FACTSHEET

Guidelines for Damage Control After a Security Breach

You may think that all your company's data is safe and secure, but the worst can still happen. In fact, 2017 has already seen 1 in 4 organizations fall victim to a data breach.[1] In 2016, 806 breaches were reported involving over 11 million records.[2]

Given that the chances of a breach are so high,there are three steps you should follow if your company's data is exposed:

STEP #1

Perform a Risk Assessment

- Find out what data was compromised and how it happened
- Assign an expert, with the knowledge and expertise, to head the investigation and locate the source of the breach
- Walk through the office and identify additional areas of risk – i.e. blue bins, messy desks, unsecured printers

STEP #2

Get Expert Legal Advice

- Bring in legal team to decide if announcement needs to be made to stakeholders
- You may not even have to disclose the breach and your legal team can explain the repercussions of any actions you may take

STEP #3

Conduct a Policy Review to Prevent Another Breach from Happening Again

- Assess current policies and see where information security gaps lie
- Bring in third party providers, like Shred-it, to conduct a comprehensive Security Risk Assessment of your business and provide recommendations for improvements
- Consider implementing a Clean Desk Policy and a *Shred-it All* Policy to shred all documents after their use
- Get buy-in from management and use a top-down approach to embed a culture of total security

Sources

1 Ponemon Institute. 2017 Cost of Data Breach Study: Global Overview.
2 https://www.privacyrights.org/data-breaches

Here are some examples of the types of data that must be disclosed if there is a security breach:

- Data that falls under IPAA, SOX, PCI or FTC safeguards or state privacy laws must bedisclosed if it's breached.

  Example: If only a computer has been compromised, you may not need to disclose that security event, as long as the rights of any individuals involved remain protected.

- Regulated data must be disclosed if it's breached, and includes Social Security numbers, government ID numbers, payment card information and account numbers. Your local regulations may specify other data covered by law.*

  Federal law requires banks to inform customers of breaches; 46 states have laws mandating that other companies do the same.

Sources

1 https://www.privacyrights.org/data-breaches
2 Security Dark Reading, http://www.darkreading.com/security/perimetersecurity/208804800/what-not-to-do-after-a-security-breach.html
* This document is not intended to substitute for legal advice. It's very important to have your attorney involved immediately when considering action regarding a breach.

"Data and privacy protection have moved from being a corporate afterthought to becoming a driving risk reduction mechanism for companies. Any CEO, COO, ISO or business owner who is not seriously evaluating the role of privacy protection and data in their operation is living on borrowed time."

– Eduard Goodman, IDT 911's Chief Privacy Officer

About Shred-it

Shred-it specializes in providing a tailored document destruction service that allows businesses to comply with legislation and ensure that their client, employee and confidential business information is kept secure at all times. Shred-it provides the most secure and efficient confidential information destruction service in the industry.

NAID-CERTIFIED INDUSTRY EXPERTS
All Shred-it® locations in North America have received NAID Certification for mobile document destruction.

For peace of mind, contact Shred-it® today
800-697-4733 | shredit.com

Shred-it®