SIMBUS 360
INFORMATION SECURITY - PRIVACY - COMPLIANCE

Dozens more tips available in SIMBUS Tracker

VENDOR OVERSIGHT & RISK MANAGEMENT TIPS

8 VERY COMMON RISKS

Repeatedly identified in vendor assessments, these eight stumbling blocks are some of the more common risks SIMBUS360 clients uncover as they look into their third-party relationships.

- Information security and privacy policies / procedures are not documented.
- Personal and sensitive data and files are not encrypted.
- There is no adequate information security or privacy training program in place.
- Information security or privacy risk assessments haven't been performed in several years (or worse, have never been performed).
- Employees are not familiar with posted privacy notices for their own employer, or your organization, and so do not take actions to be in compliance.
- Third parties subcontract business activities and processes without first obtaining approval from clients.
- Systems have not been patched and lack adequate security controls (e.g. no firewall, anti-malware or IPS/IDS).

4 ASSESSMENT TIPS

Consider these pointers when choosing the type of assessment to use for each of your vendors.

- 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.
- Choose an assessment with costs in line with what you are paying the vendor. Generally it should not cost the vendor more than 20% of the relationship's revenue.
- At or just prior to the beginning of your relationship, perform a high-level evaluation to determine the risk the vendor brings to your organization.
- Be wary of assessments that claim "100% certified" secure or compliant. Changes constantly occur in a business environment, as do the associated levels of compliance and security risks.

5 CONTRACT MUST-HAVES

SIMBUS360 clients are advised to include each of these critical terms in all vendor contracts, at a minimum. Other recommended terms are available via SIMBUS Tracker.

- Hold vendors to the same security and privacy standards you have at your organization.
- Require at least quarterly attestations from the vendor's executive management.
- Insist the vendor have a documented breach notification process that includes time requirements for notifying your organization of the breach.
- Establish who is responsible for encryption keys, as well as who has access.
- If regulatory obligations require the vendor to retain your data longer than the the period for which you've contracted them, ensure liability is built into the contract for them to continue to provide strong security for your data.

BONUS TIP: Although customization of contracts is necessary, a template of pre-approved security and privacy clauses cuts time and adds peace of mind.

3 DOCUMENTATION TIPS

Keep the following in mind as elements of your vendor relationships that should always be detailed in writing.

- Maintain a documented inventory of data items subject to security or privacy requirements for which each vendor has access or possession.
- Make sure all access vendor employees and subcontractors have to your data and systems is removed as soon as they exit the company.
- For incidents and breaches, contractually require vendors to take actions to mitigate the risks to prevent similar future incidents.

5 OVERLOOKED TYPES OF THIRD PARTIES

The following are often overlooked as third parties that impact an organization's risk picture.

- Business partners (investors, collaborators, strategic alliances)
- Government agencies (worker's compensation agencies, agencies with tax info)
- Volunteers (fund raisers, patient assistance, drivers)
- Researchers (marketing, health care, product development)
- Students (teaching hospitals, interns, shadowing programs)

4 BONUS TIPS

Here are four simple steps any organization can take to mitigate risks brought to your organization by using third parties.

- Verify your organization is named as an insured on your vendors' cybersecurity and privacy liability insurance policies.
- Determine the type of cybersecurity and privacy liability insurance your vendors have, and if/how your organization is covered in a breach.
- Understand whether your cyber liability policy covers vendor / contractor breaches.
- Request any existing recent SSAE 16 SOC 2, ISO 27001, COBIT 5 or similar types of security reports.

Dozens more vendor oversight & risk management tips are provided within **SIMBUS Tracker**

FOR MORE INFORMATION:

EMAIL: **DAVE@SIMBUS360.COM**
SIMBUS360: **SIMBUS360.COM**
SIMBUS TRACKER: **SIMBUS360.COM/VENDOR-MANAGEMENT-SOFTWARE/**
@SIMBUS360 **SIMBUS360**