RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-W10

Inside the Timehop Breach Response

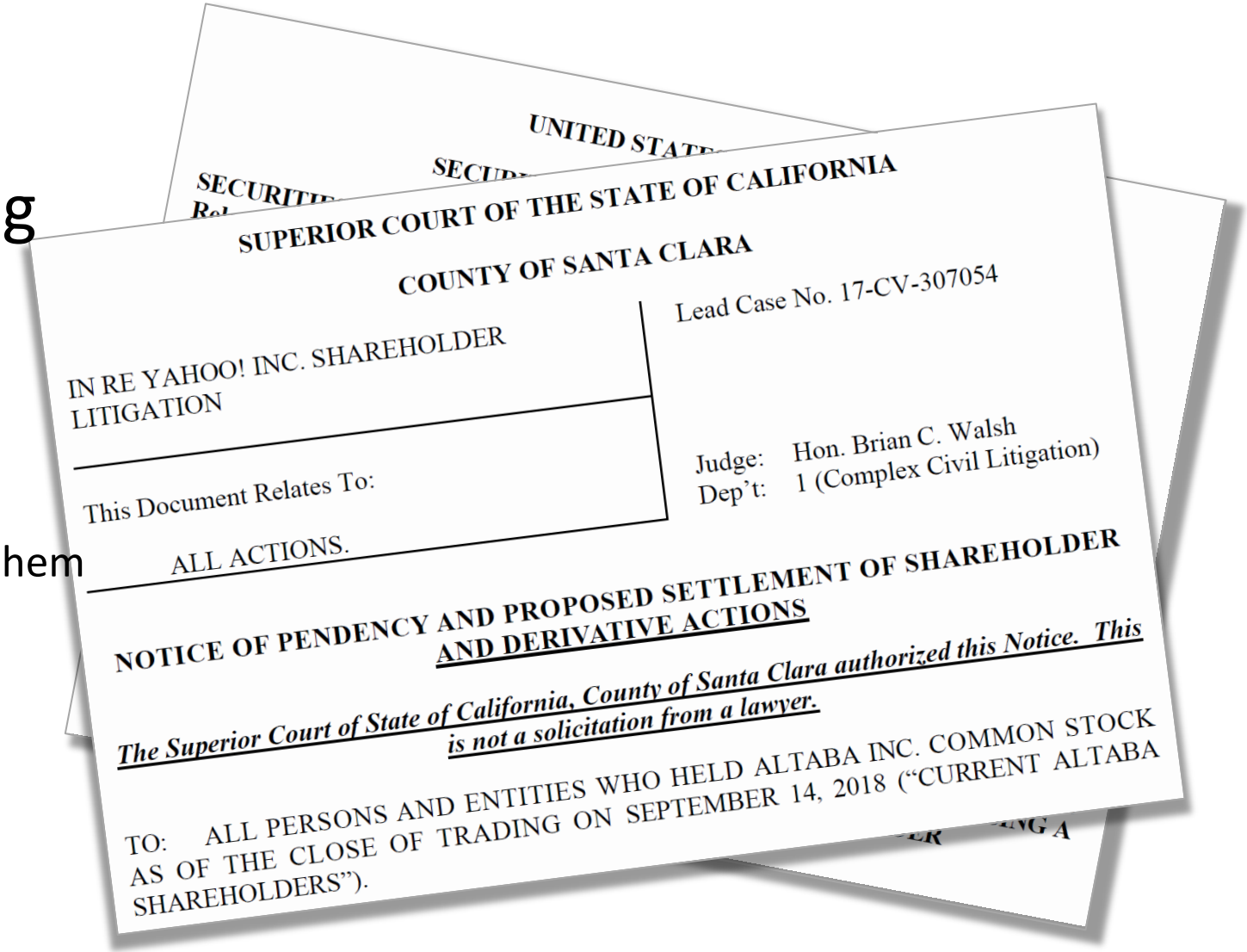
Nick Selby

Former Managing Director, CJX, Inc.

Shh!

Companies are, most often, squeamish about announcing that they've been breached.

- They are embarrassed
- They don't want the press coverage
- They're scared their customers will leave them
- They're afraid of fines
- They want it to go away



SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SANTA CLARA

IN RE YAHOO! INC. SHAREHOLDER LITIGATION

Lead Case No. 17-CV-307054

This Document Relates To:

ALL ACTIONS.

Judge: Hon. Brian C. Walsh
Dep't: 1 (Complex Civil Litigation)

NOTICE OF PENDENCY AND PROPOSED SETTLEMENT OF SHAREHOLDER AND DERIVATIVE ACTIONS

The Superior Court of State of California, County of Santa Clara authorized this Notice. This is not a solicitation from a lawyer.

TO: ALL PERSONS AND ENTITIES WHO HELD ALTABA INC. COMMON STOCK AS OF THE CLOSE OF TRADING ON SEPTEMBER 14, 2018 ("CURRENT ALTABA SHAREHOLDERS").

