Armando Caro 9/23/15 1:00 PM
210-250-0559
Dill, Silver, Hemesath

reports - don't recall
payroll. - hourly pay rate for employees
Sr. Exec at the time. over employees

IT support for several companies
- San Jose St. Comp. Eng.
- comp IT support

since 1998
Air Force - Comm. Specialist, IT infrastructe
Clear Channel Comm. Email Eng.
worked 7 Director of Infrastructure

- Tribune recruit Manage Direct. Infra, ____ &
Security Operations

Day: projects and resourcing
new tech, improving, budgeting, best pract., testing
required for all Tribune.
Corporate position
LA Times included
23 TV stations
- managed overall, not day to day (operations manager)

Tribune CMS in 12/2010
P2P was one (Power to Producer)
required log in w/ credentials
- employee of tribune and need for access
ID's managed by PZi not corporate

2 logins and 2 passwords to get to P2P
yes, function & security - mattered to his team.

Deface LA Times

report malfunction of posted article.
- originally user error was believed
- looked into it - renamed CHIPPY LEET
investig. further, title changed
- who changed? login from user no long. employed.
account active, external point
- targeted attack not sys. malfunction
- determined hacking.

Google CHIPPY - on forums, code published about
website - bragging.
- researched - IRC - posted in forum
given to FBI, Dylan & caro found name in IRC chanel

Caro:
- close account, checked accounts, logs, reset passwords
- mitigate again
- proposal to fix

hourly rate: salary $180,000
~ $75/hour

hours spent on incident?
40 hours estimate (his own time).

Direct incident response:
40 hrs to track and find CHIPPY LEET, lock door
20 hrs direct response to hack. Managing responders

Architecture work:
- weeks and months - 40% on security for 3 months

Kulesza, Rod., PZP team (Matt LNU), Tad Lin
LINUX team (lady manager)

Kulesza was in IRC chat. loiter to see what was said.

- coordinating efforts, who they needed, approved changes, reported VP above, VP of Software Develop. Status updates activity of these responders, coordinate w/ FBI.

- Took away from day to day work, changed it completely.

- does not remember anything like this.

Now: Capital Group – Equity Management / Mutual Funds
Sr. Assistant, Automation, IT development
July 2014

Before: consulting IT Cons Frontier Comm.
10 months

Before: Tribune

Left:
bankruptcy caused change, didn't like financial outlook.
wanted stability

- Didn't know keys

- Bonus tied to overall performance, could possibly include appraisal work on incident.

- $60,000 approximate bonus that year

Sam Cohen 9/21/15 7:00 pm

847-436-0374

* Send email for contact

Paul, James, Dill

Sam - flexible - Available most next week

Aka's Scholbrock

Exec. Prod. Dig & Social Media ABC10
7 mths

" " Dig Content FOX40
Started Oct. 2010 - .7 months
Senior Prod. Morning Show Aug 2009
Producer Salt Lake City, UT

Ed:

Denver, Northwestern, Chicago 2004 - Journalism

Scholbrock in Tribune system, can't change
username: sscholbrock "propably"
change 2009
login, email, CMS stayed scholbrock

Do?

respons. news content for AM show, wrote content
posted to social media accounts / website

Change:

Web producer, manage website & social media
- unknown if $ bump at the time

Matthew Keys had position before met Aug 2009
* trained on CMS prior
his title possibly One and only web producer

over Keys at a brief period, only person
- filled his role after he left.

Relation:
daily - M-F, close proximity, shifts overlap few hours
- good working relationship
- not very social

Fire at galleria mall. 40 went on air, stayed on most of day

Thurs: PM swapped anchors. Keys felt AM didn't handle well. Mercer & Keys argued. Shouting, heated. Keys left. Mercer then asked to switch to web immediately.

Fri: Next day. couldn't log into FB. no access weird. Admins couldn't log in.
Mercer was contacted. Long time that day to log
- Asked about Keys - informed no longer employed.
- no lockout known, from Mercer later.

Other probs?
After fired? Handful of FB messages.
social & prof. -
hacking - asked if they knew who did it?
↳ Dec 2010 > "contest, person hacked, email contestants" "harassing"
received emails from contestants
he asked if they found out who did it

comp. problems:

- couldn't login to CMS. couple weeks of problems. corporate would reset, work only a few hours new account, had problems w/ 2nd account end of 2010, couldn't do her job

$ salary / hourly - will look up

multiple days - lost couldn't work
only work 15 mins per day
5 days best estimate, wasted on problems

What could they do?

- manipulate website, content, words, layout images, text
- access w/ her account to contest sign ups

- no access from Europe, proxy, VPN
- no overplay

PZP = CMS >same login/password
Tivid = video server
- necessary for her job

Ryan helped w/ PZP problems

emails - negative work ~~etc~~ atmosphere
- weird feeling.
- no control, helpless, unnerving

iPAD contest

Tom Coming 9/25

Paul, James, Cauthen, Dill
• 630-750-4258

[Arrive Tues night 10:00PM
Leave Thurs 1:45PM

Thomas Arthur Comings

Ent. Archit. Tribune Publishing
20 yrs tribune - 1995

-prior Sr. Engineer
~2002
- "Engineer" maybe before

Bookstore inventory control before Trib

UIC - some college

2010-2011 - Sr. Eng w/ trib co.
located @ Chicago, IL
controlled papers and TV stations
• supported digital websites for those media

worked on CMS systems they used
• create ; edit content that appears on web
editors for each site had cms access.
2 used - Assembler - both edited same sight
P2P -
• login w/ credentials. search for story

Needed to login: employee and right group

"edited by hopper"

· hopper is a feed component, automatic (business logic rules)

Incident in 2010, asked to look into compromised
LA Times story.
mid-Dec. – email Dec. 15
in email Assem. screen grab.
w/in URL – only ran within network
content item ID – "slug" LA-DM- -1215
story in feed.

b/w 3:45 4:29 (central time)
user wasn't authorized to make edits at that time
3:49 Nonassem user determined
· IDed IP it came from
Asked to go look at logs (typically asked)

direct access to server for logs
- live files, no compression

Big deal to them. Significant event

prob. wed 9:00AM usual start verbal notification.

2.5 hrs work contained in email

[P2P has different layout log. Edits happened in Assembler
-had to look at P2P first, then found in assembler.
-into servers, logs, review, search date & times.
found IP – lookup (Ireland) – gathered for email

subsequent after email – conversations/how to fix

b/w 2.5 +2 or more – 10 hrs. * can't remember, will try to find.
"5" hrs "6-8" hours
"1" hr day before "10 hrs is accurate", plus maybe more
BOTTOM FIGURE WILL THINK

* recall that report from mobile vendor, story stayed defaced until the next day.
  - had to get mobile vendor to fix. devices/mobile vendor couldn't get updates, stayed GARCIA edits
  - worked on it, pulled up mobile version (viewed it) sent it on to others to verify

spent time resetting passwords, only those w/ active emails could do it.

- servers in LA - traffic all over country & world.
- access from Chicago and the bay in from Ireland.

- very serious breach, reasonable/proper response.
  - didn't understand how or defense, then a change can happen at any time.
  - it can affect their reputation

* they could change stories from one year ago and go undetected.

- checked perfect market, check so the archive was cleaned as well.

Shaun Davis 9/23 10:00Am

- Citrus Heights

Christmas prep - Aug/Sept 2010

competition - victo game system, great if won Christmas gift
finalist email, suspicious
works for Apple - still w/ them
sent gen. reply, ask for pirsonal details
replied to email, addy wasn't FOX40 addy

- received 3-4,5 emails from suspicious addy
maybe more - SPAM filter.

tarnished their rep, stopped activity FOX40
concerned lack of security

Jerry Del Core 9/22 2:50PM

Segal / Silver

Bio: Station side radio/TV since 1977

NY, PX, BO, Raleigh, Austin, Sacramento

- unemployed

VP General Manager - $275,000

overall op of station, protecting license, cash flow #'s

COO Atalanta Bustos Media Radio/TV, Sac being sold

in Austin, TX. Traveling back to TX on weekends

Keys: intro to staff, not specifically

met in walk through, no specifics

2 levels below - Mercer

fired for tweeting from news room. insubordinate

packed up over weekend. called in sick.

