Gmail

Peiter Zatko [redacted]

Re: Privileged and Confidential - Priority Meeting Request

Peiter "Mudge" Zatko [redacted]
To: Marianne Fogarty [redacted]
Cc: Rebecca Falk [redacted]
Bcc: [redacted]

Tue, Jan 18, 2022 at 11:16 AM

Hi Marianne and Rebecca,

Thank you for your e-mail yesterday. As yesterday was a holiday I missed it, otherwise I would have sent this response then.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Thanks. Please let me know if you have any questions or other data I need to know.

Respectfully,

Mudge Zatko

Begin reference e-mail:

Peiter "Mudge" Zatko [redacted] Dec 15, 2021, 3:02 PM
to Parag, Dalana

Parag and Dalana,

The other day, in our conversation, you suggested I forward the infosec presentation to the Risk Committee Board without modification or replacement.

I expressed concern given what I see as numerous, and some significant, misrepresentations in the document.

The document has been forwarded to the committee.

This e-mail is more for our records and to ensure there was clarity in the description of my concerns around repeated representation items in the document we are putting foward.

I'm very much looking forward to hearing from you today.

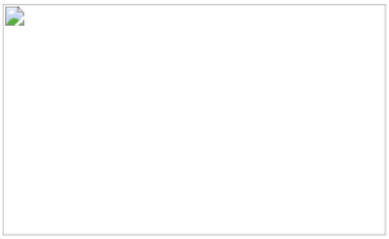
kindest,

Mudge

Notes shared with [redacted]on concerning data presentations in the Risk Committee documents

9k (of our 10k) systems have security reporting software on them.

This has been reported several times. I worry it is misleading. This security reporting software has been reporting that 50% of all of our systems are not meeting basic security configurations (for over a year). 30% of the systems are reporting as not having software updates enabled. Both of these figures have also been at these levels for over a year as well. Be careful not to confuse the board with the stating we have 90% coverage of our systems with security reporting software versus what that reporting software is telling us about our systems.



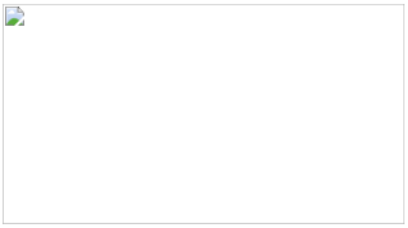
The above graph is now using a subset metric of SIMS as opposed to an expected metric of total SIMs. This could imply we have fewer SIMs, and reported SIMs than we do. In this case the chart now only shows SIMs reported to the *Irish-DPC*. The expected metric (all SIMs required to be reported to regulators) is a higher number reported (200% higher in the last bars). Please clarify as/if appropriate.

80-90% of UPL projects are now within SDLC (flyway) compliance

This is good and should be celebrated. However this could mislead as it lacks larger context. The majority of projects at Twitter are not in the UPL (RTB and local). We run the risk of confusing the board members that we are 80-90% done when other estimates are showing we are less than 20% done here. If appropriate it may be important to also remind them that the SDLC and Flyway are currently stubs/skeletons in

many ways. Good roll out through engineering. Just be careful of what message may be received

6% of our incidents are access control related



The graph tags access control at 6%. Internally we have referred to access control as more than 75% of our incident roots (sensitive data exposure internally (36.7%), externally (20%), and security misconfiguration (23.3%), are access control related). We need to be clear on this as we message that access control is a systemic issue at Twitter, we know it is one of the greatest risks in our ability to secure the environment, and that this is a key focus in regulator investigations and interest.

Server patch levels

It is table stakes to report the state of hygiene of our systems, both endpoints (clients) and servers (production). InfoSec reports have not done this to my knowledge and this report does not include this information either. 60% of our systems in production are not at the correct patch level. Many of these are unsupported (legacy) operating systems incapable of actually meeting certain security requirements. This is a potential PR issue in addition to the security risk. I am not saying this must be brought up at this Risk Committee, but this is something we should ensure is not continued to be omitted. Not mentioning this topic can lead one to infer that it is a solved issue.