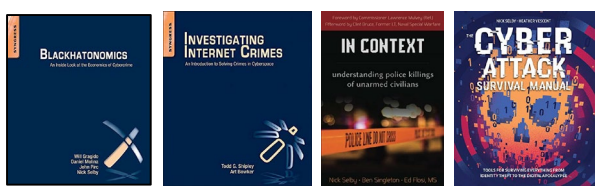
Wouldn't It Be Nice?

We've been saying for years that companies should just come clean.

- What if they just came clean?
- What if they just said, "We messed up, here's what happened…here's what we're doing about it, here's what we have done to ensure this will never happen again."
- I wonder…Would that work?

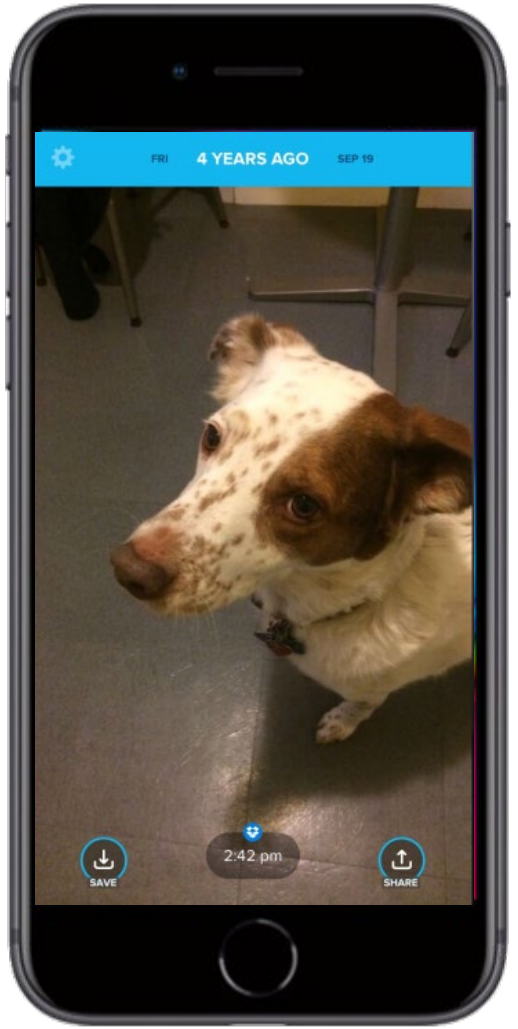
About Nick (Abridged Edition)

I am **not** speaking on behalf of the NYPD or the NYPD Intelligence Bureau



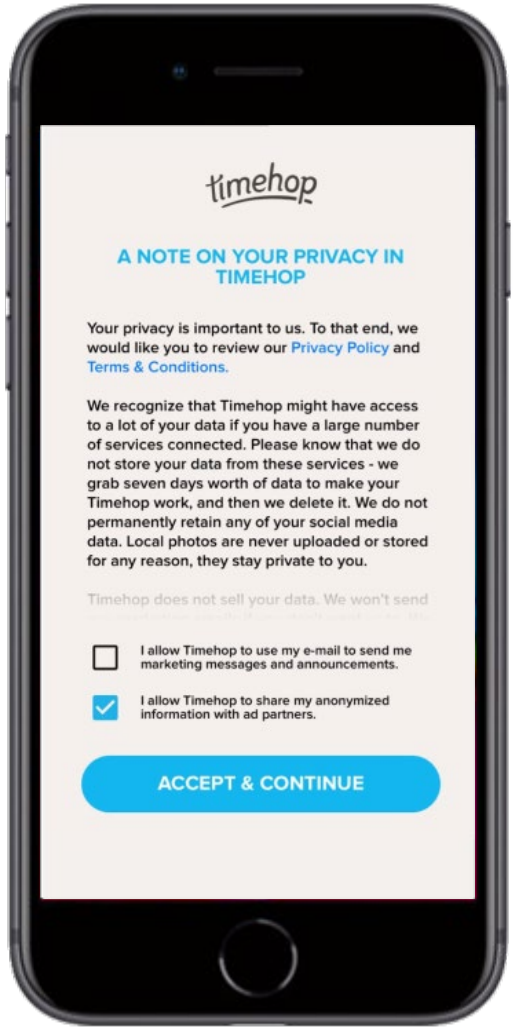
About Timehop

- A daily look at moments of your life. Retrieves posts from
- What …um… “inspired” Facebook’s, “On This Day.”
- 25 million users, millions of Active Daily Users; 7 million addicts who maintain “streaks” – consecutive days stretching for years of daily use.
- 15 employees, 5 engineers

