The Do's and Don'ts of Vendor Risk Management

James Christiansen, VP Information Risk Management, Optiv Security

Professional Techniques – T11

Agenda

- The "Risk" of Third Parties
  - Third-Party Breaches
  - Reducing the Inherent Risk
- Understanding Third-Party Risk
  - The Impact of a Third-Party Breach
  - Defining the Types of Risk
- Managing Third-Party Risk
  - Inherent Risk and Business Risk
  - Matching Security Assessment Level to Risk
- Changing the Paradigm
  - Standardized Assessments by Type of Service
  - Automation of Process

Common Industry Challenge

- Growing Problem
  - Sheer Volume
  - Costly Third-Party Due-Diligence
  - Global Regulatory Requirements
  - Data and Privacy Security Breaches
  - Fiduciary Board - Top of Mind
- Current Practice
  - Costly Manual On-Site Audits
  - Duplication of Efforts
  - No Standard of Due Care
  - No Trusted Third-Party Assessor

Third-Party Breaches

51%

of All Breaches Come from Third Parties(1)

The Cost of a Breach at a Third Party is Higher than an Internal Breach (2)

Responding is more complex and time consuming

Your are not in control of the response or communications

(1) Source: Key findings from The Global State of Information Security® Survey 2014, PWC, CSO Magazine

(2) 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014

Case Study

Can Sensitive Data Be Eliminated?

Project to Review All Outbound Data

More Than 80% of Data Being Sent had Additional Information Not Required for the Services

#1 Reason?

