Vendor and Supply Chain Security Oversight & Risk Management Tips

July 2021

Rebecca Herold

CEO, The Privacy Professor®
CEO, Privacy & Security Brainiacs
CDPSE, FIP, CISSP, CIPP/US, CIPT, CIPM, CISM, CISA, FLMI, Ponemon Institute Fellow

https://www.privacysecuritybrainiacs.com
https://www.privacyguidance.com

phone: 515.491.1564
fax: 515.864.0274
rebeccaherold@rebeccaherold.com

Table of Contents

A. Common Security and Privacy Risks

Here are common security and privacy risks and red flags we've found in over 500 vendor and supply chain security (VSCS) assessments. Be sure to look for these.

1. Vendor employees have never read their organization's posted web site privacy notice[1], and so do not perform the necessary activities to support the privacy promises made within it. And/or the same applies to their posted web site security policy.
2. Lack of documented internal organizational information security and privacy policies and procedures.
3. No use of encryption; for data transmissions, data in storage, and/or data as it is being collected online.
4. No documented business continuity / disaster recovery policies or procedures.
5. No workforce information security and/or privacy training, or really poor or outdated training.
6. No formal procedures, processes or tools are used for the disposal or retirement of computing and digital storage devices, or for hard copy information.
7. No data retention policies or procedures are in place. All data is kept "forever."
8. No information security or privacy risk assessments have ever been performed, or the most recent was performed more than two years ago.
9. Wireless access points to vendor and supply chain networks, systems, and end points are unsecured (no authorization required, no encryption is used, etc.).
10. No regular reviews of the internal network for vulnerabilities are performed by those responsible for network management.
11. No external network vulnerability or penetration tests have been performed.
12. Answers that vendors, supply chain entities, and other types of third parties provide on security and privacy assessments do not match their actual practices.
13. Third parties subcontract activities without notifying or getting authorization from their clients to do so.

[1] The "privacy notice" on a web site is also often called a "privacy policy." So, in the context of being the document on a web site that contains information about privacy practices, and for the purposes of this document, you can use the terms "privacy notice" and "privacy policy" interchangeably.

14. Lack of knowledge or understanding about legal requirements for data protection.
15. Unpatched systems and lack of adequate security, such as no firewalls, no anti-malware, no intrusion prevention system / intrusion detection system (IPS/IDS), etc.
16. No formally documented definition of “personal information,” or “personal data,” or whatever term has been chosen by the organization to mean personal information.
17. 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).
18. 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.
19. Leaving personal information in prior work locations.
20. Lack of security and privacy controls on employee-owned devices used for work activities.
21. No mitigation actions have occurred for security and privacy breaches.
22. No knowledge of contractual obligations for security and privacy controls by those who are the ones that would have needed to perform those actions.
23. No documented or formal information security or privacy responsibilities have been established.
24. Security and privacy responsibility is positioned within roles too low within the organization, resulting in ineffective security and privacy implementation and enforcement.
25. Vendors state that they believe they have no information security or privacy responsibilities if they are a cloud entity.
26. Vendors state that they do not need to implement information security or privacy controls because they believe the managed service provider (MSP) they use is responsible for all security and privacy activities.
27. Vendors state that they do not need to implement information security or privacy controls because they believe their clients, for whom they are doing work, are responsible for all security and privacy activities.
28. Using the same IDs and/or passwords for all their clients.
29. Employing disgruntled former employees of their clients, and they are providing the service to those clients.

B. Vendor and Supply Chain Contracts

It is critical to address security, privacy and compliance within your vendor and supply chain management contracts. Here are the requirements that are necessary for inclusion within most types of third-party contracts.

1. Hold vendors and supply chain entities to the same security & privacy standards as you have for your own organization.
2. Create a template of standard information security and privacy contract clauses[2]. These should be customized as necessary for each vendor, supply chain entity, etc.; but it is helpful to have a standard to start with.
3. Have a flowchart or a simple mechanism that all stakeholders agree to for vendor and supply chain entity vetting and inserting standard contract language clauses. The flowchart should take into 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.
4. Establish an agreed upon methodology for estimating the cost of a vendor or supply chain entity breach based upon the associated services provided, and types and amounts of personal information they access.
5. Check on the vendor's or supply chain entity's data retention policies and requirements. Some vendors/supply chain entities 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.
6. Regularly meet with your key internal stakeholders to discuss vendor and supply chain entity management activities and stats.
7. Have a clearly documented breach notification process the vendor and supply chain entities must follow for security incidents. Include notification time requirements.
8. Ensure all vendor and supply chain entity contracts have been reviewed by legal counsel.
9. Provide to the organization's legal counsel a summary of exactly what the vendor and supply chain entity is doing or providing for the organization.

