MY VENDOR HAS SUFFERED A DATA BREACH

If the data breaches reported in the last few years are anything to go by then any organization servicing consumer data should be striving towards stringent information security and physical security controls.

Hackers don't discriminate when looking for an asset to attack. The common theme is **not so much IF** an organization will be hacked but **WHEN it will be hacked.** Failed cyber attacks are noted on a daily basis, if not hourly basis, according to many of our industry contacts.

WHAT DOES THIS MEAN FOR YOU?

1. You need to immediately ensure that your vendors are **protecting consumer data** and check this on an ongoing basis.
2. If you experience a data breach, you're responsible for **remediating** to ensure that the risk and future fall out at the consumer level is mitigated.
3. **Be aware of your state or industry's data breach notification laws and guidance.** If you're unfortunate enough to suffer a data breach either from an internal source or third party then you'll need to follow those and, additionally, continue to follow your remediation policy. Regulators are likely to begin looking at this area given the increase in data breach notification requirements set at the State Attorney General level. Most states have now implemented such requirements, so this is an area that you simply cannot bury your head in the sand with the hopes that it goes away.

What's a remediation policy?
The policy is a response plan to quickly address the data breach and communicate effectively with customers.

So, what do you do if you or your vendor suffers a data breach?

10 BEST PRACTICES

When Handling a Data Breach that Limits the Impact to Your Brand and Your Customers

1. **Be transparent.**
While acknowledging a breach is a painful exercise, the mistrust and reputational damage caused by sitting on the news will outweigh putting off the inevitable.

2. **Ensure data breach notification requirements are documented in your contract language.**
Many organizations have shared that there is a high-level of mistrust between third parties who may not notify them of a data breach in a timely manner.

3. **Ensure you tell appropriate people.**
When required, notify the State AG, law enforcement and regulator.

4. **Define the impact of the breach.**
Understand what you are dealing with. Was the breach isolated to one individual or did it impact many customers?

5. **Adopt a customer notification process.**
It's best to notify the impacted customer directly than have it appear on the 6pm news.

6. **Offer credit monitoring services.**
Ultimately, a data breach which contains non-public personal information (NPPI) of the customer may increase the individual risk of identity theft. It's important to consider timelines as well since once the data is out on the dark web, items such as social security number data is unlikely to change.

7. **Implement more robust user authentication procedures.**
This should be done if customers have access to online tools.

8. **Perform root cause analysis and enhance security controls.**
Lightening does strike twice. Learn from this breach and build a stronger information security system.

9. **Set expectations with your vendors.**
If the breach originated from the vendor and not your internal organization then perform deep audit testing. If the vendor is unwilling to cooperate then you have larger issues and should reconsider your partnership.

10. **Perform an assessment on your overall information security processes.**
Document all updates and implement refresher training for all employees.

The goal of adopting these practices is to be able to document what positive steps your organization has taken to demonstrate how you are managing and being proactive through a risk event.

The Equifax data breach of 2017 quickly became a case study of how a respected organization made missteps in their disclosure process.

After suffering a data breach, you cannot walk away without some level of damage, so being proactive is your best defense when working with both regulators and your most important asset: your customer.