Third-Party Targeted Attacks

Third-Party Attacks

Target of Opportunity

Breach a major supplier and you gain access to multiple companies' data

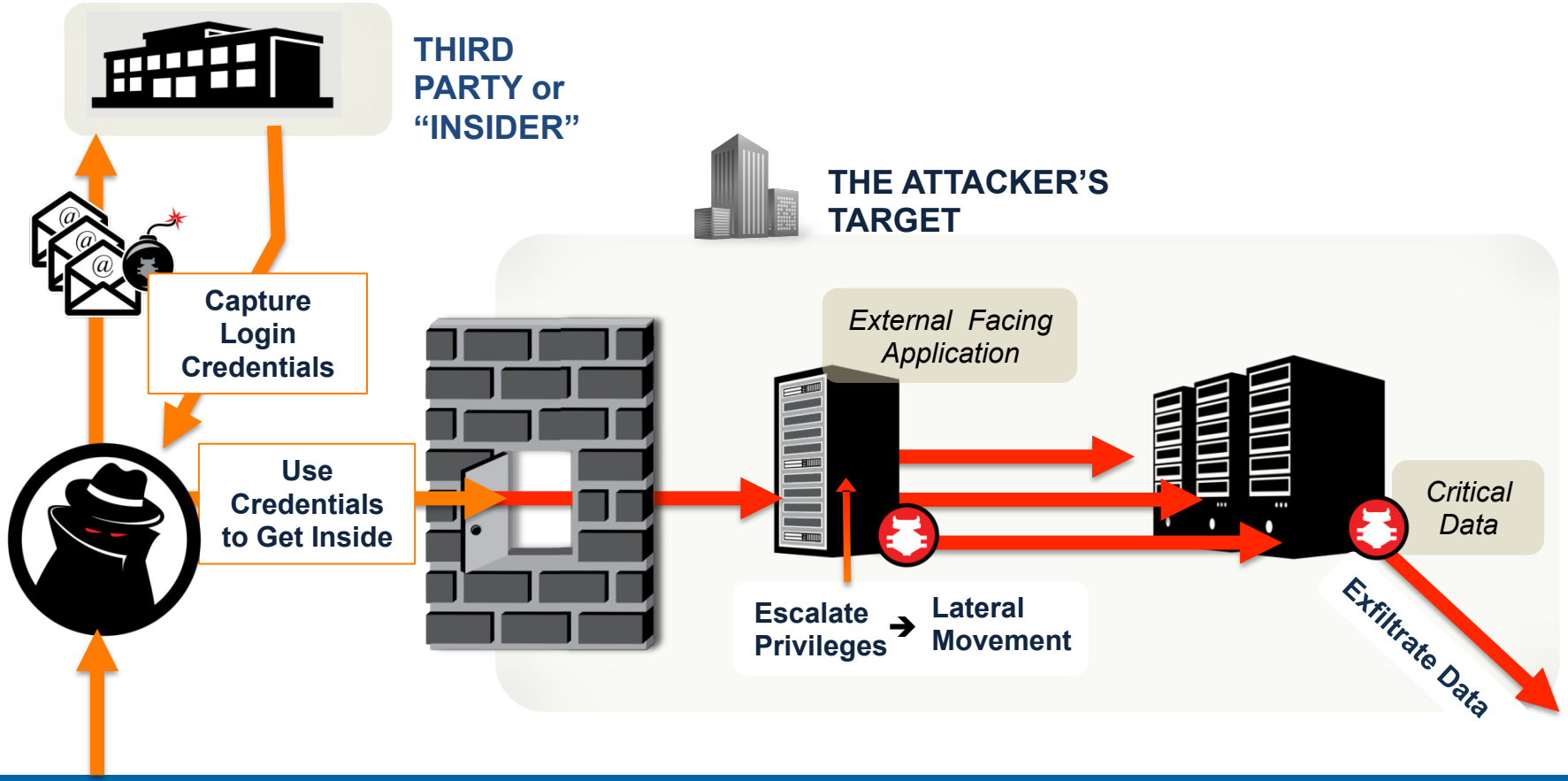
Global Problem

A supplier anywhere in the world can be the cause of, or suffer from a security breach

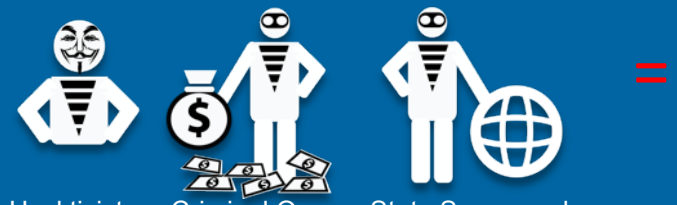
Economic Conditions

Increased outsourcing and financial stress on third parties can lower defenses

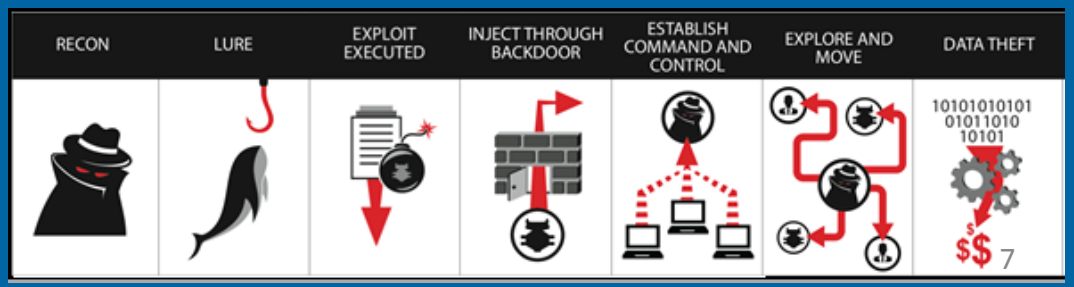
Exploiting the "Trusted" Third Party



ACTORS and METHODS:



=



Are You Responsible for a Breach at a Third Party?

Customers don't care about your business partners.
They entrust **you** with the information.

