The Need for Vendor Management: Outsourcing the Support but Not the Oversight

By Allison Davis Ward, Partner

Not too long ago, about all an organization needed to do when deciding whether to trust someone with its business was to confirm the person's reputation. Good eye contact and a firm handshake could be deciding factors when selecting an associate or company to support the business.

But times have changed. The number and types of service avenues have grown rapidly. Meanwhile, nearly every organization has expanded its cyber footprint. That means organizations now need to go further when evaluating potential third parties.

A formal vendor management program will define the standards an organization should use to vet vendor relationships and help it apply these standards consistently throughout its environment.

Why Organizations Need a Vendor Management Program

In the past, many organizations hosted all their technology, assets, and applications in-house. They employed internal developers and IT staff to support daily operations and had full management of the controls and standards to protect these assets. But with the shift toward more outsourced environments and applications hosted in the cloud by third parties, organizations are slowly giving up this level of control.

This shift does not relieve the organization of its oversight responsibility, however. The organization's responsibility has simply changed from overseeing its own staff to overseeing its vendor relationships.

Many organizations feel they can trust their vendors. And although that may be true, an organization should view vendors as an extension of its business, not as separate entities. If a vendor weakness leads to a data breach, the constituents aren't going to see the issue with the vendor. They are going to feel that the organization failed to protect their information when selecting a vendor relationship.

What a Vendor Management Program Should Include

Based on the nature of the vendor and the risk the relationship poses to the organization, due diligence and ongoing monitoring procedures should include several areas:

- *Financial stability.* It's easy to get financial reports for public companies, and many privately held companies will provide a financial summary upon request. These reports provide insight into the vendor's stability and the likelihood that the vendor will remain in business for the foreseeable future. Also, weak finances often lead to weak security. When resources are limited, IT and information systems (IS) controls and support are often cut first because they don't produce income.
- *Security and vulnerability management.* Security is a relevant consideration for vendors that store, access, or transmit an organization's data and its constituents' data. If the vendor has regular access to an organization's network or sensitive data, its controls for protecting those connections or data are critical. Vendors will often provide audit reports or summaries, security compliance certificates, internal policies, or summaries of their controls.
- *Business continuity and disaster recovery.* When vendors host and store an organization's data, their controls for ensuring the availability of the data are imperative. Vendors can often provide documentation of their business continuity and disaster recovery plans. The documentation should describe plans to ensure continued operations during a disaster situation, redundancies that have been implemented, and the results of any periodic testing of those plans.

A formal vendor management program will define the standards an organization should use to vet vendor relationships and help it apply these standards consistently throughout its environment.

- *Incident response and breach management.* If a vendor hosts sensitive data or has access to the organization’s network, the controls for protecting those connections or data are critical. The vendor should have processes to detect an issue in a timely manner. Similarly, the vendor should specify breach notification requirements that will inform an organization quickly about a breach that could affect its data and its constituents’ data.
- *Vendor management.* Just as an organization must maintain its vendor relationships, its vendors should be doing the same. An organization may contract with a vendor to host its data, but that vendor may outsource the hosting to another third party. Because it is impossible to vet every vendor in the chain, it’s critical for organizations to ensure that their vendors manage third parties properly.
- *Other.* Additional areas that can be reviewed include cyber insurance, which correlates with incident response planning. Similarly, if a vendor deals with certain types of data, compliance with various laws and regulations may be relevant. Depending on the relationship to the organization, vendors will often provide statements of compliance with laws and regulations, such as the PCI Security Standard and the EU’s GDPR.

It is important to recognize that every vendor may not provide all the requested items; however, that does not mean an organization should immediately discontinue or terminate the relationship. Instead, management may evaluate the effect of missing documentation and consider discussing the matter with its IT or IS committee or even the board. Ultimately, the security of the organization and its data is the responsibility of the board and upper management, so this high-level ownership of vendor relationships is becoming more critical.

Which Vendors to Include

Oversight can seem daunting when you think of the many vendors an organization could have. But not every vendor poses the same level of risk, and each vendor does not need to be reviewed to the same extent. Therefore, it’s imperative for organizations to determine which vendors are truly critical for purposes of ongoing monitoring.

Two primary factors should be taken into consideration:

- *The business criticality of the relationship to operations.* If a vendor suddenly stopped providing services, would it have a detrimental impact on the organization and its ability to continue operations? If so, the organization would likely deem the vendor critical for purposes of this review. In this instance, the organization would want to focus on the vendor’s financial viability. If the vendor hosts the organization’s data, the organization should also consider the vendor’s procedures for business continuity and how it would go about obtaining its data should the relationship terminate suddenly.
- *The sensitivity of the data hosted, managed, or accessed by the vendor.* If a vendor is hosting a system with very sensitive data for an organization, the organization would likely want to ensure that the vendor has the proper controls to protect that sensitive data. Reviewing security audit reports, evaluating insurance policies, and developing incident response plans help to ensure that the vendor is protecting the data and has the ability to identify and address potential issues. Similarly, if a vendor does not host the data but has 24/7 access to the network or system, a breach at the vendor location could ultimately affect an organization, and these same areas would be important.

These questions can help an organization identify its most critical vendors:

- If the vendor stopped providing services unexpectedly, how detrimental would it be to the organization? Could the organization easily replace the service the vendor provides?
- What level of access does the vendor have? Does the vendor access or store critical or sensitive data? Is the vendor responsible for securing it and ensuring it remains available?
- Where is the data hosted — in the United States or in a foreign country?
- Does the vendor have any access to the organization’s network or physical locations where sensitive information and systems are stored?
- Is the service provided complex in nature?
- Are there heightened risks with the nature of the service provided?

Ultimately, each vendor relationship differs, and the review requirements may not be the same for each. Answering the preceding questions will also help organizations determine the necessary level of review. It’s best to define each relationship, rate it on the preceding criteria (high/medium/low or in some other tiered system), and then identify the review requirements for each level.

For example, if a vendor such as a cleaning service or shredding company only has occasional physical access to locations, the organization may just require the vendor to sign a confidentiality agreement once a year.

On the other hand, if a vendor hosts the donor management system, the organization may want to review all the preceding areas to ensure the vendor remains financially stable and maintains security, incident response, business continuity, and disaster recovery controls at the same level the organization has for protecting its internal data.

When to Review Vendors

Organizations that vet vendors before signing a contract can avoid entering into a bad relationship from the start. However, the vendor management program should also define requirements for periodic re-evaluation to ensure that selected vendors remain in good standing and continue to align with the organization’s expectations. Think of how often things change in an organization. Things change just as frequently with vendors, and an organization cannot assume that a vendor’s environment will remain stagnant.

With the growing threat of cyber breaches, it’s crucial to be aware of the risks that vendors can pose to an organization and manage them accordingly. After all, major data breaches at Goodwill, Verizon, Home Depot, Lowe’s, and Target all started with security issues at a vendor.

At the end of the day, it is the organization’s network and data. Just as an organization would make sure all employees and volunteers entrusted with access to the network, data, or other critical business components followed adequate security methods, it is vital to take the same precautions with vendors.

This document originally appeared in the AICPA’s Not-for-Profit Entities Industry Developments—2020 ©2020 AICPA. All rights reserved. Used by permission.

About the Author

Allison Davis Ward, Partner
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.