

SIM STATS

terrifying ¹/₂ job work

~~an~~ we're not learning (main delay)
negative

SIN 89 not pulled to
rest of org
Election Squad, name!
TWS Starts

...

There are other uncovered

crises as well

(we were really lucky in
the repetitive war effort)

CDAP

can't cold but

no inhibitions

direct to

read

make

WCL - mobile

██████ : ██████ 5:0

operate the

non-compliant

53% 186,372 from

12% 41,443 OS

231,347

9/6/2020 - 2/6/2021

45 prod
34% ads

FTE
496

Contract
3174

Total
3670

137	609
+ 37.2(74)	+ 224.2(448)
+ 22.3(66)	+ 32.3(64)
+ 300.4(1200)	+ 2309.4(9236)
<hr/> 1477	<hr/> 10,357

let's look @ this
from ^{just a} security point of
view

There's an existential
rich

based on my experience
reason I've been brought in
if there's an existential
rich

~~let's assume we handle the
existential rich.~~

~~The~~

The what is existential rich

Then how we operate as
a company

low - 2% -
is under performing

288 ~~292~~

294

• Mission Statement

~~Verifiability~~

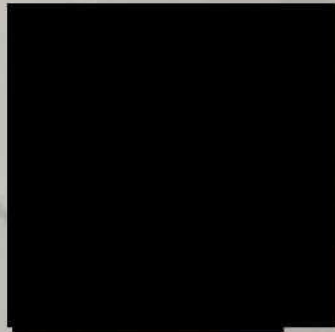
• 3 year Plan - short
version
and

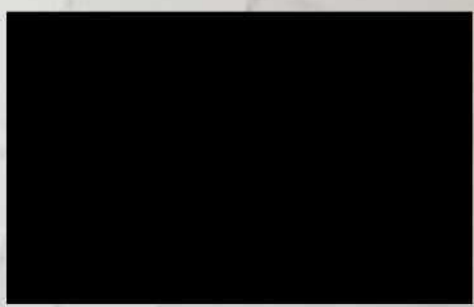
Paragraph showing
how we get there

Existential Threat -

(not

Jan 6-20th we received reports of ~~people disclosing the location of our SMF Data~~ people encouraging active disruption of our data centers.

We have  data centers and ~~the~~ ^{4ever} possible effects ~~outcomes~~ from disruptive

 Data center destroyed, we cease to exist (not surprising) - ~~in a few years~~ ~~time~~

Ishe

India

- ↳ Disinfo about NIT
- ↳ Critical of Modi

India compromised NIT

employees (NSO group)

mobile device spyware

(covering kurmure)

very little cooperation
targeting

Reporters

New Indian Nationals didn't

go further than harassing

online

Indian nationals targeted for
consumption

Paray MM Top of Mind

Splunk

~~Adm~~

Failed logins - 1.53k

per day - (550 or
low the other day)

MESOS

Reduction Accur -

STM - 144

Cochit

Deactivates an
account - after 30 days
no longer publicly ~~is~~
available -

Tweets, Emails, phone #

No DMs, IP logs,

Device level data
in logs

CNSL - is a beast on
data deletion.

- updated privacy policy 2-3 years ago
- some mitigation - daily, weekly, quarterly

DRP asks question -
we have to test if we
cannot meet our deletion
obligations

GDPR - via

FTC - via

Hacker in LEO request
when we said we
couldn't

Inability to meet our
data deletion obligations

30+ apps -

ITC - Service Cloud

Health Cloud built 30+ tools
ruby, scala, react.

Lightning web components.

Lightning design system
for react.

Session ID leaking
externally - anyone with
this could access
salesforce

Introduce myself
have each other in our
rolodexes

Tues -

~~Strong inter~~

Qc side - J T-S

- Building productive
Bridges

Shift agents from
regular work to appeal
work

Suspensions should have
a classon

Threats are suspended
was that were not
told why they were
suspended —

TWS: Corp Sec

many teams have ability
to suspend

Books suspended (we don't
track bot,)

all suspensions need to
have a reason

(fixing appeal in health kn)
We aren't tracking suspensions

TWS
Inventory all the bots
reviewed accuracy
Reason for all suspension
expulsions

Move Agents from
content moderation
to appeals

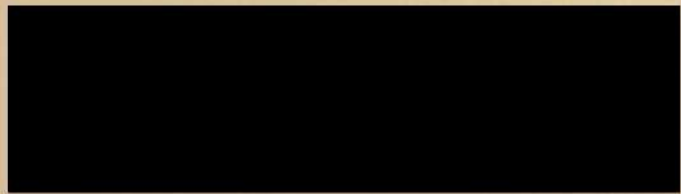
TWS moving more and more
towards Salesforce.

move more and more towards
Salesforce

June 8, 2021

RHS

Health IIEA Contract



JTBD

Make our policies
straightforward and scalable
in practice (on the platform)
and disrupt and deter
platform manipulation

Ensure the Integrity of the
platform at scale ~~and~~ ^{to}

Disrupting and deterring
platform manipulation

Disruption of malicious
parties on our platform
becomes a strategy.

Panay Ithun

Global India → future of
Engineering
presence

to 1st.

Exceptional Product

Privacy

IDN

Buy vs Build.

Inclusion: Diversity Inc/US

50k targets

65+ business execs

~~profile viewer~~

agent tool for periscope

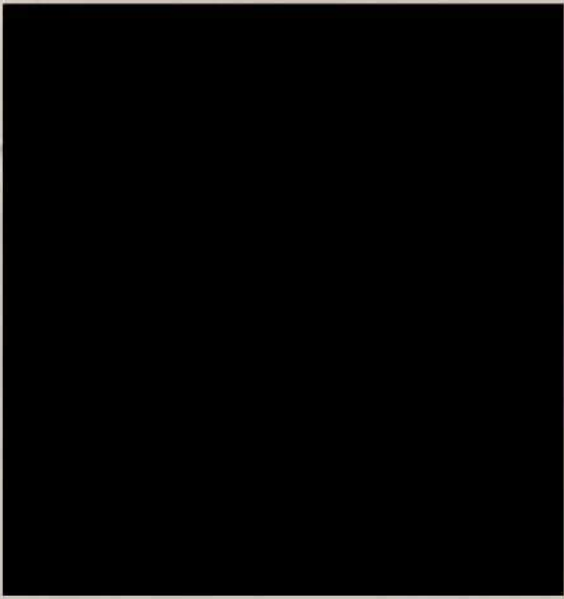
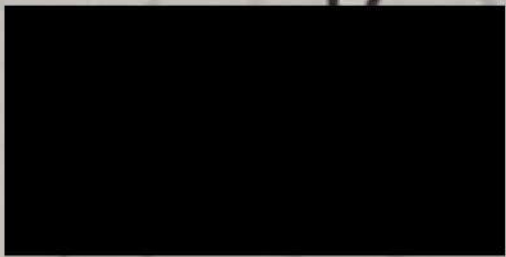
→ went to Slack

spaces
→ old profile viewer

never got the fixing that
other tools got from SIM-89

Anyone w/ access to
periscope, admin bypasses
all security

OIG Report

Ned /  - Nigeria / China
Turkey e-mail
to  etc.

July 19, 2021

✓ A P+S

✓ A3 Verification

✓ 42 Staff Doc

C3

[REDACTED]

✓ All NFO Data

C2

[REDACTED]

Follow up

[REDACTED]

C1

[REDACTED]

[REDACTED]

All hands review

[REDACTED]

Follow on w/ M-dye on

[REDACTED]

A4

Jack 360 (in Staff Doc)

gov/Healthy Conversation

Inclusion: Diversity Inc/hi

50k targets

65+ business execs

~~public viewer~~

agent tool for periscope

→ went to Slack

spaces

→ old public-viewer

never got the fixing that
other tools got from SIM-89

Anyone w/ access to
periscope admin bypasses
all security

that can I do to
support our understanding
of risk against our core
mission -

Need systemic, repeatable
solution - this is happening
elsewhere.

Ultimate systemic risk to
Twitter

Taking perspective of the threat
(adversary) - how I think about
these problems.

Essential Problem:
India - this is about radio
first.

Our ability to satisfy
the mission.

About Risk

About India.

What is the hard evidence
that shows the problem
(get out of qualitative
narrative \rightarrow go quantitative)

Bunch of facts - container
of evidence.

(2) Don't us to think about
how we will handle it
when I find evidence
of India in our
systems.

Sunlight - shock backed
operations. Indian Army

Protect our users

(1)

Separate

July 27, 2021

✓ A1 PHS

✓ A5 [REDACTED] Promo Pack

✓ A6 Quarterly Review input

✓ A3 Staff Dec Input

✓ A4 #Conf Doc.