Consequences:

Loss of Customer Loyalty

Litigation

Eroded Share Value

Brand Damage

Increased Scrutiny

Lawsuits

Higher Audit Costs

The Beginning of a Bad Day

CEO reads in the news that a major third-party provider had a security breach

UNDERSTANDING THE RISKS

Complexities in the Relationships

Vendor Management | Risk Management | Business Stakeholder | Legal and Compliance | Information Security

Third-Party Exposure	Third-Party Performance	Regulatory Compliance	Information Security / Privacy
Inherit Risk Exposure • Financial Exposure • Information Exposure • Regulatory Exposure • Availability Exposure • Quality Exposure • Contract Exposure • Performance Exposure	**Third-Party Interruption Risk** • Natural disasters • Terrorist attack • Solvency • M&A **Scorecards** • Performance Scorecard • 360 Third-Party Scorecard	**Regulatory** • GLBA • HIPAA-HiTech • Foreign Corrupt Practices Act (FCPA) • Local, State, and International Regulations **Diversity** • Minority Ownership • Veterans • Small Business • Equal Opportunities	**Confidential Information Protection** • ISO27001/2 • NIST • HIPAA CFR164 • Shared Assessments Program • Payment Card Industry (PCI) **Global Privacy Requirements** • Generally Accepted Privacy Principles

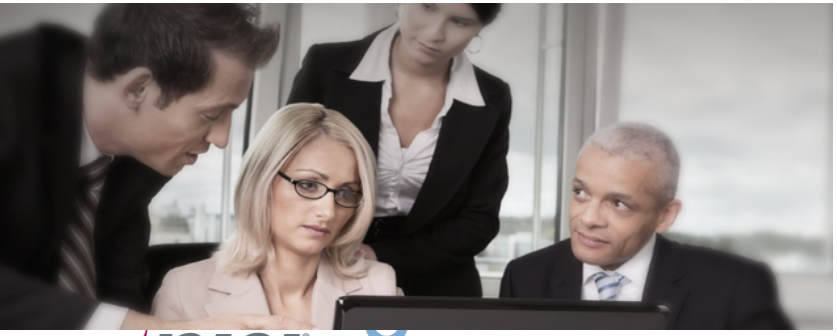
Planning, Managing and Reporting

Planning

- Steps to take to understand the inherent risk in the third-party base

Managing

- How to effectively manage the residual risk of your third parties



Reporting

- Reporting on third-party risk management process

Third-Party Types of Risk

Strategic:	*Adverse business impact*
Reputation:	*Negative public opinion*
Operational:	*Failed internal processes, people, or systems*
Transactional:	*Problems with service or product delivery*
Financial:	*Unable to meet contractual arrangements*
Compliance:	*Violations of laws, regulations, or internal policies*
Foreign:	*Country, culture, geopolitical or foreign currency*

Third-Party Contracts

Managing Third-Party Risk

Third-Party Risk Process

1. Regulatory or Contract Exposure
   - Data Exposure
   - Business Process Exposure
2. Financial Strength
   - Geopolitical / Country Risk
   - Breach History or Indication
3. Standardized, Service Type
   - ISO27001/NIST
   - HIPAA/STAR
4. Electronic Validation
   - Onsite Validation
   - Control Evidence
5. Changes in Relationship
   - Changes in Business
   - Changes in Controls

ISACA Trust in, and value from, information systems San Francisco Chapter

OPTIV

Relationship Exposure Inventory

The First Question:
"What data of ours was breached?"

- Relationship Exposure Inventory – Risk Registry
  - Maintain a relationship list (type and quantity)
- Relationship "Creep"
  - Due diligence is performed during the first contract
  - Relationship grows over time
  - Increased liability without updating the risk exposure metrics

Business Profile Risk

- Purpose: Who is The Third Party?
- Understand the Risk of Doing Business With Third Party
  - Financial Strength/Credit Risk
  - Regulatory Oversight
  - Geopolitical/Economic Risk
  - Business Risk
  - Breach History, Crime, Legal Suit
- Most often performed outside of Information Security

