Vendor Oversight & Risk Management Tips

April 2017

Rebecca Herold, FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI
CEO, The Privacy Professor®
President, SIMBUS360

phone: 515.491.1564
fax: 515.864.0274
rebeccaherold@rebeccaherold.com
http://www.privacyprofessor.org
http://www.SIMBUS360.com
http://www.privacyguidance.com

Vendor Oversight & Risk Management Tips

1. **Common security and privacy risks found during 300+ vendor assessments; be sure to look for these**

   a. Vendor employees have never read their organization's posted privacy notice, and so do not perform the necessary activities to support the privacy promises made within it.
   b. Lack of documented information security and privacy policies and procedures.
   c. No use of encryption.
   d. No documented business continuity / disaster recovery policies or procedures.
   e. No information security and/or privacy training, or really poor training.
   f. No formal procedures, processes or tools are used for the disposal or retirement of computing and digital storage devices, or for hard copy information.
   g. No data retention policies or procedures are in place. All data is kept "forever."
   h. No information security or privacy risk assessments have ever been performed, or the most recent was performed more than two years ago.
   i. Wireless access points to vendor networks, systems, and end points are unsecured (no authorization required, no encryption, etc).
   j. No regular reviews of the internal network for vulnerabilities by those responsible for network management.
   k. No external network vulnerability or penetration tests have been performed.
   l. Answers vendors provide on security and privacy assessments do not match their actual practices.
   m. Subcontracting activities without notifying or getting authorization from their clients to do so.
   n. Lack of knowledge or understanding about legal requirements for data protection.
   o. Unpatched systems and lack of adequate security, such as no firewall, no anti-malware, no IPS/IDS, etc.
   p. No formally documented definition of "personal information."
   q. Assumptions that certain types of personal information that they have been entrusted with from their clients do not need to have protections or safeguards (e.g., names, phone numbers and email addresses are common ones).
   r. Re-using and even re-selling the personal information, entrusted to them from their clients, to other organizations as an additional revenue line for their business.
   s. Leaving personal information in prior work locations.
   t. Lack of security and privacy controls on employee-owned devices used for work activities.
   u. No mitigation actions have occurred for security and privacy breaches.
   v. No knowledge of contractual obligations for security and privacy controls by those who are the ones that would have needed to perform those actions.
   w. No documented or formal information security or privacy responsibilities have been established.
   x. Security and privacy responsibility is too low within the organization resulting in ineffective security and privacy implementation and enforcement.
   y. Vendors state that they believe they have no information security or privacy responsibilities if they are a cloud entity.
   z. Vendors state that they do not need to implement information security or privacy controls because they believe the MSP they use is responsible for all security and privacy activities.
   aa. Vendors state that they do not need to implement information security or privacy controls because they believe their clients they are doing work for are responsible for all security and privacy activities.
   bb. Using the same IDs and/or passwords for all their clients.
   cc. Employing disgruntled former employees of their clients and they are providing the service to those clients.

2. Make sure you include all necessary issues within vendor contracts

a. Hold vendors to the same security & privacy standards as you have for your own organization.
b. Create a template of standard information security and privacy contract clauses. These should be customized as necessary for each vendor; but it is helpful to have a standard to start with.
c. Have a flowchart or a simple mechanism that all stakeholders agree to for vendor vetting and inserting standard contract language clauses. The flowchart should take in to account things like the type of data outsourced, the criticality of the business processes, if the vendor would affect your supply chain, and the information security and privacy regulations that come into play in the outsourcing.
d. Establish an agreed upon methodology for estimating the cost of a vendor breach based upon the associated services provided, and types and amounts of personal information they access.
e. Check on the vendor's data retention policies and requirements. Some vendors have their own regulatory obligations that make this difficult. If they need to retain your data longer than the contract period, ensure that liability for this is built in to the contract.
f. Regularly meet with your key internal stakeholders to discuss vendor management activities and stats.
g. Have a clearly documented breach notification process the vendor must follow for security incidents. Include notification time requirements.
h. Ensure all vendor contracts have been reviewed by legal counsel.
i. Provide a summary of exactly what the vendor is doing or providing for the organization to counsel.
j. Inform counsel if any PII may be collected or stored by the vendor related to the work they do for the organization.
k. Ensure all rates are clearly understood and how much it would cost to leave the agreement before the term.
l. Use clear language that describes what happens if either party defaults on the agreement and what constitutes a default.
m. Define data ownership and who can transfer ownership and when.
n. Define who may or may not have access to accurate information.
o. Establish the role or entity responsible for encryption keys and who has access.
p. Require monthly or quarterly attestations from your high-risk vendors' executive management.
q. Require vendors to perform at least annual risk assessments, for low risk vendors, to more often for high risk.
r. Ensure their definition of personal information matches your organization's definition.
s. Ensure they use basic security technology, such as anti-malware, firewalls, IDS/IPS, etc.
t. Make sure both parties clearly understand the limitations of liability and whether a separate agreement, such as a Business Associate agreement is required for matters related to personal information.
u. Ensure confidentiality is understood and required for the vendor with any sensitive information.
v. Request NDAs to be signed with the organization as well as with each employee working with PI.
w. Verify if multitenancy of data is used by the vendor and how they segregate sensitive data.
x. Ensure there is a plan in the event acts of God occur for disaster recovery and business continuity in Service Level Agreements and Operating Level Agreements.
y. Understand what provisions survive the end of the agreement, and if there is any privacy impact associated with the survivable clauses.
z. Know the value of the information stored and value if lost. Ensure insurance requirements are reasonable for general liability coverage and privacy related issues.
aa. Some vendors will not modify their master agreements, so focus on discussing amendments and possible statements of work for more definition.

