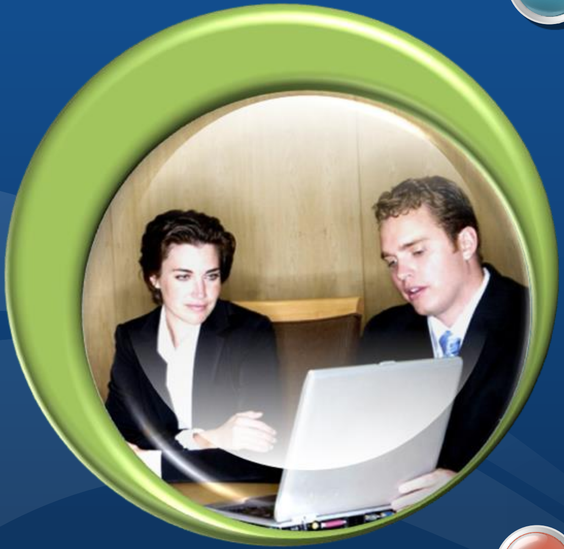
Securely Yours LLC

Top Security Topics for 2013

Sajay Rai, CPA, CISSP, CISM
sajayrai@securelyyoursllc.com

Contents



- Background
- Top Security Topics
- What auditors must know?
- What auditors must do?
- Next Steps

Background

Movement towards Cloud

- More Applications in Cloud
- More Critical Data in Cloud

Smart Devices Influx

- Critical data on Smart Devices
- Increased Data Leakage

SECURELY YOURS LLC

SECURING YOUR INFORMATION WORLD

Intensity of Attacks

- C to C (Country to Country)
- C to C (Company to Company)
- C to C (Consumer to Consumer)

Increased Regulations

- More scrutiny by Federal & State
- More demands by customers/clients

Top Security Topics

1. Cyber Insurance Policy

1. Cyber Insurance Policy

What is it?

- Designed to mitigate losses due to cyber incidents
- Vehicle to insure against cyber expenses
- Some policies cover regulatory penalties
- Some policies require minimum controls before the claims are paid
- The positive is that it is a good tool to be part of your overall security program and promotes security awareness
- The negative is that it is very expensive

1. Cyber Insurance Policy

What auditors must know?

- What is covered? What is not?
- What are the requirements of compliance?

What auditors must do?

1. Review the cyber security insurance policy
2. Understand the requirements of the policy for insurance coverage and the state of security required to file claim
3. Communicate the requirements to security group

Top Security Topics

1. Cyber Insurance Policy
2. Extended Enterprise

2. Extended Enterprise

What is it?

- Service providers outside of your network
- Typically have access to OR store your confidential information
- May even have access to OR store HIPAA related or PII information
- May or may not have an agreement in place
- May or may not have a Business Associate Agreement
- May provide the following services:
  - Cloud (e.g. Salesforce.com)
  - Backup and Recovery (e.g. Iron Mountain)
  - Delivery (e.g. Fedex etc.)
  - Smart devices (e.g. iCloud, apps which save your information in cloud)
- Potentially your weakest link

2. Extended Enterprise

What auditors must know?

- Identify third parties which provide KEY services
- The responsibilities of the service providers in terms of security
- Third party compliance with the contracted terms (including BAA)
- What steps are taken before bringing in a new service provider (cloud, hosting etc.)

What auditors must do?

1. Identify the KEY service providers
2. Ensure that the contracts with key service providers have security requirements and if needed BAA agreements
3. Review the process of risk analysis for new service providers

Top Security Topics

1. Cyber Insurance Policy
2. Extended Enterprise
3. Security Information Event Management

3. SIEM

What is it?

- Data Aggregation: Logs from various sources
- Correlation: Looking for common attributes
- Alerts: Automated analysis and alerts
- Retention: Ability to retain past history
- Automate Compliance: by collecting compliance data
- Commonly known software (Gartner top right Quadrant)
  - HP’s Arcsight
  - IBM’s Q1 Labs
  - McAfee (Nitro Security)
  - Novell’s LogRhythm
- Other known software
  - Splunk
  - LogLogic
  - Symantec and RSA

3. SIEM

What auditors must know?

- What activity is going on?
- Are their risks which are being ignored or not known?
- What action is taken once an incident is reported or discovered?
- Is appropriate information recorded to understand the activities taking place within the organization?

What auditors must do?

1. Understand the process of log management, logging, log reviewing and incident reporting
2. Identify the technologies whose logs are not reviewed or recorded
3. Are their correlation analysis done on the log data to identify advanced persistent threats

Top Security Topics

1. Cyber Insurance Policy
2. Extended Enterprise
3. Security Information Event Management
4. Data Leakage

4. Data Leakage

What is it?

- Allows organization to understand the data which is coming inside the organization AND which data is leaving the organization
  - We want to know if unwanted data is coming in (e.g. malware)
  - We want to know if confidential data is leaving (e.g. PHI or PII)
- DLP: assist with data leakage:
  - Data Loss Prevention
  - Symantec
  - McAfee
  - Websense
  - RSA
- NGFW (Next Generation Firewall)
  - Deep packet scanning
  - Sees the content before it comes in
  - Sees the content before it goes out

4. Data Leakage

What auditors must know?

