It's NOT about the breach.

5 PRACTICAL STEPS TO SURVIVING A DATA BREACH *(THAT NO ONE IS TALKING ABOUT)*

A SURVIVAL GUIDE FROM

VISTA SOLUTIONS
Uncompromised IT.

riverbed™

WRITTEN BY JILL BRITO

WHY MOST BUSINESS DON'T SURVIVE
(OR ARE NEVER THE SAME) AFTER A SECURITY BREACH

We've all heard the statistics before:

The AVERAGE cost of a data breach

$3.8 MILLION[1]

This number does not take into the "mega breaches" that occurred in recent years such as Anthem, JP Morgan Chase, Home Depot and Target (which reported a $148M loss as a result of their breach).

It takes the average company

205 DAYS

to detect they have been breached.[2]
That's 6.5 months.

60%

of small to medium businesses
(500 employees or less)
will go out of business within
6 months of a data breach.[3]

The fact that we are more likely to be breached than not is no shock to anyone... but the question is this:

> *How do I actually protect my business, my customers, my data, (and my job), when a breach is inevitable?*

The problem is not the lack of incredible technology or competent professionals... after talking with countless professionals, I believe the problem lies in the approach, our core beliefs about security and how those beliefs manifest themselves tactically which ultimately determines whether companies become statistics or not.

It has been my experience that those companies you won't read about in the headline are those that have taken these 5 steps are the ones that not only survive a security breach...but thrive in spite of one.

5 PRACTICAL STEPS TO SURVIVING A DATA BREACH

STEP 1

DETERMINE WHAT "PROTECTING YOUR DATA" REALLY MEANS.

Security is a hot topic...and nearly every company playing in that space is feeding off of the fear we all have of being hacked as their primary marketing and sales tactic.

I don't know about you, but I am constantly bombarded with messages ensuring me that:

> *XYZ product will "protect" my data or ABC solution will keep my business "safe"...but it wasn't until recently that I found myself asking the question 'So what does "protect" mean?'*

Honestly, it sounds like dumb question, but I've found that how each company answers this question (whether they have thought it through cognitively or not) tends to determine their fate in the instance of a breach.

And as I thought about this for my own business and reflected on the countless conversations I've had over the last few years with clients and colleagues, this is what I concluded:

By default, if we don't take the time to really think about the answer, most of us will give lip service to the idea of "assume a breach" and would strategically adopt that paradigm, but tactically, we have a tendency to treat cybersecurity like a castle.

We end up building "walls" around our data with preventative security like antivirus, firewalls, SIEM, (the list is endless), and hope to God that those will keep the bad guys out and the data in.

> *But the real question is... is that truly keeping us safe?*

Although most of us give lip service to the idea of

"ASSUME A BREACH"

and would strategically adopt that paradigm, tactically, we have a tendency to treat cybersecurity

These technologies are, indeed, vital to a solid security strategy, but any security professional worth their salt will tell you that none of these are impenetrable, it's just a matter of time.

In my experience...it is the companies that (consciously or unconsciously) adopt this "castle" definition of protection that tend to become a statistic. My observation is that the ones who survive are the ones who have determined that truly protecting their business begins with going beyond their castle walls and addressing the real root of the security problem: understanding what's really going on in their network.

/ STEP 2 /

UNDERSTAND WHAT'S REALLY GOING ON IN YOUR NETWORK.

If we take a moment and dissect the reasons why breaches are so devastating (and often fatal) to businesses... the loss of money, smeared reputation, loss of jobs, closing of business, lawsuits, general misery, etc., at the core, it's NOT because they didn't have proper preventative security technology or incompetent professions. In fact, it's not even because breach happened (because we're all gonna be breached, it now the status quo).

Because I guarantee you, all of the companies that had the names and reputations smeared across the headlines had top-notch security technology and dedicated teams of people whose sole job was to prevent an attack. And they got hacked.

> *The real consequences come when we don't have a clear understanding of what's really going on in our environment.*

Think of it like a building with security cameras - the camera's aren't what actually 'sound the alarm' and secure the perimeter when something happens, but it's the cameras, the visibility into our network, allows us to capture what happens before an attack, trigger alerts that something is not right, and rewind the tapes to determine what happened and the quickly remediate of the damage after an attack.

If we were to liken attacks are a continuum, a stage of before, during and after, we spend the vast majority of our time money and effort prepping our business for the "during" stage when the alarms sound, when in reality, it's the lack of security cameras, preparation the before and after stage that ultimately cause the most damage.

The real consequences come when we don't have a clear understanding of

WHAT'S REALLY GOING ON

in our environment

Because without visibility, it's taking us an average of 205 days to detect a breach. Without visibility, it's costing us an average of $3.8M to deal with the consequences of not knowing exactly what happened.

