StateRAMP

How to Protect Your Organization’s Data and Manage Third-Party Vendor Security Risks: A Checklist, in Three Easy Steps

Selecting a third-party service vendor to look after your civil society nonprofit’s information technology needs can be daunting. Selecting the wrong one could put your organization’s confidential information at risk. The following checklist, broken down into three sections, can help you in vetting current and future third-party service providers so that you can be confident in the security of your organization’s confidential data.

Step One: Know Who is Who, and What They Do

Do you know who handles your data, what that data is, and how sensitive it is? The first step is to get all of this straight. A spreadsheet is in order!

□ Create a spreadsheet-based list of all third-party vendors you use to perform specific IT tasks or services, e.g., website host, payroll software provider, stakeholder relationship management tool provider, etc. Put the names of these vendors in one column.

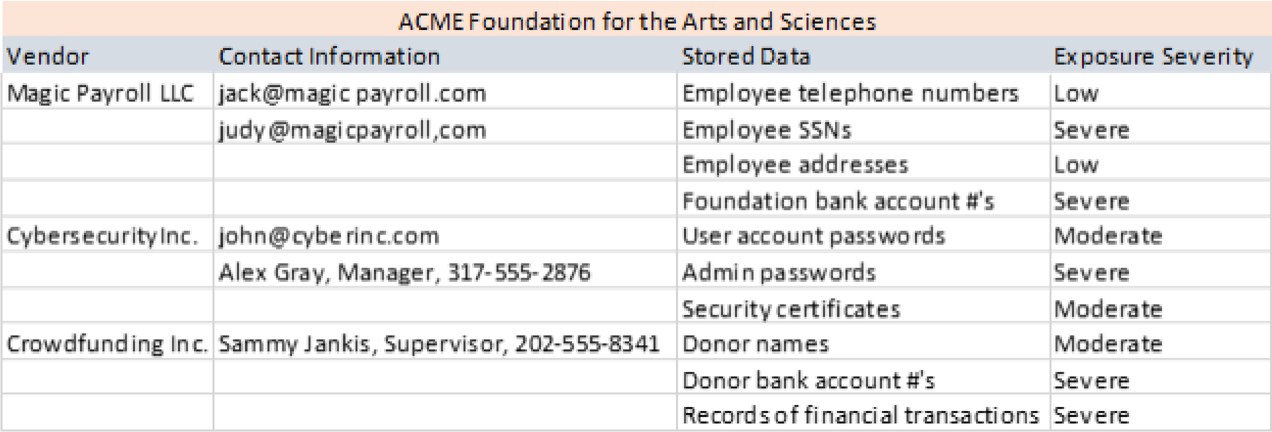
□ Verify you have contact information for representatives at all the organizations you just listed. In an emergency, these contacts will be useful to have at hand. This information can go into the list you just created, in a second column.

□ In a third column, list out all the types of sensitive data that your third-party vendors are storing on your behalf.

□ Finally, in a fourth column, categorize the sensitivity of this information. You can break the severity down by criticality based on this rubric:

- Low Impact – Loss of this data would have a limited adverse impact on your organization
- Moderate Impact – Loss of this data would have a serious negative impact on your organization
- High Impact – Loss of this data would have a catastrophic impact on your organization

When completed, the spreadsheet should look something like this:



ACME Foundation for the Arts and Sciences			
Vendor	Contact Information	Stored Data	Exposure Severity
Magic Payroll LLC	jack@magicpayroll.com	Employee telephone numbers	Low
	judy@magicpayroll,com	Employee SSNs	Severe
		Employee addresses	Low
		Foundation bank account #'s	Severe
CybersecurityInc.	john@cyberinc.com	User account passwords	Moderate
	Alex Gray, Manager, 317-555-2876	Admin passwords	Severe
		Security certificates	Moderate
Crowdfunding Inc.	Sammy Jankis, Supervisor, 202-555-8341	Donor names	Moderate
		Donor bank account #'s	Severe
		Records of financial transactions	Severe

Step Two: Get to Know Your Providers

It is crucial that you verify the security practices of all the vendors you have listed in your spreadsheet that handle your moderate impact and high impact sensitive data. This vetting does not need to be an ordeal, however. You can consult the following checklist items to quickly verify the security of your vendors. To get the information you will require to check off these boxes, you may need to make use of the contact information you just listed in your spreadsheet. For some of this information, a simple internet search may suffice. The more checks you can put in the boxes below, the more secure your vendors may be, and by extension, the more secure your data may be.

□ Service provider has completed any one or combination of the following audits within the past 12 months: SOC 2 Type 2, ISO 27001, CSA Star, HITRUST, FedRAMP, StateRAMP.

□ Service provider has completed a penetration test within the last 12 months.

□ Service provider requires phishing-resistant Multi-Factor Authentication for all administrative accounts or functions.

□ Service provider implements appropriate security controls (e.g., encryption, access control policies) to prevent unauthorized users from accessing your data and only maintains logs necessary to provide service.

□ Service provider routinely collects threat information and monitors their logs for suspicious cyber activity.

□ Service provider has the capability to detect, contain, and eradicate malicious software and intrusions.

□ You have a binding agreement with your service provider that they will notify you in the event of a breach causing exposure of any of your data.

Step Three: Use the Resources Around You

The challenge with engaging a vendor in dialogue about the items above is that they might not be entirely truthful with you about their security practices and certifications. That is why it is always a good practice to augment your search by seeing what others have to say about a given vendor. The following contact ideas are good places to start.

□ Consult CISA's website, including the ICT Supply Chain Risk Management Fact Sheet, Internet of Things Security Acquisition Guidance, and Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses.

□ Check FedRAMP and StateRAMP authorization lists to see if a given vendor is being used by federal or state governments in the United States.

□ Consult your peers in the nonprofit space. Other civil service organizations in your sphere may have had good experiences with different vendors.

Conclusion

Your organization's mission is important. Safeguarding the systems and confidential information upon which you rely is vital to ensuring that your organization can continue to strive towards accomplishing that mission. By using the checklist above, you will be not one, but three steps closer to the security you require to move us all forward toward a better tomorrow.