

10 BEST PRACTICES WHEN HANDLING A VENDOR

DATA BREACH



Hackers don't discriminate when looking for an asset to attack. The common theme isn't 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.

SO, WHAT DO YOU DO IF YOU OR YOUR VENDOR SUFFERS A DATA BREACH?

Limit the impact to your brand and your customers
with these 10 best practices:

- 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:

Be able to document what positive steps your organization has taken to demonstrate how you're managing and being proactive through a risk event.

After suffering a data breach, you cannot walk away without some level of damage, so being proactive is your best defense.



Venminder can assist with your information security and cybersecurity needs.
Download some of our work product samples.

[DOWNLOAD NOW](#)

[PRINTABLE VERSION](#)

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

Copyright © 2019 by Venminder, Inc.

venminder

www.venminder.com