✓ A2 Alarms

✓ A7 Russ Comm

B1 Slach

~~Radio Doc.~~

B2 Nigeria Dec

B3 Async Reviews

Aug 2, 2021

✓ A1 P45

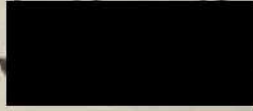
B2 Kikla Report

A3 Conf Obj to Staff/Duty

✓ A2 Staff Dos

C1 Review Pkty

B1 Answer any Agency Q2

A4 India (3 things)  (includes evidence)

45 SIM-144

B3 Rich Mod.

Rabdo Myaliri

SI - #Conf.

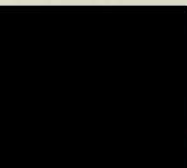
CP.

Grievance Reports - India - going to
CP, CP Kicks to SI, drawing
SI.

R,

TOS review w/in TOS.

We have been sitting on
an Indian Information Operations
Influence Op for over a year.

 - India SIM-144
Exceptional Access to Production
Client flow

India -
need to have
a conversation
inside bit it
at reading

cookies
privacy - Privacy

India/Countries - [redacted]

we don't have
options in India

we don't have
any options
no bridge - risk is
not mitigated even if
can't enter in our
fence.

• Can't mitigate the insider
threat - concern if ~~we~~

~~keep hiring~~ with PTE
in sensitive positions in

India

most of you have a lot of sensitive
our roles positions

Access - Production
Laptop Fleet

P Admin - has unique. few
access to all accounts,
(potus - etc.)

Spaces Dev team (Engineering)

want to use for debugging
(not the good tool to use
for this)

[redacted] Cy

port over some support capital. 2 is

{ Cookies Admin (Access to Production
Privacy IAM Access (h.)
India/Countries } Laptop Fleet.

Access - Case Volume
5:00 - [redacted] helping enough?
Consumer Experience

[redacted]
(?) Account Signing Best
depreciation

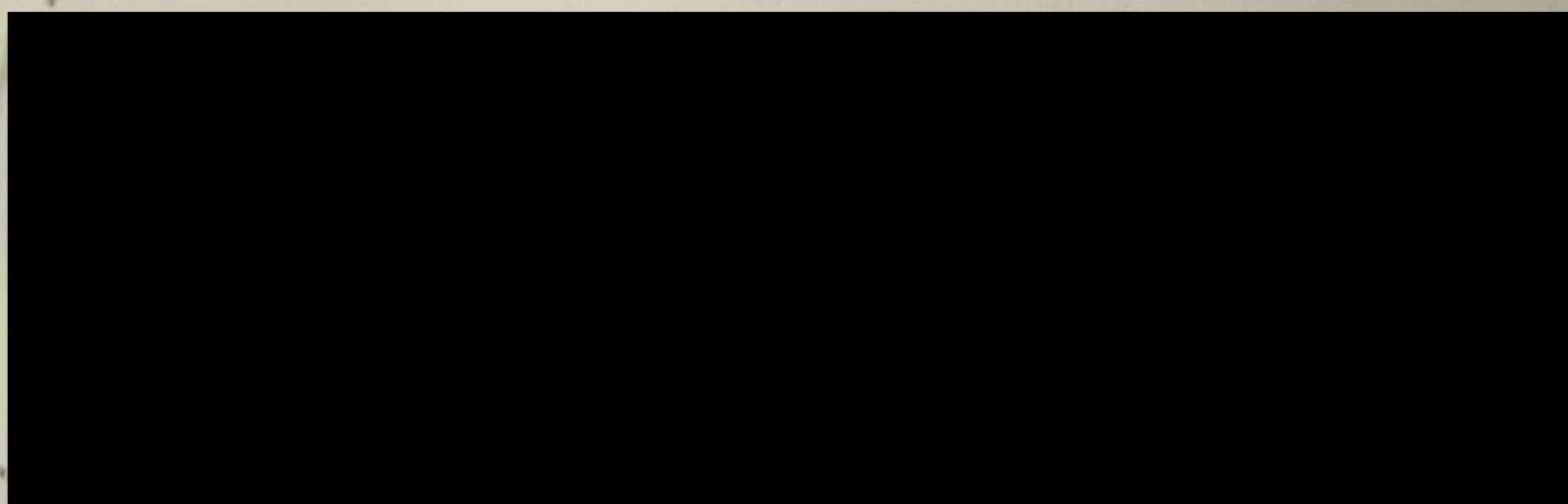
STM - 144

9/15/2019 sept
added an council
after not having
one

~~not needed.~~

May 12/21
Download your tax form
Data
ZFA

12th floor 17th side



Cognizant
Tach U1

Best retention rates for Agents

unpaid security
and privacy
bills

reaching in a crisis

content
moderation
TS - directly
engaging

144 Do-

(contract

Doc of
responsibility

writing up
for X

reading up.
for i

Ads cookies are NOT essential cookies,
multi-usr cookies pulled apart.
experiments for

A mach up

delete some cookies

Recapich → Recapich.net
(separate from CCOG)

SJM-50/52 } long term
SJM 90 } remediations
ident. find not but near
done.

The pack of wolves that
have been roaming in the west
are now @ our front door.

told are
3 year eye catcher problem
1 year backdoor agreed
to Snt no backed up/
prioritized.

now here -

5 breaches under
investigation

2018, South DPC

Inquiry report "Findings of
fact -
systemic failures in how
we launch public attacks.

Paray / MM Top of Mind

plunk

~~Adm~~

Failed logins - 1.53k

per day - (550 or
low the other day)

MESOS

Reduction Accur -

STM - 144

Cochin

Deactivates an
account - after 30 days
no longer publicly ~~is~~
available -

Twitter, Email, Phone #;

NO DMs, IP logs,

Device level data
in logs

CNSL - is a beast on
data deletion.

- updated privacy policy 2-3 years ago
- some mitigation - daily, weekly, quarterly
- [redacted]

OPC asks question -
we have to test if we
cannot meet our deletion
obligations

EDR - via

FTC - via

Hacker in LEO report
when we said we
couldn't

Inability to meet our
data deletion obligations

QC - week of sept 22nd

Muller et al revealed
some of the errors -

HRBP -

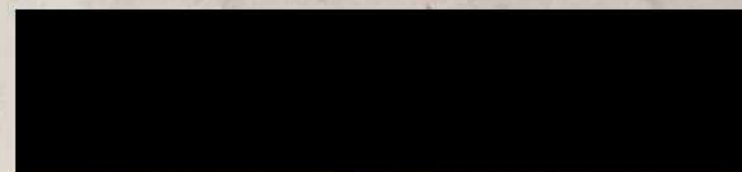
Discovered in connection w
Mueller investigation 2017
realized we had

Cold Storage - actually had
data even though it's hard
to get to.

Re-opened subpoenas and
said we made mistake - how it
is (from DB; we didn't know w
had)

removing
Deficit ; Future
Budget

Cashman -



Updated Privacy Policy

* [REDACTED] said there;
not a long term strategy.

(Want to put it together
with me? or would you
like me to give you
specific targets and
end goals, to build it
around?)

* Part 3 board / [REDACTED]


Comment - 2017 →

Data deletion / Retention
has been The TOP risk
highlighted

Teaching effort not
impact / effect

Execution Review to
Staff - added column
"Are we more secure at
completion" → No
review Work →
"all Green" ??? same
issue


Twitter tracks effort on
projects and impact to Environment

Scrapping (6% of datasets -
but  told big
progress for 3 years and
projects almost done

SDLC - Board vs reality

Both 7/19 - ~~helpless~~ ^{helpless} : 90-100%
disaster ~~helpless~~ 20-25%

Upcoming Regulatory -

Merging ( prep)


Data Deletion

SIM 144

Lechies

FTC

why didn't they
see any of this
instead, reported.
AOK

Learning - changing cultural
view of activities does
NOT demoralize Tweeps -
Staff just ~~think~~ ^{think} it
will. Tweep afraid of change
but embrace much of it go
(e.g.  - Privacy, ~~peace~~)

India and future Companies of ~~Microsoft~~ ^{Microsoft}
feedback

Flash Privacy controls

MAP data to China

customer consent

FTC ~~compliance~~ ^{Consent}

(Unencrypted
Encrypted links in our

data centers)

Election interference

Data tapping

Access controls

Insider Threat

Above all seem equally important

They aren't - if you take any

of them and do it in a

vacuum - ignore the

others. That's what we've been

doing.

How we tackle the problem
currently \Rightarrow headcount
why?

unable to prioritize projects
(no efforts get stopped,
unable to predict duration
to transfer headcount, etc.)