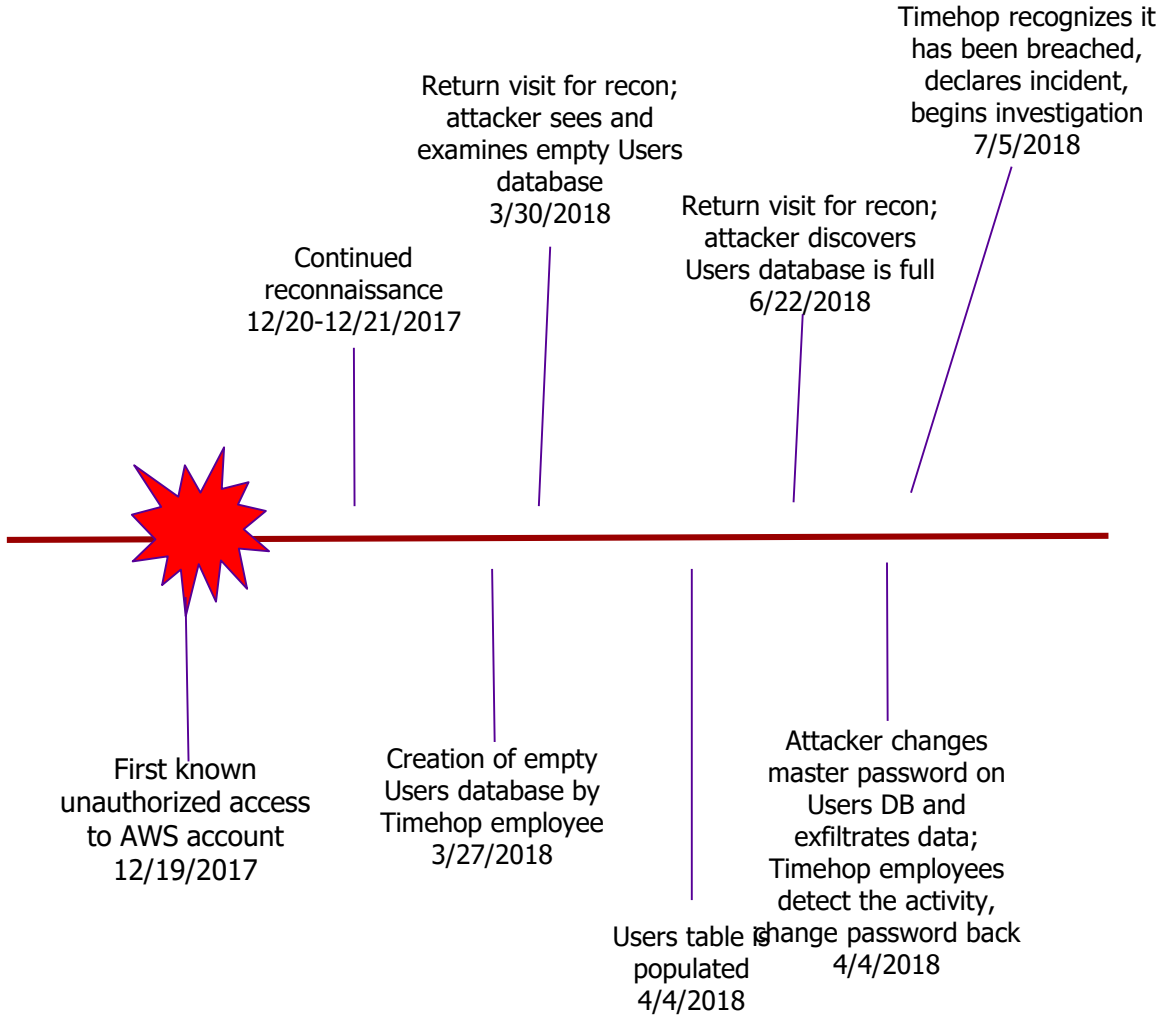


Important

- Timehop did its GDPR implementation early. They don’t share PII with ad partners.
- There were some challenges, because while it aggregates social media data, GDPR was required, but there’s no “opt-out” because the app *is* your data.
- About 5% of EU users did not accept the terms and were removed.