Mapping Risk Tiers

	Tier 1	Tier 2	Tier 3
Relationship Risk			
Strategic Risk	High	Medium	Low
Reputational Risk	High	Medium	Low
Transaction Risk	$$$$	$$$$	$$$
Compliance Risk	High	Medium	Low
Data Privacy Risk	High	Medium	Low
Business Profile Risk			
Credit Risk	$$$$$	$$$$	$$$
Country Risk	High	Medium	Low
Other Risks	High	Medium	Low

Risk Tiers Based on Inherent Risk

Inherent Risk is a Function of Relationship and Profile Risk

Match the Level of Due Diligence to Inherent Risk

Tier 1

- Strategic accounts (high revenue dependence)
- Regulatory/contract requirements
- High reputation risk
- "Trusted" relationships

Tier 2

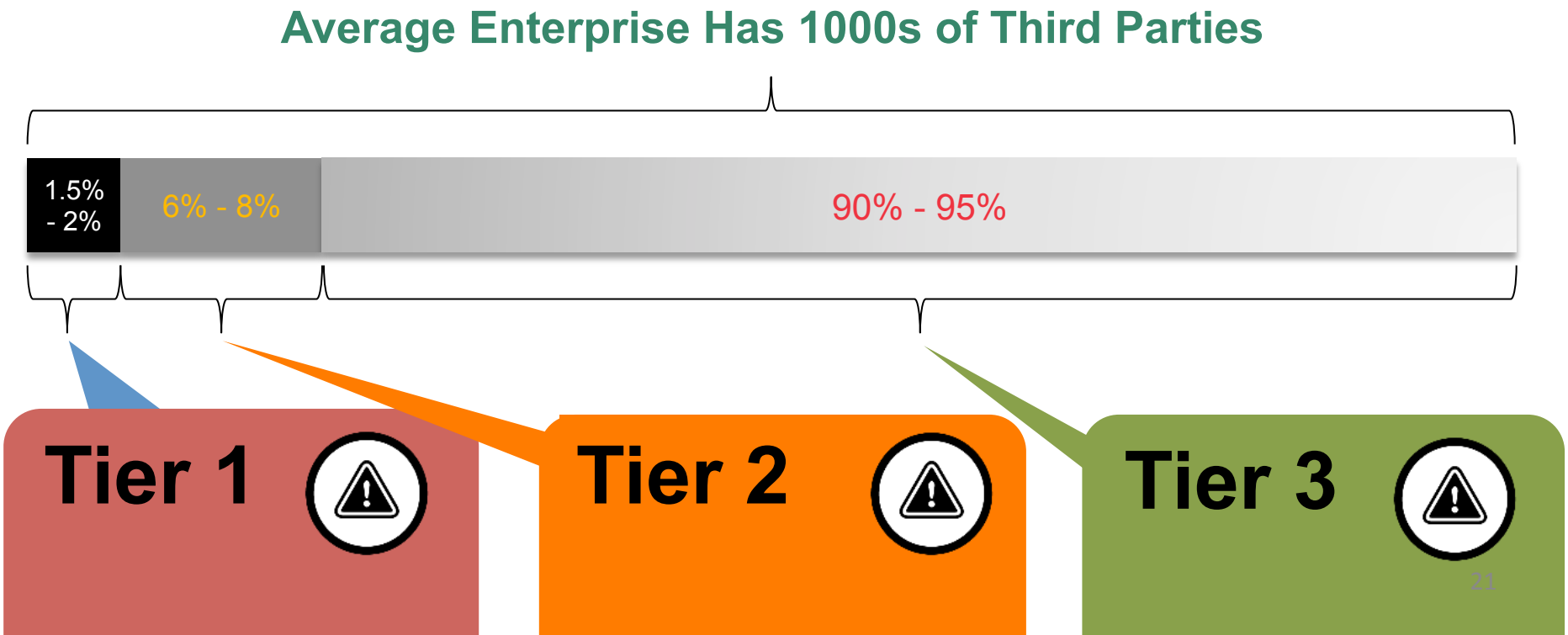
- Lower volume with no or minimal sensitive data
- Lower revenue risk
- Business operations risk
- Some business profile risk