Access to Production Servers

While we should celebrate the reduction of two small, but important, groups of access control. We need to make sure we are not showing data graphs that do not match to actual data (or that show different stories than the actual data).

The charts being shown do not match the data I have seen.

a. The direct access chart showing the reductions does not match the charts I have seen in Confidence-Staff meetings.
b. The Direct access to production systems graph seems incorrect. Our total exposure of accounts with direct access to production systems has actually increased
    i. Dec 2020 46% of employes (2,763 out of 5917)
    ii. Dec 2021 51% of employees (3,995 out of 7714)

We need to make sure the wins are recognized but that they are not presented in isolation, potentially implying they are representative of progress against the larger risk issue. The larger population of access to production has actually increased and I don't see that mentioned or captured in the graphic. Again, be mindful of what expectations and understandings are being set.

My other comments from our meetings stand on other, similar, topics in the deck.

Thanks for your attention to these items.

On Mon, Jan 17, 2022 at 8:39 PM Marianne Fogarty [redacted] wrote:
> Privileged and Confidential
>
> Mudge,
>
> [redacted]
>
> Thank you.
>
> Best regards,
>
> Marianne
>
> On Tue, Jan 11, 2022 at 4:36 PM Marianne Fogarty [redacted] wrote:
> > Privileged and Confidential
> >
> > Mudge,
> >
> > Thank you for your time today, it is greatly appreciated and I am sure it will help us conclude our investigation quickly.
> >
> > I have one follow-up request that ties in with the latter portion of our discussion - [redacted]
> >
> > I'm happy to answer any questions you may have.
> >
> > Best,
> >
> > Marianne
> >
> > On Tue, Jan 11, 2022 at 1:36 PM Marianne Fogarty [redacted] wrote:
> > > Thanks Mudge.
> > > We can chat now - be on in just a moment.
> > >
> > > On Tue, Jan 11, 2022 at 1:29 PM Peiter "Mudge" Zatko [redacted] wrote:
> > > > Or I can chat now (1:05pm pacific). I'll set an invite and be there just in case you can join.
> > > >
> > > > On Tue, Jan 11, 2022 at 4:26 PM Peiter "Mudge" Zatko [redacted] wrote:
> > > > > Thank you for your quick attention to this matter.
> > > > >
> > > > > I can be available tomorrow from 12-1 Pacific time.

If that doesn't work for you please let me know and I can see what meetings I can cancel as this is a priority for me.

kindest,

Mudge Zatko

On Tue, Jan 11, 2022 at 2:01 PM Marianne Fogarty [redacted] wrote:

> Mudge,
>
> Twitter initiated an investigation into the concerns you raised in your January 4 email regarding the substance of matters presented to the Risk Committee.
>
> In connection with this, we'd like to interview you to be sure we understand the full nature of your concerns and can follow up appropriately. Given the importance of the matter and the significance of the allegations, we hope that we can speak with you later today or tomorrow. Rebecca Falk, who leads the Investigations function on my team, will assist in the interview.
>
> Please let me know your availability and we will do our best to accommodate. The only time that I am unavailable is 7-10am pst tomorrow (Wednesday).
>
> Thank you.
>
> Marianne
>
> --
>
> 
>
> **Marianne Fogarty** | VP, Chief Compliance Officer
> Registered In-House Counsel
> Pronouns (She/Her) | San Francisco, CA
> Follow me [redacted]

--

Marianne Fogarty | VP, Chief Compliance Officer
Registered In-House Counsel
Pronouns (She/Her) | San Francisco, CA
Follow me [redacted]

--

Marianne Fogarty | VP, Chief Compliance Officer
Registered In-House Counsel
Pronouns (She/Her) | San Francisco, CA
Follow me [redacted]

--

Marianne Fogarty | VP, Chief Compliance Officer
Registered In-House Counsel
Pronouns (She/Her) | San Francisco, CA
Follow me [redacted]