

Don't be "fooled" by vendors who look safe at first glance



10 common mistakes made in vendor risk management




“The company is big, they must be safe.”

Example: A client said to us, “It’s Fiserv for goodness sake, why should I have to do due diligence on them?” – Just because the company is big, does NOT make them safe. As a matter of fact, the bigger the company, the more difficult “safe” becomes to manage.

“I don’t send *my* Non Public Information (NPI) data to them, so they’re not high risk, right?”



Example: Credit reporting agencies are a good example – any time you’re handling confidential customer/member data, you may be putting it at risk.




“The data isn’t in electronic format, so the risk is low, right?”

Example: You need to worry about your shredding company. They could still pose a threat. While they are probably legitimate, you should review their procedures and watch the process once, just to be sure...after all, they are holding “hard copy” of pretty sensitive information picked out of your shred bin.

“They are a privately held company that won’t release financials, so there’s nothing I can do.”



Example: There are many alternatives to financial statements – an accountant’s letter, a credit report on the owners or a copy of the financial institution’s statements.




“I would never fall for that kind of email.”

Example: Many people, in a hurry to clear out email, let their guard down and accidentally expose themselves to a well done phishing attack. Did your due diligence include a clear understanding of your vendor’s security training and is it adequate to prevent this type of real risk and exposure from non-malicious (yet poorly trained) employees?

“They are a well-known name so I’m sure they do data security correctly.”



Example: Does Target, Monster.com, Sarah Palin or Heartland ring a bell? They all got hacked. Make sure your information security department thoroughly reviews your vendor’s policies and procedures and watches for other news.




“They told me they were hacked but everything is fine now.”

Example: Stay vigilant, ask them to detail what steps they’ve taken to address the problem and monitor for any follow-up activity.

“They are really innovative, so they must have spent a lot to ensure their technology is safe.”




Example: Get to know the background and qualifications of their information security and development teams to be sure.



“They won’t share the information we need for proper due diligence. Are we just out of luck?”

Example: Sometimes they won’t share certain types of information, but again, look for alternatives. Can they provide any reports of penetration testing, independent audit reports, SOC reports or perhaps allow you to view, but not retain, any information to give you comfort around their cybersecurity? Can your CISO talk to their CISO?

“I’ve done all my due diligence and my vendor is buttoned up, safe and financially sound. Why is my examiner asking me about **fourth** party vendors now?”



Example: If your vendor (especially a critical vendor) records, stores, transmits or processes significant NPI, and that data is hosted in a third party cloud (third party to your vendor, fourth party to you), then significant due diligence is now warranted on the fourth party cloud provider.

Need help with getting your vendor management program in order? Learn how Venminder can help.

[Download free samples now.](#)