Tier 3

- No sensitive data
- Minimal reputation risk
- Minimal or no revenue dependence
- "Trusted" relationship with low-level access

Third-Party Risk – Current Situation

- On April 5, *USA Today* published results from survey of 40 banks and found:
  - 30% don't require third-party vendors to notify of security breach
  - Less than 50% conduct onsite assessments of third-parties
  - Approximately 20% do not conduct on-site assessments of service providers



Control Assessments

Standardized Assessments

- Match Due-Diligence to Risk and Type of Service
  - Full Assessment - Large
  - Full Assessment - Light
  - Cloud Computing
  - Application Development
  - Call Center
  - Small Office
  - Single Person Office
- No Ambiguity
  - How You Ask Questions is as Important as What You Ask

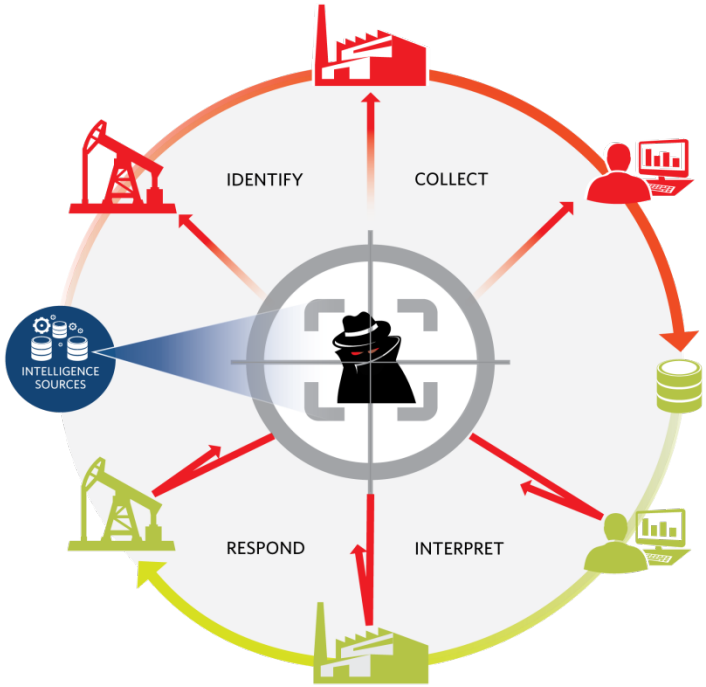
Control Standards

- ISO27001/2 Standard
  - 12 key controls that encompass security practices
- NIST
  - Cybersecurity framework
  - NIST SP 800-161 supply chain risk
- HIPAA/HITECH/Omnibus
  - Security rule CFR 164.306 – CFR 164.316
  - Requires business associates comply
- PCI Standard
  - Comprehensive requirements consisting of 12 rules
  - Requires institutions to ensure third parties also PCI certified

Validating IT Controls

- Onsite Third-Party Validation
  - Costly and time prohibitive
- SSAE16 SOC 2
  - A SSAE16 SOC 2 provides information pertaining to the IT controls that has been certified by an accredited firm

    Tip: Make sure the scope match the services being provided.
- Third-Party Breach Intelligence
  - Service that monitors for bad traffic on the internet



Tier 1 Due Diligence

Fully Validated

Tier 1 Assessments

Tip: Multiple sites and outsourcing by third party significantly increases level of effort

- Self Attest of Controls
- Validate (not a complete list)
  - Security policies
  - Incident response plan and procedures
  - Detection and monitoring systems (e.g. SEIM, SOC)
  - Business continuity/disaster recovery plan and test results
  - Vulnerability management procedures and sample reports
  - Security awareness, training and completion log
  - Last independent security assessment - status of high risks