To do

The danger of locally optimizing,
tactically, w/o global goals &
milestones:

all risks are equal,

all risks are "catastrophic"

w/o global prioritization

must defend equally against
everything.

example:

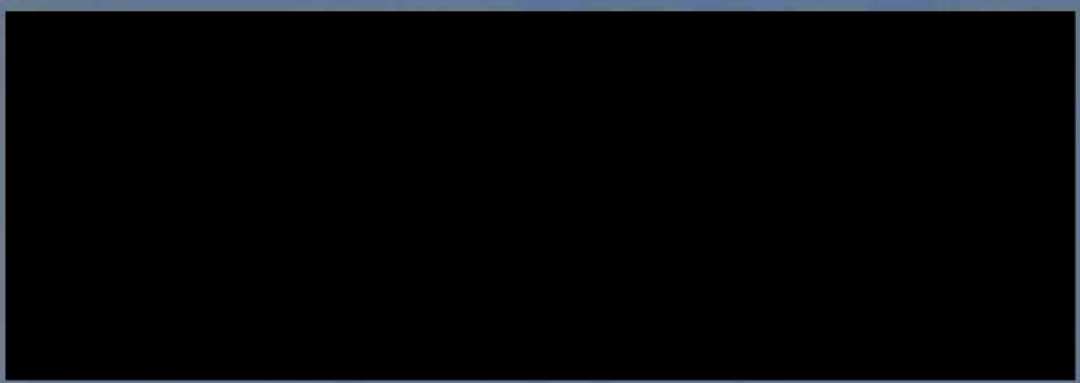
Sect. 230

need

(3)

- 1 Transparency around content mod.
- 2 appeals (rebuttal)
- 3 algorithmic choice

Bob Zoellich -



removing Trump
removed 72% of ~~misinfo~~ "misinfo"

2 digital ~~ack~~ moving
forward in EU (?)

• Treatment of Foreign Leaders

57:00 outline write to •;

Incidents

Stats

Intro

you should be alarmed
(it doesn't need to
be this bad)

- We're great in crisis -
we drop the ball learning

Eg. SIM 89 learned in 1
place but didn't

repeating tactical lifts
Rep: failure
Prod - huge over provisioning

- other crises waiting to happen
COAB visibility

other areas ~~not~~ ~~Security~~
SMP/ATC

- Setting of Confidence to address
↳ where are there on the web
web is a ~~rich~~ rich to
company (journal)

Grounding day - Crisis?

Missing the Basics

SIM Stats 2020

lacking ownership of
systems, data,

not following processes and
not owning configuration

not taking lessons learned

Feb the Grounding day
why?

not taking lessons learned

Ex SIM Stats

Ex offboarding

Ex SIM 89 for special
restriction but not
for rest of company

(broad access - taken
with it to figure out what
they actually need/used)

Action: Threads v3

~~12 m~~

12 m

84k RPO

.007

7 tenths of 1 percent

1.7% of our

spam bounces are
appealed.

~~37% of~~

12M suspension - 11M
215k Appeals cases
84k ropo appeals

70% of 215k appeals
are ROP

Access Appeals —
Team

Smite & Bohner
E-mail

No central live
dashboard for
Bohr

May 4, 2021
P+J

Conf Obj -

Short Term: Long Term

Alarms

Thread,
ITCA

ToP - Own: Drive

MM: Mady Cap: BT - (corporate)
FIC - SIM 122

Extended Leadership (Emas)

on [redacted] - deliverable

Threat Model w/ options

{ June old Boot test

{ in PD X !!! - How long
Down (lowest possible)

Confidence
ToR

~~T: S~~ pr -> Confidence

Ownership is important -
but where is the unified
basic process enforcement?
Are unit tests optional?

ALL -

Figure 5001

{ SIM - 122 easy figure
regulatory impact
for 10 w/ FIC negotiation pending

May 18, 2021

A1 P+S
B2 [redacted] feedback

A3 Alarms

A2 Actions

A4 Board Async Q's

B1 Interview

B3 [redacted] → [redacted]

Board Voice track

Stack

[redacted] [redacted] [redacted] ~~###~~

~~Letter~~ strategy

Workday Request - [redacted]

Lashmi's Doc

[redacted] - not way to let me know about

50% of spacer broadcasts had wrong language detected (in English queue)

15 min / new staff summit

Confidence Objective
hampred by TWS
extract Nicole
roch
hard pla
2 pillar land
to be m

IT - need to uplevel

[redacted] not to

executing ~~###~~
Privacy (FTC)
looking to be real

④ Confidence - new org
just getting underway

currently [redacted], Privacy, Cybersec,
TUS, IT

safety, integrity, risk → privacy
systems / services /
customers / employees
manage: anticipate people who may
do harm to twitter or who
twitter to do harm to others.

The more we can clear these
risks out of the way
the more confidence twitter
we have that
can execute our mission.

(2) ~~still early~~ nascent org

as such you'll see
some changes

Today you'll hear about
[REDACTED] and Privacy from

our

and our CPO (Damien Kieran)
you'll also meet our newest

member - [REDACTED] - our

Distinguished Privacy Lead.

Later I'll be sitting in on
Health as TWS is in confidence
TWS is Safety @ Scale for
our customers. (searor)

(4)

current

good:

3) In BCP and DR you are going to hear about improvements against accidental disruptions -

~~anything accidentally~~ can be anything that can be caused by accident can also be made to happen (intent)

~~For~~ For this section I'd like to draw your attention to ~~exceptional~~ ~~prior~~ systemic access control issues and

④ the significance of our
FTC obligation —

~~This is the first domino —~~
~~quite likely~~

~~This isn't it — this when~~

~~the~~ are

Tyidher i been

~~we~~ were carrying a lot of
technical debt ~~before~~ ~~and~~
security/privacy for a while

Came on board

we will likely not get
ahead of this before
another incident.

(5) we need to make significant
progress to demonstrate
we are taking this seriously
when the other stock drops

~~This will slow the company
down~~ Paying off this
long overdue debt will
slow the company down.

We will work to minimize
this impact.

Access control -

Flash - install during
presentation

Robert Zeillich

Clean production is
is 3x as fast

Patrick Pichette

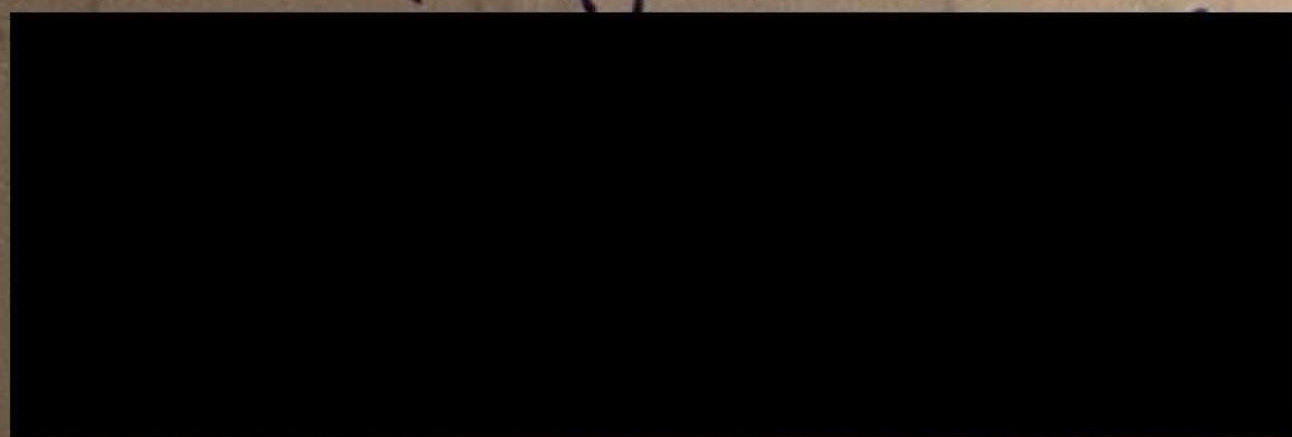
readiness -

Indic
Extricating Manish
RAT - intercept ^{extradition} if
informed via e-mail intercept

Put them into a
quandary as to whether
they should act upon
intel.

Vol, Del, TWS, Confidence

~~Over~~ Health Tools —



ITCA

• Take ~~any~~ no action in
verified acc
w/o human

2 items -
escalate quickly
info sec on intrusion
panels

- Madge - [REDACTED] / DACIN(3)
Commerce - Export Control ✓

a) compliance doesn't know
what controlled technologies
are, specifically and
where they may live
(Lit, Slack, G Suite, etc.)

b) ~~would~~ need to figure out
access control solutions
Rules - Confidential / Compliance,
Legal)

find perimeter ~~for~~ ads -
scrub there.

log - lacking discipline
global issue

Irish DPC is under huge
pressure to do stuff

Banner is a gimme.

came up with enough information
to say it's not wrong.

