Managing Security Risks of Vendor Relationships

Terese Thomas, Director
Terese.m.thomas@uhc.com
UnitedHealth Group
March 15, 2018
Agenda

• Who will Benefit
• Regulations
• Major Risks
• Key Stakeholders
• Data Governance
• Identify Your Vendors
• Minimum Necessary
• Contracts
• Appropriate Risk Tier
• Developing a Closed Loop Vendor Assessment Program
• Questionnaire
• Risk Identification/Monitoring/Reporting
• Summary
Who Will Benefit

• Information Security
• Information Technology
• Business Owners who use/engage Vendors (Vendor Relationship Owners)
• Procurement
• Financial Officers
• Risk/Governance
• Operational Managers
• Board Members
• Legal
• Internal and External Auditors
Regulations

Most industries need to adhere to Regulations:

Financial, Health Care, Pharmaceuticals, Government, Higher Education

Domestic & International
Major Risks

- Overwhelming Statistics
  - A survey by Soha Systems places the percentage of all data breaches linked directly or indirectly to third-party access at 63% according to IAPP.
  - According to PwC’s Global State of Information Security Survey, the number of data breaches attributed to third-party vendors increased by 22% since 2015.
  - Only 52% of companies have security standards for third-parties, according to PwC.
  - 28% of organizations have experienced an advanced persistent threat attack, and three-quarters have failed to update their third-party vendor contracts to include better protection against APTs.” Source: 2015 Advanced Persistent Threat Awareness Study, as quoted in Trustwave Security Stats.

- You MUST Protect your Organization’s Reputation
  - Risk of Reputational Harm

- You MUST Protect your enterprise
  - Accountability

You can Outsource Security
You can Outsource to your Vendors
You cannot Outsource Accountability

THOMAS
Key Stakeholders of Vendor Management

- Business (Vendor Relationship Owner)
  - Supporting the Process
  - Document business requirements
  - Escalation to Vendors for Non-Compliance
- Executive Team/Board of Directors
  - Oversight
  - Documented Accountability
  - Support
  - Budget
- Information Security
  - Developing, maintaining, and communicating a comprehensive Vendor Management Program
- Legal
  - Developing contractual language
  - Consultation on applicable laws and regulations
- Data Governance
- Procurement
  - Facilitation in Contract Negotiations
Data Governance Program

Data governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures, and a plan to execute those procedures.

- Do you have a Data Governance Program?
- Do you know what data is leaving the organization?
  - Which vendors (customers/providers/others) are getting what data?
  - How do you know WHO (internally) is sending WHAT (data classification/quantity) to WHO (externally)?
    - Is that person APPROVED to send the data?
    - Are they using an APPROVED method of delivery?
  - Do you have a defined release owner, data custodian and risk approver for each data release?
Identify your Vendors

Do you have all of your organization’s vendors identified?
- You should know who your vendors are and what kind of data they store/host/transmit/receive and/or if they have remote access to your system(s).
- These vendors are an extension of your organization (i.e. liability)
- Ensure you have included vendors from Acquisitions

Ensure you understand the scope of work the vendors are supplying
- Has the Business Owner shared the requirements of the Vendor?
- Has the Business Owner properly followed all channels for on-boarding?

Ensure you have a contact(s) at the Vendor site in case of a issue (i.e. world wide vulnerability)
Minimum Necessary

Data Classification

- Identify the risk to the organization by data classification based on Sensitive, Non-Sensitive, Proprietary, Confidential, Secret, Classified, Protected, Public, Other

Minimum Necessary

- Ensure the vendor absolutely needs to store/host/transmit/receive data
- If the data does leave your environment, remember **Minimum Necessary**
- Implement technical controls to monitor data leaving the environment. Ensure vendor accesses only applicable system(s)/data.
It all STARTS and ENDS with a Legal document.

