Effective Vendor Management
SecureState

- Management consulting firm specializing in information security

Amy Black, Sr. Associate Management Consultant

- Engagement manager with a hybrid experience in sales, project management & consulting
- SecureState representative for Shared Assessment Program
"Man who live in glass house should change in basement."
Why Are We Here?

- Why do we keep hearing about Third Party Vendor Management?
- What is the Vendor Risk problem?
- Why should you care?
- What is a Vendor Management Program?
- How can you start a Vendor Management Program?

- Question and Answer Session
Two Sides to the Problem

Third Party Vendor Management (Company)

Responding to Security Questionnaires (Service Provider)
Background on Vendor Management

- Financial institutions mandated for years by OCC to have effective vendor management program
Why do we keep hearing about Third Party Vendor Management?

• Regulatory Requirements or Guidance
  – GLBA, PCI, HIPAA
  – OCC Guidance, FFIEC, FDIC, ISO 27001
Wall of Shame

Neiman Marcus

TARGET

UNIVERSITY OF MARYLAND

Michaels

SONY

CyberVor

eBay

PF Chang's

1.2b

309k

70m

80m

70M

145M

??

You Logo Here
What is the Vendor Risk Problem?

1. How are my vendors protecting my data?

OR

2. What type of data do my vendors have access to?

“He who want pretty nurse, must be patient.”
Zero-sum Game

• Is it all or nothing, or can we provide an acceptable level of risk in association to our vendors?
CMMI Level and Associated Security

Adaptive Industrial Control System (ICS) Testing

Traditional Penetration Tests
Why should you care?

• Risks:
  – Reputational, Compliance/Regulatory Fines, Operational/Business Interruptions, Legal Liability
• Increasing reliance on 3rd party vendors
  – Cloud applications
  – Outsourced business functions
  – Next-shoring vendors
Why people don’t pay attention to Vendor Management?

• No formal program or owner
• No formal framework or guidance, so people don't know where to start
• Time consuming
• Too many vendors to assess OR lack of vendor inventory to know who to assess
• Manual process – Spreadsheet driven
• Vendors may be brought in as personal referrals
What is a Vendor Management Program?

4 Step Program:
• Risk Assessment
• Due Diligence in Selection process
• Contract Structuring/Review
• Oversight

“Man with hands in pockets feels foolish, but man with holes in pockets feels nuts.”
Risk Assessment

• **CMMI**
  – Level 1 initial ad/hoc
  – How to progress to next level

• **Test the effectiveness of the controls at each level**
Due Diligence

- **Vendor Selection & Questionnaire Deployment**
  - Assess Risk of Vendors
    - Deploy Scoping Questionnaire
      OR
    - Assess business process flows and data access
- **Vendor Response: Deploy questionnaire's**
- **Documentation Review and Questionnaire Analysis**
  - Follow Up Questions/Request additional Info
  - Identify gaps - Initiate Remediation (or select new vendor if part of initial process)

“For mature programs (financial industry), you may want to include your top customers.”
• Validation of High Risk Vendors
  – Technical Validation
  – Onsite audits

“Wife who put husband in doghouse soon find him in cathouse.”
- Scope of engagement
- Benchmarks and identify KPI's
- Responsibility for compliance/Legal Responsibility
- Compensation
- Confidentiality
- Insurance
– Evaluate performance (KPI's)
– Accountability
– Ongoing monitoring
– Documentation & Reporting
Where should you begin?

– Vendor Inventory
  • Who are your vendors?
  • What type of data do they have access to?

– Vendor Risk Criteria
  • What type of vendors do you want to assess?
  • Phased approach - Tier 1 vendors first (Access to key/high impact areas)

“Man that go to bed with itchy butt wake up with sticky fingers!”
Vendor Perspective
• Another questionnaire to fill out
• Starts with are you “ISO 27001 certified”?  
  – Small % of US firms are ISO certified
• Can have as many as 750 questions  
  – Financial and Operations  
  – Security
• Have to remediate all gaps identified  
  – Risk based decisions?
Malicious Compliance in Distress

• Vendors (Service Providers) are not doing the “right” thing, they are just trying to comply and not lose the contract or relationship
• Not every “gap” is a high risk
• Need to realize the maturity of the organization
Tips on Responding

• Based on risk criteria
  – Every vendor will get the same questionnaire
    • No conformity to questions (BITS, SAP etc)
  – Answer each question, and have a remediation plan to support any gaps
  – Don’t just “jump”, reactive to questions can cause the vendor to spin without getting any substantial changes implemented

• Have proper representation
  – Knowledgeable security and business to negotiate risk based decisions
Thank you!

Amy Black
ablack@SecureState.com

“Man who drop watch in toilet, bound to have shitty time.”
Third Party Vendor Process Flow