BREACH RECOVERY CHECKLIST FOR YOU AND YOUR COMPANY

No business or individual is immune to a cyber breach, yet I hear many people say they don't think they will be affected. They believe that their company does not have anything valuable enough to be

stolen, but every company and individual has data that is valuable to a cyberthief that they might overlook. While we're all focused on our money in bank accounts, cyberthieves are looking elsewhere. But before I lay out a breach recovery checklist, let's not forget the following noteworthy breaches:

2013 Target – 70 million records compromised
2014 Ebay – 145 million records compromised
2014 Home Depot – 56 million records compromised
2014 JP Morgan – 76 million records compromised
2015 Anthem – 80 million records compromised
2016 IRS – 700,000 accounts affected
2017 Equifax – 145 million American accounts compromised including SS#s and driver's licenses
2017 Yahoo – 3 Billion user accounts compromised

These are just some of the greatest hits in data breaches. Now ask yourself if you have any ties to any of these breaches. I would venture to say- yes! Perhaps you have not been compromised yet,but it could only be a matter of time.

Damage control

Compromised data stolen from a company or directly from an individual is used for 3 primary payouts: identity theft, medical fraud, and credit card fraud. Thieves looking for social security numbers, account numbers, date of birth and mother's maiden name can glean additional data just by stealing one of these and leveraging the inherent security weaknesses found on social media and in security challenge questions.

Before you can take any action, you must determine specifically what was compromised. Perhaps your address or name were compromised - this is not too alarming as anyone can obtain this information in less than 30 seconds through an Internet search. This would be a low security threat, but do not be lulled into a false sense of security because each piece of data, no matter how seemingly harmless, is still another piece of the security puzzle. When we build a jigsaw puzzle, even insignificant pieces can sometimes lead to an unexpected breakthrough. And once the puzzle becomes clearer, the time required for completion only shortens. So time is of the essence, but what about post-breach?

Post-breach – take immediate action

As soon as you know you have been compromised, take immediate action. Since weak passwords are involved in nearly every breach, create new, long and strong passwords of at least 12 characters using upper/lower case letters, numbers and special characters.. If that sounds like too much to handle, use a password manager such as Dashlane to help you create and manage all those new passwords. It is important to also make sure you are not reusing any passwords across multiple sites. Despite endless warnings on the dangers of password reuse, it is still a tremendous problem that hackers gladly exploit.

If you believe your credit card was compromised, it is essential to immediately call your issuing bank. The majority of credit cards have a toll free number printed on the back allowing you to speak to an actual person to relay any suspicious activity. They will cancel and re-issue the card immediately, ensuring safety. Time is of the essence as most credit card thieves move quickly to go

on shopping sprees in the first few hours of stealing a credit card. Your liability exposure is $50 on a credit card (although they often waive that fee if you ask) and you have up to 60 days to file any suspicious charges. In contrast to this a debit card only allows you 2 days to report fraud with a liability of up to $500. This is another reason why I strongly discourage the use of debit cards. In either case, regular credit monitoring and immediate reporting of suspicious activity are paramount to security.

A good next step would be to contact one of the credit reporting bureaus and place a fraud alert to TransUnion (800-680-7289), Innovis (800-540-2505), Experian (888)-397-3742), or Equifax (888-766-0008). If you report a fraud alert (aka 'credit alert') to any one of the credit reporting bureaus, they are all required to alert the other three bureaus anyway.

If you suspect your identity has been compromised, you may want to take a stronger step, which is a credit freeze (aka 'security freeze'). Anyone whom you already don't do business with cannot run a credit report on you or open an account in your name without your explicit authorization. To unlock your files temporarily, the credit agency will issue you a PIN. It is important to follow that up with a formal report of identity theft to the FTC.

If you have had your identity or credit compromised, you may opt to get a monitoring service such as LifeLock Ultimate Plus. This is not as much a preventive measure as it is an early warning service that scours the dark web for potential compromises and threats by cyberthieves. The idea is that the faster you can be alerted of suspicious activity, the faster you can react to protect your digital identity.

When your company is hacked

As much as a nightmare it is to have your own identity hacked and stolen. having your company hacked can be a nightmare of a higher order. Since you are dealing not only with internal company data - such as financials, emails, passwords - but potentially all your customers' data, no required post-breach steps can be overlooked.

The first thing you need to do is to immediately reach out to your customers and alert them. In fact, the law requires that you inform any customers who had their data compromised. This can be difficult when organizations still have not fully ascertained what has, or has not, been compromised. It is more important to alert customers first so that they can be prepared, giving you time to work out the details later. This can help them avoid major financial damage as well as help avoid future class-action lawsuits against your company. This alert should be followed up with a formal written data breach notification detailing all known compromised data and what to expect in the way of security responses and future correspondence.

Customer notifications should always clearly state what happened, how the damage has been contained, and any preventive actions put into place to protect from future breaches. If your company does not have a clear understanding of what happened, they should hire an outside cybersecurity firm to carefully advise on the next crucial steps.

Laws vary from state to state as to the level of transparency required as well as the obligations to provide free credit monitoring. For example, a breach of sufficient size requiring notification of over 500 customers may require filing a formal notice with your state attorney general's office. There may even be a need to notify federal authorities depending upon the scope of the breach and the industry you serve. Also, look within your industry to determine if specific regulatory bodies require

additional filings. For instance, the healthcare services industry's HIPPA requirements stipulate that if over 500 customers are affected, you need to notify prominent media outlets.

Companies should have an annually updated incidence response planwhich includes a game plan for response to a serious breach and key contacts that need to be informed to provide assistance, including a third party cybersecurity IT forensics group.

I recommend annual vulnerability assessments alongside regular penetration tests to identify vulnerabilities that in-house security and IT teams may overlook.

With the aforementioned breaches affecting everyone, it is also prudent to further minimize impact by putting an effective cyber insurance policy in place. These policies become crucial after a significant breach as numerous legal expenses, forensic fees, customer credit monitoring fees are sure to follow.