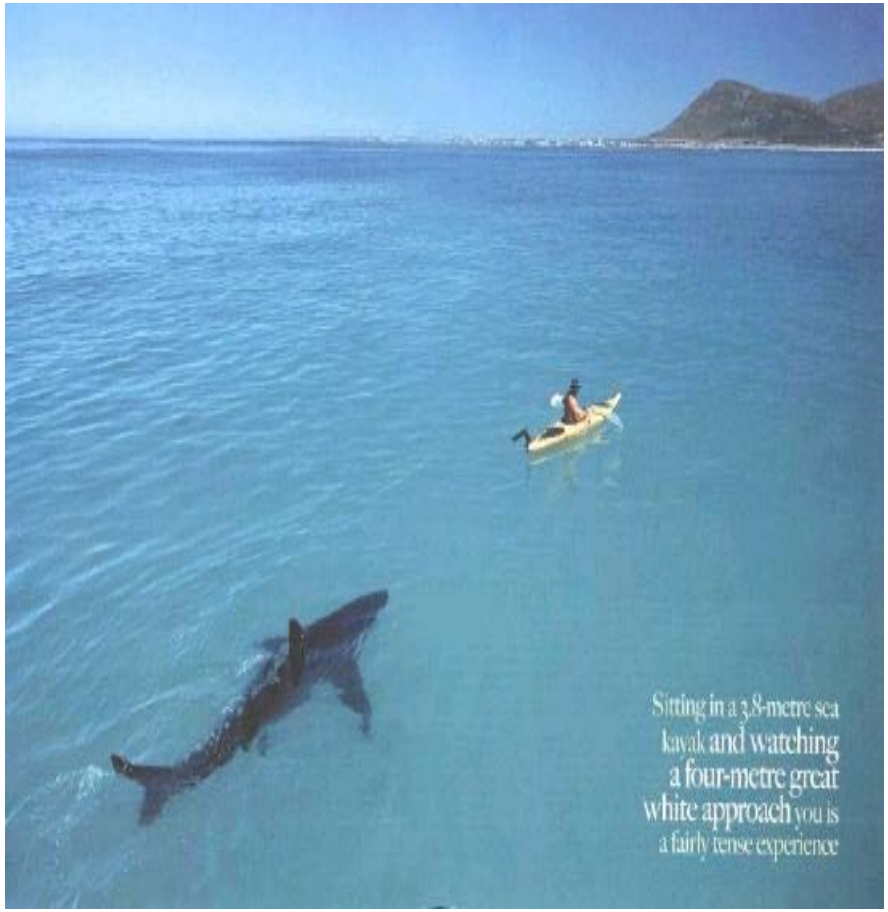
Cyber Fraud Risks to Banks and Their Customers

Randy Romes

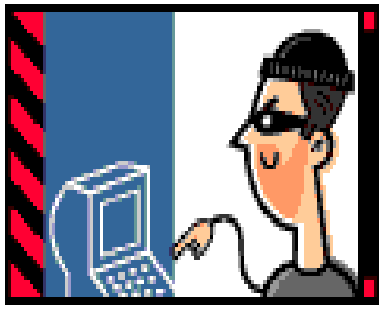
What do the following have in common?

- Mining company
- Electrical contractor
- Catholic church parish
- Critical care hospital
- Industry trade association
- Collection agency
- Long term care facility
- Public School District
- Credit Union
- Community Bank

- On and on and on and on…….



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
  - Identity Theft – Loan, Credit, and Tax Return Fraud
  - Fraudulent use of stolen credit cards
  - "Cash-out" schemes
- Hackers are "targeting" everyone, from individuals and (very) small businesses to large enterprises…

Hackers, Fraudsters and Victims

- Verizon Breach Analysis Report: Organized Crime…

	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%

- According to Symantec, cyber fraud is costing the global economy more than the global drug trade…

Social Engineering Opens the Door

- **Pre-text phone calls**:

  "Hi, this is Randy from <*vendor*> user support. I am working with Kevin, and I need your help…"

- **Facilities/Physical Security**:

  We say: "Hi, Jeff in IT said he would let you know I was coming to fix the printers…"

  They say: "Thank god you are here…"

  - Sumitomo Bank (2005)
  - Barclays Bank (2013)

- **Email Phishing**…

Case Study – ACH Fraud

- Texas hospital and community bank
- Events occur from March → August
- Bank customer (hospital) gets phished/hacked…
- Two ACH payroll files totaling > $150,000.00
- Lessons learned…

Case Study – Cash-Out Schemes

- In the news…

  http://www.bankinfosecurity.com/atm-fraud-c-245

- Last week…
  - Polymorphic malware infects network (phishing)
  - Hackers create Windows domain accounts
  - Hackers hijack core application accounts (knew them?)
  - Cash deposit of $90K
    - ◊ After hours / bank staff person did not work that day
  - $-Mule attempts to withdraw funds next day

FACT: There is NO Industry Concentration

Do you our your customers:

- Have personal financial information on their system (payment info; payroll; HR data)?
- Perform ACH or wire transfers online?
- Accept or process credit card payments?