[2] Examples of such clauses are available from Privacy & Security Brainiacs. Contact us at: info@privacysecuritybrainiacs.com

10. Inform counsel if any personal information (PI) may be collected or stored by the vendor/etc. related to the work they do for the organization.
11. Ensure all rates are clearly understood and document how much it would cost to leave the agreement before the term.
12. Use clear language that describes what happens if either party defaults on the agreement and what constitutes a default.
13. Define data ownership and who can transfer ownership, to where, and when.
14. Define individuals and entities that may, and those that may not, have access to information.
15. Establish the role or entity responsible for encryption keys and document the individuals that have access.
16. Require monthly or quarterly attestations from your high-risk vendors' and supply chain entities' executive management[3].
17. Require low-risk vendors and supply chain entities to perform at least annual risk assessments, and vendors and supply chain entities of higher risk to perform them more often.
18. Ensure their definition of personal information matches your organization's definition.
19. Ensure they use basic security technology, such as anti-malware, firewalls, intrusion prevention system / intrusion detection system (IPS/IDS), etc.
20. 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.
21. Ensure confidentiality is understood and required for the vendors and supply chain entities with any sensitive information.
22. Request non-disclosure agreements (NDAs) to be signed and returned to the organization as well as with each employee working with PI.
23. Verify if multitenancy of data is used by the vendor or supply chain entity, and how they segregate sensitive data.

[3] Privacy & Security Brainiacs (https://privacysecuritybrainiacs.com/) has examples of such attestations available. Contact us for more information: info@privacysecuritybrainiacs.com

24. Ensure there is a plan in the event acts of nature occur for disaster recovery and business continuity in Service Level Agreements and Operating Level Agreements.
25. Understand the provisions that survive the end of the agreement, and if there is any privacy impact associated with the survivable clauses.
26. Know the value of the information stored and value if lost. Ensure insurance requirements are reasonable for general liability coverage and privacy related issues.
27. Some vendors and supply chain entities will not modify their master agreements, so focus on discussing amendments and possible statements of work for more definitions.

C. Considerations for Vendor and Supply Chain Risk Evaluations & Assessments

Performing security and privacy risk evaluations (typically high-level) and risk assessments (typically more detailed) for vendors and supply chain entities is highly recommended. Be sure to perform such assessments for at least the entities that have the most operational and legal compliance impacts to your organization, as well as for those that have access to personal information and intellectual property. Here are the issues to consider for such assessments.

1. Assessments for vendors and supply chain entities that store, collect, process or otherwise access in some way personal data, and other types of regulated data, will necessarily be longer than those where such data is not involved. Such data inherently increases risks, so as a result more questions are needed.
2. Assessments for vendors and supply chain entities that are located outside of the country where the business is based will typically require more questions related to data transfer issues, and issues for countries that have established laws governing the countries with which organizations can do business, due to political sanctions and/or global commerce restrictions.
3. Perform a high-level risk evaluation at the beginning of the relationship with the vendor or supply chain entity, or better yet, prior to establishing the relationship, to determine the level of risk the vendor or supply chain entity brings to your organization.
4. 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 risk assessments and risk evaluations used should align with the types of vendors and supply chain entities.
5. Do not use an assessment that will cost more for the vendor or supply chain entity to take than the amount you are paying them for their work or service.
6. 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 claims.

7. Do an online search of the vendor or supply chain entity 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.

D. Critical Documentation

Information is often not documented that needs to be to validate practices, to demonstrate due diligence, and to support consistently performed practices. Here are some of the types of such information documentation that are often overlooked.