Mercer - talked, showed tweets, jaw dropper

called legal, Brandon sent home, legal cleared to fire

called in sick. cleaned desk

he's reached out, blogger, tries to get inside scoop.

asked about Rville fire

Brandon had dialogue, he wasn't a part of it.

Rewards

freq. f * Started before Del Core

company - do sales. + Group deal to restaurant $50 for $25

Name, Addy, CC #.

x rounds of golf - $100, 5 rounds of golf

+ 20,000 accounts

< 3,000 switched over to new database
3 yrs to get back to 20,000

Del Core created sheet
pieced by as many as he could remember
1-2 yrs after the fact

Time log - outlook calendar

conservative on #'s - salary

Friday 11:00 Am

unsettling - someone could hack station communication.
reputation was damaged
serious. called the FBI.
high = ID intruder
didn't have internal resources to do it. knowledge.

Dylan Kulesza 9/24 9:30 AM

James, Paul, John, Matt

- never met Keys

Dylan Thomas Phil Kulesza

- Director of CISO Service Delivery
  Optive Security
  ~~Kan~~ KC, mo
- remotely, travel to job sites

- perform sec. assessm. posture, improve to add. threats
- provide CISO services if needed

2 weeks

Before:

Tissora Corp. oversee enterprise architect.
6 weeks • voluntarily left

Tribune
VP of Engineering, Security, & Architecture
- oversaw enterprise archit. / biz applications
  * account payable / receivable

2011/2012 reported to Arcangelo as manager of Cyb. Security
- then changed to reporting to someone else (2013)

Left 2015, joined 2010 March

Educ: Bach in Manage Infor Systems - 2006

Before Trib
1 USAA -
2 Clear Channel Comm. now (I heart Media)
Tribune Co. - Tribune Publishing / Tribune Media 2014

Tribune spun off. Publishing left.
by choice, pursue job in S.A., TX

2010 - Salary - $105,000 (minimum)
no more than $20,000 bonus if received

End 2010 Security
Largest incident - CHIPPY 1337 hack.
website defaced, under 1 hr.
outward incident was significant
jeopardize brand, reputation

informed by Caro or T.Rod./prob. Caro bc his manager

team started to triage incident / exposure / risk

in Tribune San Antonio office

Role: ID source of attack

Teams
#1 imc. recover / restore content - how to minimize access
#2 research how someone could have accessed system / breach website

- how did break in, how did they identify assets, what measures to do to prevent.

example
role: police showing up = needed to make sure no one is in house
they still in, backdoor access, changed settings leaving access
- time & resource spent to check system
~20 hrs - several months
super user isnt easier, only if no longer w/ company

— time spent was 20-60 hours in initial response
how someone broke in? 20 hrs - following weeks discovery
work for who broke →

Activities

1. work w/ teams to capt. security logs
   super user or normal user mode changes
   took > time
   "where from? how they get in? level of confidence of found access or person of trust? brute force."
   - logs = web access logs IP addy of who connected
   - LDAP authentic. logs – captured usernames
     ↳ P2P system. = Assembler
     queried for changes, manual work to pattern or trend attempts before if targeted or calculated.

spent 4-6 hrs review logs / user accounts of employees who no longer work there. shut down all accounts
12-18 hrs how did they get usernames & passwords
Google – understanding CHISPY 1337 and Tactics
- chat server - used by hackers. spent time in server to understand actor - get comms if they talk about breach.

* knowing who hacked and the risk they pose how they could do it again / knowing their tactics in order to properly secure the system.

- recomm. and deployed the upgrade
  for more $ and time for this
  - comfortable knowing more than likely that intruder had usernames & pass's for employees.
  - needed view into overall security posture of organization
  - others may try this if he shared w/ others

- AM to PM – IRC monitor, worked it at home when left and into the next week to a
  11 hrs spent on it.

- friend that has experience helped, not paid
- time could be understated on sheet, not documenting time spent on finding info on who did it.

* 10+ hrs + multi months, signif. resources to upgrade.
  - formal process
  - this event caused all upgrades

IRC - used IRC in past, familiar w/ it
program to connect to server, comm. b/w people logged in.
very fam. w/ dialect/lingo used
IRC channels = used to connect to certain people, like rooms
- can be in diff. channels at the same time.
- set up servers, done before 15+ yrs
- overall it hasn't changed much.

MIRC client used at the time
IRSSI = Linux, used Apple IRC = pigeon before
"priv" message = private communications

Principle Security Engineer 2010

8/28/15 1:00 pm Conference Call

SA Chris Dill 916-486-5520
SA John Cauthen 813-253-1005
AUSA Matt Segal > 916-554-2708
AUSA Paul Hemeseth
DOJ CCIPS James & Silver 202-616-2644
Timothy Rodriguez ~~312-471-7343~~ 224-315-7343

1:03 pm

American College of Surgeons
- medical learning institutions
- learning
- collect data from hospitals
- S.S. info for trauma surgeons
- Security Analyst / Egineer (IT)

47 y/o
1995/6 in IT sector
- TripRight - Tech support
  - phys. comp
  - network / servers
  - securities
short compliance 6 mos.
- Auditing
- IT sec. windows / linux
MPK 001 - he wrote
- consulting now @ anytime
billing thru consulting co.
~~$150~~
$150 - 250/hr
this → $250 b/c heavy skills - forensics, SANS cert's
knowledge pen testing / digging through

Tribune Co. Media - split into multiple.
LA Times
2011 - 2012 - 2013
$105,000 salary starting plus benefits
Interviewing day after it happened
Jan 1 or 3, 2011
Armando Cruz gave him this project
MKP 1513
- Dec. 4 meeting - not attended
- Diane & Chris Phillips lead meeting
* didn't work directly w/ editors and comp ppl (LA Times site)

Jan. 4 - second day (received it)
- still looking @ network
- no DHCP, IP etc. trying to find if ongoing
still damage assessment

LA & Tribune set up different internally
diff. security postures
- share email system
- board of trustees
- semi-autonomous -

TIGER team - non-exec's - Technical ppl
Armando lead overall
Rodriguez lead investigator
2,900 applications - figure out weaknesses
ex. if sys. egineer left or compromised then how to exploit over all shared systems

- weren't confident it was all over
had to prove they didn't still have access

- integrity needed to be guaranteed / no tarnish of company

- task Is this over? yes?
- linux based systems.
- windows
  - checked ID's, look for change, only by legit users.

Jan. – March or longer ← compromised user names
100's of servers Assembler, Oxygen > systems
- mult. tasks by tribune. workers
- didn't bring in outside help

Armando Caro might have quote of outside work
~ $100,000's (hundreds of thousands)
initial investigation $17k #'

review system for article and ~~posting~~ bylines
Tom Cummings
p. 4 TimeLine - assembler . CRV
582664801 - who made changes / track user

Cost Spread doc. or Pg 10/11 of report

Preventative - found issue, prevent reoccuring

Software/Code/Redesign - redesign and testing of systems that were ~~edit~~ changed

Investigative - ppl who worked to find info, go through lo
users, user ID, IP's
*damage assessment

made chart - T. Rod.
Armando Caro pulled hourly $

---

emergency for Tribune - LATimes had lots of threats
hackers, email threats

emergency ended after manual review to make sure

weeks or months and wouldn't have known
through~~t~~ March

initial incident only
2-3 other reports after this one

1/25/2011 - one document after that

Post incident write-up - not mandatory

4USA — Armando Caro emails 2011 to find info
emails primary source of communication
weekly email updates

Armando - gone
Dylan - gone

broke into other servers

All security events @ tribune
- CNC incidents

- this was highest priority while there.

