Third Party Risk and the Role of the Cyber Security/IT Risk Officer

Robert “Satchmo” Anderson
Overview

- Third Party Risk Management (TPRM) (vendor management, new acquisitions, and joint ventures), Fourth Parties, and Fifth Parties—Stop the Madness!!!!
- Cyber Security/Information Security Risk
- Tools to aid in Risk Analysis
- Risk Analysis
- How to be successful (Understand the threats, vulnerabilities and controls—Defensive measures)
My goal: Identify and highlight TP risks; in order to, understand and mitigate the risks associated with security and controls.
Cyber Security and Information Risk (When the business cares)

- Reputational Risk – (New Acquisition)–$$$
- Strategic Risk–
- Credit Risk
- Liquidity Risk
- Legal/compliance Risk (New Offering-China)
- Operational Transactions Risk — from Supply chain risk

**Taken from the FFIEC IT Examination Handbook Info Base

- Frameworks include: COBIT, ITIL and ISO
- Risk Mgt framework (RMF) for DoD IT formerly DIACAP—operating under FISMA and NIST 800-37
Risk Analysis

• Who are Third Parties? New unit standup, military partner (combined operations), financial partners, Uniformed service (Air Force Space Command) or a unit command—Anyone providing you a product or a service

• Corporate vendors are Amazon Web services, Azure, Oracle, anything you contract out for—SaaS, PaaS, IaaS

• Know and understand the threats, vulnerabilities and controls

• Know the risk appetite (what is expected, what data is flowing, internet accessible, security tiers, etc.)

• Bottom line: Do the gumshoe work. SIG analysis, trust but verify—read logs, analyze signatures, look at the AD groups, bring in audit friends for a full exploration of the vendor
Tools in Risk Analysis

• Risk Registers (Archer)—Authoritative sources—Regulatory requirements (To Policy, to Standard, to Tasks to complete) annotate, revisit, document, ratings, plus

• Vulnerability Scans, App scans, and Penetration Tests (dig deep)

• Payment card industry-qualified security assessors reports

• Service organization control reports (SOC 2 Type 2) Show and prove

• Automated reports (AV, Patching, asset mgt)

• Accurate inventory!
Tools in Risk Analysis

• Others--Interviews, Diagrams, screen captures, etc
• Standardized Information Gathering (Santa Fe Group)
• Vendor Risk Management maturity model (your own—Santa Fe Group)
• Cyber protection teams should incorporate most of the above, COCOMs should understand the 3rd, 4th and 5th party relationships and the potential effect to military operations (Good luck)
• Provide your TLAs your intel requirements have them give you threat based intel (works at the Company too 😊)
Risk Analysis

Who: Qualified, certified, common sense, cyber security guru (generalist)

What: Identify, define and validate the risk

When: Constantly

Where: on-site, off-site, cyberspace

Why: Capture and assess the risk; Identify and Propose risk reduction options

How: Everything you can get your hands on
Oh, Math hurts

- Elements in your risk calculus (Understand the risk appetite first)
  - Business—1st
  - Architecture and design (tiers, restricted, internet facing)
  - Human Resources (new employees, seasoned, clueless)
  - Risk Management (SOPs, guidelines, concrete, enterprise, business)
  - Asset Management (What is known, where, who is watching it)
  - Identity and Access Management (multi-factor, Active directory, RSA-tokens)
  - Key Management (dynamic vs static, rotated)
More Math

• Elements in your risk calculus
  • Data Security (encrypted at rest, back end secure, TLS 1.2)
  • Endpoint (USBs allowed, AV, patched, etc)
  • Apps (Secure development, QA, separation of duties)
  • Network (segmented, VLANs, ACLs)
  • Physical security (cameras (IP or CCTV), private/public—PCI, guards)
  • Vuln Mgt (How often, criticality, can they spell it?)
  • Change Mgt (Is it practiced, accountable, verifiable)
  • Incident Mgt (Planned, Go-kit packed, HMFIC, exercised)
  • DR/BCP (Plan, business impact analysis, exercised)
How to be successful

• Know the risk appetite and adhere to it

• Identify and allocate appropriate resources to the TPRM program (legal, financial, Cyber Security, auditors, etc)

• Ensure senior management is on-board with a governance framework based upon risk and compliance—develop policies, standards, SOPs, and site visit checklists

• Ensure linkages between audit, TPRM and cyber security to ensure gaps aren’t present

• Don’t be steamrolled, don’t do business as it has always been

• Play nice in the sandbox (Internally)

• Dig deep (externally)—visit the site, read the policies, understand data flow and architecture, DR/BCP, read the SIG (yawn)
How to be unsuccessful

• Poor contracting without metrics, SLAs, etc
• Lack resources (technical, audit, vendor mgt personnel)
• Unfettered access to data by the Vendor
• Poor adherence to polices, standards, outside compliance
• Undefined processes, none or little governance, lack of priority, no data classification standards
• Stay at home
• Not watching Security/Sys Admins
Where to go for info (depends what you are looking for)
digitaltransactions.net/issues/current/
securitywizardry.com/
secureworks.com/
iso.org/iso/home.html
nist.gov/index.html
ssae-16.com/
ithandbook.ffiec.gov/
isaca.org/Pages/default.aspx
Questions

- Robert.satchmo.anderson@gmail.com