1) Do you have specific language in your Contract that contains security requirements for Vendors who store/host/access/receive/transmit Sensitive/Confidential Data and/or remote access to Sensitive/Confidential Data?
   • The contract needs to have clear expectations on the vendor including data security/privacy and the vendor’s ability to protect your data.
     • Describe how the Vendor is permitted and required to use sensitive data.
     • Require that the Vendor not use or disclose sensitive data other than as specified in the contract or as required by law.
     • Require the Vendor use appropriate safeguards to ensure the sensitive data is used as detailed in the contract.
     • Ensure you have the “right to audit” both via electronic questionnaire and at Vendor location(s).
     • Discuss Business Continuity Needs with the business and add those in the contract.
     • Incident reporting
     • What are you promising your customers?
       • Are you promising your customers a 8 hour window for a potential breach? Vendors need to provide notice of incidents regarding YOUR data to you sooner than 8 hours
       • Include a right to Terminate based upon any reason, including failure to adhere to security requirements.

2) Establish SLA’s in SOWs and MSAs
   • Incident reporting
   • Remediation
   • SLA’s should not only include timeframes.
     • It should also provide remedies when requirements aren’t met.
     • It should Include consequences
Appropriate Risk Tier/Ranking

If you have a large number of vendors that store/host/transmit/receive Sensitive data, you may want to develop a tier model by assigning a tier level based upon risk level and data classification.

Questions:
- Will vendor store/host/transmit/receive data?
  - Can Vendor access data remotely instead?
- What is the data classification?
- Will vendor have connectivity to your systems?
  - Is there a secure method in place for remote connectivity?
    - Encrypted channel
    - Logging
    - Data Loss Prevention

Criteria:
- Your level of due diligence could be based on risk.
- If you have a smaller organization with a few vendors, perhaps a Tier structure is not necessary.
- Considerations:
  - Business Scope
  - Risk
  - Quantity of records
  - Data Classification
  - Frequency of data delivery
  - Where the data is stored
  - Method of delivery
Developing a Closed Loop Vendor Assessment Program

- Vendor Onboarding
  - Contracts
  - Security Risk Assessment
  - Minimum Necessary
  - Data Governance
  - REMEDIATION

- Ongoing Oversight
  - Periodic Risk Assessment
  - Periodic Business Requirement Check
  - Periodic Regulation Check
  - Data Governance Renewal
  - REMEDIATION

- Vendor Termination
  - Consistent/Documented Termination Process
  - Logical and Physical Access is Termined
  - Formal Data Destruction
Risk Questionnaire

- Decide which framework to use

- Review applicable questions based on Risk
  - Samples can be found on the internet
  - Third party vendors available to assist

- Establish a Software Repository for Vendor Assessments (source of truth)
  - Many tools are available in the marketplace for Vendor assessments.
    - Software that will enable you to automate and streamline ongoing oversight of third party relationships
    - Software that is accessible by the Key Stakeholders
    - Automation Opportunity
    - Vendor questionnaire and artifacts
    - Allow the vendor to access a Portal to answer questions and supply information (Use 2FA)
    - It can be worth the expense (especially when you have many vendors that carry large risks)

- Establish a Remediation Program/Plan

- Require Artifacts to substantiate Vendor’s replies i.e. Information security Policies (including but not limited to Asset management, clear desk, physical security, data classification) print screens of various security settings, de-identified network diagram, etc.
Risk Identification, Monitoring, Reporting

- All the information gathered and analyzed during the identification of risks serves as a foundation for further risk analysis, evaluation and estimation.
- Tracking identified risks, monitoring residual risks, identifying new risks, throughout the lifecycle.
- Timely, accurate and effective risk reporting is an integral part of a strong risk management framework.

Risk Identification

Risk Monitoring

Risk Reporting
Summary

- Know the Regulations for your Organization
- Ensure a contract with the appropriate provisions is executed with each/every Vendor
- Review Minimum Necessary
- Establish a Data Governance Process
- Ensure you have Support and Involvement from Legal, Business Areas, Procurement, and possibly Board Members
  - Identify a person/group to handle vendor escalations and/or vendor non-compliance
- Design questionnaire(s) based on risk
- Establish a repeatable closed-loop process
  - Ensure there is accountability and monitoring from various areas
  - Ensure there is a Follow-up for Remediation
- Review Vendor Management Software for applicability
- Monitor data exchanges and Data Loss Prevention tools for anomalies.
Thank you!

Terese Thomas
Terese.m.thomas@uhc.com