- compromised integrity of institution

- could have edited plates for actual printing of paper

hack - loss credibility among other ~~...~~ news organizations
- change public confidence of product
- substandard if can be changed by anyone
- can't untarnish

Jason ~~Potkanski~~ Potkanski - PHP - put together how it could have been done
Tom Cummings - IDed which by line was edited in applicat
Sabrina Downard
Grey Hancock
> gathered logs

MKP-0102667

Richard Benjamin
Diane Yamazaki > still. may be @ tribune

certs: ↓ before tribune

SANS Cert. Level 5 Auditor -abnormalities
Cisco
Checkpoint

other major networks published causing loss of face

Wayback machine forever there

8/28/15 1:00 PM Conference Call

SA Chris Dill - 916-484-5520

SA John Cauthen - 813-253-1005

AUSA Matt Segal > 916-554-2708

AUSA Paul Hemesath

DOJ CCIPS James * Silver 202-616-2644

Timothy Rodriguez ~~312-471-7343~~ 224-315-7343

1:03 PM

American College of Surgeons
- medical learning institutions
- learning
- collect data from hospitals
- S.S info for trauma surgeons
- Security Analyst / Egineer (IT)

47 y/o

1995/6 in IT sector

- TripRight Tech support
  - phys comp
  - network / servers
  - securities

short compliance 6 mos.
- Auditing
- IT sec. windows / linux

MPK 001 - he wrote

= consulting now @ anytime

billing thru consulting co.

~~[illegible]~~

$150 - 250/hr

this → $250 b/c heavy skills - forensics, SANS cert's

knowledge pen testing / digging through

MKP-0102670

Tribune Co. Media - split into multiple
LA Times
2011 - 2012 - 2013

$105,000 salary starting plus benefits

Interviewing day after it happened
Jan 1 or 3, 2011
Armando Cruz gave him this project
MKP 1513
- Dec. 4 meeting - not attended
- Diane & Chris Phillips lead meeting
* didn't work directly w/ editors and comp ppl (LA Times site)

Jan. 4 - second day (received it)
- still looking @ network
- no DHCP, IP etc. trying to find if ongoing
still damage assessment

LA & Tribune set up different internally
diff security postures
- share email system
- board of trustees
- semi-autonomous -

TIGER team - non-exec's - Technical ppl
Armando lead overall
Rodriguez lead investigator
2,900 applications - figure out weaknesses
ex. if sys engineer left or compromised then how to exploit over all shared systems

- were it confident it was all over
had to prove they didn't still have access

- integrity needed to be guaranteed / no tarnish of co

- task is this over? yes?
  - linux based systems
  - windows
    - checked ID's, look for change, only by legit users.

Jan. – March or longer ← compromised user names
100's of servers Assembler > systems
- mult. tasks by tribune workers Oxygen
- didn't bring in outside help

Armando Caro might have quota of outside work
~ $100,000's (hundreds of thousands)
initial investigation $17k #'

review system for article and ~~posting~~ by lines
Tom Cummings
p. 4 Timeline - assembler . CRV
582666801 - who made changes trash user

Cost Spread doc. or Pg 10/11 of report

Preventative - found issue, prevent reoccuring

Software/Code/Redesign - redesign and testing of systems that were ~~was~~ changed

Investigative - ppl who worked to find info, go through to users, user ID, IPs
* damage assessment

made chart - T. Rod.
Armando Caro pulled hourly $

---

emergency for Tribune - LATimes had lots of threats hackers, email threats

emergency ended after manual review to make sure

weeks or months and wouldn't have known
through~~t~~ March

initial incident only
2-3 other reports after this one

1/25/2011 - one document after that

Post incident write-up - not mandatory

AUSA — Armando Caro emails 2011 to find info
c emails primary source of communication
weekly email updates

Armando - gone
Dylan - gone

broke into other servers

All security events @ tribune
- CNC incidents

- this was highest priority while there

compromised integrity of institution

- could have edited plates for actual printing of paper

hack - lose credibility among other ~~[illegible]~~ news organizations
- change public confidence of product
- substandard if can be changed by anyone
- can't untarnish

Jason ~~[illegible]~~ Potkanski - PHP put together how it could have been done
Tom Cummings - IDIO which by line was edited in applical

Sabrina Downard
Grey Hancock } gathered logs

Richard [redacted] Benjamin
Diane Yamazaki > still. may be @ tribune

certs: ↓ before tribune

SANS Cert. Level 5 Auditor - abnormalities
CISCO
Checkpoint

other major networks published causing loss of face

Wayback machine forever there

el cure
Nove
10/9/14
2
12/19/14
+ More

Jerry Del Core 9/27/15

my worksheet from after BM left went outlook & made estimates.. "whole incident" cost. The biggest # is from database & what was done to it.

I had access to BM's emails but not his calendar. I did it off of emails.

Dept leads at Dept mtg.

DH's → Darren Sherman CFO 300K
Davis, Jack 90K
BM
Laurie Masica 150K
Phil meldeno 150K
Del Core
Saunders, Greg 100K
Misty Dvorak 75K
Caroline Shirgene 50K
Karen Hoffman 40K (sick)
Ray Nelson 8.5K
(program mgr) Bill Gee 45K

std weekly Dept lead mtg. - updates.
45 — 1½ hr. → [½ dedicated to this issue. — There were lots of ?'s.

1/6

MKP-0102676

Responded appropriately cuz they could have really bad effect & it affected loyal viewers. If you lose loyal customers, it can change our sales - our most important customers.

I was in the mtg - Bm & I had weekly ones on the mon 12/6 w/ the B.M. + + and w/ the FBI. in the mtg going through with everything.

Bm had most if not all direct contact, as we discussed it Bm was POC. but reported to me, so we did discuss our responses - Bm try to get more info. by FBI, but also cropped by legal dept or ourselves.

We contacted FBI cuz he was smarter than us, but not FBI, I decided to prosecute him even before FBI, cuz we needed to know who, once we know who we wanted to prosecute.

We wanted to know who for Business reasons.

MKP-0102677

when target expanded to Tribune
when it expanded then corporate
really got interested. I'm not
sure they would have really been
interested if it was just the
11 c.l. station. but once it went
corporate target, it got corp. attention
Jack Davis & Ky Nelson were
the technical people.

I read the emails - most
at least. → be specifically met
about some phone calls from
furious customers. -

Sam Olen. I read emails
o estimated cost based on lower
salaries. → not producing for
a week. → she was very intense,
great employee.

Charlie - Sr. VP. of News
big clout from Trib.

Golden was head of IT.
at Trib.

vaguely remember this mtg. -
happened when we talked about
Fox Mulder event. - Before we
even knew about the LA Times

Goodwill - value of benefit company gets the doz right thg.

Dec.
Gale

Foxmulder & Jeff Emil. → Keys reached out all the time.

---

on release → 1st calls
call with record member.

(Schonbachs call my be double counted, → but there were actual 3 calls. → Schonbach included by weekly calls with him.
then there were separate calls as well.

Jeff, Kertz, Schonbach my be reflected on that page. - not sure.

~ 50 in total. (275 plus $50K loan)

mtgs. → 4 1/2 hours. @ 150 hour

total $325K.

→ Based on status & co performance last yr. 2010.

MKP-0102679

orig s.

{ $325 subj → 3½ hrs.

emails / conversations

phone calls. → Keith / Shobek (3/2)

(5/6.) → recently (10/81 hrs)

No (less.) info (people complaining based on format in emails.)

Thurs briefs & phone calls on

with of Dec 1-6

2nd Pkg come up, There are

a fallout cost

→ onto contract

→ start new contract

are that in 11.

1.) Try to figure out extent of the interest. That's why we talked with customers.

2.) Also, consider how much more we lobby for

could you have delegated.
- I did but he needed direction.

No technical experience, —
I'm responsible, I'm trying
to keep an license.

Q5. →

JERRY DEL CORE

BIO

Radio + TV since 1977
NY, Phoenix, boston, Raleigh, etc.
FOX40 fired him b/c boss didn't like how he ran stn

2010 Hired as VP/GM Salary $275K
Resp: overall op of stn. Protecting
Licence. Stn delivers cash flow #'s.
To Tribune.

Prior was COO for another media co.
Ran Sp. language stns. in Austin, TX
"Border Media" RADIO

Prob met Keys when intro'd to staff.
Then met him in a walk-through.

