****

**KPM Consulting, LLC**

**Quick Reference Checklist from the Presentation on Ensuring Your Financial Data Security**

**While Discovering the Next “Normal”**

**Recent changes can increase risk of compromising data security. Have you recently:**

* **Moved staff to Remote/Work from Home?**
	+ Did they receive training on how to set up their new home/work environment?
	+ Were they trained on what to use if only free public accessible wi-fi was available?
	+ Do you have a formalized policy or procedure document that covers all the above?
		- If so, is it easily accessible by the staff?

For additional reference, see the: April 14th Strength Matters webinar on
 [“IT Response to COVID-19 Issues”](https://strengthmatters.net/resource/4-14-20-it-response-to-covid-19-issues-webinar/)

* **Added any new technology?** Examples could include video conferencing and Help Desk applications.If so:
* Was the new technology properly vetted by the IT Department before put into use, to ensure there were no security issues, and it would not conflict with existing technology in your system?
* Has your staff been made aware of “Shadow IT” and the dangers of installing new applications without validation by your IT team first?
* Did your staff receive full training on the new technology so as to avoid introducing additional security risks?
* Were your existing operational controls reviewed and updated or new ones created to address any changes in operating procedures introduced with the use of the new technology?

**Lack of Cybersecurity / Data Security Training increases risk of compromising data security.**

* **Do you have a formalized Cybersecurity / Data Security Training program?**
	+ Management should be making sure that your employees are receiving cybersecurity training so that they are aware of some of the current attacks that are out there.
	+ How to identify them.
	+ How to deal with them if you suspect one.
	+ Including validating a request by separate email or phone call, and how to report to IT and Management.
	+ Training should be “ongoing”, ex. timely, not just a once a year “read this policy and sign off”.
	+ Training should empower your employees to ask instead of just blindly acting upon a request.
	+ Employees need to understand they are not going to get in trouble for validating a request.
* **What are you using for measures to ensure your IT Team/Vendor are following best practices?**A review by an independent outside firm can provide validation that your IT services are:
	+ In agreement with contract or IT plan.
	+ Data Security controls are in line with current best practices.
	+ Similarly, if you are using service providers, such as AWS or Google for your Cloud, or ADP for your payroll, you should be obtaining their independent auditor reports (such as SOC 2 or SOC 1 respectively) to validate their data security measures are in line with your organizations standards.
* **Access changes, at network or financial application level, can increase risk of compromising data security if they did not follow best practice guidelines.**
* **If you had any recent accounting staff turnover, or people having to take on extra duties, have you performed a review to:**
	+ Determine there were no segregation of duty conflicts?
	+ If there were, were they acknowledged and properly documented before the access was granted?
	+ For any temporary changes, is there an automated end-date, or will they have to be manually removed?
	+ For those already expired, were they reviewed to ensure access was removed timely?

If you have any additional questions, please feel free to contact me:

**Dan Keleher, CGEIT, CISA, CRISC**

Executive Director

**KPM Consulting, LLC**

617.997.7320

dkeleher@kpmconsulting-us.com