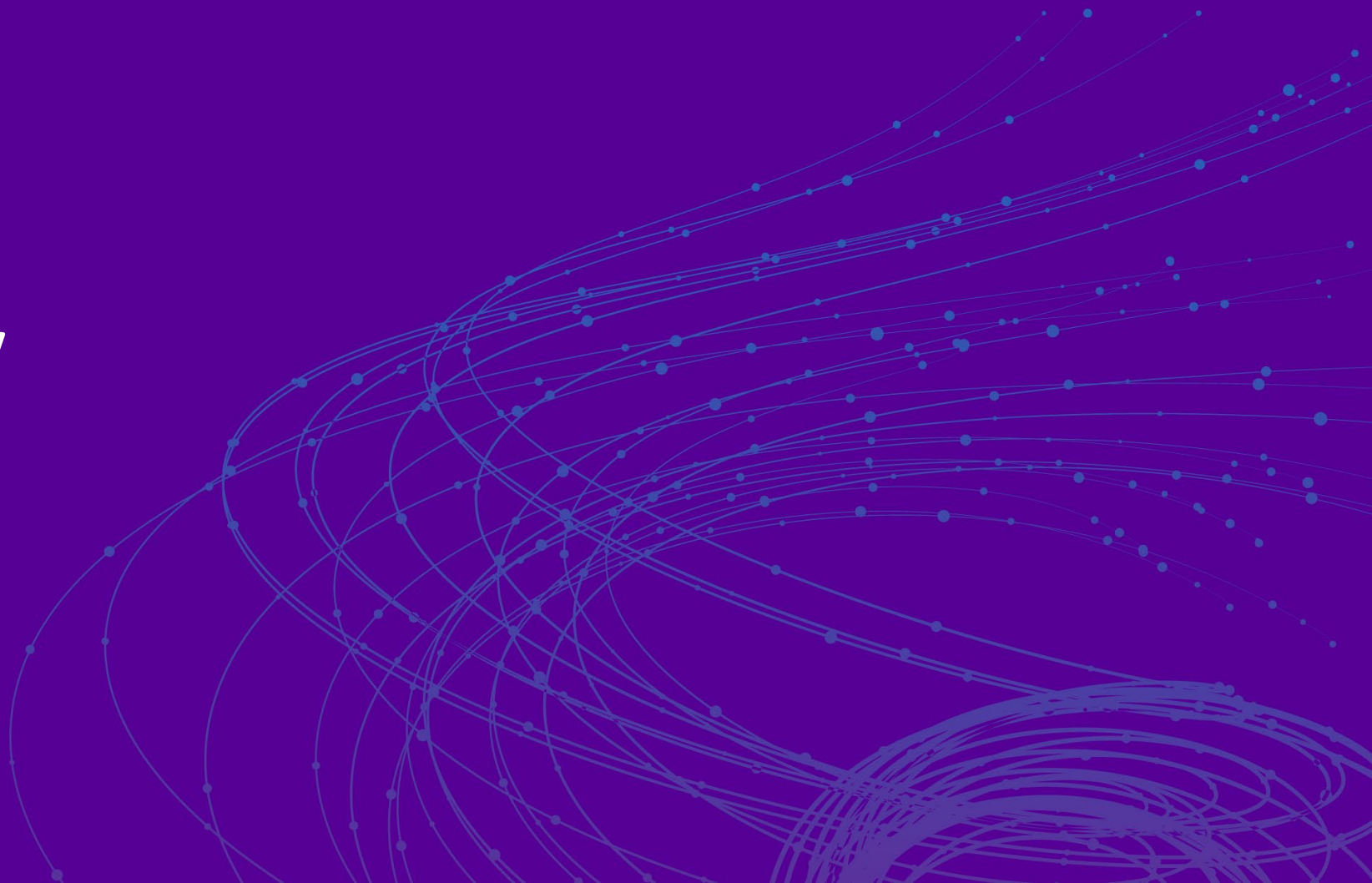
Our Story So Far



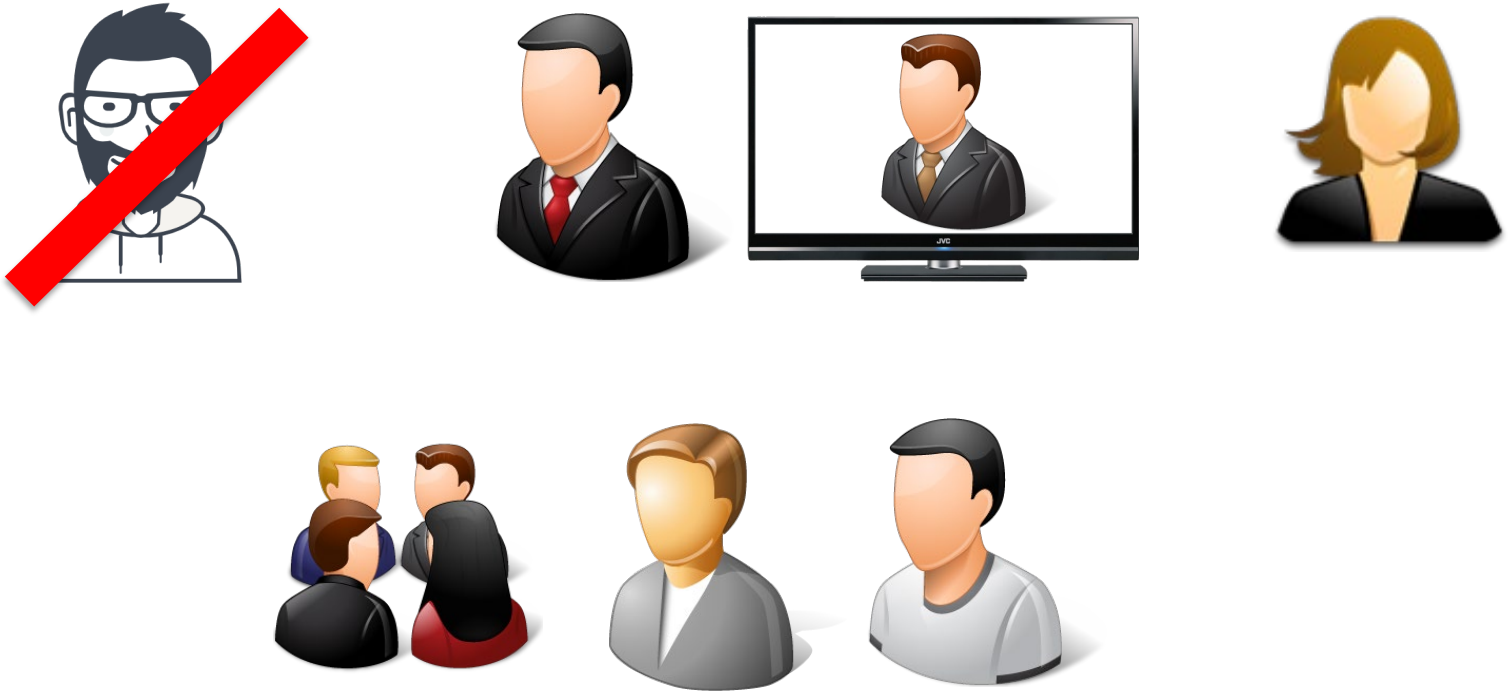
RSAConference2019

The First Day

5 July 2018



Cast of Characters



July 4, 2018

- Engineer's barbecue is interrupted by an alert: a password has been changed on the main User database.
- Engineer checks it out, confirms the password has been changed, *changes it back*, begins deleting non-mission-critical accounts, notifies management, logs out, and returns to barbecue.
  - This has happened before, during failover for misconfigured instance
- In hindsight, this order of operations could have been handled better.
- Note, in lieu of formal procedures, the engineer did OK.

July 5, 2018

- The engineer continues to investigate and that's when he notices names and emails (more specifically, the User database) have been compromised.
- Notifies CEO and COO (CTO is unreachable in Cuba); an incident is declared.
- While C-Suite makes notifications, gets lawyers, asks board for recommendation of IR pro, considers GDPR consequences, engineers continue audit.
- Timehop had been in the middle of a 2FA rollout. The account breached had not yet been updated. That account's access was deleted.
- 2FA is added to all remaining accounts in a quick audit and cleanup.

Apply: Incident Recognition and Response

- Next week you should:
  - Review (or create) your Incident Response policies and procedures.
  - Identify critical services and systems whose investigation, if jacked with, should be escalated as a matter of course
- In the first three months following this presentation you should:
  - Create an incident response notification system that involves
    - Someone from IT/Dev/DevOps side
    - Someone from Information Security
    - Someone from The Business
- Within six months you should:
  - Create an incident response alerting system

July 5, 2018

FBI

BOARD

LAWYERS

GDPR

CRISIS COMMS

IR

July 5, 2018

NICK:

What's your most important goal here?

RICK:

Protecting our customers' data.

NICK:

What's *really* your most important goal here?

RICK:

I swear to God, protecting our customers' data.

July 5, 2018

- Other things the engineers realized: Not only did the bad guys get the usernames and emails, they got the OAUTH tokens to access Facebook, Twitter, LinkedIn, Google Photos, etc…