How many levels btw? Keys rptd
to Mercer, Mercer rptd to Del Core

What keys did needs to be addressed
Heir a little asshole. Biggest thing
was he was tweeting from Newsroom
how bad coverage was of Roseville
College fire. Insubordinate.

Brandon showed DC Keys tweets.
As GM, it was a jaw-dropper.
Unfathomable. NOT the place/forum.
Didn't kn why anyone wld watch.
Embaressing. (GYST)

Fox40 called legal. Brandon sent
K home. Said talk next day
(to fire). K called in sick.
Then cleaned stuff out. Term'd
over phone.

✓ K has reached out to DC
re DC's firing.

Rewards Acct

Like Freq Flyr Prg. Reward Word.
Groupon $ ≈ how many members?
~ 20K. Was in place when DC
sat there.

two purposes
- Ratings Fox40 was btw3+5, except late news
- Revenue 2010 was high b/c elxn

What was K trying to do? Tell customers their
info was compromised.

Why such a big deal? Hyge amnt of distrust. Like Target breach, etc. People don't want to do bus. Had 20K people who cared a lot.

↳ when xfered, it was opt-in & only 3K went back in. Took 3yrs to rebuild for 20K

K may have kn real dmg, b.t not sure b/c not sure how smart/mean K is.

VALUATION

DC made it. How?
1-2yrs After by looking at email

It's not in here if it wasn't in Outlook email or calender entry

↳ whatever it was set for in calender

SAM COHEN EST: Tried to be conservative

Fox Mulder emails were unsettling

- Severe cld health sfty comms
- Scared of potl for more damage
- Product/Rep'tn ~~dmg~~ damage
- Speculation who/why. Very important to figure out who did. That's why called FBI. People need to know they can't. Plus wanted to ID intruder to re-secure system. Fox40 cldn't do on own.

Don't do the intro

design

Where's the Page attempt?

Sam Colen "coincidentally"

↓

Almost like...

he was

Prediction but that

Don't adv. $ value of edit control

Wins — who worked @ comp.

Thurs: 6pm -

Interviewed replies

Problem for the station.

Keys Responsible

Security at station

↳ Personal files on Keys. →

~~###~~
916-

IMPACT ←

Records on keys

Interview

Gerald "Jerry"
~~Jerry~~ Del Cole

9/20/57

1241 Carter Rd.
Sacramento CA 95864.

916-612-1422.

2 Things happened. → Stations

Rewards Account did hacked

& emails sent to members.

Says there credit card &

personal info was comprimised

MKP-0102687

There concerns. -

- Complaint from customers.

- Financial Impact - Lineral needs to be done on that

Revenue Alc - viewers into like Lequel, Algen. - watch news casts & if they get the words they get prizes.

We do that so more people watch us so we can sell more advertising → we ask for C.C. so they can make purchases. - like Group On deals.

Gearing with people, → went sideways after that. - The model has pattern on it, I need to clarify a fact.

(SCOSPHER)
→ Emotional - got people involved.
rewards program.

- Some employees were upset
because of the problems w.r. the customers.

corporate legal involved. →

M.K had the "skill set"
"SMART"
on "Digital expertise"
& Angry - terminated
the case.

1.) Knew about how to access peoples accts.

2) All his access would have been removed, That's S.O.P. → not digital guy.

[→ Roy Nelson -]
I.T. responsible.

3.) Why terminated the case
- fire at Roseville Galleria

MKP-0102689

Telling us that our college
was the "poorest in town;"

→ He was in trouble already.

<u>Human Resources</u> → Can get then

[redacted]

☆

[illegible]

[redacted]

12/15/14

Kersting - CEO of Tribune
College Tokens - requesting
update →
Raj Shoubak - COO →
(San Diego)

Greenlink - wave of data,
e-mail contact list →
inputted D.B. →
people put in VISA or CC
#. Those people cancelled
transaction - we (Tax)
lose of revenue
loss of 28K people
risk 3 years to get re-bill
w/ another co. -

effect of buying these programs.
net loss — 200K
each person $10.00
we lost it, → it took
years to build the database
(e-mail list)
$25K. → sell program
to advertisers we would
send messages to the
database, (value to advertisers)
– we also sold – things eg.
"Golf cards". → people
would buy $2500 card
to go to golf course
to play golf at golf
courses around town.
– That went away.

News Ratings — declined.

$163 million is

size of the market

11. = 1.6 million

The database went away.

The reason for Rose

people to watch

went to do went

away. The motivation for

audience went away a

ratings declined.

[out of 20,000

only 1,000 were

retained. (5% retained)]

Not root of all Nos
= 929K.

Client trip
(Mon 4-12.)

Samantha

Cohen

10/9/2014

9/27/15

Samantha Cohen

I made 50K/YEAR
(47K SS waiver)
at time of incident.

Samantha Cohen.
847-436-0374
05/16/82

4404 Ulysses Drive
Sacto CA 95864.

1) Executive Producer of Digital Content.
Started this 26 OUT OCT 2010.

2, I was hired August 2005 as senior producer for morning shows, helped with web. outside of Matthew who knew most about website and social media. when MK was terminated I moved into his spot. we were already talking about me managing MK. prior to his MK termination we were congenial nice to each other. we did go for drinks after work. After he was terminated, it didn't really Δ. I didn't reach out. I was there the day he was terminated. We did stay in contact, over Facebook, careers wise, etc. still congenial.

webpublishing program - "P2P"

sschilbrack. - user name. Other people came for help on how to use system. after Keys left, they did give me user name & pw. - before that I did with my user name.

MKP-0102697

After MK, I wasn't an admin. -
Things were rapidly Δ'ing - a couple ~~weeks~~ weeks.

He locked us out of our a/c's
I knew that the next day. (Facebook & Twitter)
1st I logged in as me, I could mark the story w/ the d.d. -

If someone had trouble I would help.

P2P — Text
assembler } same login
Tivid → VIDEO.
→ Text (thrown into P2P

After Green Army Acc
Dec 6th I couldn't access the system.

The only a/c I used was sclolbrol.
I don't recall any test user a/cs

I use a MAC, → Personal P2P
ISP was "Comcast"
making admin level. -
then taking away

After the 1st, I don't recall any problems.

1.) I don't know how to access my user A/C. - if I don't have access.

~~I don't remember~~

what cases pay. -> Those are with the PIP system.

& logout of page. it's the commands you have access. to email content & stories.

I didn't attempt to log into the A/C via proxy server in Europe. If at him, it would be concern, if at home it would be the N.bum (sic)

I don't know how to use proxy servers.

test 1234 # Ø Dan H loan

Eventually I switched back to sscholbrock

did not log into foxmulder 4095

Email problem:

(Big Impact
Mixed Pearl to quit
time consuming.)

lots of time.

never Did find out what caused my a/c to be logged.

whenever developments of story came out I wrote stories about it,
I felt I did due diligence. → There are stories.

Andy Soto

1/6/15

1.) Andy Soto

3/9/74

2.) 858 - 243 - 4420

95oto 6201 eh.ymail.com

1. Registered @ Fox website.
Don't Think I put
my cc info in.
name, address, phone.

Got weird email
back.

email'd Fox to
express diss content.

They sent back saying
"Sorry".

I didn't opt out

damage has been

done. Never participated

in any other of

This promotion.

my view of of

Fox40 has decreased

in part to this

incident. Their credibility

went down.

"Mon Afternoon"

after 4pm until last flavor

Shaun Davis

1/6/15

1 Shaun Davis

7/8/81

~~6016~~

Sdavis24 @ mac. com

Remember Being a customer getting the event. looks like a scam. people get hacked all the time.

I didn't post it at that point. Vulnerable

Brian Hanrahan

11/24/2014

HANRAHAN

Today works for company that does classic car auctions

1980 - 2013

Copy editor
Page designer
Writing
Mostly - editor
Was @ LAT 23 yrs ; 33 yrs in business

Editorial control hugely important. Unearthed very bad.