3. Issues businesses need to consider for their vendors when determining the types of assessments to use for them

a. Perform a high-level risk evaluation at the beginning of the relationship, or prior to establishing the relationship, to determin the level of risk the vendor brings to your organization.
b. One size does not fit all. A one-person business doing a very dedicated type of work for your organization should not be expected to do the same type of assessment as a large, decentralized, and complex organization that offers multiple services. Types of assessments should align with the types of vendors..
c. Do not use an assessment that will cost more for the vendor to take than the amount you are paying them for their work or service.
d. Be wary of assessments that claim "certified compliance." Compliance levels vary on an ongoing basis as changes in the business environment occur, new threats and vulnerabilities are discovered, and as new legal requirements arise. There is no such thing as "Certified 100% Compliance" or similar.
e. Do an online search of the vendor to see if there has been any adverse information published, reported by news stories, lawsuits or breaches. If so, include questions to determine if the vendor has mitigated the associated issues.

4. Often overlooked information that should be documented

a. Document all the types of information items to which each vendor has some type of access or possession.
b. Document the map of data flows with vendors, including the types of information items, types of transmissions, and security controls associated with each transmission.
c. Document the names of vendor personnel with access to sensitive personal information and mission critical information. Make sure employees get disconnected when they leave the vendor, and when they are no longer involved with the client's work. Establish a procedure for the vendor to follow to notify you when one of their workers who had access to your data/systems leaves their organization.
d. Document all the subcontractors your vendors use with access to your data and systems.
e. Determine if the vendor has had any security incidents, or privacy breaches. If so, what kind were they, and have they mitigated the weaknesses that allowed for them?
f. For incidents and breaches, did the vendor take actions to mitigate the risks and prevent similar subsequent incidents?
g. Determine if their require background checks for personnel authorized to access personal and sensitive information.

5. Other overlooked but important third parties for you to consider and mitigate risks that often have access to an organization's network, systems, data, etc.

a. Business partners (investors, collaborators, strategic alliances, etc.)
b. Government agencies (worker's comp government agencies, agencies with tax info, etc.)
c. Volunteers (fund raisers, patient assistance and drivers, etc.)
d. Researchers (marketing, healthcare, new product development, etc.)
e. Students (teaching hospitals, interns, shadowing programs, etc.)
f. Etc.

Vendor Oversight & Risk Management Tips

6. Additional Due Diligence

a. Ask others in your industry to see if they have performed due diligence for specific vendors to gain additional insight.
b. Ask others for references to vendors you are considering.
c. Determine if and how the vendor detects advanced persistent threats. Research to understand how this vendor may be targeted.
d. Determine the type of cyber liability insurance they have, and if/how your organization would be prioritized in the event of a breach.
e. Verify you are named as an insured on their privacy liability insurance.
f. Determine the coverage your cyber liability policy provides in the event of a breach at a vendor (contractors are often not covered).
g. Regularly review the network connections with vendors to detect changes.
h. Request any existing vendor SOC reports, SSAE 16, and other types of security assessment reports.
i. Consider if using a third-party rating service would be beneficial for your business.
j. Set a news alert for your vendors.
k. Regularly check to ensure vendors are adhering to agreed-upon record retention obligations.
l. Monitor to ensure that contacts from your company provided to vendor remain valid, for example who to contact in the event of a breach.
m. Send a Request for Information (RFI) to vendor competitors to compare and contrast agreement language.
n. Verify the amount of insurance coverage your organization has for privacy related issues.
o. Identify the educational options are available for employees and possible vendor employees from your organization.
p. Ensure vendors adhere to third-party audits and provide their clients with annual reports.
q. Some privately held companies may not divulge financial information. However operational, security, HR, and basic financial controls should be provided upon your request.
r. Ask for evidence of security and privacy training and education.
s. Send a reminder at least six months before the expiration of vendor contracts to review any scope changes to allow for time to negotiate terms.

See more in-depth discussion of many of these vendor security and privacy management topics at:
http://privacyguidance.com/blog/category/ba-and-vendor-management/

For more information:
rebeccaherold@rebeccaherold.com
SIMBUS360: https://www.SIMBUS360.com
SIMBUS Tracker: https://simbus360.com/vendor-management-software/
Twitter: http://twitter.com/PrivacyProf
http://twitter.com/SIMBUS360