6 Important Questions

TO ASK YOUR TECH VENDOR

Your clients trust you with their private financial data, and you probably feel a responsibility to protect that data. But what you may not know is that securities regulators hold advisors accountable – not their technology vendors – when client data is compromised. That can amount to fines and settlements with the Securities Exchange Commission, regardless of any harm or loss of information.

Don't let flimsy security policies cost you. Here are six important questions to ask your tech vendors to make sure the technology used by both you and your clients meets the highest standards.

1. How frequently do you update your security defenses?

Online threats are constantlyevolving. Your tech vendor should fully understand the security landscape and take steps to continually evaluate and strengthen their infrastructure. Ask your tech vendor if they conduct annual audits, penetration tests and how often they monitor their production network for intrusion.

2. What level of data encryption do you use?

Encryption is a way to ensure only authorized parties can decode and read sensitive information online. Various levels of encryption exist, meaning some do a better job of safeguarding data than others. Your vendor should take a well-rounded approach and encrypt data both at rest and in transit. Make sure you also understand their key management policy (KMP), which is a set of rules a business has to protect information.

3. Do you manage your own servers and storage infrastructure or do you use a third party or a cloud service provider?

This question has less to do with which method is preferred, and more to do with accountability. If a tech vendor manages their own servers and storage infrastructure, you're dealing directly with the people responsible for protecting your client data. But if the vendor outsources these components, your vetting process should extend to those third parties.

4. Do you monitor for breaches and service intrusions?

Data breach attempts happen more often than you think. Fortunately, organizations have gotten good at detecting and stopping the staggering amount of online threats that face the global market. The best tech vendors monitor their infrastructure for intrusions 24 hours a day, seven days per week.

5. Are both your company and your data centers SOC 2 compliant?

SOC 2 is a type of compliance standard that measures how information is protected online. Businesses seek to become SOC 2 compliant after a thorough audit of security, availability, process integrity, privacy, and confidentiality by a certified third party. Before partnering with a tech vendor, be sure all aspects of their service are SOC 2 compliant.

6. Does security permeate through your company culture?

Your tech vendor should prove, beyond a shadow of a doubt, that protecting your data is a top priority. That means their security policies should run deep within their culture. Find out whether they perform security training for all new employees, if employees need to take annual security assessments, whether background checks are necessary for employees, and if they have an incident response team.

eMoney Advisor is a leading provider of comprehensive planning and needs based analysis solutions that maximize your client relationships.

For more information, please visit our website at www.emoneyadvisor.com or contact us at 1-888-362-4612.

4 Radnor Corporate Center, Suite 300 | 100 Matsonford Road | Radnor, PA 19087 | 888-362-4612

www.emoneyadvisor.com | Join the conversation! We're on Facebook | Twitter | LinkedIn