You choose a public paper b/c brand.
History of trust & credibility

This is related to edu / circulation

Esp. in online world - clicks measured.

Hanrahan was chief of Morning Copy Desk
Started 6AM. Read everything that went on the web site.

Manage grp of editors who read stuff.
Often 1st & only

If print, another round of editing.

Henriken wrote/approved headlines.

Tribune Wash Bureau. Group of rptrs, many were @ CAT pre-Trib. Then shared btw all Trib papers.

Wires: AP, Bloomberg?

H's group read staffer/freelancer stories Sometimes web group w/d put up wire stories w/o Henriken's group.

Import of own staff stories. Try to get things right, factually, details, some checking, some fact checking.

2010 workflows were evolving from print.

Reporter → section editor → Henriken → web

(or)

Reporter → Henriken → web

2010 – cont so on Web site w/o Brian H.

use of CMS

At that time, didn't go directly to publish b/c getting things right takes time

You need to have a 2d pair of eyes for anything pbld in a legit news org

spelling & grammar, too. Show care

Procedure to / Promote on google
↘ promote w/in paper

These controls relate to informed citizenry in a democracy.

CMS — Had 2. Assembler was used by web site for designing + fixing things on web site.

First Noticed

2PM noticed. Night people took over, so he went back to things they'd done to check on.

Clicked & story was Altered. Headline & content.

How alarming? Very. B/c it was H's responsibility to make everything right. It was on him.

BP ↑ way up. Stunned b/c never saw.

Went to web site producers. Thinks story was linked on home page.

Changed link b/c wanted fewer readers to see.

Then H went into Assembler

How much of Hanrahan's Time?

Fixing & dealing aftermath. (1hr) 1ST day.

Also wanted to find out who did it. Cooked e logs to ID users.

Saw a new name.

15-20mins identifying user name & doing search on Trib employees.

Checking w/ dif. people in news room & telling what happened. Fixed text. 10-15mins

~~4~~ versions were:

1 CCI Newsgate from West Bureau

2 exported to website (Assembler) & Auto Published. That was live

Henriksen put CCI Newsgate version in Assembler by manually typing it in. Wldve taken layer to restore electronically.

↘ But it had been worked on, prob. in headline, in the interim.

↘ So Henriksen isn't confident that it's exactly the same as it started. Word-for-word? Cant say. Close. Depended on Hs memory, not the computers.

CCI had a backup, but complicated to access. Possible the org still existed

Screen grabbed the altered story to preserve a record.
B/c security issue needed to address, figure out why, & make sure not again.

In 33yrs, how does this compare? Probably the biggest incident. Was editor 33 yrs. Was site 7yrs.

Worst outside breach of security in 33yrs. Never possible w/ newsprint.

If people did this to retaliate against stories

to

Can't say dollar value it's worth.

If hacker had charged FP, w/drive more sensors, more noticeable.

626-798-1535

(v) Found it. Brought it to
[illegible] attention.

↓
not yet web producer.

↓
Tenny Tatusian → (I told her
↓ web manager. about it.)
Jimmy Orr (Assistant Mgr of website)
↓

Dan may have been there.

I don't remember if my group
edited the story

This is bad, bright to people
attention → we need to fix it.
it was me.

"Chief of Copy Desk"
&
moving Copy Desk — we
handled edits on the
website — 6 — 3 pm
A.

& http publish → I was
using CMS (publishing) to make the
Δ's.

Very important → very big deal that this happened. makes LA Times look stupid inaccurate & incorrect.

This is to figure out who did this. We spent alot of time on this.

Fact that story was allowed to be because we didn't have so many checks & balances. To prevent bad stories.

Back in day we are instilling a culture of big stories. Once you publish, it's published. - if error, publish correction

So making a $ is more than just clicking a few buttons.

- permission
- culture.

in theory I could do this
easily. But the process needs
to be followed.

Many e-mails but a lot
of this has to be verified
even corrections to officers.

I have never seen a track
like this or it never
happened again.

The protocol back then was for me to go into assembler & fix it, & Republish it. It's not terribly difficult to fix the story.

ed. [illegible] with CCI newsstr which was used to export to assembler.

Tim Garrick was home producer of [illegible] page [illegible] [illegible] home before the [illegible].

I'd [illegible] stops - depended on which copies we using at time.

→ brian.hanrahan@ymail.com

4/22/60.

Left LA Times 2013

Valerie

McCann/Ellsworth

Valerie McCann

nee Ellsworth.

→ 916-862-6090

(w) 483-9064

7/19/69

barbieval@sbcglobal.net

entered online Fox 40
Rewards. to win an
iPAD.

→ I saw I
one 2 to call
station. - person,

never knew about
this assumed it
was a hoax.
still watch Fox 40

Armando

Caro

1/10/11

1. [illegible]
2. # arseta

Armando Caro 1/10/11

1/6/76

User → anon1234
pass

CMS → content mgmt system.
system all published articles and
where you, Titles, byline, modify articles

- not advertising -

[illegible] in permissions
what stages can [illegible]

assume, [illegible] interaction

video → upload to post on website.

← MercuryNews.com → [illegible]
content dev (reporting images [illegible])

- Lakers
- Chicago Tribune
Balt Sun
Orla Sent.
Hartford Courant
& others -

Dylan
Kuluza
Notes
3/16/15

3/16/15 -

Dylan Kulega: 6/1/83, Through Jeff Glasser

- Senior most person who knows about the Tribune Report.
- at Tribune for past 5 years
- V.P. Engineering & Security (past 1 yr.)
- In Dec 2010 I was princ. security analyst, (pretty sure)

→ Logging services → After the Keys incident with LA Times, we invested $ to better provide security. Logging was performed individually for each computer.

→ Assurance Expert = TAD (?) all user request went thru LDAP server, for someone got into system, it went through LDAP server. The logs let us see user activity

→ The web server captured external IP. address, in conjunction with LDAP.

Tribune Report. — I helped peer review the report, I can't remember if I authored any of it, but I likely helped shape it.

→ Teresa Rodriguez & I were peers

→ There was 2 lists of (One Lois Dillon lost) →

I spent at least 10 hours on this

immediate resolution to deal w/ compromise, remediate compromise, & get back into business or run

I bet talked what threat compromised us? How.

→ Threat analysis.

– research ch pp 1357

~~[illegible]~~ online research

Damage Assesment. → hard to determine damages to brand.

→ I spent my time trying to figure out the level of Threat - online research - my 10 hours there

- but I also spent time not on the report. (we performed a risk assesment, controls in place to address the risks;

. Time-sheet (we kept Time sheets. → Specific for this incident.

→ Accounting for this Time sheet we provided by Jim Rossiyeg.

→ ~~we don't have~~ not all the people on the report, in the kept their time sheet as Dylan Kulga.

→ How we track time:

All in IT Dept. - (Only IT tracks time.)

If a breach - we assign time to "Unplanned Security Incident" & we work on it. Assigns Time & Ref Bucket.

↳ The Time doesn't break it down into specific incidence.

Concern Facing Threat increases a security Report. Such as the one we sent to FBI.

(Frequency of reports? —

A: Not uncommon.

We did several in This time frame.

The system of record for documents

both would try slow globally

to all "incidents."

1st incident of material value

all the reports stemmed from this

incident.

The Time sheets may reflect

the same info as that found on

the report.

TAD or Brian Hughey [illegible]

would have provided the

Logs to the FBI

10 have:

1. Orig Threat Assessment

to gather info on

who had compromised

us. to share with

FBI

2. Did not include

post-mortem analysis

MKP-0102726

→ TAD & Tharn - Verified Logs
Looking for unauthorized users.

→ hourly rate — as per expense report.

Daniel Gaines

notes

11/18/14

9/25/15

Daniel Gaines. 5/17/55.
(800-528-4637)

email: daniel.gaines@lakes.com

attorney jeff.glasser@lakes.com

I remember the email. I remember someone saw a problem + my job was to fix.

