8 TERRIFYING THIRD PARTY RISK MANAGEMENT STORIES

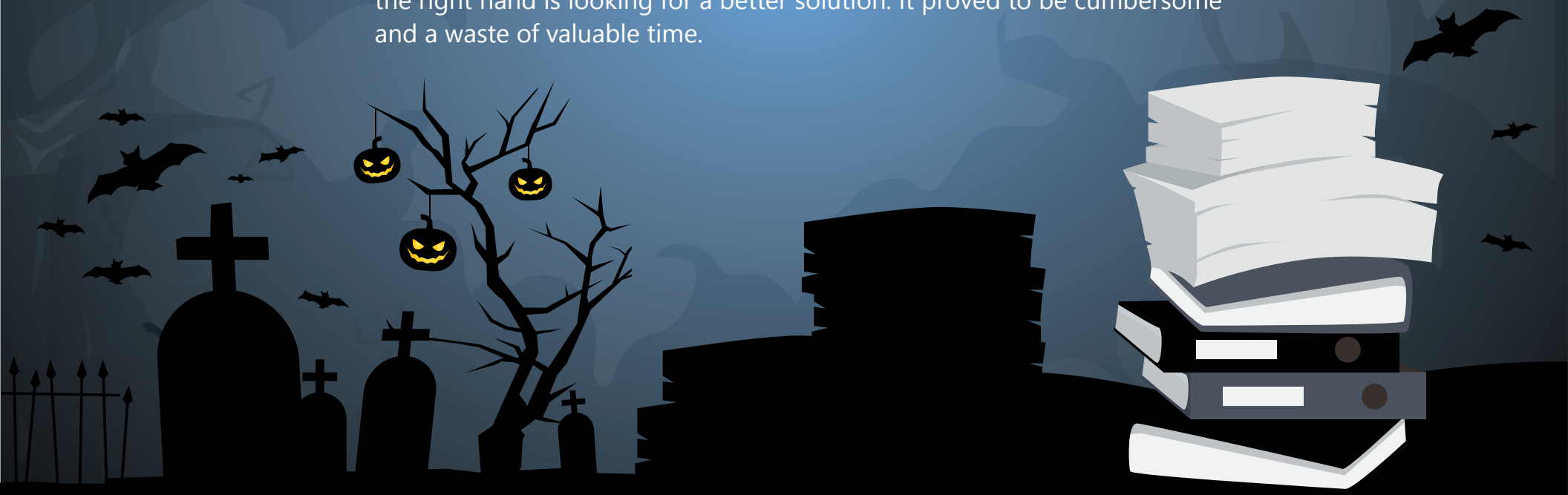
Venminder reached out and gathered 8 “terrifying” real-life third party risk management stories from compliance officers and vendor management teams across various sizes of organizations. Check out some of the chilling responses that we received. We hope that you find these stories enlightening and shed some light on what NOT to do at your organization.

venminder

1 THE BINDER

Upon arriving at a new position for a new organization, I found they had a 2-inch-thick third party risk management 'binder' in addition to an inefficient software. Everyone at the organization was printing, scanning, uploading and redoing contracts constantly.

I was shocked at the inefficiencies and hamster-on-a-wheel approach. The entire time it was like you didn't know what the left hand was doing while the right hand is looking for a better solution. It proved to be cumbersome and a waste of valuable time.



venminder

2 WHAT'S HAPPENING?

Our organization used a decentralized vendor management framework for quite some time. We thought all was well until we realized each department was setting different expectations for vendors. This was leading to inconsistencies across the board, and even opened the door to some reputational risk. One vendor owner did not share a customer facing vendor's poor service levels that they were experiencing; therefore, it went missed for a long time and was not addressed in a prompt manner.

We now run a centralized framework and communication has significantly improved.

3 ALERT! ALERT! ALERT!

Unfortunately, my organization was victim of a data breach and we were not prepared. We thought that it was unlikely to happen to us – lesson learned - it can, and probably will, happen at any organization. It was a critical third party vendor that was breached, but we had never discussed with them what their plan of action was should a breach occur. Due to this, we first heard about the breach in news headlines when performing a daily search of our vendors.

We now make sure to contractually oblige vendors to notify us as soon as possible when a breach occurs.

venminder

4 WE DIDN'T PRACTICE

When Superstorm Sandy struck havoc in 2012, the organization I worked at lost power which, of course, made our computer systems inoperable for a period of time. We needed branch employees to assist with operations by manually processing transactions for customers in the meantime. There was just one problem with this...

While we had what we thought was a solid disaster recovery plan in place, and an efficient manual transaction process, we had not had our employees ever practice doing this when testing our plans, so you can imagine the confusion and amount of questions that came up. It caused huge inefficiencies and unnecessary headaches for both the organization and the customers.

5 MISMATCHED MESS

We had a terrific well-documented policy and program at the organization, but the work product of the third party risk team didn't match at all.

