DON'T PANIC!

6 STEPS TO SURVIVING YOUR FIRST BREACH

www.alienvault.com

So you've come to terms with the truth of the world; eventually, you're going to suffer a major security breach — maybe not this month, not this year, but, as the great sage Tyler Durden so incisively observed,

> "On a long enough timeline, **the survival rate for everyone drops to zero.**"

Being breached doesn't determine whether or not you've got a good security program in place, but how you respond does...

Disavow yourself of any notion that the work you do in network security is “protecting” the company’s assets. Your job is to merely choose how the network can be attacked, with the hope that you can control the battlefield elegantly enough to be able to respond to all attacks adequately. Network security is as much about technology as the game of chess is about little carved figures on a checkered board.

Once you accept that everything that can go wrong will gleefully do so at the worst possible time, there are things you can do today that will help rein in the trials of the future — things you can set in place to allow you to expect the unexpected.

So, what can be done today and then set aside for that rainy day? What actions can you take now that will bear fruit when you have the entire executive team breathing down your neck for answers they wanted an hour ago?

It’s not the technical aspects of a security breach that will test you — indeed such events usually give people opportunity to bring the full brunt of their skills to bear — but the organizational duress that results.

Repeat after me: “**Don’t panic!**”

1 Build relationships outside of the IT department.

If you like meeting new faces around the organization, a security breach provides ample opportunity to do so — albeit at the worst possible time. A breach is going to involve personnel from a whole slew of departments: legal, executive, and PR to name the most obvious candidates. Maintaining an established channel with these groups and an understanding of how both your and their jobs will interact during a security breach can save a lot of rushed paperwork and tense meetings during your time of crisis.

2 Get the **"I told you so"** off your chest now.

There's a notion in info-security that the work we do is possibly the most important thing in the company — that without us, the whole organization would fall to its knees and succumb to raiding bandits. It's time to accept some cold hard facts.

There are much greater risks to a company's operational capacity and profitability than a security breach. Remember, your job isn't to prevent this from happening (which is nearly impossible,) but to lessen the impact when it does. Think more along the lines of: "It would have been much worse without us."

3 Comply with regulations, **and then go further.**

This may be preaching to the choir — we understand that "Compliance Is Not Security™" — but understand that a security control that isn't monitored is even worse than no control at all. The Intrusion Detection System that doesn't have someone actively administrating it and looking at the alerts is just another avenue intruders can use against you (and one with significant access to all network traffic!)

Just because you're in an industry that requires you to keep all log data for 90 days doesn't mean you shouldn't store everything for a year. After all, storage is ridiculously cheap and security breaches don't happen inside a matter of minutes — the initial signs of intrusion and persistence may show up in logs from months ago. When you need them, you'll be glad you kept them.

4 Give everybody the answers they need, **not the answers they deserve.**

From end-users to executives, the number one priority during a breach is information — information that's going to take time to acquire. Making clear decisions and acting on them is the top priority during breach discovery and recovery. Give your users clear, absolute answers on why you're shutting down large portions of the network unannounced, and then do it if that's what's necessary.

Sell them a convincing lie if you need to, but an answer is an answer and cuts down on uncertainty and water cooler conspiracy theories. Don't be a slave to spending a quarter of every hour updating the management chain on how there are no new updates on the investigation because you're investing 25 percent of your investigation time in updating people about the investigation.

5 When you have eliminated the impossible, whatever remains, no matter how improbable, **must be the truth.**

The perpetrators of the crime you are investigating are just human beings — it's unlikely they possess psychic powers, supernatural levels of intelligence, or the ability to travel through time. During the investigation, you will encounter many "How did they do that?!" moments. The simplest answer is usually correct. Keep a clear head, and first assume that they didn't crack your super-secret cryptography, but that they probably found the passphrase in a text file on an administrator's compromised machine. Don't assume they knew to target the administrator's account because of some insider information, but first consider it could be because he states his job title on his LinkedIn profile. What you are trying to unravel in days, may have taken the intruder months to put together, but you do have an advantage: You're able to work backwards to the beginning of it all.

This is the time when that checklist of things to cross-examine during more mundane investigation tasks become invaluable. You're going to be chasing leads down a lot of rabbit holes and running after a lot of wild geese —almost certainly following a lot of hunches — but nothing helps you hold on to your sanity like a good list of things to reference against to reassure yourself you've left no stone unturned and no metaphor unexplored.

6 Practice makes perfect.

I know this one is obvious, and I don't mean to insult your intelligence by including it here, but I also know you've been wanting to get some bench exercises performed within your security group for quite some time — and yet, it keeps getting postponed in favor of more pressing, "real," work.

Stop it right now.

Your work as a security professional is absolutely centered on the inevitability of the worst-case scenario. Why aren't you preparing for it? Practicing it? Has your company engaged the services of a pen-testing company recently? Did you treat their actions as a breach to be investigated? Did you match what you were capable of detecting and investigating against the report of what they did?

No matter what it takes, get the practice in now — because when the time comes for points 1–5 to take effect, the last thing you want to be doing is making it all up as you go.

Now, if you could learn everything you needed to know about investigating and recovering from a security breach in a six-point article, those who have been through one before would not speak of their experience in hushed, fearful tones. Unfortunately, like many things in life, only experience through the real thing is going to prepare you for the next one.

Get more on Incident Response from AlienVault:

- The AlienVault Incident Response Toolkit
- Incident Response Orchestration: What is It and How Can It Help?
- Speed Incident Response with AlienVault USM

www.alienvault.com