I don't remember who found the problem.

Oxy = oxygen A/C - original of CMS. (I was easy to figure out who (Lampe) the content. There is a list of who touched). Not everyone can see this, but some could. I was a superuser & had this ability.

TI = Tribune Interactive =
Chicago tech group who
Jason worked for.

Jason was visual person
I called the technical person.

We had some how A'd
a piece of content, like we
can analogize A.

The problem is that
inaccurate info would go to
public, reduce our credibility
our business is based on.
Same A'ing content would be
a big problem with what we
are
captured by Google immediately
it images. The public were
able to see this. I don't
remember. (½ hour by memory.)

I hung Gogle would have captured.

I don't recall exact series of events. → My moral belief

- not a common occurrence
- I'm not aware of any one from outside coming in.
- Mistakes have been made
- not aware of this ever happened at Latinas
- 21 year experience at Latinas. an educator 14 years, Manager since 11 year.
- 1997 - 2000
  - ↓ started
  - ↓ out! Nice I can remember.

T Garrison – Morning producer, NBC
p-r stay up
Frank Farran n added photo

Edit & "Happn"
expunge the print system.

T Garrison tasks it → turn live n
carded photo
n facial rgtn.

Frank Farran – would have been
of Farran
n Farran was matched
Farm. – an item
or contact or

Significant concern →

5 minutes is a
long time to be
seen online &
distributed across
the entire world
on the Internet

our business.

-> at some pt we thought it might be nothing more serious than an internal error.

Even stories about we were docked damages. or credibility.

I'm in Palm Springs.

Palm Springs

10th back

leave 12th

Wants. witnesses to by atty

Tom Comig
notes 11/24/14

only able to view the modified
story when you log into cms

URI Less Domain

IP Date/Time "

Request File()

what the browser asks
server to return:

Status code

200 - success

Size of response

refering URL the Request

was made From, ON

homepage & click on..

(CMS.) → assucllam.

tribune.com.

https. it's encrypto connection

(USER Agent) FD

type Browser.

(54) → 6 WAS on

an email

page

GET - Necessity That page

mKleyne was logged in

At The This happened we
were sig for Asscallen +
fax template
Pod Producer → more Δ

BTL
Courses to edit online
content (User Interface)

Inhouse Systems:

(search xtxl)(10)

(11) → A new user being created.

Tom Comings.
2/[illegible]/07

Sr. engineer
→ Enterprise Architect & Co.
Tribune Publishing Co.
Tribune Co.

Get access//ldap/editusers,

~~us~~ need to be a superuser
to use this.

ldap is standard
Directory

Ldap:
Username] → primary username
logic
Access Rights
outside LDAP.

every user
is in ladp database.

Username "test 1234."

[Dylan - head of security group
work on auto database.]

→ how we limited the damage.

V.P. engineering (Security) → Damage.

210 - 775 - 6435

→ △ at 3:49 - [illegible] user

at 4:29 more entries

4:30 more entry → correction

← Bhavna →

→ only [illegible] modification stage.
The version was live
until 4:29.

MKP-0102739

GAINES Sept 25, 2015

BIO 30 yrs → SUNY Albany

College, internship → H.S paper
College became interested
Minor Journalism
Major communication

1979-1991 Riverside Press-Enterprise (daily)
every imaginable position in newsroom.
Eventually editor → Asst Mgg Editor News.
Ran evening newspaper work. Decided
what went into the morning.

1991-93 Taught Cal State Fullerton. Journ 101, Civics Journ.

- Function of profn in our democ to provide accurate/useful info & also entertain. Sense of community.
- P/s make some money
- If people retaliate for stories, threatens the integrity of people
  - Wld that concern you if you learned it happened here.

Entire job categories exist to make sure info is accurate. Corrections policy.

1993 CAL

Part-time copy editor in bus. sctn

Mkts Editor (Asst Bus Edtr.)

~2000 Moved to Web Site. One of first to join the op.

Early News sites were connected to prodigy. Open Internet '98.

Idea was it was new Way for people to get information.

Came Business Editor
Home Page Editor
Dpty to Head of Web Site

→ Still #2 on web site

Creating News

Reporter, traveled, collects information. Photographer. Reads things & talks

Writes News story. Back-&-forth w/ line editor/assignment editor.

Copy editor. Fact, sentence, grammar, play role of independent reader. Adhere to CAT Style. Policies.

* Why bother checking for grammar & spelling? Easier to read & more credible. Meaning more clear. Don't look sloppy b/c people will doubt substance. People won't read a paper run by illiterates.

→ Comments/Ltrs re obscure pt of grammar.

Maybe other editors, too, depending on story.

* Where was Gene's? Admin/tech/search/hiring/budget Troubleshooter. Didn't routinely touch news, but did.

Gaines was senior to people doing the day-to-day, & fill in ad hoc

↓

Hernahen was copy editor.

Where the news room? It's really all news-side employees. Everywhere.

Physical layout:

* Not in day-to-day news ops. Farther from news editors. Down a hall near rptrs. 30 secs - 1 min.

Annual income in 2010 ~ $99-100K
Bonus was est $10-15K. Jobs have benes. ~30%.

In 2010, there was stress among copy editors about wanting to put up news quickly. LAT was more careful than peers about editing pre-publication.

2010

Remember seeing Chippy?

Yes occupied most of a day.

"TI" is "Tribune Interactive"

Jedlinski was Chief of Market Svcs.
Based in Chicago. In charge of
web for all newsrooms.

Elevated Blood Pressure, his boss's, his boss's

Running back/forth btw his office +
boss's Sean Gallagher.

* Worried whole web site wld have
to come down if didn't stop it.

Hav important to Stop + ID
who did it? Most imp. that
day. Rsrch'd who had tracked
Story. Agencies: there was none

Spent most of day 1/2 - 2/3 searching site looking for more problems. Users stories, etc. who had touched stories.

Google/Yahoo for < Anything Chippy

Then Jason / TI took over.

(+-6hrs total)

Now available to do regular stuff
Delayed all other regular work.

- Anything that distracts us interferes w/ work of getting info out.
- How does this effect the credibility of the enterprise? Think less of it. Wonder what's else wrong. That's most serious thing he can do.

+ (Home page takeover is worth ~ $50K
Santus $10-20K)

MKP-0102745

Hostile posts whole front page
new? Give revenue back.
"Make good" is what it's called.

K wld've known. Obvious.

Good will as an accounting concept.
Credibility of the operation.

This WAS worth more than
$5K in good will.

Make LAT look ~~[illegible]~~ sloppy & bad.

Part of Den's role is to work w/
ad dpt on ads. That's how
he knows.

$5K doesn't seem like a big number.
Prob more than $10K.

That wld've been a major story.
Huge in media about media.
No problem saying that's worth
more than $5K

Wld've paid at least
$5K to [illegible] tarnishing
reputation.

To a Comp
Notes from 7/16/15

Tom: Comiga 2/18/67

current title → enterprise Architect
~20 employees & 7.6mm (3-4 yrs
under current title

- title in Dec 2010 was
Sr. engineering in Infrastructure technical

→ what did you do
in 2010. - on day of events
I did a log investigation
who modified a story.
I did 2 pr
① logged in user system
called - Assembler - looked up
slog. - did screen grab
of Δ log.

② → looked at log file
to isolate time stamps +
post activity. I don't
know assembler really well.

I do know what the
fields mean.

I did look at activity for that day.

Asseltine - creates & modifies content. - I don't use it at all.
→ I did use it but not expert on it.

- web server log files.
I do know this.

→ I never assisted people in putting up content, but did know how to use it.

I extracted log data on that day.

I read coding report, the report referenced logs, → so the logs for Dec 16th were pulled by me.

Dan Corrigan – Fire Spot.

✓ couple of hours a flash dig but → more over time

✓ Time sheets for projects but I don't think there was a category for this event.

✓ The report shows accurate Fire Spot.

↓

Reviewing best practices
Don't recall any steps
meetings
data review
assembled data for Tink.
Don't recall 100K for any other work.