Tier 1 Due Diligence

Fully Validated

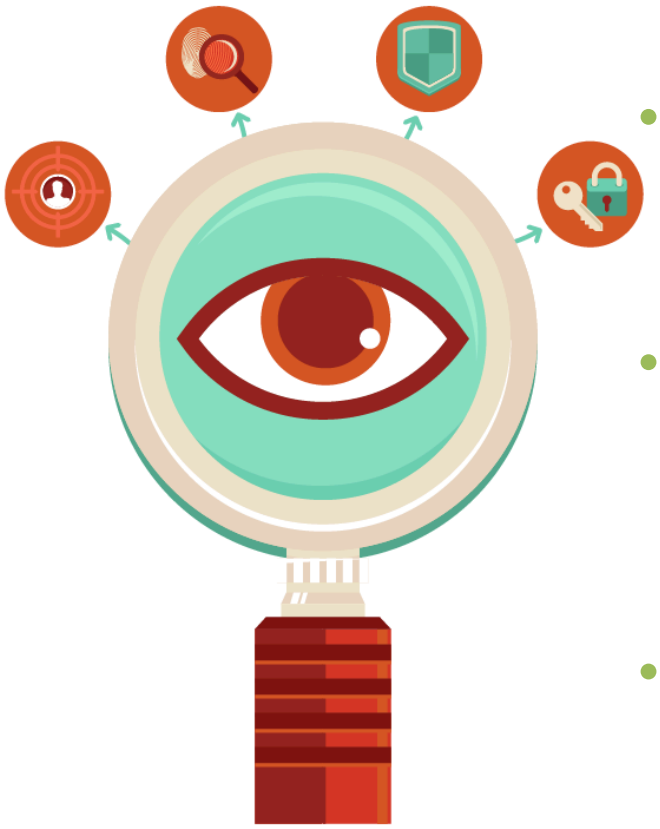
- **Minimum Documentation**
  - Security policies
  - Information security org chart and job descriptions
  - Incident response plan and procedures
  - Business continuity/disaster recovery test results
  - Vulnerability management and sample reports
  - Security awareness and training materials and log
  - Independent security assessment results and current status of high risks
  - Evidence in any area of controls that are critical to the success of the project or suspicion from prior answers

Define Validation Plan

Fully Validated

- Validation
  - What are the controls of most concern?
  - How can I verify they are functioning properly?
  - What kind of evidence can they produce?
  - What is acceptable and what is not?

What to Watch For



- Response Red Flags
  - "Sorry I can't give you that. It is confidential."
  - "I'll send it to you after our legal review."
- People Red Flags
  - Evasive answers -Shifty eyes.
  - Long explanations.
- Governance Red Flags
  - No formal training and awareness program.
  - Security organization is a side job, no executive oversight.
- Security Technology Red Flags
  - Vulnerability management is not fully implemented.
  - Threat management is incomplete or nonexistent.
  - No IM, privileged access, two-factor authentication.

Tier 2 and 3 Assessments

Partially Validated

Tier 2 Assessments

Self Attest of Controls

Electronic Validation

- Policies
- Access Management
- Vulnerability Management
- Threat Management
- Penetration Tests
- Endpoint Management

Tier 3 Assessments

Self Attest of Controls

- Review Responses
- Random Audit

Due Diligence Frequency

- Match Due Diligence to the Associated Risk
  - **Tier One**
    - Annual – Fully Validated Controls Assessment
    - Quarterly – Penetration and Vulnerability Scan Results
    - Monthly – Touch Base For Incident Response and Contact Management
  - **Tier Two**
    - Annual – Validation of Primary Controls
    - Monthly – Incident Response Contact Management
  - **Tier Three**
    - Annual – Self Assessment and Random Audits When Possible
    - Monthly – Incident Response Contact Management