The following 3 steps are ones we guide our clients through in order to tactically understand what is going on:

/ STEP 3 /

IDENTIFY WHAT'S THERE.

A. Today's IT networks are incredibly complex, with thousands of moving parts, making it very easy for there to be areas of the network that IT is unaware of, and, thus vulnerable. Hackers are taking advantage of this complexity to infiltrate areas and sneak in undetected and wreak havoc for months.

B. Because if we don't identify what's in our environment, how can we expect our defense tools to effectively protect them? There are lots of technologies like that test for vulnerabilities within the network, but they will only test for elements in the network that they are aware of. If they can't see it, they can't protect it.

C. Network visibility technology enables the creation of network maps that allow security teams to identify everything that is in their network and monitor everything in real time.

/ STEP 4 /

BASELINE WHAT'S NORMAL.

A. Visibility technology provides companies with a baseline understanding what "normal" behavior is for your business allows security to quickly identify when something is abnormal.

B. For example, let's say all credit card swipe terminals should be registered to IP# x.x.x.x in Denver, and only that IP address. If you have baselined that as normal behavior, and anything outside of that as abnormal, you can quickly raise an alert when those credit card terminals start communicating with and IP address in Russia.

Because without visibility it's taking an average of

205 DAYS

to detect a breach.

Without visibility it's costing us an average of

$3.8 MILLION

to deal with the consequences of not knowing exactly what happened.

| C. And in going through this exercise, you can designate what is important, monitor communication, and in doing so, it will allow them to quickly identify abnormal behavior deeper in the network that might otherwise go unnoticed.

| D. Because not all security issues will manifest as a blatant attack – a lot of security issues disguise themselves as performance problems.

| E. Think about it – if someone is sneaking terabytes of data out of your network, it's not unlikely for that to create a bandwidth issue that will result in applications or networks that are under-performing. This technology allows you to quickly drill down to the root cause of those performance issues and determine if was a server glitch, bad application code...or something else.

/ STEP 5 /

REWIND THE TAPES.

| A. If you were attacked, could I easily go back and "replay the tapes" to see what happened, triage the damage, and remediate before irreparable damage is done?

| B. Without a doubt, one of the primary reasons companies lose millions (or go out of business) is because, after a breach, they have to spend months or years investigating what happened, how it happened, or the extent of the damage.

Think about it like this... how much faster could you solve a crime, if you had access to the security tapes vs. if you didnt?

WITH PROPER VISIBILITY IN PLACE, YOU CAN OBSERVE SYSTEM BEHAVIOR, IN MINUTES, BEFORE AND AFTER A BREACH...

FINAL THOUGHTS

In 2012, FBI Director Robert S. Mueller III, was quoted saying this:

> *"There are only two types of companies: those that have been hacked and those that will be."*

Whether we want to admit it or not, the reality of a breach is imminent...and if we want to survive, we HAVE to start thinking about security differently. And that starts with understanding what's going on in our network.

How this is actually done will vary from company to company, but without these 5 components, we will be hard pressed to understand what's really going on...and surviving a breach will become a game of Russian roulette rather than a strategic plan.

ABOUT VISTA SOLUTIONS

Vista Solutions works with business and IT professionals that are concerned about how to really protect their data in an environment where businesses are hacked every day. Approaching security from a different paradigm, we help our clients understand what's really going on so they can be confident that not only they would survive a breach, but thrive in spite of one. Learn more about why it's not about the breach at vistasolutions.net/visibility or contact us at vistasolutions.net/contact-us

ABOUT RIVERBED TECHNOLOGY

Vista Solutions partners with Riverbed Technology, the leader in Application & Network Performance Monitoring. Although not a security company, Riverbed's unique Network Performance Monitoring (NPM) solutions can be leveraged to ensure you know what is happening on your network, that no one is doing things they should not, and, in the worst-case scenario of an intrusion or other violation, you can determine what happened and then identify proper mitigation factors. Riverbed's 25,000+ customers include 97% of both the Fortune 100 and the Forbes Global 100. Learn more at www.riverbed.com.

ABOUT THE AUTHOR

Jill Brito is the Marketing Director at Vista Solutions in Fort Collins. She works with IT and business professionals who are worried about how to protect their data in an environment where breaches are inevitable, and are serious about developing strategies that give them confidence that their business would not only weather a cyber-attack but thrive in spite of it. Jill holds an MBA from Colorado State University and has been working in technology for over 5 years.

1. http://www.reuters.com/article/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527
2. http://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/
3. http://www.inc.com/graham-winfrey/how-to-protect-your-company-information-in-the-digital-age.html