Screen grab – I determined it was a glacier – based on the slope on sky – ice.

~~Dan worked~~

This was a serious event. It was serious – "because integrity of the news is everything right".

→ did a search for other changes that we didn't

→ we kept looking for other interviews. – needle in a haystack. (For other Post commands – lots of these efforts)

Brian Hussenfeld –

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/03/2014

Brandon Mercer, previously interviewed, was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, Mercer provided the following information:

Mercer will gather records and information he has relating to the costs involved in dealing with the stolen e-mail list and suspicious e-mails received in about December 2010.

Mercer recalled, Matthew Keys, in his capacity as web producer had a hand in setting up accounts to access the content management server. Mercer was not sure whether Mercer created the accounts or if corporate did it, but it was Mercer's understanding that Keys' would have known the passwords to access some accounts.

Mercer was read a list of names and asked to comment about what he knew about the accounts.

a) mkeys - This was Matthew Keys account. Mercer recognized it by the name and the fact that it was also used in connection to Matthew Keys work e-mail account.

b) nshanafelt - This was a free lance reporter who formerly worked for Fox40 News.

c) eharrington40 - This was the account of a journalist named Elissa Harrington.

d) mtomaselli - This is the account of a producer for Fox40 News who is currently employed there.

e) mdemsky - This is the account of a current employee of Fox40 News.

f) lkeys - This is the account for Leigh Anne Keys, who was an executive producer for Fox40 News.

g) sscholbrock - This is a current employee of Fox40 News who took over as web producer about the time Matthew Keys departed.

h) apenny - This is a current Fox40 News employee.

i) test1234 - Mercer does not have any specific recollection, but believes this was a test account set up to practice on the system. Keys or corporate offices may have created the account.

j) test5678 - This is the same as test1234

k) bmercer - This was Mercer's own account. Keys would have had access to while he was employed by the firm, but would not have had access to it after he left.

l) Mercer did not recollect anything about the following accounts: rburrow, jaclark, scooley, cooper, krcraig, dbenton, misilva.

m) prrossey - This account belongs to Paulette Bleam, a Fox40 emmployee.

n) jczahor - This account belongs to a current morning show producer at Fox40.

o) afriedman - This account belongs to a corporate officer, a Vice President of Digital Operations.

9/24/15

Brandon & Mercer

Listened to tape - consistent w/ recollection.

Email from Bun to C/S - chuck should bill $1000/hr - C/S reply were past that, on 12/2. → was there an effort to run up tab? - No - we were already past $5000, but wanted to make sure it was documented to that effect. - we wanted the info there so it would be prosecuted. - In Fact I sent email - to Friedman, news mgrs + others. → talking about logs time/rate. spent handling. I put in spreadsheet, I gave to Jerry.

Jason J. → oversaw websites. like a Freidman (Team) - oversaw engineers - sent email asking for list of logins to P2P to the compromised Sys. - Reply → I recall working with these guys. - Documenting email? I could have put wrong dates.

99869 ~ Jedinski email → primary pt of contact

12/2 - 5:30 pm - dealing w/
J. Hueta. → Sennet advised to
leave alone.

Dec./3 self cancel. - 2 hours last night
plus more this morning.
common for me to

$64/hrs.
62 - 67/hrs.
hired at 25 make $/30
or so i- 2010
(at least $62.50/hr)

0101177 - Spreadsheet showed
"Brandon mirow@gmail.com
* This was done by me. →
not completely done. - but
accurate when I sent it
does cover all - it's formatted
bad

I was at the mtg 12/6 mtg 1/2

Mary Nelson

Dellone

me

Gary Saunders

Sam Cohen

Bill G

Jack Davis

Mike Duell

Phil Stelakus

Laurie Misicka

Karen Hoffman

Candace Shropshire

stopped keeping records after we cleared $5,000

+ Chuck told us we were well over the $5000 limit. so didn't do much documenting after that

in Dec 20 hours 1st few days maybe 30 hours in Dec plus other times later on

under FBI direction made call

weird feeling making the call as a journalist - not normal.

if convicted, interested in Ms. yes! why is that

E in capitol, it's
the elderly woman plus
threat to free speech.

MERCER SEPT 24, 2015

310

1987 School Paper Woodrow W. Glendale

USC '97 Exec. Prod College News TV
Journ/Pol Sci

Tucson Producer, Assign Ed. KOLD CBS13
97-2000

Phoenix KPHO TV-5 Producer
2000-2001 Stacks stories, oversees →

San Fran TechTV SF Cable Network
2001-2004

2004 KMAX SACTO Cable 12) Exec. Prod
KQVR ch 13 overseeing 5
other producers

2008 News Director KTXL 40
Hired Keys 2008 as web producer

consultant for Trib. Around time Del Care
went out. That's the business.

Old people @ company serve as references.

sfgate.com

2008 Keys was about to start internship.

2-3 mos later Mercer hired him b/c big Twitter followly & he'd broken a lot of stories

† Keys tweets as a fictitious character. Homer Simpson.

Socially awkward, cocky, contemptuous.

Web Producer
~ $35K, if remembers right
Duties
Run web site
Run social media accts (FB, Twitter)
Grow social media followy

Soc media accts were in Keys's name (ema.1)

2008 Social Media in its infancy. This was all new. Keys pass did launch FB page.

Mercer was hands-off & it worked. Keys was self-starter. Very intelligent & effective.

Challenges. Young. Didn't kn how to behave in corp environ. Disrespectful of coworkers & superiors. Called women a b-words.

Explosive outburst 'bitch' Possibly Leanne Keys, producer above him. Maybe Sam Cohen.

Mercer wrote him up. Counseled for insubordination.

Thought he kn best & didn't want to back down from argument.

Mercer said he was new to ofc enviro & needed to adjust

few social skills. Wanted to rile people up. Assumed & many comments were anti-women as it turned out.

2 verbal warnings & 1 written.

Roseville Mall Fire

One of biggest stories @ fox40

Went down & then went back up.

K was on Twitter & something on website Bus. function is to get viewers & keep them.

At some point, K didn't like what fox40 was doing on air, & tweeted in substance that fox 40 was worst.

K found some social media acct & fox40 went on air w/ it. He was upset by that.

Tiff in newsroom. Mercer sent him home Choice words. Shouting. Cursing. Angry.

* Physical description of news room - small! Everyone really close.

* Mercer cut off Keys's internet Fox 40 / Trib accts. & changed PWs.

MKeys

Mercer said 'don't work,' & K said 'I can't guarantee that'

Oct 28, 2018

Wldlife given 2d Ch, not sure, but anyway needed all these approvals.

Mercer talked to Del Cave & they deliberated. Were going to talk to Keys. Called him in for Mon, instead K cleared stuff out.

K then started dropping Twitter followers. Today, Mercer says worth ~ $1. Purpose is they'll view move. S/C ya reach them.

Problems went on. Gave Twitter on affidavit. FB restored w/ K's fox40 mail.

Festives was first sign it was K

Dec 1

6y, 3y, 5 mo kids. Mercer dealt w/ this.

Breach of trust w/ viewers. Phrased b/c thought it was K ?

- Tried to be like terrorist negotiator
- Didn't want K to hurt company
- " " " " " self

GX 101

Bought 15 iPads, too, to build loyalty.

Wanted to confirm it was keys ? talk him out of it.

* I wasn't running newsroom. I was in crisis Mngmnt w/ all other exec. producers.

*

Then had doubts if it was keys.
Trying to figure out

GX 102

That's when we ~~[illegible]~~ decided to get everyone involved.
Lots of calls w/ corporate in Chicago.

* Sennet, Corp Comms, ~~[illegible]~~

5 or 6 people on call.

~$130K/yr in 2010

Many of ~~[illegible]~~ these responses were round-tabled

GX 103-002 Was after Del Core said they wld cut his legs out from him & do everything possible.

Mercer had keys in mind w/ this email & really was trying to help him. Didn't want to be shitty in crim now.

GX 103 When Mercer fin it was K. Smug & contemptuous. That brings down smart people.