Detangle cookies

Trash DIC - web site.

sent us a letter -

www.tn.thr. hey what are you doing
w/ all of your cookies.

want us to tell them

cookies, trackers,

local storage

what we are doing w/
them -

Need to correspond to
reasonable cookie banner

We don't know what
we are doing w/ them.

same cookie, for ads, logging

vs login abuse

-- visitor ID = abuse = ...?
= ads

June 14, 2021

P+J

360° on Me - How?

Vaccination card.

Addressing cookies: about
cookies & same one used
for each.

weekly 1 on 1 w/

Parag

Biggest thing is
for you and I to
align

if we disagree on
some thing there's an
issue -

if we agree then
it's just a matter of

Parag - not aligned

↳ need to align w/ Parag

go out of way to align

w/ Parag

get no-bullshit

"real talk" = feedback

"real talk" - good code word
why for for Parag.

Rise or question

I would want the CTO
to know...

~~Four~~ [redacted] is their leverage.

Unlikely [redacted] will be asked
to leave the country -
he is their leverage point.

3 weeks
or
directed

narrative - 1 way ticket

2 journalists - both got ambushed
[redacted]

ATAA-31

Pages 6, 17, 18

Summons -

Delhi Police summons - copy of letter

will not visit police station w/o having protection against arrest.

Police - all pillars - isolated

Silo

NETT - Ministry of Econ. & ST

no. return ticket - (1 way)
family

Turn up heat

legals

add supported platform

add cookies are essential

bugging time

(maybe come out a bit on
our side?)

~~IB~~ Immediate to long term BULL

u/RC -

~~Q~~ low hanging fruit that is B
! OK and argument will not
cover.

Q: what is example of

① low hanging fruit:

Analytics some of our analytics
cookies are used for a
variety of things but
various teams can't articulate
their uses - so we can't
describe our analytics cookies
we have to be able to define

Max Shrems

Privacy advocate
Champions and takes
companies to court over
Privacy.

Shrems 1 and Shrems 2

Max has sent complaints
to Twitter there will
converge w/ Irish DPC

(2)
low
hanging

Google analytics (cookies)

we give Google the
ability to use the data
we get as well.

Google refuses different terms

(3) We have cookies we don't know what they are used for.

(4) Cookies that have dual use - e.g. Analytics & Ads have to disentangle

examples of 6

systemic failures in

Twitter, prod. launch
process

- 5 branches reported in 5 mos.

Fines of up to

49,000

but more likely competitive disadvantage

Irish-DPC

attention will attract
attention

(A) (other 26) Cochran is GDBR except
27 other DPA, could take
a crack at it for Cochran
expense by paper cuts (expensive)

- (B) Irish-DPC ~~could~~

- have many other open investigations

- Could get pissed - lose good
will on other investigations

- More aggressive on other
investigations - to open GDBR
some serious

People who authorized
the rules? which rules

ssh-prod
ssh-next

taking

Everything in production
has no authorization -

[DB's, services, computers
have no authentication

Debuter interface
was interface

- Manhattan Debuter

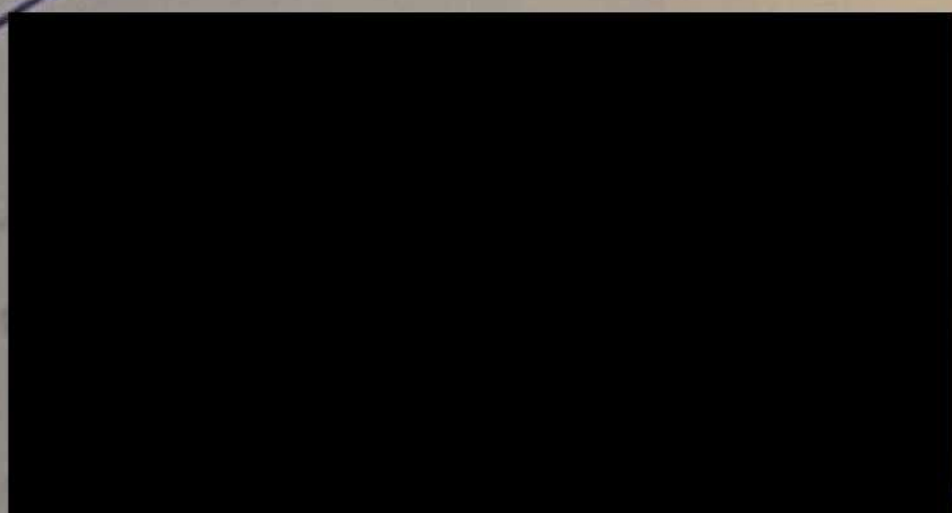
or je

Clients can make
requests directly into prod
- there is no auth

- Dev -

run copy of Twitter
on desktop & this copy
makes calls directly into
prod (w/o creds)

Q1) Such
State of Confidence
2)



Insider Risk - India
Leaks

Privacy

SIM-144

Cashier

Date Deletion

(Regulator)

~~Following~~

Clearance)

Indonesia -

forced him

- forced

hire

Farminde

Public Policy

Failed even the simple
background check

Built on plan of
2 Markets ~~with~~ ^{with} ~~the~~ ^{the} ~~same~~ ^{same} ~~risk~~ ^{risk}
India
Nigeria
Revenue - China

16 page pdf - JTB

Sept. 8, 2021

P+J

To Do List

Capturing overarching

IT Leadership update on VP of IT

Robin - Fun Data Sets

Eng Credentials

India Docs to Susan:
1 page - Confidence version
to Board

Admio,
→ Threads

ITGA → Health Tools
VP-IT

DynamoDB, S3, EC2 level

Azure

Spencer - ? fewer than 1k
datasets

870 on DynamoDB

AWS - 5-10k datasets

Two Birds - Plan coming out

Why Can't Privacy Do all of This?
Would have to Guess @ Data
Sets.

Tell us what data is what...

Launch Review. Data Sets that
support Deletion

Transition NAS - 1.1 → 1.2a

Sept. 21, 2021

P+S

Cont. Obj to Staff

Rish Cmt: Voice Intro

very night I go to
willing if India intern
already want our intern
to start to target and fill
→ as long as we are within
Indi: borders not able to migrate

4b • we don't have the
technical ability (yet)
to mitigate this situation

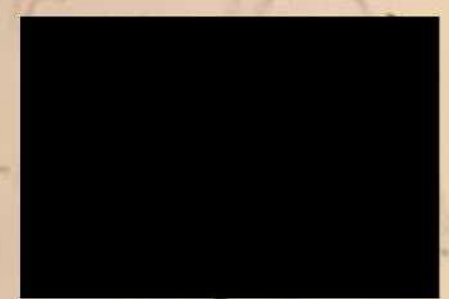
4a
status
this
• the path to mitigation
is to serve India from
outside Indi: borders
(Geopolitical Boundaries) since

Provide additional perspective
on rich management + on
a country

perspective on the rich analysis
portion of our presence in

India

|| from



doc.

also
1. We have an active
inside

2. India will continue to
attempt to influence on
twiffr
3. They will attempt to gain access
to the int

Turkey - on DAI

Business risk today

Take

unknowns - dynamo DB
(species)

HDFS/DB

SIM-154

Day 1st for targeting of
certain keywords (illegal)

Went in to see what we're
actually doing - becoming
apparent we don't know

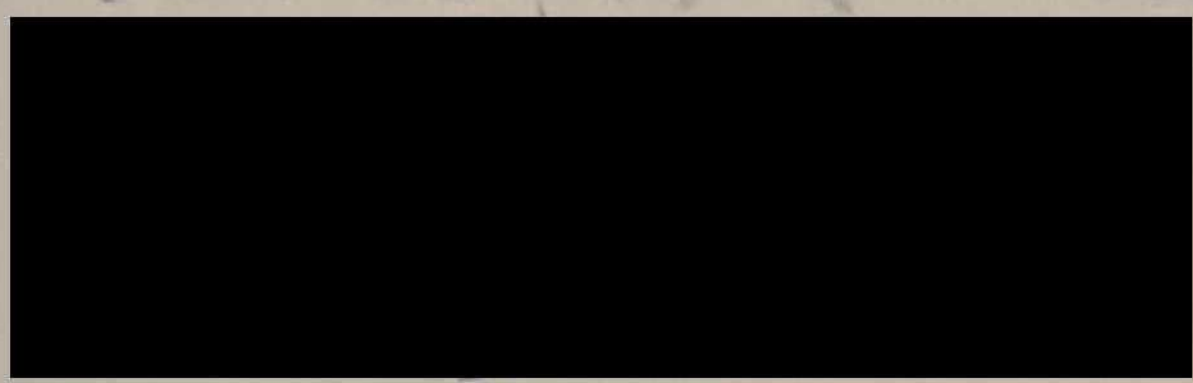
how the system works.

