Painting the Whole Picture: Managing Third-Party Risk on the First Try

W. Jackson Schultz CISA, GSEC
Who is this guy?

Current Role:
Lead Information Security Analyst, Corporate Risk Management – Discover Financial Services

Duties:
- Reporting on information security key risk indicators (KRIs)
- Performing and managing vendor risk assessments
- Contributions and membership to a number of information security and vendor-risk related steering and governance committees
- Designing and implementing enhancements to third-party information security framework/standard

Certifications:
- CISA – ISACA
- GSEC – SANS Institute

Past Speaking Events:
- ISACA AGM
- The Warren Group’s Bank Summit
- The Warren Group’s BankWorld
- The NEACH Payments Conference
- Cloud Security Alliance (CSA) Boston Chapter
- ASIS New England Security Expo

Education:
- B.S. in Computer Science – Salem State University
- Executive Master in Cybersecurity (EMCS) – Brown University

Contributions to Publications:
- bankinfosecurity.com
- Sophos Naked Security
- CIOReview

Past Roles:
- Senior Audit and Security Consultant - OCD Tech
- Security Consultant - GraVoc Associates
Disclaimer

Nothing in this presentation speaks to or is related to processes within Discover.

The views expressed are mine and are not necessarily those of Discover.
Third-Party Risk

- Third-party risk and diligence is a challenge for organizations across industries and ranging in size.

- What industries are represented in this room?
- How large is your organization?
Third Parties = Risk

Increasing Number of Third Parties*

*This is not a scientific chart
Managed Services

Of course outsourcing activities is critical to the business, but with that comes added risks.

https://www.microsourcing.com/blog/the-ultimate-list-of-outsourcing-statistics.asp
Only 35% of enterprise security professionals are very confident in knowing the actual number of vendors accessing their systems.

Vendors are accessing your network more than you think. On average, 89 vendors are accessing a company’s network every week.

75% of businesses saw third-party access grow over the past two years.

69% of respondents say they definitely or possibly suffered a security breach resulting from vendor access within the last year.

*Source: Bomgar survey*

On average, organizations spent $10 million responding to third-party breaches over a 12-month period in 2016.

*Source: CSO Online*

63% of all cyber attacks could be traced either directly or indirectly to third parties.

*Source: Soha Systems*
Risk is Relative

• Large companies have thousands of vendors
• Smaller companies can have hundreds
• Tracking and monitoring risk can be a major challenge for these companies for any of the following reasons
Challenges (Raise your hand)

• Knowledge and Education
• Resources and Staffing
• Contracting/Legal
• Documentation and Tracking
• Reporting on Risk
• Approval and Acceptance
Some Regulations re: Outsourced Services

• GLBA Safeguards Rule (16 CFR 314)
• HIPAA
• GDPR
The vendor management process should have a life cycle, and information security should play a role in each area.
The vendor management process should have a life cycle, and information security should play a role in each area.
Qualifying and Quantifying Vendor Risk

Vendor Management Life Cycle

- Renewal
- Identify Requirements
- Contracting
- Management & Assurance
- Onboarding

Third-Party Information Security’s Role

- Work with business to identify security risks surrounding requirements
- Work with legal to ensure that all important and key information security related clauses are in the contracts (including right to audit clause)
- Perform an inherent risk assessment to identify a risk baseline for tiering
- Perform an assessment/control analysis to identify deficiencies in third-party environment in key risk areas
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal

Qualifying and Quantifying Vendor Risk

Vendor Management Life Cycle

- Renewal
- Identify Requirements
- Contracting
- Management & Assurance
- Onboarding

Third-Party Information Security’s Role

- Work with business to identify security risks surrounding requirements
- Work with legal to ensure that all important and key information security related clauses are in the contracts (including right to audit clause)
- Perform an inherent risk assessment to identify a risk baseline for tiering
- Perform an assessment/control analysis to identify deficiencies in third-party environment in key risk areas
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal

Qualifying and Quantifying Vendor Risk

Vendor Management Life Cycle

- Renewal
- Identify Requirements
- Contracting
- Management & Assurance
- Onboarding

Third-Party Information Security’s Role

- Work with business to identify security risks surrounding requirements
- Work with legal to ensure that all important and key information security related clauses are in the contracts (including right to audit clause)
- Perform an inherent risk assessment to identify a risk baseline for tiering
- Perform an assessment/control analysis to identify deficiencies in third-party environment in key risk areas
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal
- Report on these findings, track KRIs, and ensure vendor has remediated during contracting term prior to renewal
Risk is relative. Meaning, my risk may (will) differ from your risk. Single-entity solutions will not solve the problem.