GX 104-3

Members. Afraid of damage to company reputation.

Trib was in BK & this wld hurt.

Maybe wld work bc K lived w/ g'ma

GX 106 Huerta registered keys & gave that email.

Feels like 3 mos, was 3 days. Did nothing but this & eat.

GX 108 Penn. Holy fuck how are they still doing this? Andy Friedman, Chicago.

GX 109

Going Rogue. 10pm Sat.
~~Doing this instead of working.~~

↓ Important to figure out what was going on.

Remembers Sam Cohen had PW problems. She took H's old job, but became a managerial posn.

Couldn't work from home.

- Didn't log time when it was happening.

- Dec 1 – 6. Mtgs, conf calls, emails

+ recorded call time → At least 20 hrs @ $64/hr : $1280

~~[illegible]~~ Maybe [illegible], if recorded call time.

1A2

FD-340 (Rev. 4-11-03)

File Number ~~288A-SC-74639~~ 288A-LA-258500

Field Office Acquiring Evidence SC

Serial # of Originating Document 6

Date Received 12/3/10

From _____
(Name of Contributor/Interviewee)

_____
(Address)

_____
(City and State)

By SA John M. Carter

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☑ Yes ☐ No

Title: Matthew Keys.
KTXL - FOX 40 - Victim
CIP;

Reference: FD-302 Brandon Mercer
(Communication Enclosing Material)

Description: ☑ Original notes re interview of
Brandon Mercer.

1A2

MKP-0102767

Kepp was terminated late october 2010. He was a web producer . techie blogger. Very smart & intelligent; he got insubordinate.

Oct 25th he posted something on Twitter that was a problem for station. He was told to go home. On 29th I wanted to help him go. I turned off access to his Tribune files then home. When cut off he went to Twitter & Facebook - shut us out.

-> a huge source of Revenue -> page views

Brandon Mercer, 10/15/1974,
News Director, Fox 40 News,
4655 Fruitridge Rd.
Sacramento CA, 95820,
Over the news room, 80
employees. Over TV +
website operations [illegible] news
budgets., sets, directing
crews in field.

Fox 40 News is owned
of Fox 40, TV station 40/41
owned by
Tribune Mgt. (company
in Chicago) med.

We carry Fox network
programs (24) & sometimes pay
22 hours per day.

to FoX 40 ~~news~~. count. 8,000-
5,000 followers on ~~Facebook~~ Twitter
→ a ~~Twitter~~, "10K" on Facebook
~~the~~ web person he
was creator of these pages.
he blocked "web person".
he created Twitter a Facebook
Twitter he used with his
own e-mail, & when he
lost password, never
could get the PW back.
I don't know what
e-mails he used to
open the Twitter A/c. →
we could no longer
update & have control
over it. he then
deleted 6,000 Followers
so it was like from
8,000 - 5,000 - to
2-3 K. followers

MKP-Q102771

Then he set up
Twitter that started
seeing at head line
the competition. → seeing
on news head line the
other news stations
using "Twitter Fact" →
This what on the 4
days before we could
control it>

2nd → take a sick
day come in always
"I created the ALL's
they are mine."
→ no you no

give it back to us.

On Facebook (2 pages)
-> Fox 40 Live - Keys controlled & later agreed to give back to us.
Fox 40 News ->

he created those from his work address
mathew.keys@fox40.com

I asked over it many to give me right to his work e-mail, Logged in using his work e-mail to get control back.
(he made the same argument about Facebook)

By Nov 3rd 4th
everything was taken.

on Monday. Nov 1st
I Konstantin there.
→ (He had taken
his stuff & with files
home on Sunday)

→ Mac Laptop.
→ Modem from Compsys?

3381 Shadow
Tree Dr
327
SC 95834

SSN: 560-93-8618

NMT

DOB 2/5/67 → Geo (Google search) 916-572-5057

916-769-4493.

916 265-0941

Email. matter@radiomatter.com

Radio matter is his blogger name. He blogged about Local radio at KFBK I hired

---

He still has Twitter bio "Fox 40 Business" and other stuff.

MKP-0102774

vervee set re

Chmels.

Joseph is a photo graph

-> when to Kys tenbral pgr.

Fox [illegible] ?

FD-340 (Rev. 4-11-03) 1A19

File Number 288A-LA-258500

Field Office Acquiring Evidence Los Angeles & Sacramento

Serial # of Originating Document 61

Date Received 10/4/12

From Matthew Keys' interview
(Name of Contributor/Interviewee)

5201 Riverside Station Blvd
(Address)

Secaucus, NJ
(City and State)

By SA Gabriel Andrews

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☒ Original notes re interview of

MKP-0102776

Middle of Dec 2011, coffee w. Brandon

Oct 2010 left →

917-751-9942
4 Matt's cell #

"I was Bored & I felt stuck"

"Colloquy" to get on IRC

AES Cracked username

Diplomatic Cables from Wikileaks had AES encryption; MK didn't know what AES was, but thought they would.

From his bedroom in Sacramento logged in to IRC w. Colloquy. Turned off text logs.

#Operation Payback was the channel he joined to lurk. Learned of this IRC b/c of Twitter. Saw members of LOIC.

Threw out Fox in IRC, got Sabu's attention.

Told Sabu he had credentials, Sabu asked for them, MK gave them
to hurt Fox vs gain cred
"it's a little of both"

In #internetfeds that night:

MK found out re Gawker dump when everyone else did; MK saw Kayla taking Gawker credit (later saw Gaorett was a partner of hers/his)

MK felt inexperienced as he moved to ~~a different job~~ Disney Job

(Fox had Monsegur case first, MK's room-mate is fox employee Tangental Thought

~ 33-36 hackers / usernames

~~IF~~ channel participants could "Do significant damage" & without cause. caused MK stress, lack of sleep.

MK thought:
"I have the keys to a house that were never taken away"

Tribune didn't take away MK's security credentials.

MK was removing former employee CMS access, not as part of his job, but b/c he knew that former employee's having access was potentially dangerous to the Company.

Tribune hadn't

password was silly, involved "456" or something.

Tribunes CMS was "forward facing", MK saw Sabu gain access to CMS.

Then & Still ~~today~~ MK has no good grasp on what #Internetfes could do.

Now feels "had low impact"

Re: Chippy "To be honest, I felt like I incited it"

MK saw Saba refer to "those accounts", & be upset when ____ wasted it w a low impact

---

MK doesn't know how proxy's work, but googled how to watch British TV, signed up to OverPlay, & then installed their software. MK checked his IP & verified his IP showed up as ~~British~~ not Sacramento (allowing BBC /etc).

Emails written were hooliganism. He wrote emails to viewers to say "this is what's going on":

"Cash Grab" contest; a number is flashed on TV; content is delayed for some customers, not others; had this gotten out, viewers would be upset. MK thought this was unfair. [redacted]

MK obtained emails from a seperate CMS server. MK used it.

MK was angry w Mercer/Fox for a long time. ✝hurt

There are so many incredible/good people working there (Fox); MK would sincerely apologized.

MK in Dec 2010 wanted there to be consequences for Fox for MK's hurt, in the end it didn't make MK feel any better.

Thats why he had coffee, wanted them to be able to work together again.

Party in December 2010, "who is fox mulder?" didn't know that Keys was Fox Mulder. MK didn't ~~know~~ get the sense that they weren't terrified.

iPad giveaway contest emails were those that MK had access to & used ~~[illegible]~~ ~~[illegible]~~ to "create consequences"

MK tried Jack Davies for a news story, no response to text
received via Parmy, her idea for story.

In Jan 2011 was MK's last access. Room shut down b/c Keys' leak to PBS.

MK had, at the time, not realized he was breaking fed law on PW trafficking.

MK gave Adrian Chen (sp?) at Gawker some of the screen grabs.

Calling SADC post reuters hire was for a story.

- Cybertroll 69 isn't Matt Keys -

MK did log in again (in ref to AJS cracked line user ID) w/o VPN forgetting mistake

MKP-0102780

SG dump 1 on external HD's contains screen grabs.