Third Party Management
Best Practices for All Organizations

By: Gary Sheehan  CISSP, CERP, Certified Third Party Risk Professional
CSO / Director of GRC Services
ASMGI
gsheehan@asmgi.com
Introduction

Gary Sheehan  CISSP, CERP, CTPRP
CSO / Director - GRC Services
ASMGi – Greensboro
gsheehan@asmgi.com

Gary Sheehan
Executive Director
Information Security Summit
cso@informationsecuritysummit.org
Agenda

• Third Parties
• Risks
• Vendor Management Program Development
• Best Practices
• Q&A
Define Third Party

Entities or persons that work on behalf of an organization, but are not employees. Includes vendors, suppliers and service providers;

- Consultants
- Clients
- Partners
- Service Providers
- Subcontractors
- Vendors
- Suppliers
Define Third Party Risk Management

- Third Party Risk Management is a process for identifying, assessing, monitoring and remediating risks created when hiring a third party to provide goods or services to your organization.
  - Provided Services
  - Business Impact

- By 2020, 75% of Fortune Global 500 companies will treat vendor risk management as a board-level initiative to mitigate brand and reputation risk. *(Gartner)*

- Downstream Liability - companies are held accountable for their vendor’s failings.
Define Third Party Risk Management

Vendor Risk Management
• Risk are generally associated with the logical or information supply chain
• Compliance / security / privacy

Supplier Risk Management
• Physical supply chain – tangible commodities of services or manufactured goods
• Quality / timeliness / availability

Third Party Risk Management
• Financial
• Reputation
• Business Resiliency
What are the Risks

- Third Parties are popular targets for cyber attacks
- The regulatory environment is becoming more complex
- Third Parties are being viewed as strategic business partners which introduce additional risks such as:
  - Financial
  - Regulatory
  - Reputation / Brand Risk
  - Workforce
  - Business Interruptions
- On average, more than 60% of an enterprise's IT budget is spent on products and external services. (Gartner)
- 63% of all data breaches can be attributed to a third party. (Soha Systems)
Creating a Vendor Management Program

• Strategy
  • Who, What & How

• Structure
  • Organizational Structure
  • Responsibilities

• People (Who)
  • Program / Process / Procedures

• Process / Procedures (How)
  • How will the goals of the program be achieved

• Technology (What)
  • What tools will be used to achieve the goals
Creating a Vendor Management Program

- **Strategy (Executive)**
  - Executive Sponsorship
  - Know the Business
  - Program Goals and Objectives
  - Funding
  - Program Governance and Oversight
    - Scope
    - Policies / Documentation
    - Structure
    - Operations
    - Metrics
    - Review and Improvements
Creating a Vendor Management Program

• Structure (Team & Program)
  • Organizational
    • Executive Sponsor
    • Steering Committee
    • Program Operations
  • Operational
    • Program Alignment to Strategy and Business Goals
    • Program Components
Creating a Vendor Management Program

• People (Who)
  • Program Responsibilities
  • Process Responsibilities
  • Procedure Responsibilities
Creating a Vendor Management Program

• Process / Procedures (How)
  • Inventory
  • Vendor Classification
  • Communication Plan
  • Assessment (survey / onsite)
  • Decision Making Process
    • Authority / Risk Acceptance / Exception
  • Systems / Application Integration
  • Incident Resolution
  • Remediation
  • Metrics
Creating a Vendor Management Program

- Technology (What)
  - Vendor Inventory
  - Data Storage
  - Risk Analysis
  - Document Retention
  - Assessment workflow
- Solutions are still evolving
- Should address Bimodal IT delivery concepts (both stability and agility)
Third Party Risk Management Best Practices

- Documented policy, process, procedure and workflows
- Establish a comprehensive TPRM governance and reporting process
- Frameworks
- Collaboration
- Contract Management / Monitoring
- Consistent and Objective Vendor Assessment
- Exception Management
- Remediation Management
- Product Integration
- Include fourth-party relationships
Questions and Answers