Gmail

Peiter Zatko [redacted]

lawyer letter sent to Twitter

Peiter Zatko [redacted]
To: Patrick Pichette [redacted]

Wed, Feb 2, 2022 at 5:20 PM

Hi Patrick,

I'm attaching the letter I had my lawyers create.

I also want to give you a preview of some of the things I'm putting in the documents I'm creating for yourself and the Risk Committee. It has become apparent to me that Twitter Information Security, and other areas, were not accurately characterizing the environment and the risks. It's important to me that a correct characterization of the risks and Twitter's environment are conveyed.

There's a lot of "present wins", "celebrate effort", and "avoid quantification and context" going on there. It predates me and it strongly resists change (even at the exec level).

I hope it is apparent that I am *still* trying to help. I joined because I felt an "attachment to mission". I'm different from a lot of the world that way. I had assumed that and the need to actually figure out what's going on under the hood at Twitter was why Jack tapped me.

Some examples of items I'm putting in to the "corrected q4 report" (I will make sure to send you copies directly):

I'm pretty sure that based upon your comments you were realizing parts of this at the same time it was becoming apparent to me.

E.g.

A)
I called out that engineers have access to production systems and data. Testing and development largely happens directly in production because there is no testing/development/staging environment to speak of.

At a risk meeting you correctly asked if this was normal, to which I replied "no".
51% of FTEs (more than 3k people) have production access. This is up from 46% at the beginning of 2021. This is outrageous.

B)
I brought in (actual) data for where Twitter was in their initial mock-SDLC roll out (Q1 or Q2). You were shocked and frustrated by the data. Apparently Parag and Mike Montano had been telling you for several years that "things were going really well" and that they were "really far along". Perhaps they had been providing qualitative descriptions of effort, because the data showed a very different story.

This situation appears to be uncomfortably common.

C)
In my first Risk Committee meeting you called out the need for straight forward dashboards. I entirely concur! I have never seen a company lack simple dashboards to the extent Twitter does. Twitter is also, it turns out, incredibly resistant to creating them. I pushed on these for the 12 months I was there. I received every excuse under the sun for why they couldn't be done, or were always "almost there".

It turns out that some of them already exist... but people do not want to advertise them. They stay hidden and are not briefed "upward".

For instance in Q3, after having been repeatedly denied accurate data, I personally went and gained access to the dashboards endpoint security (these are the 10,000 employee laptops). Whereas the CISO had been reporting that "we were in good shape", that was/is definitely not the case:

30% of the all Twitter employee computers (laptops etc.) are reporting that they have software updates *disabled* (this is Equifax level bad).

60% of the servers in the data centers are running non-compliant Operating Systems (often too old for support and also not being able to support basic data encryption requirements)

It's not surprising, with the raw data present, that we find (D).

D)

Of the (very) large number of incidents that Twitter experiences (~1 per week) more than 50% of the issues are related to access control and more than 25% are related to security configurations, patching, and software versions.

In closing, thanks for reading Patrick. Typing this up and knowing that someone who has a long standing reputation for ethical behavior is reading this is comforting. It really feels that at the end of all of this I had gone in acting in good faith, trying to help improve things but perhaps that good faith was not met with good faith in return. :(

The circling of the wagons and all the rest of this is all very disturbing (including the NYT "leaks" and follow ups from Parag describing a less than favorable exit.

I'm still looking to do the right thing for Twitter and also amicably close this out.

kindest,

Mudge Zatko

PS - In Privacy Engineering and Twitter Service there are dashboards now! Unsurprisingly these two organizations made more progress while I was at Twitter than they had across multiple years prior. They are now set up for long term success. :)

Marianne Fogarty 2-2-22.pdf
57K