- What sensitive data is leaving the organization?
- In what form the data is leaving?
- What regulatory requirements does your organization have or what agreements you have with your clients (Encryption etc.)

What auditors must do?

1. Review the process of data leaving the organization via different vehicles: emails, Flash drives, FTP, website etc.
2. Understand the technology implemented to assist with data leakage
3. Verify that regulatory or contractual requirements are met

Top Security Topics

1. Cyber Insurance Policy
2. Extended Enterprise
3. Security Information Event Management
4. Data Leakage
5. Appropriate Access

5. Appropriate Access

What is it?

- Knowing the identities
- Knowing the roles
- Knowing the access
- Reviewing the access
- Logging the violations
- Technologies which can help:
  - Work flow
  - Identity and Access Management
  - Password sync and password management
  - Single Sign-on
  - Federated Id

5. Appropriate Access

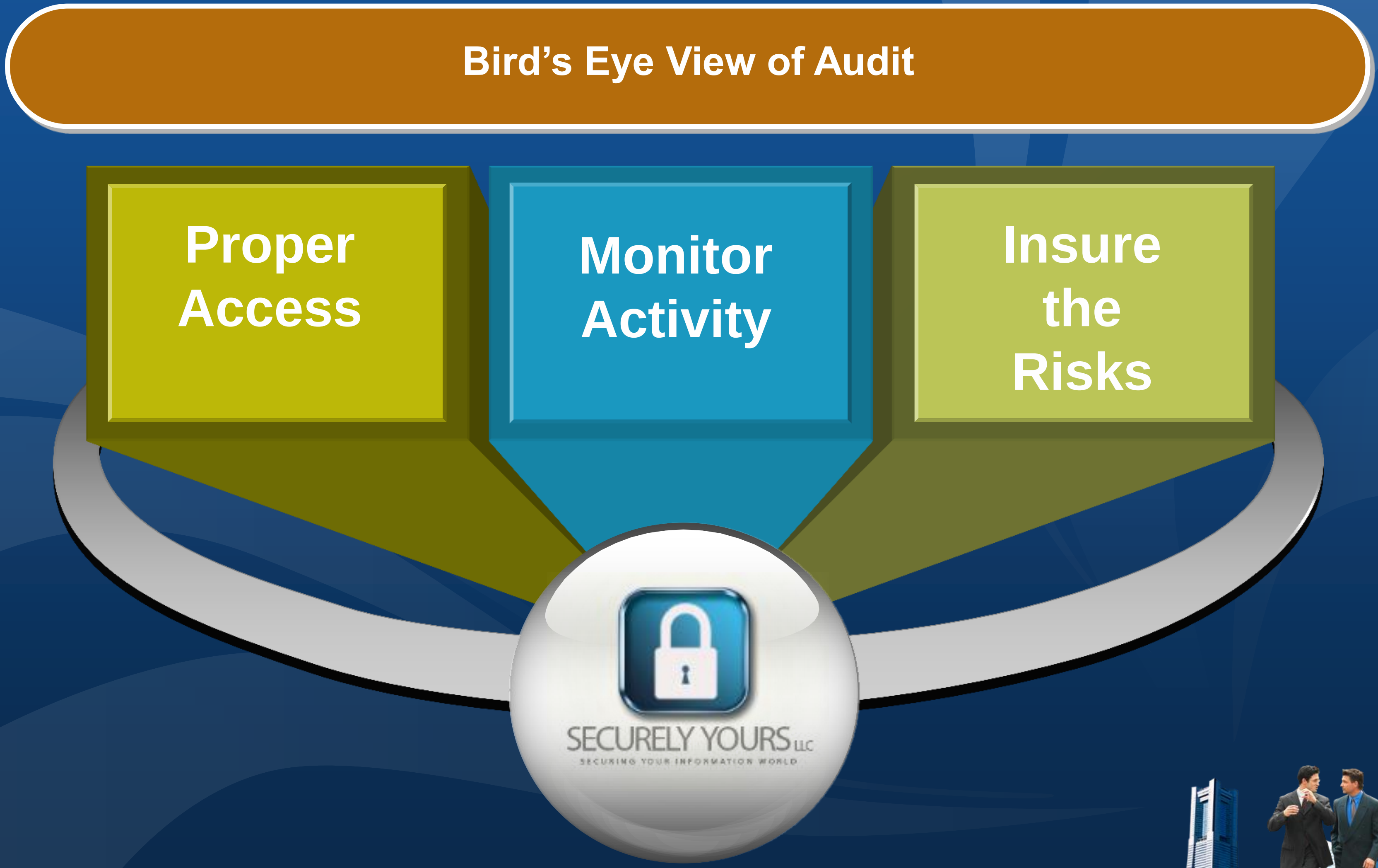
What auditors must know?

- Does sensitive data have appropriate access?
- Is Access to sensitive data reviewed by appropriate owners?
- Is Identity and Access managed appropriately within the organization?
- Are sensitive data protected through a layered defense?

What auditors must do?

1. Ensure that the access review is performed periodically
2. Review the provisioning and de-provisioning process for accuracy
3. Review how third party service providers get access to sensitive data
4. Understand how the system logs are reviewed and managed

Next Steps



Bird's Eye View of Audit

Proper Access

Monitor Activity

Insure the Risks

Thank You!

Sajay Rai 248-723-5224 sajayrai@securelyyoursllc.com