- This put a real damper on our plans to go public: before we could go public, in the event that the bad guys didn't know what they had, we needed to kill those tokens.
- Then we could tell everyone.

The IR Plan

- Work with providers to expire all external tokens; then expire Timehop's, forcing all users to log back in. As we do that, we make the notification.
- Simultaneously, suss out what got taken and how; ensure the attack is over;
- Build a recovery architecture to stop the leak while longer-term fixes were undertaken; and
- Protect against the intrigue and curiosity about our systems' conditions that the announcement would aggravate.

The IR Plan

- This meant building a team to work with the Internal team to discover and fix at the same time:
  - **Marcus Ranum**: Log Analysis and network forensics
  - **Rocky DeStefano**: Log re-architecture and re-implementation
  - **Joel Yonts** (Malicious Streams): Disk forensics
  - **Ashish Prashar** (Ashes to Ashes): Crisis Communications
  - **Moeed Siddiqui** and **Ben Singleton** (NetGenius) Re-architecture and re-implementation of LAN Security
  - **Mr. and Mrs. X**: Web and Dark-Web Monitoring & Intelligence
  - **Gal Shpantzer**: General hard-core helpfulness
  - **Carla Geisser** (Layer Aleph): Application and AWS Environment Re-architecture

Immediate Technology Purchases

- 2FA/NAC
- Single-Sign-On
- Managed Endpoint Security Monitoring
- AWS Environment Scan and Repair
- Upgrade AWS Support Package

Apply: IR Team

- Next week you should:
  - Ask yourself whom you would call in the event of a breach
  - Identify the skills you have in-house and those you would need to augment
  - Ask yourself what visibility you have into hosts, subnets, networks, and your outbound Internet traffic
  - **I have no skin in this game – I'm out of the business**
- In the first three months following this presentation you should:
  - Interview three Incident Response companies
- In the first six months following this presentation you should:
  - Put one of them under retainer. Speak with them semi-annually or when you make major changes to apps or infrastructure.
  - Get visibility. By hook or crook.

The IR Plan

- Only one problem: GDPR - they want notification within 72 hours, and that was literally not possible. It simply took longer to expire all the tokens than we had.
- GDPR through the Timehop Paris lawyer ended up giving us more time.