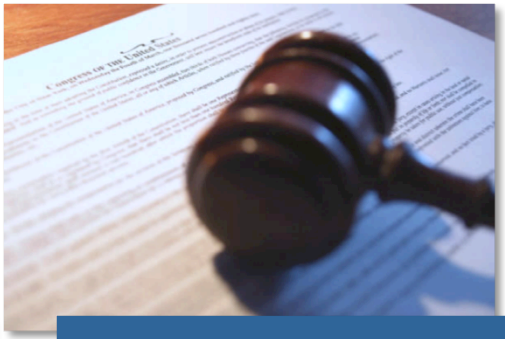
Remediation Plan

- Third Party Not Meeting Required Standards
  - Does control deficiency impact services?
  - Provide third-party list of required improvements and dates
  - Third party will:
    - Commit
    - Require additional time
    - Reject
  - Remediation plan – agreed upon improvements
    - Trigger follow-up

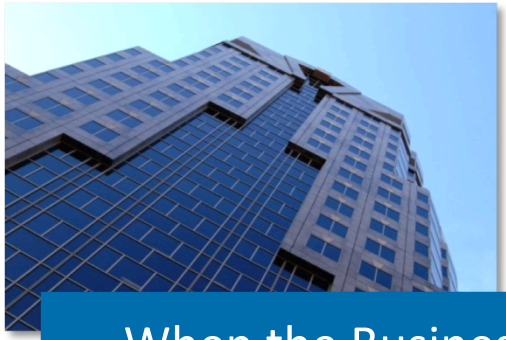
When to Review

During the RFP Process

When the Relationship Changes



When a Regulation Changes



When the Business Profile Risk Changes

At Least Annually

Monitoring and Reporting

Ongoing Program To Monitor Quality of Service, Financial Condition and Applicable Controls

Quality of Service

- Overall effectiveness of vendor
- Customer complaints and the resolution

Financial Condition

- Financial stress
- Insurance coverage
- Change in control (M&A)

Risk Management

- Security control reports
- Regulatory compliance
- Business continuity

Risk Management Reporting

- Periodic summary report
- Total completed, pending
- Vendors approved, rejected
- Remediation status

Third-Party Due Diligence Process

PUTTING IT TO PRACTICE

Internet Banking Test Plan

Change Management

- Authorization
- Emergency Changes
- Back Out

Access Controls

- ID And Password Management
- Provisioning And Termination
- Remote Access

Laptops/Desktops

- Encryption
- Antivirus
- Firewalls
- Wireless

Incident Management

- Cyber Incident Response
- Intrusion Detection
- Electronic Forensics
- Customer Notification

Mobile and Removable Devices

- Encryption
- Synchronization
- Destruction

Application Development

- Secure Coding Techniques
- Vulnerability Management
- Testing Security Controls

Internet Banking Test Plan

Information Backup

- Schedules
- Retention
- Offsite Storage

Business Continuity

- Planning
- Testing
- Alternate Sites And Capacity

Network

- Firewalls and DMZ
- Encryption
- FTP

Compliance

- Independent Verification
- Regulatory and Industry
- Penetration Testing
  - Network
  - Systems
  - Applications

Messaging

- Email
- Instant Messaging
- Data Leakage

Changing the Paradigm

- Inefficient, Cost Prohibitive and Sheer Volume
  - Performing assessments - Often only small percentage assessed
  - Responding to 100's of risk assessments are disruptive takes incredible resources
- Time For a Change!
  - A standard set standard set of criteria that serves 90% of the needs
  - Gather the information once and share many
  - Automate the process of audits and remediation

How to Apply What You Have Learned

Within Three Months, You Should:

- ✓ *Begin due diligence on critical third parties*
- ✓ *Evaluate your risk inventory and assign risk tier*
- ✓ *Start slow – Get quick wins*

Beyond Three Months, Establish:

- ✓ *A tiered program to evaluate risk*
- ✓ *A remediation plan to address deficient controls*
- ✓ *Reporting program*

Questions?

James.Christiansen@Optiv.com
www.optiv.com