STOPWATCH Q1 or ~~Q2~~ board only (only allowed my voice)

You have who I am, my mandate, what you can expect to see from me over a defined time period…

Before I get into a bunch of data points, I want you to understand another purpose of this talk: allowing you to have context for other documents and things you hear. For instance: FTC risks. If we have an incident or breach after the settlement we have to report it to the FTC. If it is similar in nature, e.g. access-control, then the FTC is going to want to dig in and find out if we have a systemic problem here.

Boy, I sure hope that doesn't happen.

In 2020, we had 40 incidents (70+ were access control related) and 20 breaches (90% access control). That's more than 10 incidents a quarter and more than a breach a month. with this Data Damien and I came up with the wording

Then context changes to "we are almost guaranteed to have an access control related breach and the problem is systemic". We should expect this situation with the FTC to happen before we can address it. you keyed on

Let's get into it: - high enough level but with the first stats / data based view

---

When I come into a company the first thing I do is to interview across a range of people.

I've interviewed ~40 Tweeps (executive team, managers, ICs, across the company).

1 Question is always: What is it that Twitter does better than anyone else?

We are great in a crisis!

Seems good, but is it? People or organizations that *only* excel in a crisis…

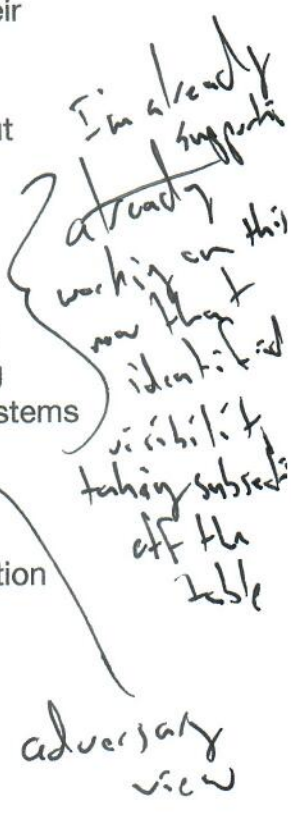
- Do not build strategically to avoid them
- Begin to seek them out (subconsciously or consciously)
    - Have confidence in their ability to execute and dig out of a crisis
    - A crisis can provide structure that is lacking in other efforts
        - Target metrics
        - scope
        - Priority
        - Time frame

        - Milestones
        - Reward and recognition structures

When I see this I begin digging for indicators that we may subconsciously seek crises or neglect to build strategically to avoid them:

- Do we Hop from crisis to crisis? (yes):
    - 2020:
        - More than 10 Incidents a quarter and more than 1 breach a month
        - Many of these were very similar in nature
            - Some groundhog-day happening
            - 70% of incidents (28 of 40) access control
            - 90% of breaches (18 of 20) access control
- Hygiene (living with poor hygiene is another indicator)
    - Updated systems and software in our data centers?
        - 53% (186,372) data center servers are running non-compliant kernels
        - 12% (41,443) non-compliant operating systems
    - In general Poor visibility (difficult to clean things up if you don't know what/where things are)
        - Estimated 10% visibility across systems, services, clients (laptops, phones)
            - No centralized logging across engineering
    - Lack of positive control (looked at client side here)
        - No MDM on Tweep phones
            - These are personal devices that access Twitter sensitive information and used for authentication to Twitter networks
        - Lack positive control over software Tweeps can install on their work systems

- Access Control - this has been raised to the board before (perhaps without stats)
    - Engineers build, test, and deploy directly in *Production (with live Customer data)*
    - Systemic challenges in Access control
        - 43% (2662) of FTEs have access to our production systems (makes sense since we don't have a development or staging environment and engineers work directly with production systems and data - but is still alarming)
        - 10% (>1000) FTEs have access to Advertiser information
            - Campaign data
            - (likely) Billing (bank and routing) and account information



Are we performing manual processes, repeatedly, instead of automating? Tactically instead of strategically? Yes

- Site ops demonstrated a ~10+ step investigation (repeated each time)
  - Action taken was cheap to adversary and expensive for us
    - Ban a fake account (opponent spun up new ones more cheaply than this banning process)
- Twitter Service handled 100% of 1st person safety reports (yay! - Sept 2020 though Feb 2021)
  - >80% of the responses (114,641 out of 133,812) stated "Not a violation"
    - Does this take the Customer perception into account?
      - Does this message to the customer they should change how they engage in public conversation?
    - Does this take the antagonist's view into account?
      - Does this message: You've found an acceptable/approved lane for harassment. Good to go.
    - Can we respond in ways that discourage adversaries and do not imply that the reporting party should self censor?

More manual v automated examples and also living with extra risk because not understanding the threat…

- In 2020 496 FTEs and 3,174 Contractors were de-badged (terminated)
  - There were a total of 1,477 days (FTEs) and 10,357 days (Contractors) where we knew the person was leaving but they still had full internal access to systems and data.
    - Any evaluation of inappropriate access patterns (insider threat, competitive intelligence, etc.) was not easily accomplished - it would have been manual
      - Poor visibility
      - Poor positive control
      - Poor logging
      - Remember the exposure (i.e. "so what")?
        - 43% of FTEs have direct access to production
          - Full copies of source code
        - 30% of FTEs have access to sensitive Advertiser information
        - Unknown amount have access to our finance data
        - "Leaking is the norm" - I have been told this repeatedly

teaching

With all of the above helping to provide context around our environment, and some of what is slowing us down or making it difficult to execute on our strategy and operations, let me share the existential threat that surprised me.

- We have [redacted] data centers
  - This is not publicly known
  - Jan 6 - 22 there were threats against our data centers
    - Threat matrix of effect:
      - [redacted] data centers physically destroyed
        - Twitter unable to do business - full stop (not surprising)
      - [redacted] goes down (hard or soft)
        - Twitter continues to run out of [redacted]
      - [redacted] goes down (hard or soft)
        - Twitter operates, but impaired - and more impaired as time goes on
      - [redacted] data centers gracefully go down and come back up
        - We don't know - best guess is weeks to months to bring the service back online
        - We can't boot(?)
        - Known unknown we really should know
    - We had to consider these scenarios from the 6th onward
    - More likely when we removed Trump's account than when suspended
    - Insider threat during this period
      - Think about the above access control, hygiene, visibility
  - SVR (Russian Foreign Intelligence Service) and DPRK (Reconnaissance General Bureau)
    - Both engage in ransomming organizations
    - SVR supports disinformation operations
    - I can think of ways to move inside our systems and networks to get to our DCs and work towards rebooting - they can too (don't fix the specific symptoms - cure the disease)
    - Both organizations would find this ransom an extremely valuable lever to keep (use?)
  - We now know to understand this and quantify it (make it a known known)
  - We are standing up a new datacenter - great opportunity
  - Partly cloudy is a ways off for continuity of operations
    - But we can about this