Some
Cave
Japan
Prater
US.

Paray - Ischerka still on
the table?
place 1 in Spain and 3rd in
US

Jan 13, 2022

7:5



We have AI Models built on
sets we did not have rights
to the training data we
used.

Models are going to be a
problem.

Jan 18, 2022

AI P+S

7th CI Empire CLS, finally
End of Day Itinerary to SZ
Staff Doc

Risk Calc Doc

✓ A2 Alarms

✓ A3 Reply to Marianne - Audit

~~The~~ CorpSec Principles

Five dech - track
CEO Security Follow up

Staff Doc

Audit Comm. Doc

✓ Exec Coach

Care in as
Change agent

trying to move the ball forward
understand how culture reaches
this information -

How do I take what I have and
what I know and help the
~~agent~~ org/staff receive this
and become an effective agent
of change.

not about me assimilating here

Started properly prior to
XMA/ Break


Ukraine

- effort to get in front
and be pre-positioned

#Retreat

by 45 - Free of current compromise
~~at~~ @ highest risk addressed
"we think" - how what

~~RE~~

Unblock  so I can
ach by 45 and resolving
there.

Parag has ~~intended~~ ^{encouraged} transparency
~~Decision to offboard~~
~~in October~~
Performance.

(A) Parag → transparency
(for moving parh)

In October ^{Nov} decided to start
the offboarding process for
[redacted] performance.

~~The Rish Centre we spent~~
~~through a number of HR/EL~~
~~issues she is still here~~

It was not intended that
[redacted] would be here for the board
or Rish Committee.

Jan 18,
2hr notice to meet
w/ Omid (Rish Chair)

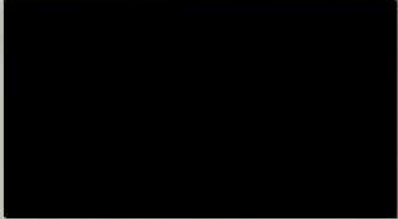
Access Control
incident root cause

~~to be working towards~~
offboarding [redacted]

The do

(A)
cont.

I put together the
Board section of the

 update to ensure
we were correctly setting
understandings of top
risk areas:

- Total Incidents
- Security Patches and SW
Versions
- Access Control
- Process Compliance

We spent the majority
of our Privacy/Infosec
time on Privacy.

Risk Committee had

~~I brought~~ A

~~I at~~

I triggered an audit investigation
on what was communicated
to the risk committee.

Background:

~~...~~ decided to
offboard early Nov,
for various HR/ER concerns
offboarding dates repeatedly
blocked

It was not intended ~~...~~ would
present to Risk - ~~but within the~~
~~prior week~~ but ultimately ~~...~~
~~...~~ had to be put forward. ~~short~~
notice

*2 I have concern over
what was presented at the
Risk Committee in the

~~One Area~~

Privacy / ~~...~~ Section

(Specifically ~~...~~) - ~~I brought~~

I documented these concerns
(hence we are here)

~~the~~
~~the~~

The concern is around how
it ~~is~~ ~~the~~ ~~in the~~ ~~the~~ ~~in the~~
intense document (a slide deck)
could be interpreted - they lacked
a narrative and context that the
privacy doc had. And as from Ms ~~...~~

The [redacted] / Privacy
(Focused on Privacy)

[redacted] verbally presented one item:
An improvement and progress
in access control.

Also stated a plan we
are executing

§3 Need ~~to~~ to call out 2

items

1) thing ^{ac} [redacted] verbally presented,
(which was basically the only thing
presented as that section was
Privacy Focused. Access
Control)

2) Address the Deck that
was sent for pre-read.

Unlike Privacy document,
lacked a narrative.

w/o context and description)
I believe parts can be
misleading or incorrect

4 I ^{am} ~~will be~~ putting
together a document to
capture and correct ~~any~~
confusion or misunderstanding
the [redacted] section and
deck ~~may~~ is at risk
of causing

Verbal
Access Control -
"small" project represented as
a win - a group of 300 work
with production access
~~will~~ ^{recently} reduced, ~~temporarily~~,
to 100 -

The larger context is
/ context
from 2020-2021 ^{prod} access grew from 2.7k
to 4k - faster than our employee # grew.
~~Mentioned there was a plan~~
~~that is being executed.~~
~~The small win~~ A similar

3441
5421

8862

1. Info conveyed not accurate
represent

2. I identified and documented
(hence we are here)

3. Significant efforts to avoid
sending confusing or misleading
info

4. As part of that [redacted] was
to be offboarded Oct/Nov

performance.
(not intended to present)

I am looking to gather
concise document to
advise and correct.

- ② [redacted] has used Retaliation and ~~the~~ tactics, since offboarding, apparent to repeatedly block
- Escalated repeatedly until ultimately to Parag and Disha (David: Risk becoming imminent)
 - Parag Promises to look into and resolve by ~~with~~ ^{personally} beginning of week
 - Calls Wech & Risk - not going to keep promise - apologized.
 - I ~~suggest~~ ~~I~~ ~~prepare~~ bring up replacement doc. Parag instructs the doc, and [redacted] present to board and that it attempt to mitigate

• threat to personally follow up w/ Risk

- ① Simple history
- 1st 3 Qtrs supporting [redacted] and providing room to build and execute
- Q4 goal → offboard (HR green light)
- Margen - "I see a manager who gave their report room and support."
 - Work to ensure incorrect info go to Board: Risk
 - ~~multiple offboarding, key~~
 - key targets always: Board: Risk to prevent this

Predictions / Issues
Raised - fulfilled

1) Dual outage - Black Swan

6) Nigeria - lengthy

8) Release of Paperchase

India - Govt - Insider

6) Lack of visibility (since first report)

↳ Log 45, and inability to
ensure problems fixed

8) Access Control - enabled
Black Swan, constant fix
and gets up / expanding

internationally
Privacy tie in

(3)

• I express discomfort with this
and inappropriate.
Full document in e-mail to
Barry; Dalene w/ Details

• After Dish I ^{took you} ~~followed~~ up
~~requesting~~ ~~taking you~~ up on your
offer to ~~to~~ follow up for
good measure. - You
expressed disappointment
to my handling of a
situation you prevented
me from avoiding.

• You suggested we meet up over
the break to work on these
issues - I eagerly agreed.
- You had your trip but cancelled on another
Confidential

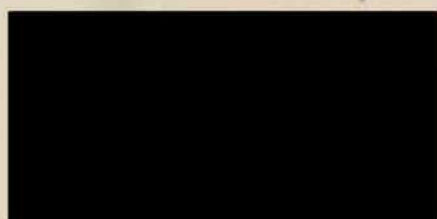
Oct 29, 2021

P+J



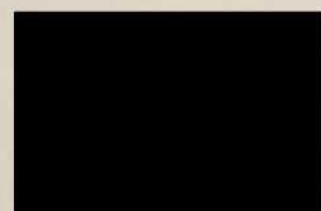
360

#Conf Deck and User track
Quarterly reviews



VPN - Spreadsheet to Shift

Recess:



Graph

6

Sierra Staff

We can tell other companies
they should have a presence to engage
customers

31 as employees vs
contractors.

@Twitter Support

Get slightly
bigger and
measure

6 people responding to 2%

Because responding on platform
to Customer (1 to many)
not at scale
not contractors (employees)

6.5m

measured w/AM 1:1 2%

net neutral cost w/

measurement

it

Nov 1, 2021

A1 P+S

A2 Harms

B1 Stocks - personal

→ ESP : 40/k

A6 Interviews Read CVs and choose
items for questions

A5 [REDACTED] Doc.

→ Purchase Plan

A4 Jack notes

A3 Staff presentation

183 (900)

117 (800)

Teams sign on owning service
not problem

206 PØs last year

Disney - 3-5 PØs

Notre Christ Hannah
team

you've
got this!

Not Body willing to run

no - in over her head.

Analysis: Porcelain

Senior members are buried under 17 or
18 things - not prioritized - only
person on project.