There are a number of third-parties that claim to be a one-stop-shop for vendor risk analysis and management. HIPAA risk is different than GLBA risk which is different than GDPR risk.

Only information security partitions who are intimately familiar with the business outsourcing activities can accurately qualify and quantify vendor risk.

Every vendor relationship is different, and should be examined with a fresh lens. Inferences can lead to gaps.
Vendor risk assessments are a key component of strong vendor management. There is a lifecycle to these as well.

1. Request initial call with third-party to question accuracy of inherent risk assessment
2. Examine the inherent risk assessment for inaccuracies
3. Tier vendor appropriate to categorize them based on risk presented to the company
4. Perform in-depth analysis on control environment (and legal documents) to ensure your information is safeguarded
5. Share any findings with business representatives (ensure that they are issue owners for accountability)
Risk Assessment

The assessment should be commensurate to the level of risk that the company presents.

You are not going to assess a vendor that prints marketing materials as in-depth as you would a company with which you are sharing PII.

This is an important distinction.

Risk must be prioritized and monitored.

Tiering vendors based on volume of data, transfer methods, resiliency requirements, criticality and sensitivity of data, (among other fields) is a must to ensure prioritization is in place to support efficiency.
The vendor risk assessment is a critical piece of the vendor management cycle. Vendor due diligence is essentially a requirement of every data privacy and security regulation, and is covered a best practice within information security.

Vendors can be assessed using a number of frameworks, or an amalgamate of a few (i.e. NIST CSF, SANS Top 20).

Vendor diligence is no small order.

During the diligence process, an assessor must identify (among other things):

- Internal ownership specifics
- Company size
- Location of HQ
- Products
- Usage
- Environment access
- Type of data received
- Type of data processed
- Financial position
- Resilience requirements
- RTO/RPO defined and met
- Control strength
- Location of data
- Cloud usage
- Usage of fourth-parties
- Internet footprint
- Data access
- Control gaps
Which Poses More Risk?

Vendor A
- **Volume**: 250m Records/Year
- **Criticality**: Low Risk Data
- **Transfer** Method: HTTP

Vendor B
- **Volume**: 15k Records/Year
- **Criticality**: High Risk Data
- **Transfer** Method: SFTP
Which Poses More Risk?

Vendor A
- **Volume**: 250m Records/Year
- **Criticality**: Low Risk Data
- **Transfer** Method: HTTP

Vendor B
- **Volume**: 15k Records/Year
- **Criticality**: High Risk Data
- **Transfer** Method: SFTP

I hate to sound like a lawyer, but...
Which Poses More Risk?

Vendor A

- **Volume:** 250m Records/Year
- **Criticality:** Low Risk Data
- **Transfer** Method: HTTP

Vendor B

- **Volume:** 15k Records/Year
- **Criticality:** High Risk Data
- **Transfer** Method: SFTP

I hate to sound like a lawyer, but...

**It depends!**
Figure out what your critical services are.

- What lines of business are most important to your business?
- Do you have to secure a certain data type for regulatory reasons?
- Are there critical elements of your business that a vendor controls?

These are the questions you should ask yourself before you identify your criteria for risk ranking.
As mentioned above, the risk assessment process should be all encompassing, but for information security, data and resiliency requirements should be the priority. The assessment process should be as follows:

• Understand data/services third-party is providing

• Ensure contracts are in place with relevant clauses related to security and resiliency (Appendix J for financial institutions)

• Examine vendor infrastructure based on preestablished mandates (where third party information security meets or exceeds internal requirements)

• Evaluate data flow diagrams to understand exactly where data is going

• Understand fourth-party relationships (who else has access to your data)
As mentioned above, the risk assessment process should be all encompassing, but for information security, data and resiliency requirements should be the priority. The assessment process should be as follows:

• Review with understanding that a vendor’s environment expands past your data, and your data may only traverse in small subsection

• If short on time, focus only on areas where your data flows

• Weigh risk appropriately (physical security prioritization if vendor is storing hard copies of PII)

• Understand control gaps

• Ask questions (avoid questionnaires where possible)
The depth of an assessment process can vary by third-party, but should be memorialized in policy.

