Tech Risk Q & A

By Melanie Lockwood Herman & Erin Gloeckner

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Q: What questions should we ask the references of a prospective new tech vendor?

A: Checking references for any new vendor is a good idea and sound risk management practice. When checking references for a new technology vendor, try to ask questions that will enable you to get a sense of the quality and responsiveness you're likely to experience as a customer. If possible, ask for two current client references and at least one former client reference. Here are some questions to help you get started:

- Did the vendor honor the contract and warranties?
- Have you had any disputes (e.g., about contract terms and conditions, quality of service, etc.) with the vendor? If so, how were they handled?
- How would you rate the vendor's technical capabilities?
- How many people at the vendor do you work/interact with? Is customer service consistent or spotty?
- Has your nonprofit experienced any tech challenges or downside risks (e.g., data breaches) that required the tech vendor's responsive action? If yes, did the vendor respond in a timely fashion and was it able to resolve the problem you experienced?
- Would you recommend the vendor to other organizations? Why?
- What do you wish you had known before you started working with the vendor?

Q: I'm concerned that some of our staff are spending up to four hours each day posting photos and material to their personal Facebook pages. What action should I take, if any?

A: Virtually every nonprofit employee spends some time during the workday on personal matters, such as making medical appointments, answering calls from children, parents, caregivers and schools, and checking personal email or perusing social media accounts. Yet most employees understand that these tasks should constitute a small portion of the workday. As a result, most employers do not place strict time limits on such activities. However, when personal tasks and activity consume more than a fragment of an employee's paid work time, there are a number of potential negative consequences, including:

- Frustration or anger by co-workers who observe policy abuses;
- Organizational culture that places little value in HR rules and policies;
- Decline in productivity impairing the ability of the nonprofit to achieve its goals;
- Exposure of the nonprofit's tech resources to viruses, malware or other threats introduced by personal use of organization resources.

There are two general approaches to address the abuse of your existing "acceptable use" policy that asks

employees to limit time spent during the workday on personal matters. The first approach is to rework the policy to include specific examples of acceptable and unacceptable uses of the nonprofit's systems, and provide training to the full team on the language and intent of the policy.

The second approach is to enforce your existing policy by addressing misuse with policy violators. Meet with any staff who are violating the policy and reiterate the negative consequences of policy abuse. Explain clearly what the staff member must do (or not do) to demonstrate compliance with the nonprofit's policies, and a timeframe for doing so. Clearly state the consequences of continued policy abuse.

Q: What are the three most important considerations in selecting a Cloud storage vendor?

A: A primary consideration is that the vendor meets your technical requirements. Do you understand your storage needs and existing IT infrastructure? If not, talk to your internal IT wizard or get help from an outside expert. Once you understand the scope of services you need, you will be in the best possible position to identify and then compare suitable vendors.

A secondary consideration is to select a vendor with a good reputation in the market. Hype surrounds the cloud and a vendor's capacity may not meet your expectations. Before entering a contract with a vendor, validate their claims. Request references from current and former clients and ask the vendor's clients if their expectations were met.

Another consideration is to request training and guidance from your candidates for cloud services. Require a training package with your contract, particularly if you don't have an IT expert on staff. Keep in mind that any cloud services you purchase should integrate seamlessly with other IT operations. One of your goals should be to find a vendor/partner who will empower your staff to use cloud services to achieve maximum benefit.

Q: What are the risks, if any, of using donated PCs for our staff (from different sources) rather than buying or leasing new machines?

A: One of the risks of using donated computers is that it may be hard to predict the total cost and time required to maintain these machines in working order. Before accepting donated computers, establish guidelines for determining which donations are suitable. Here are a few questions to resolve before you invite stakeholders to donate equipment to your nonprofit:

- Is your nonprofit able to accept both PCs and Apple products, or does it make sense to use only one or the other?
- What are your minimum requirements for any donated machine? If service delivery is dependent on every staff member being able to access custom case management software, make certain that you understand and document those minimum requirements.
- Do you have the resources to "clean" a donated computer of data and programs that you don't need?

Q: Where can I find information about which insurers offer Cyber Liability policies?

A: Consider searching for insurance providers using online insurance directories like www.kirschners.com. Remember that liability for loss of client or employee data is not typically covered in standard insurance policies. As discussed in the article titled *Insurance for Cyber Risks*, in most cases you'll need a cyber liability policy to protect against data breaches and other information age risks.

Q: What are the first steps we should take if we become aware that personal donor information has been compromised?

A: When your nonprofit experiences a data breach, PCI, HIPAA, and your state's regulatory requirements will dictate what you must do. Aim to understand your requirements long before this type of risk event occurs. Check in with your nonprofit's staff, contract or volunteer general counsel, tech vendor, and other partner advisers to develop a clear plan you can follow that will ensure a legally compliant response to the crisis. After the breach occurs and you have taken the necessary immediate steps, invite a third party firm to investigate if your IT department does not have the capacity to do so. For example, you may want to engage a computer forensic investigator or information security specialist. Keep in mind that you may be required to notify partners, customers, and/or government agencies about the breach; if possible, prepare draft crisis

communication materials before the event. Finalize and disseminate your materials as soon as the breach occurs. You may also need to engage a credit monitoring firm to provide assistance to those who have been affected by the breach.