TWS 25 HC

6 people on @TwitterSupport (new thing)

responding to 6.2% of
addressable public
messages

Experiments show increase in WTM
customers engaged (2.1%)

\$1.9 incremental revenue per month

slight increase in revenue cost

full coverage 14.6 M (cost)

revenue + 15.1 M (.15M)

net 2.6 M for 100% scenario

given size of network

doing 3M target test

Nov 9, 2021

A P+S

A3 Set Dates for [redacted]

A2 Dry Run #Con

A5 Functional Strategies Review

A4 Staff Doc Assign

within 30 days
of coming on board we
will be making
progress on these
standards

Run of Show

Get [redacted] on point -

CR completion dates

Board, Risk

my role is the integrity of this org
make sure the ball is not dropped

Job 1 is the technical foundation
of [redacted] - the strong fundamentals
identifying the core areas of
highest exposure and highest
likelihood of happening -

- The standards by which the confidence
organization lives by and is evaluated
clients, servers, data, services, ~~outcomes~~
incidents - closing (understanding)

Nov 19, 2021

P+S

Harm

10651

Deposit Cheques (MS)

Threads response (deb. id)

#Protect

Tong Hawkin, Stage 2

Privacy

Functional Strategy for Privacy

Google Workspace Contract

Regulatory: Compliance only
Context

MOU to Dev Birds

(For the record) requesting Privacy
be the top priority in 2022

12:11 Nov 23 Jack tells
staff time for him to step

Dawn

Paray as CEO

Brett becoming chair (Board)

PATRICK leaving

- Patrick

Jack on the Board

Nov 30, 2021

A P+S

B1 Remove reference to [REDACTED]

Katrina in AS Doc.

C1 Twitter holiday card info

C2 [REDACTED] Invoice

[REDACTED]
[REDACTED]
[REDACTED]
Attachment to mission

A { Confidence - Ory Driven
Protect Objective

my mission

see would though get I secure by

Attachment to Mission

Driven

Jack call - Jack call

Pat [REDACTED]

my mission
who I surround myself with

UNC site lead

staff support for Twitter block

Hygiene - End Point
Access Control

IAM

5K

133

44

3077

9K 9000

- 5940

33

$\frac{1}{3}$

9000

Systems

3060

do not have

Software updates
enabled

End points

90% of systems
have security
updates enabled

only 50% of laptops are
security compliant

Dec 2 2021

Q3 2020 \rightarrow ~~13~~, 5

Q4 2020 \rightarrow 4, 3

Q1 2021 \rightarrow 7, 1

Q2 2021 \rightarrow 16, 7

Q3 2021 \rightarrow 13, 6

Q4 2021 \rightarrow 4, \emptyset

8.8, 3.4

Q3 2020 - Q4 2021

Q2 2021
16, 7

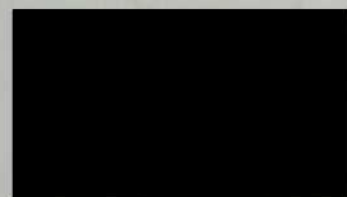
9.6, 4.4
incidents reported to
regulators

Dec 6, 2022

PLS

Stuff Doc

Board Voice track



Concur

Kudo Board

Access Control

Compliance - Sec Config

Incident tracking : root cause

Date Deletion

1100 off boarding

2020 : 2021

345

751

6506 - 2021/year

~2k reduction = 38%

very

100 reduced in ~~the~~

(not even) 2 small high risk

pockets

High risk pockets that need 90% +

March 16, 2021

✓ A1 P+S

✓ A3 Alerts

✓ A2 Shots

• A4 Strategy for Risk Community

A5 Stats for Risk - Quorians &
IT

B3 UPL Follow up (2nd pass)

B4 Confidence Board

B5 Pipeline assignment

B2 Bot Inventory

B1 ITCA/Health

115 PB of data in HDFS

3x increase (36PB) 2015

32 PB not registered (27%)

41% of Data sets active
but unregistered

Total Data Set: 39,303

20% (7k) not accessed
in 4 months

Nov 31, 2020

- ✓ A1 PHS
- A2 Unity Health election
- ✓ A3 [redacted] refill,
- ✓ A4 Stocks
- A5 Mindfulness
- C3 get Learning
- B4 60 Day doc.
- A4 Advisory Board
- A5 CoS JD's
- B1 Eng: Sec Roadmap Doc
- A6 Set Alarms
- C2 CITL Checks to bank
- B3 Eng @ Survey (Google Form)
- B2 Board Docs: Responses

Advisory Board: Jack, Ned, [redacted], Jennifer

[redacted]

Specific goal / Fire Jack
Ivan goal is keep an eye
on Jesse - Ivan report
Jack.

1 year stand off period
end of January 2021
Shareholder Vote

Why did we miss MFP
why didn't we capitalize on
Covid

Dec 2, 2020

✓ A1 P+S

✓ A2 Harms

✓ A3 Mindfulness

B4 go/learning

B5 60 Day Doc

B6 Advisory Board

B7 CoS JD's

B3 Eng: for Roadmap Doc

B2 Eng @ survey Form Doc

B1 Board Prep

A4 E-mail

B8 Contracts - Althea / Kieria
(see notes)

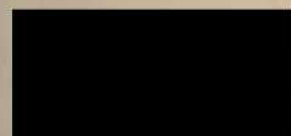
A5 Eyeglass metrics gr-
Board

Althea - Kieria, Caldwell, Oscar, Sherry
~~etc~~

Advisory Board: Jack, Ned

Sean, V. Jago, Jennifer

Jack Notes

 isn't ^{entirely} wrong

Everything can be traced
to lack of metrics
and goals @ staff
quantified ^{know}

- Example: Crisis

- haven't seen any docs (contract
revenue) with measurable
and goals or milestones &
data values.

- ~~the~~ global prioritization
not matching local work flow.
(?)

October 1, 2021 at 11:26 PM

Oct 1 --

Are you tracking that the Nigerian President said today that he will lift the ban?

He says Twitter has only agreed to 7 of 10 conditions, though

<https://punchng.com/breaking-buhari-orders-conditional-lifting-of-ban-on-twitter/>

Here's the full text in a local outlet:

<https://www.premiumtimesng.com/news/top-news/487593-what-buhari-said-about-twitter-ban-nnamdi-kanu-igboho-insecurity-others-full-text.html>

Paragraph 70-74

70. To address these negative trends, the Federal Government of Nigeria suspended the operations of Twitter in Nigeria on

Paragraph 70-74

70. To address these negative trends, the Federal Government of Nigeria suspended the operations of Twitter in Nigeria on June 5, 2021 to allow the Government put measures in place to address these challenges.

71. Following the suspension of Twitter operations, Twitter Inc. reached out to the Federal Government of Nigeria to resolve the impasse. Subsequently, I constituted a Presidential Committee to engage Twitter to explore the possibility of resolving the issue.

72. The Committee, along with its Technical Team, has engaged with Twitter and have addressed a number of key issues. These are:

- a. National Security and Cohesion;
- b. Registration, Physical presence and Representation;
- c. Fair Taxation;

d. Dispute Resolution; and

- a. National Security and Cohesion;
- b. Registration, Physical presence and Representation;
- c. Fair Taxation;
- d. Dispute Resolution; and
- e. Local Content.

73. Following the extensive engagements, the issues are being addressed and I have directed that the suspension be lifted but only if the conditions are met to allow our citizens continue the use of the platform for business and positive engagements.

74. As a country, we are committed to ensuring that digital companies use their platform to enhance the lives of our citizens, respect Nigeria's sovereignty, cultural values and promote online safety.

Few other local outlets, mostly saying the same thing:

<https://www.pulse.ng/news/local/buhari-orders-twitter-ban-lifted-but-with-conditions/w3tmwqe>



<https://www.pulse.ng/news/local/buhari-orders-twitter-ban-lifted-but-with-conditions/w3tmwqe>

<https://techcabal.com/2021/10/01/buhari-gives-conditions-to-lift-twitter-ban/>

<https://www.thisdaylive.com/index.php/2021/10/01/buhari-orders-lifting-of-twitter-ban-only-if-conditions-are-met/>

<http://saharareporters.com/2021/10/01/twitter-reacts-buhari%E2%80%99s-conditional-lifting-4-month-ban>

Sept 18 —

I am uncomfortable that Twitter has been silent on this. I fear we are now positioned to play the heel.

Nigeria can make whatever "demands" and (within the Nigerian market) if we do not give them everything they state it

looks like we are going back "on our word".

I am uncomfortable that Twitter has been silent on this. I fear we are now positioned to play the heel.

Nigeria can make whatever "demands" and (within the Nigerian market) if we do not give them everything they state it looks like we are going back "on our word". A word we never actually gave but that the world will believe we did.

Similarly If nigeria decides to continue the ban it looks like Twitter is the one at fault.

In the State department this tactic is pretty much known.

