Sean: Keep your cool during a data breach

Hi, my name is Sean. I'm a Technical Program Manager in Google workspace. I am a 30 year security veteran within the security space across six different industries. During your first data breach, the most important thing that you can do is keep your cool. Everyone around is going to be freaking out. If you are on the security team and you are managing the incident, you have to legitimately be the cool guy in the room. Be that person that has the pause in the conversation. Somebody might be like, do you know what's going on? I absolutely do. I think the biggest breach I've ever had was a phone call. An engineer for another financial, bought a server off eBay. That server fired it up hadn't been wiped. Twenty million credit card records were on it. That triggered a whole review of we had not been controlling for how do third parties because we were now outsourcing data centers. How do third parties wipe the servers that we no longer use? The first thing you're going to do is to contain the breach. If you are still hemorrhaging data, you go through your progressions to stop hemorrhaging data. So if that means shutting down a server, shutting down a data center, shutting down comms, whatever, stopping the data loss is that is your number one priority. Your job as an incident manager or as somebody working a breach is to stop the breach and then investigate the breach. So executing your incident management by plan is the most important thing that an entry level person can keep in mind.
(Required)
en

Revision #2
Created 2023-05-30 22:39:56 UTC by naruzkurai
Updated 2023-05-31 14:44:19 UTC by naruzkurai