CAPINTECH

Why Your Organization Needs a Vendor Management Program

By Allison Ward, Partner

In the past, many organizations hosted all their technology, assets, and applications in-house and employed individuals with technical expertise to support daily operations. Organizations 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 giving up this level of control.

This change does not relieve organizations of their oversight responsibility, however. The responsibility has simply changed from organizations overseeing their staff to overseeing their vendor (service provider) relationships.

Outsourcing the Support — but Not the Oversight

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

Similarly, if a vendor weakness results in your data being compromised, your organization may be the one with hindered operations. Although the issue may have been caused by the vendor, your organization must deal with the impact.

A formal vendor management program will define the standards your organization should use to vet vendor relationships and help you apply these standards consistently. Follow the three steps below to develop and maintain an effective vendor management program.

1. **Define what your vendor management program will assess.**

The first step is determining the scope of your vendor management program. Your due diligence and ongoing monitoring procedures should include the following areas, based on the nature of the vendor and the risk the relationship poses to your organization:

- **Financial stability** – Financial reports are available for public companies, and many privately held companies will provide a financial summary if you request one. These reports provide insight into the vendor's stability and the likelihood that it will remain in business for the foreseeable future. Weak finances can also lead to weak security. When faced with limited resources, many companies cut their investment in information security first because it does not produce income.
- **Security and vulnerability management** – Security is a relevant consideration for vendors that store, access, or transmit your data and your constituents' data. If a vendor has regular access to your network or sensitive data, its controls for protecting those connections or data are crucial. Vendors will often provide audit reports or summaries, security compliance certificates, internal policies, or summaries of their controls.
- **Business continuity and disaster recovery** – It's imperative that any vendors that host and store your organization's data have controls in place to ensure the availability of the data. Vendors can often provide documentation of their business continuity and disaster recovery plans. This documentation should describe the vendor's plans to ensure continued operations during a disaster situation, the redundancies in place, and the results of any periodic testing of those plans.
- **Incident response and breach management** – If a vendor hosts sensitive data or has access to your network, its controls for protecting those connections or data are critical. The vendor should have processes to detect an issue promptly and breach notification requirements that ensure you are informed quickly about a breach that could affect your data and your constituents' data.
- **Vendor management** – Just as your organization must assess and maintain your vendor relationships, your vendors should be doing the same. While your organization may contract with a vendor to host your data, that vendor may outsource the hosting to another third party. (These are known as fourth-party relationships.) Because your organization can't

possibly vet every vendor in the chain, it's critical to ensure that your vendors manage *their* vendors properly. It's also imperative to understand the nature of these fourth-party relationships. Over the past few years, there have been numerous supply chain attacks where organizations were impacted by a breach or compromise at a fourth-party vendor. Organizations that were aware of these relationships were able to mitigate the impact of the breach much more effectively than those that did not have this knowledge.

- **Other** – Consider reviewing the vendor's cyber insurance, which correlates with incident response planning. Compliance with various laws and regulations may also be relevant if a vendor deals with certain types of data. Depending on the relationship with your organization, vendors will often provide statements of compliance with laws and regulations, such as the PCI Security Standard and the European Union's General Data Protection Regulation (GDPR).

You may not be able to obtain all the requested items from every vendor, but this doesn't mean you should immediately end the relationship. Instead, your management can evaluate the effect of the missing documentation and consider discussing the matter with your information technology team, security committee, or even your board.

With the growing threat of cyber breaches, it's crucial to be aware of the risks that your vendors can pose and manage them accordingly.

2. Determine which vendors to include.

Oversight can seem daunting when you think of the many vendors your organization has. But not every vendor poses the same level of risk, and you don't need to review each vendor to the same extent.

To determine which of your vendors require ongoing monitoring, consider these two primary factors:

- **The business criticality of the relationship to your operations** – If a vendor suddenly stopped providing services, would it have a detrimental impact on your organization and your ability to continue operations? If so, it's likely important to review this vendor and its financial viability. If the vendor hosts your organization's data, you should also consider the vendor's procedures for business continuity and how you would obtain your data if the relationship ended abruptly.
- **The sensitivity of the data hosted, managed, or accessed by the vendor** – If a vendor is hosting a system with highly sensitive data for your organization, you will likely want to ensure that the vendor has the proper controls to protect that data. Review these vendors' security audit reports, insurance policies, and incident response plans to evaluate whether they are protecting the data and can identify and address potential issues. Do the same if a vendor does not host the data but has 24/7 access to your network or a critical system, as a breach at the vendor location could affect your organization.

In addition, consider other aspects of the relationship that may affect the level of risk associated with a vendor. For example, some vendors may hold very sensitive data, but if the volume of the data they retain is small, it may justify a more limited or less frequent review.

Ask the following questions to help identify your most critical vendors:

- If the vendor stopped providing services unexpectedly, how detrimental would it be to our operations? Could we easily replace the service the vendor provides? Is the service complex?
- What level of access does the vendor have? Does the vendor access or store critical or sensitive data? Is the vendor responsible for securing the data and ensuring it remains available?
- Where is the data hosted — in the United States or a foreign country?
- Does the vendor have access to our network or physical locations where sensitive information and systems are stored?
- What type of data does the vendor maintain or access? What is the volume of data?
- Are there legal, regulatory, or other requirements that warrant evaluation and monitoring of this relationship?
- Are there heightened risks with the nature of the service provided?

Each vendor relationship is different, and the review requirements may not be the same for each. Answering the questions above will also help your organization determine the level of review needed for each vendor. We recommend that you define each vendor relationship, rate it based 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 your locations, you might decide that having the vendor sign a confidentiality agreement once a year is adequate.

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

3. Specify when to review vendors.

Evaluating vendors before you sign a contract can help you avoid entering into a bad relationship. Your vendor management program should also specify the requirements for periodic re-evaluation. This will help ensure that selected vendors remain in good standing and continue to align with your organization's expectations.

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

Ultimately, your organization's systems and data are your responsibility. Just as you ensure all employees, contractors, and volunteers with access to your network, data, or other critical business components follow adequate security methods, it is vital to take the same precautions with your vendors.

Please contact us with questions or if you'd like to discuss how CapinTech can assist you with vendor management.

About the Author

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

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services for nonprofit organizations, financial institutions, health facilities, educational institutions, and a variety of other organizations. She stays current on changing threats to design review procedures to aid clients in implementing appropriate controls to protect against evolving cybersecurity threats. Allison speaks on information security topics for various banking, state CPA, higher education, and nonprofit societies.

About CapinTech

CapinTech, 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 capintech.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. For over 50 years, 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.