Is it too late to send a letter to Nigeria? Something along the lines of:

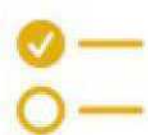
"we are reading that you appear to be in negotiations with someone claiming to be Twitter. We have not had these conversations and want to make sure you are protecting yourself as this appears to be a potential imposter. We are still very



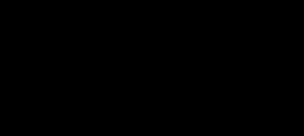
"we are reading that you appear to be in negotiations with someone claiming to be Twitter. We have not had these conversations and want to make sure you are protecting yourself as this appears to be a potential imposter. We are still very interesting in meeting and working with Nigeria to come to an amicable solution to the current situation. You are an important country and market to us, one we respect very much. We are also aware of the financial loss your people and businesses are suffering from this ban (██████ -I have figures if you need them - we are actually very well leveraged for negotiations here -Mudge) and we want you to be able to support these businesses and your citizens."

At that point we subtly slide the open letter to a trusted journalist to give the truth a bit of light that can be cited and referenced in the future... when we need to be able to defend our position.


Or do you have other suggestions / ideas?



June 5, 2021 at 11:27 AM

 I want to share some thinking that Nigeria has spurred. Something to add to our tag ups so you can have input on prioritization in regards to all of this.

I came in a bit late on the evaluation of Nigeria as a target location for offices and employees. I quickly sided with LGL and CorpSec due to some knowledge of government stability versus other countries in the region. I appreciated the work product from both teams. I was a bit surprised by the apparent ordinality and timing of the work versus the push to stand up an office.

One of our visions is Confidence can help support "whole of company" assessments
Informed by: TwS, T&S, LGL, PP, , Privacy.

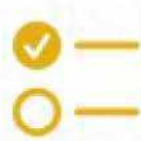
Capturing a holistic understanding of what {\$Country} (eg Nigeria) is doing, table top what they could or would do given specific

Capturing a holistic understanding of what {\$Country} (eg Nigeria) is doing, table top what they could or would do given specific moves, and then use this frame to incorporate additional external knowledge we could gather.

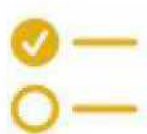
Before prescribing changes and a path forward, our first questions are how did we administratively handle this, and is that our "standard" approach. Knowing that, then we can find ways to optimize.

We are in the process of running tests on a few {\$Country} targets. In addition to ones of ongoing interest such as India, China, Turkey, and Nigeria, we want to have options to provide in order to support forward progress.

How Twitter currently assesses country-specific risk is in flux, as there is a joint Infosec-CorpSec-Legal-PP project to change how a country risk assessment is built. As an example of new data input an example that concerns us is that Taiwan is



How Twitter currently assesses country-specific risk is in flux, as there is a joint Infosec-CorpSec-Legal-PP project to change how a country risk assessment is built. As an example of new data input an example that concerns us is that Taiwan is listed as low risk across the board. From the perspective of human rights and stability, sure, low risk. But it's also China's Ministry of State Security's (MSS) backyard, and putting a Twitter office in Taipei isn't so radically different (from a Customer protection perspective) than putting it in Beijing. Different risks, but not non-existent risks.



We

Good morning [REDACTED] be and Kayvon,
thank goodness qr eq

Sea A

In relationship to **Nigeria** and India I saw
the WaPo article on Koo yesterday.

<https://www.washingtonpost.com/world/2021/11/16/india-twitter-koo-social-network/>

The section on how Koo executed around
the **Nigeria** ban is interesting. Fast acting
as well.

Given the value the **Nigeria** ban provided,
and continues to provide, to Koo, and the
non-neutral leanings of the platform, their
strategy in relation to Twitter is straight
forward. They even spell it out in the
article:

"We'll expand into Africa, then Southeast
Asia, South America, Eastern Europe — all
this in the next couple years," he said. "We
want to go very aggressive."

September 3, 2021 at 11:37 PM

Cost in millions to regional economy from blocking Twitter

Cost in millions USD:

Myanmar \$2,500

India \$368

Nigeria \$367 (and counting)

<https://netblocks.org/cost/>

Nigeria:

39.6M users, mostly upwardly mobile economically and politically, 20% use for advertisement, 18% to look for employment

Are you tracking the Nigeria issue?

My concern is the false narrative they are pushing in the media:

My concern is the false narrative they are pushing in the media:

They have refused meetings with Twitter to date. Yet they are publishing media articles saying they are in the midst of negotiations with us and are almost at the point of agreement to end the ban.

Their most recent article claims the minister flew to New York to meet with Twitter execs.

Meanwhile their economy loses 6M a day (360M and growing) while they ban us.

We have not commented on any of the articles saying that we have not met with the Nigerian government yet.

Depending on why they are taking this tactic leaves a few unwanted scenarios as options. One scenario is Twitter being set up to take the blame when negotiations "fall apart at the last minute". Possibly while they drive up their competing

Depending on why they are taking this tactic leaves a few unwanted scenarios as options. One scenario is Twitter being set up to take the blame when negotiations "fall apart at the last minute". Possibly while they drive up their competing

<https://www.top10vpn.com/vpn-demand-statistics/>

Disregard:

<https://punchng.com/twitter-ban-remains-says-ncc-as-nigerians-lose-n220-36bn/>

October 14, 2021 at 10:24 PM

10/14/21 FYSA - my team has just confirmed a further 132 accounts registered by the Chinarr Corp this year. Majority caught automatically and suspended - but several slipped through. Engaged in exactly the same behavior. They're clearly unrepentant - and absent disclosure it doesn't seem like we have a viable strategy other than perpetual whack-a-mole.

September 23, 2021 at 12:30 PM

1. we have high confident
we have an existing
insider threat in India -
we believe this person
to be placed by and
working for, or
otherwise supporting,
the Indian government
(and/or Intelligence
agency) and not
working in the best
interests of Twitter
2. The Indian govt. will
continue to push to
influence Twitter and
control content on the
platform - both
externally and

influence Twitter and control content on the platform - both externally and internally.

3. The intelligence agencies/government will work to gain further access to internal Twitter data about people on our platform - if they have not already done so. They will use this information to target people who speak out against the government, are dissidents, or otherwise "of interest". The actions

dissidents, or otherwise "of interest". The actions taken based on this information will not necessarily be on our platform. I view this as being in opposition to our mission of "serving the public conversation".

4. There is a geopolitical boundary issue here.

4a) As long as we are operating within India's borders we are not able to technically mitigate this threat at this time.

 Search

July 20, 2021 at 9:10 PM

Ned,

I wanted to share a bit of context about the tweet thread you reported to me as suspicious.

In a matter of seconds, to evaluate the account you flagged, we intimately knew the individual. Phone numbers, where they lived, other accounts they control, their non-public ring of "friends", type of phone/computer,... and more.

While we did this through certain agent tools that have been somewhat restricted, any engineer could figure out how to do this under the hood without needing to use those tools.

I just wanted to quickly check the account to see if they were a threat. Was the person a Twitter employee? No. Were they physically inside the Twitter offices? No. Were they actively engaged in other hostile actions and planning? Was it a network of people? Were they physically within striking range of Twitter execs?

I just wanted to quickly check the account to see if they were a threat. Was the person a Twitter employee? No. Were they physically inside the Twitter offices? No. Were they actively engaged in other hostile actions and planning? Was it a network of people? Were they physically within striking range of Twitter execs?

they weren't).

All of these areas want to shape their country's public conversation. They want to control what is said and they want to know who is speaking badly about them, where those people are, and who they are communicating with behind the scenes.

In other words they want to know the type of information that we just looked up about the account you flagged.

We haven't adequately paid past security bills for many years (10+ according to Parag. I believe that). No blame or finger pointing. That's not helpful and I can guarantee the choices were likely appropriate given the information available/presented.

We haven't adequately paid past security bills for many years (10+ according to Parag. I believe that). No blame or finger pointing. That's not helpful and I can guarantee the choices were likely appropriate given the information available/presented.

Each time we want to expand into a new country, with a physical presence, most countries will see us as an ability to monitor their "adversaries". Be those adversaries foreign or domestic.

As it stands, if we have engineers working there or if we have people supporting spaces there, or several other roles... (even sales roles)... the foreign entity will quickly realize they have the keys to our kingdom.

India is particularly worrisome.

We know they want detailed information about the individuals involved in the Farmer's Protest. We know they want information about the people criticizing the Indian government's handling of Covid.

We know that the Indian government

We know they want detailed information about the individuals involved in the Farmer's Protest. We know they want information about the people criticizing the Indian government's handling of Covid.

We know that the Indian government wants to silence these people and remove them from the public conversation.