Apply: GDPR Deadlines

- Next week you should:
  - Discover whether your firm has a plan in place for interacting with the EU Privacy Directorate
  - Recognize that the worst time to make new friends in a French bureaucracy is when your hair is on fire.
  - Decide to make the plan.
- In the first three months following this presentation you should:
  - Create an GDPR notification system that involves
    - Someone from IT/Dev/DevOps side
    - Someone from Information Security
    - Someone from The Business
    - Someone from a French law firm (or with your lawyers' correspondent office in Paris)

The Weekend

- We worked the plan.
- Throughout the night Friday, through Saturday, we got hold of the partners and had them reset.
- By Sunday, all had confirmed that
  - All tokens had been de-authorized; and
  - No token had been used for an unauthorized purpose
- Outside counsel helped write the breach notification; by Sunday at 2 PM we had de-authed millions of users, forced them to read the notice and to log back in. Users began to do that.

Notification: The Beginning

We told the press. Ash called everyone he knew, and announced. Loudly.

INDEPENDENT

JOIN US? SUBSCRIBE REGIS

NEWS VOICES SPORT CULTURE INDY/LIFE INDYBEST VIDEO DAILY EDITION COUPONS

TIMEHOP HACK: 21 MILLION USERS'

threatpost Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne Spotlight

Timehop Breach Impacts Personal Data of 21 Million Users

Andrew Griffin

Timehop is a
leaked the p

People who
media accou
happened in
sensitive inf

The app say
attack, and
had occurre
many of tho

Author:
Lindsey O'Donnell

July 9, 2018 / 9:52 am

3 minute

Skip to:

How di

Share th

Timehop Inc. managed to cut off access two hours and 19 minutes after the hack began, but only after the data had been stolen.

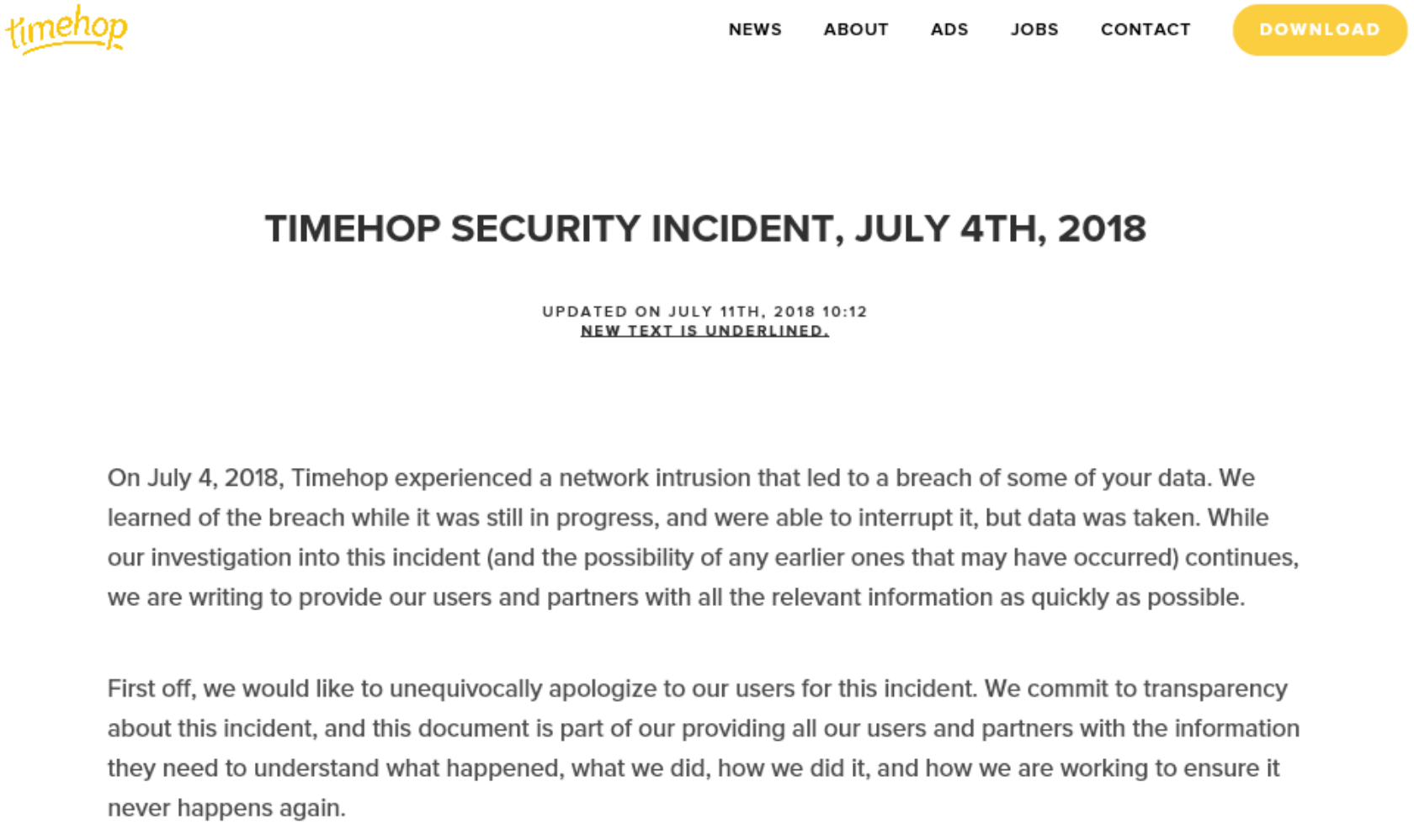
James Lerud, head of behavioral research team at Verodin Inc., told SiliconANGLE that Timehop should be commended for their transparency and handling of this situation so far.