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

E. Determine the Third Parties Supporting Your Organization

Many organizations do not know all the vendors, supply chain entities, and other types of third parties that they do business with, of some type, in support of their own business practices. However, this is absolutely necessary to be able to determine the security, privacy, and legal compliance risks to the organization. These types of organizations must be identified and documented, and then assessed for risk levels they bring to the business, to not only meet a large and growing number of legal requirements for such vendor and supply chain security (VSCS) and privacy oversight requirements, but also simply to support key business management practices. Such third parties often have access to an organization's networks, systems, software, data, hardware, and other types and forms of information and technology assets.

There are a very wide range of such third parties. Many of them are often overlooked, but important types of third parties for which every organization needs to be aware, to have documented, and to manage risks. Organizations need to ensure they include all the types of following third parties when building and updating their VSCS management practices and programs.

1. Business partners (investors, collaborators, strategic alliances, etc.)
2. Supply chain entities (manufacturers of software, firmware, hardware, etc.)
3. Government agencies (worker's comp government agencies, agencies with tax info, etc.)
4. Volunteers (fund raisers, patient assistance and drivers, etc.)
5. Researchers (marketing, healthcare, new product development, etc.)
6. Students (teaching hospitals, interns, shadowing programs, etc.)
7. Etc.

F. Additional Due Diligence

Here are some additional recommended actions to take to further strengthen your VSCS management program and practices.

1. Ask others in your industry to see if they have performed due diligence for specific vendors/supply chain entities to gain additional insight.
2. Ask others for references to vendors/supply chain entities the organization is considering.
3. Determine if and how the vendor/supply chain entity detects advanced persistent threats (APTs). Research to understand how this vendor/supply chain entity may be targeted.
4. Determine the type of cyber liability insurance they have, and if/how the organization would be prioritized in the event of a breach.
5. Verify the organization is named as an insured on their privacy liability insurance.
6. Determine the coverage your organization's cyber liability policy provides in the event of a breach at a vendor/supply chain entity (contractors are often not covered).
7. Regularly review the network connections with vendors/supply chain entities to detect changes.
8. Request any existing vendor/supply chain entity security operations center (SOC) reports, SSAE 18, and other types of security assessment reports.
9. Consider if using a third-party rating service would be beneficial for your business.
10. Set a news alert for your vendors.
11. Regularly check to ensure vendors are adhering to agreed-upon record retention obligations.
12. Monitor to ensure that contacts from your company provided to vendor remain valid; for example, the list of contracts to use in the event of a breach.
13. Send a Request for Information (RFI) to vendor/supply chain entity competitors to compare and contrast agreement language.
14. Verify the amount of insurance coverage your organization has for privacy related issues.
15. Identify the educational options are available for employees from your organization, and possible vendor/supply chain entity employees.
16. Ensure vendors/supply chain entities adhere to third-party audits and provide their clients with annual reports.

17. Some privately held companies may not divulge financial information. However operational, security, HR, and basic financial controls should be provided upon your request.
18. Ask for evidence of security and privacy training and education.
19. 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.

Do you have additional practices that you've found helpful for VSCS practices that are not listed above, and are not elsewhere in this Tips guide? Then please let us know! We may include them in our next update of this document. Send your ideas and suggestions to: info@privacysecuritybrainiacs.com

G. Foundational Vendor and Supply Chain Security Management Practices

The following recommendations are based upon guidance from the National Institute of Standards and Technology (NIST) SP 800-161 Rev 1: Cyber Supply Chain Risk Management Practices for Systems and Organizations[4]:

1. Establish a core team to manage vendor and supply chain security (VSCS) that will oversee managing and monitoring VSCS security and privacy risks. Include key stakeholders from within the organization, with subject matter expertise in key areas (read on to find those).
2. Ensure adequate resources are dedicated and allocated to vendor and supply chain information security and privacy management to ensure proper implementation of policy, guidance, and controls.
3. Establish and incorporate VSCS security and privacy requirements into the organizational security and privacy policies and supporting procedures and practices.
4. Develop a process for identifying and measuring the criticality of the organization's suppliers, products and services.
5. Raise awareness and foster understanding of the business criticality of VSCS management, for business management and employees with vendor and supply chain related job responsibilities.
6. Develop and/or integrate VSCS management activities and requirements into acquisition/procurement policies and procedures[5].
7. Establish and begin using supplier risk assessment processes on a prioritized basis (inclusive of criticality analysis, threat analysis, and vulnerability analysis) after the impact level[6] of each vendor has been defined. See sections A, B, and C for considerations when determining risk.
8. Establish explicit collaborative and discipline-specific roles, accountabilities, structures, and processes for supply chain, and vendor, cybersecurity, product security, and physical security (and other relevant) processes (e.g., Legal, Risk Executive, Human Resources