The articles I shared today in the staff doc show how willingly the Indian government marks reporters, dissidents, executives of foreign companies for targeted surveillance and espionage.

We have seen how they have targeted our employees and controlled their local media to portray [REDACTED] as the person responsible for Twitter's non-compliance.

We believe the Indian government has already planted a government agent within Twitter.

We will have to figure out how to conduct business in such environments safely. Presently, though, when we rush into this situation we are directly working against

We believe the Indian government has already planted a government agent within Twitter.

We will have to figure out how to conduct business in such environments safely. Presently, though, when we rush into this situation we are directly working against our mission of serving the public conversation. We are handing the keys to a surveillance apparatus that is intending on using our platform against our own mission. Silencing and targeting and undermining the public conversation.

May 24, 2021 at 11:54 PM

RAW (India's intelligence agency: Research and Analysis Wing) uses Special Cell as cover to provide access to targets in forms of technical access and compromise of target entities (such as ourselves).

I would not be surprised to find that some of the "squad" were not standard police. This is very much an example of a target of interest where they (the govt) would seek compromised access into Twitter.

I recommend very sensitive plans or information, particularly on this topic, be shared out of band where possible (signal, voice, etc.).

If that is the case they are running a big international risk if they are caught. This may mean that we can send a message to RAW through certain posturing in our systems or even physical support on the ground. A message that we have capabilities to identify, and that we are looking, could be enough result in some extended safety periods for Customers

February 16, 2021 at 12:20 PM

80 Indian employees

Handsome severance packages - not their fight, they should be able to opt out.

For 118 - message that once you take a payment the adversary will have leverage. What they will ask you to do next will be much worse and you will be stuck.

General FYI on insider threat campaigns to employees and contractors.

April 20, 2021 at 4:02 PM

TNIO (Turkey's National Intelligence Organization) is a very capable service.

For local assets (people or offices): TNIO has extremely capable physical access capabilities, so, any physical presence would be something to consider as compromised (listening, monitored, internally accessed at will).

As you are already aware, their ability and willingness to "lean" on people with pressure campaigns (including physical tactics) is known.

Specific to cyber, they're capable but not particularly advanced- more "near abroad" and regional interest (w/r/t targeting) vs. global intrusions and collection (that being said, this calculus can change based on the "hardness" of the target). What this means for us is that we may not be presently compromised by TNIO but can expect Twitter people and devices in country to be compromised and used for access into our systems, communications, and data.

Specific to cyber, they're capable but not particularly advanced- more "near abroad" and regional interest (w/r/t targeting) vs. global intrusions and collection (that being said, this calculus can change based on the "hardness" of the target). What this means for us is that we may not be presently compromised by TNIO but can expect Twitter people and devices in country to be compromised and used for access into our systems, communications, and data.

It would be ideal if we can keep Twitter employees in **Turkey** to *only* Gsuite and Slack (or some subset thereof).

Happy to work with you to figure out the strategy here for our various scenarios.

February 5, 2021 at 7:54 PM

LDAP

```
ldapsearch -xLLL -h [REDACTED]  
-b
```

```
"cn=groups,dc=ods,[REDACTED]"  
-s sub "(objectclass=*)"
```

```
ldapsearch -xLLL -h [REDACTED]  
-b
```

```
"cn=groups,dc=ods,[REDACTED]"  
-s sub "(objectclass=*)"
```

Try this instead:

```
ldapsearch -xLLL -h [REDACTED]  
-b "cn=users,dc=ods,[REDACTED]"  
-s sub "(objectclass=*)"
```

I'm not sure why the [REDACTED] isn't working. [REDACTED] says to use the LDAP server "local" to your zone (zones are sorta kinda like enclaves, but not really in any useful security sense).

December 22, 2020 at 10:12 AM

BLUF: we have many datasets within Twitter that are primary targets for entire classes of attackers. Twitter may not presently perceive them as high value because we may be looking at them through a lense of "what is valuable to Twitter". Here's a walkthrough of a criminal's playbook against Twitter using the Ledger data breach of two days ago as an example. All possible simply from Customer name, address, e-mail, and phone number.

I am in the process of identifying several types of datasets that are high value to Criminals and quantifying their value and exposure.

In the following section I detail:

Name and address -> retrieve SSN for \$20

SSN, name, address -> take over email account

Phone number -> determine phone carrier

SSN, name, address -> take over email account

Phone number -> determine phone carrier

Phone carrier, number, name, address, SSN -> SIM slamming

Above = control of target's crypto currency accounts, stock trading, bank accounts, etc.

Details

I type this on my iPhone, lying bed, isolated, sweating out what I hope is not COVID. I get the results back within the next 12 to 24 hours. Apologies in advance for autocorrect and "phone" grammar.

I wanted to share with you what happens from an adversary's perspective after a "simple" data breach. This will be similar to what happened to Jack but more opportunistic.

Let's suppose we lose a bunch of seemingly innocuous Twitter Customer information. All it has to be is as little as email address, Twitter handle, and phone

Let's suppose we lose a bunch of seemingly innocuous Twitter Customer information. All it has to be is as little as email address, Twitter handle, and phone number. Turns out it's not so innocuous.

TwS owns/accesses some very valuable stashes of adversary gold. Stashes that we don't recognize being super sensitive. particularly when sitting next to Agent accounts and tools. How strictly are we controlling access to underlying datasets by other means and from other systems?

In this case the real world example is Ledger, a maker of a product used with cryptocurrencies, who suffered an information leak two days ago (12/20/2020).

From their data breach, which contains names, email addresses, phone numbers, and home addresses, the adversaries has all they need to get going. This will be a lucrative payoff.

The adversary already has a correlation between Customers in this data set and people who ~~have cryptocurrency~~ wallets.

The adversary already has a correlation between Customers in this data set and people who have cryptocurrency wallets. For Twitter that correlation may require a quick download of historic tweets and tagging, or mentions, of crypto exchanges or financial organizations.

Adversaries will go through the dataset looking for e-mail addresses that will be easy to **compromise**. (.edu, [att.net](#), etc.). They will then attempt to correlate these users with higher value accounts on Binance, Coinbase, Bitrex, etc. In Twitter's case it may be that the adversary identifies "easy" to **compromise** email accounts and then downloads the twitter handle tweets (via public API) and auto scan them for keywords or key accounts. (There's an opportunity for our analytics here) The key here is that a subset of the total targets are opportunistically qualified. You'll see why next.

Let's assume they now have a list of accounts they want to take over. They lookup the target name within {jstash, dehashed, snusbase} and receive the SSN of their target for \$20. (This is possible

< Search



Let's assume they now have a list of accounts they want to take over. They lookup the target name within {jstash, dehashed, snusbase} and receive the SSN of their target for \$20. (This is possible due to the Equifax breach)

Because the above step costs the adversary money, it is performed after there is some confidence that the target has an online cryptocurrency account, or that the target performs online banking and has a sufficient level of funds to be of interest. A guesstimated few thousand dollars in a bank account could be sufficient. Or, that they want to takeover the target's Twitter handle.

The adversary calls up user support / tech support of the email provider and with the name, phone number, address, SSN, convinces them to change the password and/or redirects the email. You can imagine how easy this is for accounts such as .edu or AOL, etc. Name, number, address, and social are the only identifiers these email providers may have.

The adversary now controls the target's e-

identifiers these email providers may have.

The adversary now controls the target's e-mail.

If the adversary needs to **compromise** a phone number to complete the account takeovers (remember they already control email at this point), they already know the target phone number from the breach and they just need to identify the carrier. A lookup on 'freecarrierlookup', or similar service, tells them if it's att, t-mobile, etc. Some of these carriers let you switch the SIM attached to a number online with just the information listed above. No social engineering needed. For other carriers some social engineering is conducted at this point.

The more direct effort the adversary needs to perform, such as multiple social engineering attempts, a carrier that doesn't allow online automatic sim swapping, etc., the more likely the adversary has qualified the target as having sufficient funds to warrant the cost.

Any account in the Ledger **compromise**

The more direct effort the adversary needs to perform, such as multiple social engineering attempts, a carrier that doesn't allow online automatic sim swapping, etc., the more likely the adversary has qualified the target as having sufficient funds to warrant the cost.

Any account in the Ledger **compromise** that is used elsewhere for cryptocurrencies or banking, is at risk. The same would be true for any Twitter account where we exposed (or lost) valid email addresses, real names, phone numbers, and handles. *Especially* since the public Tweet history provides enough opportunity to spot juicy pointers to financial target affiliations. "Hey @{BofA, Coinbase, Etrade, ...} I love/hate your service!", and qualify high value targets through their conversations.