Peiter "Mudge" Zatko [redacted]

# InfoSec Risk Committee Presentation Items to be aware of

4 messages

**Peiter "Mudge" Zatko** [redacted] Wed, Dec 15, 2021 at 2:49 PM
To: [redacted]
Cc: [redacted]

[redacted] and [redacted]

Tomorrow is the Risk Committee and I want to wish you luck!

I want to reiterate items that we have covered at meetings for this risk committee (and others).

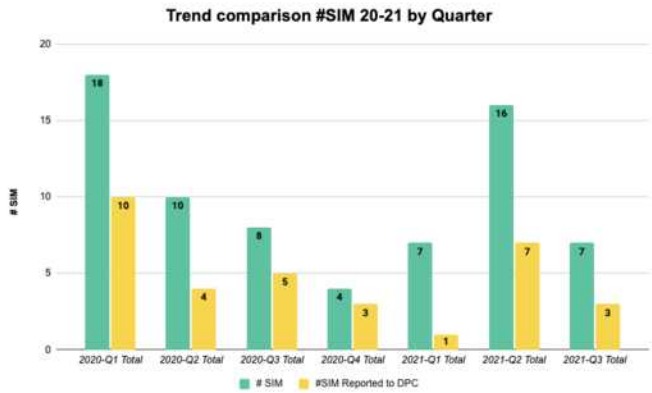
As you know, it is critical we do not misdirect or mislead the board members through omission, or framing, of specific data. You ([redacted]) no doubt remember their surprise when they learned the difference between what they had been briefed in meetings prior to your arrival versus what they learned the actual environment was. Wow! We need to avoid putting them in that situation again.

Here are some specific areas in the slides that I think could send the wrong messages. I've brought these up before, so they will likely be familiar. I am citing specifics in this message for clarity in communications here, not that I am suggesting you overwhelm the committee members in specific detail.

---

*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.



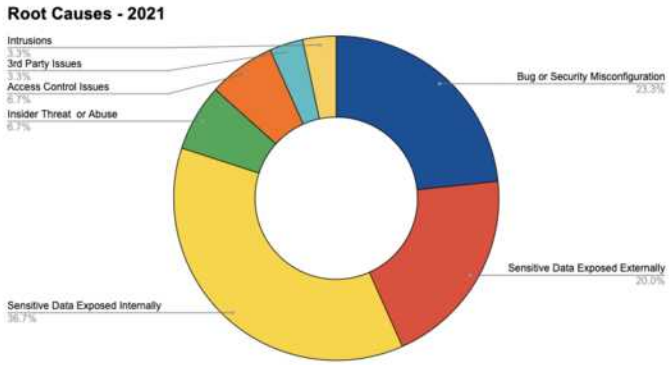

The above graph is now using a subset metric of SIMS as opposed to an expected metric of total SIMs. This could imply we have fewer SIMs, and reported SIMs than we do. In this case the chart now only shows SIMs reported to the *Irish-*

*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.

---

**Peiter "Mudge" Zatko** [redacted] Wed, Dec 15, 2021 at 3:02 PM
To: Parag Agrawal [redacted]
Bcc: Kathleen Pacini [redacted], Peiter Zatko [redacted]

Parag and Dalana,

The other day, in our conversation, you suggested I forward [redacted] 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
[Quoted text hidden]

---

[redacted] Wed, Dec 15, 2021 at 6:02 PM
To: Peiter Mudge Zatko
Cc: [redacted]

Mudge,

It's unfortunate that you've had this content for review for the past week and a half and waited until after the content was already submitted to the risk committee to provide feedback and less than 24 hours before the committee meeting. This isn't enough time to adjust content and points of discussion. I therefore will not be adjusting content, but can take your feedback into consideration for future meetings.

Now, to address your feedback. Most importantly, I have never misled or misreported data to the board or risk committee. If anything, my voice has been muted, and I've been excluded from these meetings. Furthermore, none of the content provided is a misrepresentation of data, nor is it intended to mislead. The data points explicitly call out what they measure, and the context provided during the discussion is intended to add color and context (as we elaborated on during the dry-run which you were part of [but perhaps you were disengaged during that part of the dialog]). On your first point for example, the message is one of visibility and ability to measure. It's a statement suggesting marked improvements in our visibility and ability to measure many things, including those associated with the one point you bring up, auto-update enabled. As you know, auto-update being enabled is a tool to ensure timely update of systems, but is not in and of itself a measure of risk (systems without auto-update enabled, for example, can also be up-to-date, as a generic example). This translates to being one of many signals that help us understand the state of endpoint health. This however is not in scope for what this metric is intended to portray, which is one of capability and completeness **visibility**. I can expand on this point with the risk committee and share objectives that we have in-flight to address a broader endpoint metric program that will help us get to more granular measurements without complicating the discussion with the risk committee by getting too tactical (which we have many times received feedback on being). Also, can you provide more detail as to where you are getting data from? If it is our dashboards, it may

On your point around SIM reporting, I'm not sure what you're trying to portray here, or what you believe is misleading or inaccurate. Can you clarify?

