ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Nonprofit Knowledge: Protecting IT and Data Security When Using Vendors

Law Department Management

Nonprofit Organizations

Technology, Privacy, and eCommerce

Banner artwork by Graphic Farm / *Shutterstock.com*

All nonprofit organizations maintain an IT system that is critical to its operation. Nonprofits receive, process, hold, and transmit confidential information, including legally protected personal data, relying heavily on vendors. For that reason, a general counsel's job is much easier if business practices select better vendors and hold them accountable for security measures that protect the nonprofit's IT systems and data — and improve legal compliance.

Partnering with an IT professional, in-house counsel can be more confident the implementation will be successful.

Define the scope

Before seeking proposals or courting vendors, staff should draft the scope of services. It should specify what IT systems or data are involved. The scope informs what protections must also be included in the scope or a request for proposal. A well-developed internal policy may already have classifications for protected data and require data security measures, serving as automatic requirements to the vendor.

Before seeking proposals or courting vendors, staff should draft the scope of services.

In its absence or as a complement to less detailed policies, a series of questions can help staff define exactly what is exposed to risk. Example questions include:

- What IT systems will the vendor access generally (e.g., finance software and data)?
- What specific data will be held or processed by the vendor (e.g., all historical data on services to specific children extracted from constituent relations management platform)?
- From what countries is data sourced, processed, or stored (e.g., contact information for European individual donors)?
- Is there limited access to certain information that will be shared (e.g., fundraising development strategy notes will be shared in Google Docs)?
- Will the nonprofit's data be removed and maintained in vendor systems on an ongoing basis (e.g., outsourced HR service provider's platforms)?
- Will data be transferred to or processed on the vendor's systems and returned to the system (e.g., prospect wealth vetting)?

Different vendors require different security levels

Answers inform the measures of security that should be required of the vendor. Legally protected personal data and transfer across borders are two examples of the highest risks that would require verifiable security practices.

> Legally protected personal data and transfer across borders are two examples of the highest risks that would require verifiable security practices.

Ideally, standard security requirements can be specified in policies for different categories of data or access. VectorMine / *Shutterstock.com*

A nonprofit's highly valuable prospect database may require similarly strong protections. The scope details will help in-house counsel and IT professionals craft controls in advance of circulating a request for proposal. It may also prompt a closer review of whether there is an opportunity to anonymize data.

Ideally, standard security requirements can be specified in policies for different categories of data or

access. Some examples of different levels of requirements that may be listed in a request for proposal:

- Because services involve personally identifiable information or access to critical IT systems, the vendor is required to have a certification under ISO 27001 or a satisfactory third-party compliance report issued about its security practices, specifically a System and Organization Controls (SOC) 2, Type 2;
- Because the services involve financial data, the vendor is required to have satisfactory third-party compliance report of its internal controls in the form of SOC 1, Type 2; and
- Because the services involve access to confidential information (that is not specifically regulated personal information), the vendor is required to have a satisfactory third-party compliance report about the vendor's security practices at a minimum a System and Organization Controls 2, Type 1.

IT security experts within an organization may have more specific requirements, but these are examples of a vendor's general qualifications. For reference, the American Institute of Certified Public Accountants SOC standards focus on the security of processes and systems companies. It is common for cloud computing companies and similar firms holding sensitive information to have third-party reports that describe compliance.

Certification of compliance with the ISO 2700 standard for information security, cybersecurity, and privacy protection is developed by the International Organization for Standardization. In cases where a vendor is accessing information that does not present a legal risk, but may present a reputation risk, other requirements can be set in the scope.

Conduct due diligence

Any vendor with access to the nonprofit organization's IT systems or the data should be subject to due diligence early in the selection process. While due diligence can be customized to the scope of service, use of third-party review or certification described above may be a quick way to vet out unqualified vendors. In the case of SOC reports, someone qualified should read it and determine if there are weaknesses that are not acceptable.

Other due diligence approaches can include requesting a copy of key policies, reviewing their incident response process, interview with their privacy or IT officer, or requesting an explanation of any data breaches. If a nonprofit organization is short on expertise, it may engage a system security expert to develop and/or do the due diligence that aligns with the nonprofit's policies.

Establish standard terms for security

While one-size-fits-all data security terms may not suit all vendor agreements, in-house counsel can develop standard terms with a few options to cover heightened protections for certain data. Service terms can also serve as an element of the RFP, indicating the baseline security requirements. It gives the vendors an opportunity to respond and informs the nonprofit if the vendor will involve an intensive negotiation or poses higher risks. Here are some of the key provisions of security terms:

- Require the vendor to comply with laws, including specifications about laws applicable to the nonprofit. Examples of specific compliance are a charitable health organization's Health Insurance Portability and Accountability Act or an educational provider's Family Educational

Rights and Privacy Act and any associated state laws;

- Require the vendor to comply with any industry standards to which the nonprofit is bound or is applicable to the activity, such as the Payment Card Industry Data Security Standard (PCI DSS) for payment processing service agreements;
- Require maintenance of SOC reports or ISO certification and a mandatory delivery to the nonprofit organization of updates. Any SOC report will expire in 12 months; certifications will indicate the expiration. Require written notice of material changes and reserve the right to terminate if the vendor's report is unsatisfactory or the certification expires;
- Specify the nonprofit's specific safeguards requirements and indicate the nonprofit's requirements may reasonably change. For example, a nonprofit organization may require a vendor's employees to have criminal background checks if they are accessing children's records;
- Require procedures for redundancy and business continuity to secure data;
- Provide right of data and system auditing by the nonprofit organization. It may be particularly important when there is no third-party review report or certification. Nonprofit's valuable information, such as the donor and prospect database, can be easily lost or misused when smaller vendors do not have strong controls or oversight;
- Expressly require a waiver on any limit on liability when damages are caused by the vendor as a result of a material breach of the security terms;
- Set out the standards for cyber security insurance. Consider requiring the nonprofit organization to be listed as an additional insured; and
- Allocate risks in indemnification appropriate to value of the data or scope and the reliance on the vendor's data security.

Secure insurance

While most nonprofit organizations have obtained cyber insurance, it is time to read the policy and ask critical questions about the amount and the incidents covered when a vendor is involved. Some basic questions to ask include:

- What limits, if any, are placed on covering the nonprofit's loss of data caused by the vendor's breach?
- Are there specific requirements that the nonprofit must place on its vendors?
- Does coverage, including notifying data owners, include data that is considered private or confidential by the nonprofit, even if the data is not legally covered by law?
- What coverage levels and types would the insurance company recommend for your vendors accessing critical IT systems or private data?
- Does the insurance company have any free or low costs vendor vetting tools?

While every in-house attorney knows the importance of internal policies and training, leveraging vendors with strong data and systems security will improve a nonprofit organization's chances of protecting its assets — and reduces the legal, financial, and operational risks.

Anita Drummond

Member

Outside GC LLC

Anita Drummond is a member and general counsel of Outside GC. She has been in private practice, general counsel of ChildFund International, USA, an organization working in 20+ countries, assistant general counsel at the American Cancer Society and The Nature Conservancy, and director of Legal Affairs at a trade association during her career. She specializes in corporate, charity, tax exemption, political, and social enterprise law in the United States and abroad. She is a member of

the ACC Nonprofit Organization Network.

Lakshmi Sarma Ramani

Member

Outside GC LLC

Lakshmi Sarma Ramani was the general counsel of the National Association for the Education of Young Children and senior attorney at The Nature Conservancy. She is currently a member of the firm at Outside GC LLC where she is the outside general counsel to multiple nonprofit organizations.