- **This data and these payment processes are being actively targeted by organized crime!**

FACT: The Attacks Are SIMPLE!

- Verizon: 96% of attacks are preventable with simple controls in place

- Trustwave: 90% of successful attacks use DEFAULT passwords

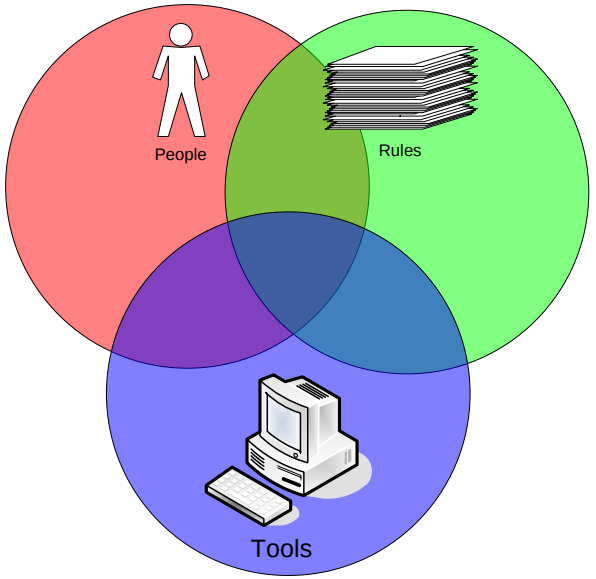
Organizations are not doing the most basic things to protect themselves! They think their IT staff has it covered…

Security is a Business Issue – NOT an IT issue

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



Two different disciplines:

- IT Administration
- IT/Information Security

Cybersecurity Leadership - FFIEC

- https://www.fdic.gov/news/news/financial/2014/fil14021.html

Executive Leadership of Cybersecurity

What Today's CEO Needs To Know About the Threats They Don't See

Presented by
Federal Financial Institutions Examination Council (FFIEC)
Cybersecurity and Critical Infrastructure Working Group
May 7, 2014

Cybersecurity Leadership - FFIEC

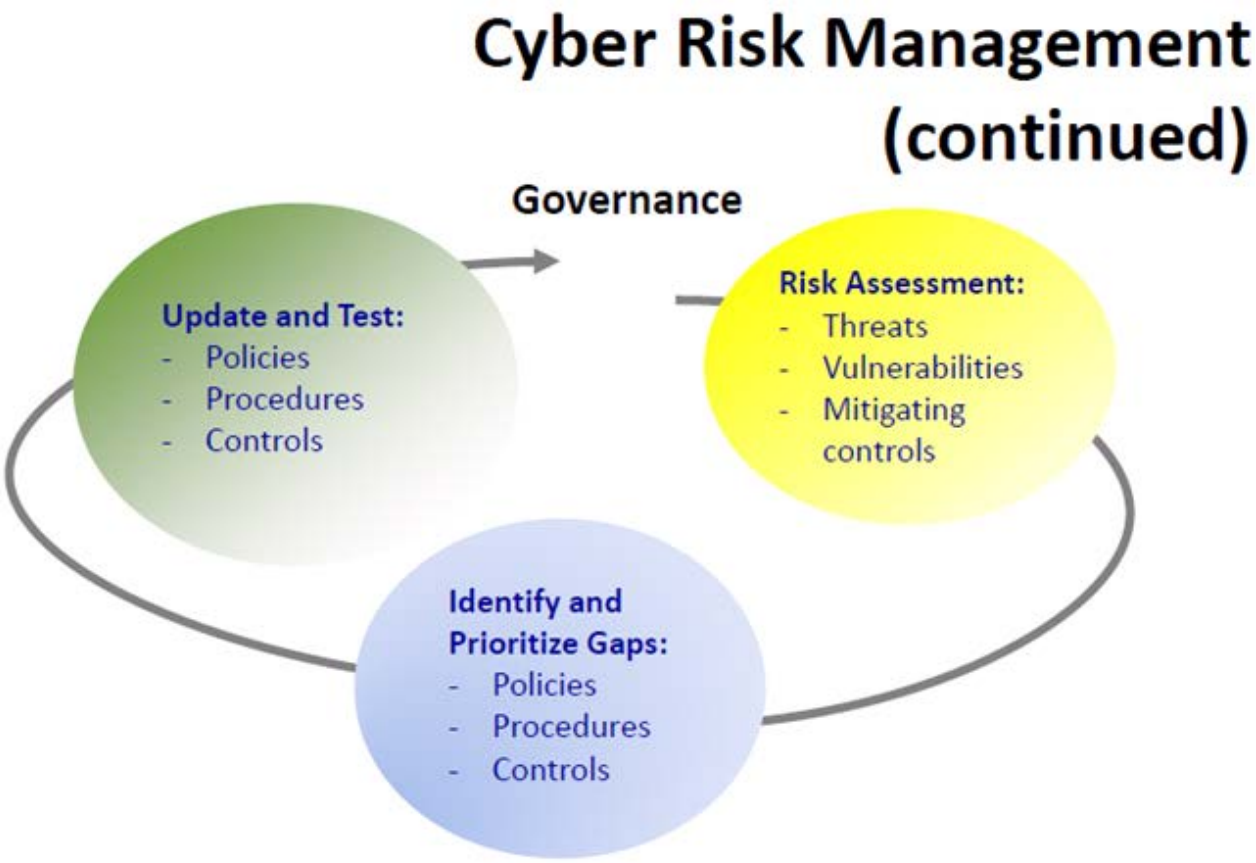
- https://www.fdic.gov/news/news/financial/2014/fil14021.html