"They were able to begin remediation actions about two hours after detecting malicious activity, which is a very good response time," he said. "Their decision to deactivate access tokens is the right move, but should also serve as a reminder to regularly review what apps have access to your social media accounts."

A massive breach has impacted up to 21 million users' personal data and their social media "access tokens."

Notification: The Beginning

We put up a 4000-word, cathartic, total catalog of everything we knew to date.



Notification: The Beginning

We also put up a 1900-word technical page, that gave geeks more information without blowing the entire investigation

TIMELINE

12-19-2017

- [Employee]'s credentials were used to log into our Cloud Computing Environment from an IP that resolves to the Netherlands; we will refer to this unauthorized user as [The Unauthorized User].
- [The Unauthorized User] creates an API access key on [Employee]'s account and a new user '[account_name]', attached admin access to that account, and creates an API access key on that account as well.
- [The Unauthorized User] logs into [account_name] using the API and starts scraping the list of tables, accounts, roles, and alarms - in short, [The Unauthorized User] was conducting cyber reconnaissance. There was no Personally Identifiable Information available in the environment at this time.

12-20-2017

- [The Unauthorized User] logs in again and conducts more reconnaissance.

Flashback: The IR Plan

- Work with providers to expire all external tokens; then expire Timehop's, forcing all users to log back in. As we do that, we make the notification.
- Simultaneously, suss out what got taken and how; ensure the attack is over;
- The way this was done was each team reported on their findings, in a big conference room. All findings, all notification drafts, everything, was vetted with this whole room.

Monday, July 8

- In a conversation about the contents of the User database – you know, emails, usernames, phone numbers – someone said,


Monday, July 8
“Oh, and dates of birth.”
- Engineer, the day after we disclosed all PII types lost, which did not include dates of birth.

How Did This Happen?

- I didn't check the database tables myself.
- I took my eye off the ball and didn't backstop my team-mate.
- The engineer who'd been put in charge of understanding the DB (not typically a backend engineer, and also not the guy who reset the password and went back to his barbecue) did not correct us at any time during our deliberations when we said what data had been in the breached DB.

Apply: Disclosure Basics

- When Running an IR You Should:
  - Always review personally the actual database table data (not a report on same) prior to signing off on any disclosure as to what was breached in the database.

OK… So, Let's Re-Group.

- The worst thing in the world has happened: we under-disclosed, loudly, and now we have a rolling disclosure.
- I call three reporter friends. They all assure me I am in the middle of a pleasurable act.
- I tell the COO and CEO we need to go full-tilt transparent; loudly. Get a TV and print journalist in the war room now.
- Unbeknownst to me, Ash has said the same thing.
- We're all agonizing. It's excruciating.

OK… So, Let's Re-Group.

- Finally, I say something that no incident responder ever has said…"Want the easy way out? Fire me. Loudly. I'd like you to pay me first, but fire me. I'll make sure we get someone to help run the IR."
- "Why would you do that?" Rick asks.
- "Because you guys all have to come to work tomorrow, and I don't."
- And then Rick said the thing that made me sure that everything he had said previously was the truth:

“Fire me.”

“No. That would give the impression that this was your fault. This was our fault. Thanks for the offer, but we’re not gonna talk about this anymore.”

-Rick Webb, COO

Ash Shines

- Ash gets NBC News and Tech Crunch to come in to the office for exclusives (TV and print)
- We give the reporters a step-by-step account, allowing them to speak with every executive, every staffer, and me; they spend time in the War Room; look at all our notes on the whiteboard. . .
- They're there for hours.
- We show them how we missed it. We show them the tables. We show them our internal memos, emails…

We Release the S… Schema

These are to be considered separately of one a…
number of breached records was approximat…

Type of Personal Data Combination	
Name, email, phone, DOB	
Name, email address, phone	
Name, email address, DOB	
Name, phone number, DO…	
Name and email addre…	
Name and phone …	
Name and DO…	
Name tota…	
DOB t…	
E…	

…nglish Description What this is:
…crementing ID number
…user ID associated with a user; this has been …n this table, and is public information
…e at which the record was created
…time at which the record was last updated
An authorization token that kept the user's session active. deprecated and no longer used
The email address of the user
The user's first name as listed in social media sites (not necessarily the person's legal first name)
The user's last name as listed in social media sites (not necessarily the person's legal last name)
Whether the user's subscribed to legacy Timehop email. Deprecated and no longer used. Historical artifact from when Timehop was a daily email
Whether the person has privileges to conduct some testing on local, native mobile applications

This Worked.