If a vendor is tiered on the lower end of the risk scale (defined in a framework or standard), and open-source intelligence report alongside diligence evidence (such as a SOC2) may be sufficient for documentation.

If the vendor poses larger risk, an interview, on-site visit, and in-depth evidence review may be required to sufficiently yield an opinion on a third-party’s risk posture.

Legacy reports should be retained. This is not only for regulatory reasons, but to track process of the strength of a vendor’s environment.
Often times, vendors may not have strong enough control environments to your liking. This is an opportunity to identify findings and inspire change throughout their organization.

Findings can be identified and issued to the third-party. The important piece of this, however, is that the business unit responsible for the third-party is the one tracking them and ensuring that remediation takes place.

Information security does not have the rapport with the vendor, and does not have influence on the contracting process (even though we like to think we do).
If the business unit requires the vendor perform remediation, and the vendor is at risk of losing a contract if they do not, they often will make the changes required to safeguard their, and in turn your infrastructure.
Key Risk Indicators (KRI) can be incredibly useful metrics to understand what risks exist in your vendor portfolio. Some examples of KRI are:

- Number of vendors involved in resiliency
- Number of RTOs that don’t align with internal requirements
- Past due findings
- Elevated risk vendors
- OSINT data changing on an ongoing basis
- Metrics produced by a third-party
- Number of companies with remote access to systems
- New supplier arrangements
- Residual risk composite score
- Inherent risk composite score
- Number of known incidents related to highest tier third-parties
Key Risk Indicators (KRIs) should be tracked, updated on a regular basis, and shared with a committee or executive management.

KRIs that reflect the highest risk can even have a place in the board room.
Now, it wouldn’t be third party risk management if we didn’t talk about incidents.

Incident management is an important part of the vendor management process, but not one that typically falls under the diligence team’s requirements (by policy).

As mentioned earlier, “69% of respondents say they definitely or possibly suffered a security breach resulting from vendor access within the last year.” – Source: Bomgar survey
Third-party information security plays a crucial role in incident response, but don’t get confused – third-party information security is **not incident response**.

**Don’t act as forensics or as part of SIRT (unless that is your defined duty).**

Too often, individuals without training try and employ themselves in recovery from a breach. These are personnel without proper training. Incident recovery, particularly in regulated industries, can be a very sensitive area. Mistakes can be very expensive.
Third-party information security should absolutely partner with the recovery teams as requested, and can provide significant value.

Third-party information security can:
- Provide a list of the unique data attributes, and volume, that the third-party is retaining, storing or processing
- Can provide information about how the data is transferred to them
- Can provide information about security control gaps and environmental hazards that may have led to the incident within the third party
- Partner with incident response to help contain the issue

Third-party information security should not:
- Act as IR.
- Take over the investigation.
- Perform hands-on-a-keyboard analysis without proper approval.
Roles and responsibilities should be clearly defined in a company’s incident response plan.

*Third-party information security can play a role in any of these areas, with proper approval.*
Third-party information security is a cyclic process.

Third-party diligence the best way to really understand risk posture when outsourcing activities.

It requires a wide understanding of risk areas, because it encompasses aspects of information security, physical security, legal, and incident response.

Because of its complexity, ongoing training is a must.

Third-party information security can inspire real change in a company’s vendors.

Third-party information security should not act as the only legal insight, or take over during incident response.
Let’s have a conversation

Where do you feel your biggest challenge lies with vendor diligence?
• Understanding vendor access to systems?
• Tracking data attributes and transmission methods?
• Legal clauses and contracting?
• Convincing vendors to let you perform diligence?

What do you wish you could change about your vendor management process?

Do you feel as though your vendor diligence team is sufficiently staffed and educated?

Do you feel as though you need additional resources to focus on this area?

Are challenges typically related to data transfer or resiliency?

Are you confident in your incident response program as it related to third-parties?
Questions?
Thank you!

W. Jackson Schultz CISA, GSEC

Lead Information Security Analyst

Discover Financial Services

willisschultz@discover.com