[4] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft.pdf
[5] For assistance with this, or policies and procedures templates in touch with us; we can help! info@privacysecuritybrainiacs.com
[6] See FIPS 199 for NIST recommendations for determining impact level. And/or contact info@privacysecuritybrainiacs.com to get more information and/or training materials.

(HR), Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/Procurement, Supply Chain Logistics, etc.).

9. Ensure there are sufficiently cleared personnel, with key VSCS roles and responsibilities, to access and share VSCS-related classified information. E.g., intellectual property, personal data, etc.
10. Implement an appropriate and tailored set of baseline information security controls, such as those found in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations[7].
11. Establish internal checks and balances with established contacts in vendor and supply chain entities who can be contacted, as needed, for your organization to ensure their compliance with security, privacy and quality requirements.
12. Establish a VSCS management program that includes documented guidelines for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers.
13. Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents and privacy breaches from within vendors and supply chain entities. This program should be capable of identifying causes of security incidents, including those originating from throughout the supply chain, as well as identifying necessary information related to personal data items, locations, sharing, safeguards, and other key information.
14. Provide training for processes involved with VSCS including but not limited to information security, procurement, risk management, engineering, software development, IT, legal, marketing and sales, physical security, internal audit, and HR, to name a few of the key areas typically involved with vendor and supply change management. (See the Privacy & Security Brainiacs continuously growing training library[8] for such classes.)

[7] Obtain NIST SP 800-53 Rev 5 (free) from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Privacy & Security Brainiacs has worked with NIST, and the SP 800-53 controls, since 2009, so we can provide a wide range of support for you if you need help using SP 800-53.
[8] Go to: https://privacysecuritybrainiacs.com/training/

H. More Mature Vendor and Supply Chain Security Management Practices

Slightly more advanced practices are recommended, but may not be feasible in some-to-many small to mid-sized businesses, or businesses with limited resources[9]. These include:

1. Use in-person third-party assessments, site visits, and formal certification to assess critical suppliers.
2. Use the organization's understanding of its VSCS risk profile (or risk profiles, specific to mission/business areas) to define a risk appetite and risk tolerances to empower leaders with delegated authority across the organization to make VSCS decisions in alignment with organization's mission imperatives and its strategic goals and objectives.
3. Embed VSCS specific training into training curriculums of applicable roles across the organization.
4. Integrate VSCS considerations into every aspect of the organization's system and product lifecycle, implementing consistent, well-documented, repeatable processes for system engineering, cybersecurity practices, and acquisition.
5. Integrate the organization's defined VSCS requirements into contractual language found in agreements with vendors, contractors, MSPs, cloud services, suppliers, developers, system integrators, external system service providers, and other information communications technology / operational technology (ICT/OT) related service providers.
6. Include key suppliers in contingency planning, incident response, and disaster recovery planning and testing.
7. Engage with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to improve their cybersecurity practices.
8. Define, collect and report VSCS metrics to ensure the organization has a vendor and supply chain risk aware leadership, enabling active management of the completeness of VSCS implementations, and driving efficacy of the organization's VSCS processes and practices.

[9] If this is your situation, get in touch with us; we'd love to help! info@privacysecuritybrainiacs.com

I. Additional Resources

Find tools, information and more in-depth discussion of many of these vendor security and privacy management topics at:

- https://privacysecuritybrainiacs.com
- https://privacysecuritybrainiacs.com/resources/
- https://privacysecuritybrainiacs.com/training/
- https://www.linkedin.com/company/privacy-and-security-brainiacs
- http://privacyguidance.com/blog/category/ba-and-vendor-management/

For more information: info@privacysecuritybrainiacs.com

Privacy & Security Brainiacs

LinkedIn: https://www.linkedin.com/company/privacy-and-security-brainiacs

Twitter: @PrivacyProf
@PSBrainiacs