NEWS

Webb, imehop CEO Matt Raoul, th neering team and an
esponse consultant gave NBC News an exclusive play-by-
play on Tuesday of what happened in the hours and days after
hackers broke into the third-party server that handles their data
and knocked the app offline for an hour.

Webb said that generally companies balance the race to report
security issues and the desire to be transparent with being
conscious of their image and the need to make sure they have all
the facts.

"If everybody in the world always disclosed in 72 hours, and it was
routine for people to update later, then it wouldn't be so bad," Webb
said. "But because it is so abysmal from a PR perspective to keep
reporting, no one wants to be quick."

"It's a chicken-and-egg problem," Webb said. "So we were like,
'Screw it, I guess we'll be the egg.'"

ata

TC

To understand what happened, and what Timehop is doing to fix things, I spoke to CEO Matt Raoul, COO Rick Webb and the security consultant that the company hired to manage its response. (The security consultant agreed to be interviewed on-the-record on the condition that they not be named.)

To be clear, Timehop isn't saying that there was a separate breach of its data. Instead, the team has discovered that more data was taken in the already-announced incident.

Why didn't they figure that out sooner? In an updated version of its report (which was also emailed to customers), the company put it simply: "Because we messed up." It goes on:

> In our enthusiasm to disclose all we knew, we quite simply made our announcement before we knew everything. With the benefit of staff who had been vacationing and unavailable during the first four days of the investigation, and a new senior engineering employee, as we examined the more comprehensive audit on Monday of the actual database tables that were stolen it became clear that there was more information in the tables than we had originally disclosed. This was precisely why we had stated repeatedly that the investigation was continuing and that we would update with more information as soon as it became available.

Not with all journalists…

Timehop Inbox ×

Nick Selby <nick.selby@[redacted]
to [redacted]

Jul 9, 2018, 12:00 AM Reply

Happy to help arrange a conversation with the CEO, COO and me (I am helping with the incident response and would only speak off the record; they would speak on). Yep, you got it, it was bad. If you read the article here, I think you will see there's some interesting stuff and quite a bit of integrity in how they handled it. Hope it is of interest.

https://www.timehop.com/security/technical
https://www.timehop.com/security/

nick

[redacted]

Jul 9, 2018, 12:01 AM Reply

to me

No point. On record or nothing. This was an absolute catastrophic and unforgivable screwup, but so glad that people's "streaks" are safe.

•••

Nick Selby <nick.selby@[redacted]
to [redacted]

Jul 9, 2018, 12:03 AM Reply

I said that the CEO and COO would be happy to speak on the record!

•••

..But absolutely with customers.

- Revenues up 262% over 1H 2018
- Total users up by 370,000 since breach
- Total active daily users up by 65,000 since breach
- Engagement up (using whatever metric marketing weasels use to measure that)

Meanwhile, Back At The Incident Response

- Marcus is informing us of the extent of what's been accessed, what's gone out the door (that we can tell)
- Joel is running disk forensics on the boxes that we know were touched
- Timehop CTO and staff are doing a bottom-up assessment of absolutely everything.
- Rocky is developing a new logging and (more important) alerting strategy and preparing to implement;
- Moe and Ben have beefed up the LAN
- Mr. and Mrs. X are looking for leaks or drops.

Immediately Post-Breach

- Migrated employees to single sign on
- Migrated all accounts to TOTP 2FA
- Engaged Secure Ideas penetration testing firm
- Retained incident response specialist to help with ongoing security improvements
- Engaged security architecture & process consultant for ongoing security improvements.
- Radically expanded alerting and monitoring.
- Working towards security/trust scoring systems /SASE-type frameworks and verifications

RSAConference2019

Lessons Learned

Single-Sign On and 2FA is Important

- There is literally no excuse not to have this on every single web account
- There is almost no excuse not to have this on every single application you access

Instrumentation and Visibility are *everything*

- I cannot believe how many times I have stood on this stage and said this, and it's neither original nor novel, and yet…
- Get your visibility in order.
- Start with outbound DNS (he says for the zillionth time since 2010)
- Logging and visibility are more important than ever in cloud environments, where stupid happens at cloud speed.

GDPR is so much more reasonable than PCI

- GDPR does not tell you how to run your shop. It tells you that they will kill you dead if you hatch this up and breach.
- GDPR authorities seem more concerned with us getting our houses in order than shifting blame (Heloooo, PCI!) or fining people.
- The people we dealt with were reasonable, probably because we lived up to the spirit of the legislation. That's a good place to be.

Check The Data Table Yourself

- I am so humiliated by this.

RSAConference2019

Questions?

nick.selby@gmail.com

Have A Plan

- Review your IR procedures and get the Deltas between what you will need, and what you will actually have available, down on paper.
- There is literally no excuse not to have a retainer relationship with an IR company. Most of them offer no- or very-very-low cost retainers. Every dollar you spend in advance is worth $10,000 later
- Take advantage of your IR retainer: bring them in and tell them about updates/upgrades, have them run tabletops…
- I cannot tell you how many times each year I get called by someone with their hair on fire and an incident in progress and they're like, "Say, do you know anyone in IR?"

RSAConference2019

Thank you.

nick.selby@gmail.com