Cyber Risk Management

- Governance
- Threat intelligence
- Third-party/vendor management
- Incident response and resilience

Cybersecurity Leadership - FFIEC

- https://www.fdic.gov/news/news/financial/2014/fil14021.html



Cybersecurity Leadership - FFIEC

- https://www.fdic.gov/news/news/financial/2014/fil14021.html

Cyber Risk Management (continued)

Third-Party Relationships

- Risks
  - Connectivity of systems
  - User access
- Controls
  - Initial due diligence
  - Monitoring

Current Threat Example: Software End of Life

Cybersecurity Leadership - FFIEC

- https://www.fdic.gov/news/news/financial/2014/fil14021.html

Cyber Risk Management (continued)

Incident Response and Resilience

- Preparation
  - Incident response plan and policy
  - Incident response team
- Escalation: internal
- Notification: external

Cybersecurity Leadership - FFIEC

- https://www.fdic.gov/news/news/financial/2014/fil14021.html

Cyber Risk Management (continued)

Incident Response and Resilience Key Takeaway

- How often is my institution testing its plans to respond to a cyber attack? Do these tests include our key internal and external stakeholders?

Mitigation Themes

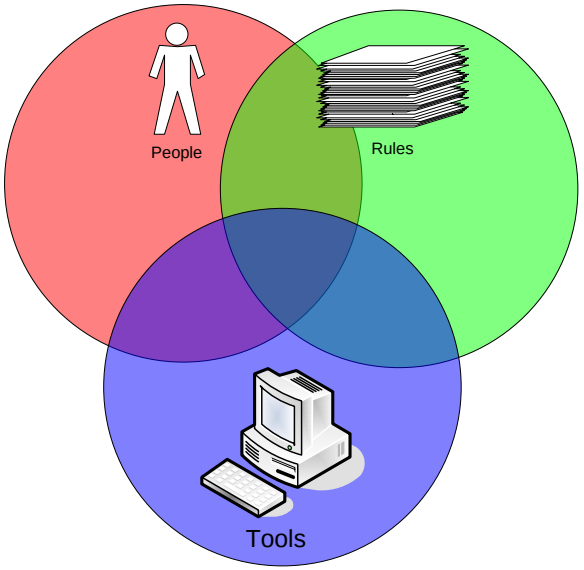
- Employees that are aware and savvy
- Networks resistant to malware
- Relationships with vendors “validated”
- Business customers use of online tools maximized

Call To Action

Thoroughly assess your risks

Thoroughly validate your controls

- "Belt and suspenders" approach
- High expectations of your vendors
- Penetration testing
- Application testing
- Vulnerability scanning
- Social engineering testing



References

- FFIEC Cybersecurity Guidance
  - https://www.fdic.gov/news/news/financial/2014/fil14021.html
- Verizon Breach Analysis Reports
  - http://www.verizonenterprise.com/DBIR/2014/
- Intrusion Analysis: TrustWave
  - https://www.trustwave.com/global-security-report/

Questions?

Josh Juergensen, CPA
Manager
(612) 397-3261
joshua.juergensen@CLAconnect.com

Laura Espeseth, CPA, CFE
Manager
(612) 397-3241
laura.espeseth@CLAconnect.com

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
(612) 397-3114
randy.romes@CLAconnect.com