Feb 21, 2025 (9:20am PT)

Hello Sirs:

This is probably above my paygrade, but it seems like a big deal, so I'm cc'ing everyone in our corporate directory to find someone to help.

I tried to forward a message from a reporter (below) to our comms crisis response mailbox, but got this out of office reply:

> "Note that I'm heading to Tahoe for the weekend (or so) and will be off the grid for a while."

Is anyone on point for crisis management or incident response now?

When I asked my supervisor, they said that this is a process breakdown because of the merger (and that I should not hold my breath for things to get fixed).

Is anyone trained to deal with this stuff or pull together a war room? Do we have some process to follow? Does anyone know an incident response expert who can help us?

If not, I have a friend of a friend who may be able to help, so I'll reach out and see what they recommend. Don't worry, I'll mark the message as "attorney client privileged" to make sure that no one can sue us because of this massive data breach.

I'm not sure what else to do and I'm starting to FREAK out. Does anyone want me to start a Slack channel for this? Otherwise, I'll just assume that everyone cc'd has read this and close this incident ticket.

Justin Time

ICE + SDK IT Helpdesk/Customer Support

From the Desk of:

February 20, 2025 (5:00pm CT)

To SDK Public Relations:

I am a cybersecurity reporter and I'm writing to inform you that I will be publishing an online story within the next 48 hours. The story will look similar to the following:
https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old/
https://krebsonsecurity.com/2025/02/teen-on-musks-doge-team-graduated-from-the-com/

Specifically, I believe that your servers may have been pwned. I've seen known bad actors on the dark web, chatting about gaining access and exfiltrating your company's threat intelligence database. They have uploaded a sample of the data to pastebin (which looks legit) and are offering to sell the full dataset for 10 bitcoins.

The data they claim to have obtained includes email addresses and passwords. I don't know exactly how or when the alleged unauthorized access may have begun, but the 'chatter' I've seen is as recent as 18 hours ago.

This chatter suggests that they may have used a combination of phishing, elevated access, Log4j flaws (CVE-2021-44228), and backdoor techniques, including exploiting weak passwords (apparently all passwords are name of the CEO's dog at some third-party vendor you use for hosting, called Weak Web Services, Inc.).

In addition, I understand that a member of your engineering team, a 19-year-old high school graduate named Edwina Cortisol, who reportedly goes by the nickname “Big Orbs” online was recently granted “read only” access to a number of U.S. Government databases. Chatter on Discord and Telegram channels allege that Edwina has already extracted, transformed, and loaded some of this sensitive data into the SDW systems that were compromised.

Should you wish to comment before I publish, note that I’m primarily interested in verifiable facts that may refute or add additional detail to my reporting (based on a qualified investigation and analysis of your computer network, administrative access of your database(s), and third-party service providers). Also note that my investigation into this matter will be ongoing.

I look forward to receiving an on-the-record statement from the appropriate representative (or anyone) from your firm.

Respectfully,

Briana Crabcakes