Third-Party Breaches

James Christiansen
VP, Information Risk Management
Accuvant, Inc.
Polling Question
The Beginning of a Bad Day

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

Did we do a recent security review?  NO

Do we outsource to this third party?  YES

Do we have insurance to cover the costs?  NO

Are we prepared to respond to the media, our customers and the board of directors?  NO

Have we contacted our regulators?  NO

Have we been contacted by the media?  YES
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
Managing Third-Party Risk

Third-Party Business Profile

Relationship with Third Party

IT Controls Analysis
Process for Managing Third-Party Risk

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/PCI

4. Electronic Validation
   - Onsite Validation
   - Control Evidence

5. Changes in Relationship
   - Changes in Business
   - Changes in Controls

- Relationship Risk – What Are They Doing for Us?
- Business Profile Risk – Who Are They?
- How Are They Protecting the Information?
- Monitoring and Reporting
- Control Validation

ACCUVANT + fishnet SECURITY
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
Managing Third-Party Risk

- USA Today survey of 40 banks 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

Average Enterprise Has 1000s of Third-Parties

Tier 1

Tier 2

Tier 3
Polling Question
Validating IT Controls

- Onsite Third-Party Validation
- 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
Polling Question
Other Ideas on Third-Party Risk Management

What other ideas do you have on best practices for third-party risk management?

(Please step up to the microphone and let’s discuss)
Polling Question
Changing the Paradigm

- Third-party risk assessments are disruptive to your third party. Getting assessed 100’s of times a year takes incredible resources!

- **It is Time For a Change!**
  - A standard set standard set of criteria that serves 90% of the needs
  - The ability to gather the information once and share many
  - Automating the process of audits and remediation
Polling Question
Big Question – Best Practice or Bust?
Apply It

✓ Assess your program to make sure you have a risk-based process
✓ Consider the alternatives we discussed today

✓ Complete your third-party risk inventory and classify third parties into tiers
✓ Formalize your plan

✓ Establish a monitoring and reporting practice for managing third-party risk
Questions?

jchristiansen@accuvant.com
Test poll