It proved to be a real problem from both an audit and a business perspective. When we received notification of exam, we had to scramble around to quickly make necessary changes to our work product across the organization. We knew if we didn't, the exam results would be a disaster.

venminder

6 WE NEED BACKUP

Due to inefficient tracking, my organization failed to update its risk assessment on a critical third party vendor. Key changes went unnoticed and the first person to catch the problem was the business manager when he called to the tell the vendor manager that the vendor had gone out of business.

As you can imagine, everyone was quite frantic when we realized that a vendor that was critical to our business operations suddenly shut their doors and we did not have a backup vendor readily on hand.

7 MONEY TROUBLES AND BAD PRESS

One of my colleagues who was responsible for performing financial reviews was collecting the documentation and simply "checking-the-box". She would note that we had a financial report on file and that year-over-year numbers either looked positive or poor and then dug no further.

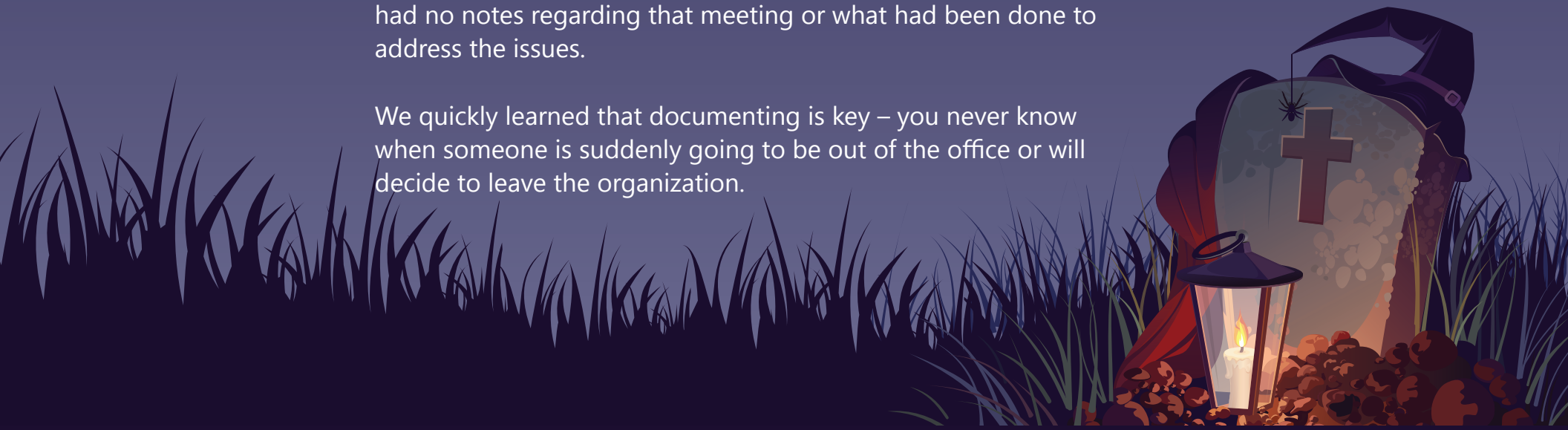
By cutting corners we didn't realize that one of our critical vendors was actually struggling financially. A more thorough analysis, that went beyond the numbers, would have helped us to see that fairly significant lawsuits were pending at the time and the organization was quickly declining in the service levels being provided and, therefore, receiving a great deal of bad press.

8 UMMM... I DON T KNOW

At a small organization that I was previously employed at, we weren't the best at documenting our vendor management process. It was a small team and we usually had a good grasp on what the others were doing to manage their vendors accordingly.

We had a big year-end meeting with the board and my co-worker was suddenly out of the office sick with the flu. You can imagine the board's concern, and our embarrassment, when they asked very specific questions regarding one of my sick co-worker's vendors as a follow up from one of their previous meetings and we had no notes regarding that meeting or what had been done to address the issues.

We quickly learned that documenting is key – you never know when someone is suddenly going to be out of the office or will decide to leave the organization.



SO, WHAT DO WE LEARN FROM ALL OF THESE TERRIFYING SITUATIONS?

To sum it up, remember these **8 best practices**:

- **Implement a streamlined process or system** that meets your organization's third party risk management needs. In addition, be sure that everyone is on the same page.
- For smaller to mid-sized organizations, we'd encourage you to **run a centralized third party risk management model**. If you're a larger organization then a hybrid approach may work best.
- **Data breaches will happen.** Have plans in place to be as prepared as possible and to help you communicate to your customers in a timely manner.
- **Be sure to test all components of your business continuity and disaster recovery plans.** Repeat the testing periodically.
- **Comb through your work product** and verify it matches what you say you do in your organization's policy and program documentation.
- **Track all key dates.** Don't let a contract renewal or expired risk assessment be missed.
- **Never just "check-the-box" when performing due diligence.** Always have a certified expert collect and analyze the documentation.
- **Document all vendor reach-outs and keep meeting minutes.** Store it all in a secured, centralized location that's available to your team to reference as needed.

Download free due diligence samples and see how Venminder can help you reduce your third party risk management workload.

Download Now

400 Ring Road, Suite 131, Elizabethtown, KY 42701
(270) 506-5140 | www.venminder.com

venminder