On point 3, what we're suggesting, accurately, is, of the UPL items, or in other words, the most important cross-functional efforts, a MAJORITY, are in the flyway v2 process. We intend to add color that this is a very important but first step toward improving the processes across all efforts, but as with all things complicated, we start with the most important things (which UPL suggests).

On your next point around access control related incidents. The graph here is suggestive of the "primary root cause" as identified by our retro process. It doesn't necessarily suggest that there aren't secondary or tertiary (or more) reasons for them. If we went into that level of detail, we would risk devolving the conversation into one about semantics and would draw away from the primary point, and would once again move us toward being too tactical, which we have been called out for in the past on numerous occasions. I will of course also verbally add (as I did during our dry run, see comment above) that thematically access control is one of great importance, which is why we have a massive cross-functionally supported effort on access reduction which has its own section in the presentation (which accurately represents the importance of the topic, calling it out as one of our critical endeavors in the coming months).

On server patch levels, I'm not even sure what to say here Mudge. We have discussed this one to death. Not only have I conveyed this to the risk committee, in detail, but we've identified this as a critical path item for us from a visibility and measurement standpoint, which we are actively scoping as an objective as part of our endpoint metrics strategy. This of course requires involvement of (and commitment from) peer organizations in your charter, which we are working alongside to address this. I will of course add more color to this during the discussion with the risk committee, but your points here don't resonate as it's been a consistent point during these sessions.

On the final point around access, my first point is one I'll redirect to you above. We have already identified this as a critical goal for the organization, and the organization around this item cross-functionally is commensurate with this. Second, I feel you're being disingenuous in your statement around two small wins. I would characterize this as several big wins, starting with significant reduction in the number of users with broad access to all of production (if you remember, the topic we began with in this journey), by >66%. This is accompanied by several other wins associated with IPMI and

SUDO access reduction, which are significant in reducing overall risk. If the point you want to convey is, "there is more work to do," rest assured, it's already part of the talk track for the risk meeting (as conveyed, once again during our dry run session, see comments above).

Now that I've addressed your comments, there is a point I don't want to neglect in surfacing. I already made the point that giving feedback in this form, last minute ahead of such an important meeting is unfortunate, I'd like to take this one step further. Doing so does not set me up for success, is not indicative of your support for this organization or myself, and is written in "gotchya" framing. This is exacerbated by the fact that you've copied a member of my team, which is not in the spirit of creating a collaborative or supportive environment. I've provided this feedback to you on countless occasions, but it is worth bringing up once again.

Regards,
[redacted]
[Quoted text hidden]

---

**Peiter "Mudge" Zatko** [redacted] Wed, Dec 15, 2021 at 10:26 PM
To: [redacted]
Cc: [redacted]
Bcc: Kathleen Pacini [redacted]

I'm confused and concerned by the tone and content of your response. I will (re)read your email in greater detail later and we will address.

I agree that if this had been new information it would be inappropriate at this juncture, but it is not. We have covered each of these items on numerous occasions. This includes in meeting review of this specific deck (with Privacy and HRBP present). None of this should be news.

In the first email on this topic today, to both Privacy and InfoSec teams, I shared that I would provide comments and specific observations to help narratives in tomorrow's meeting. Rather than including [redacted] and Damien, out of deference to you, I narrowed the distribution of InfoSec comments to you and [redacted] Seeing as you included [redacted] in every stage of this effort I assumed you would want her to be included in the feedback.

The InfoSec presentation does not include a written narrative so while I have requested modifications, clarifications, and change on these data points and topics in the past, here I am not requesting a rewrite. I am suggesting ways to help the narrative and items to be mindful of in Q&A.

Much like in the example provided in the email, where the board had become misaligned with what Parag and Mike had been briefing on SDLC (effort vice progress from 2020 and before), we always run the risk of mis-setting understandings and expectations when we brief.

I am looking forward to the meeting. We have a lot to cover on very important topics.

Regards,

Mudge Zatko
[Quoted text hidden]