SFMTA
Municipal
Transportation
Agency

APTA Legal Affairs Seminar

Security Session

SAN FRANCISCO CITY ATTORNEY'S OFFICE

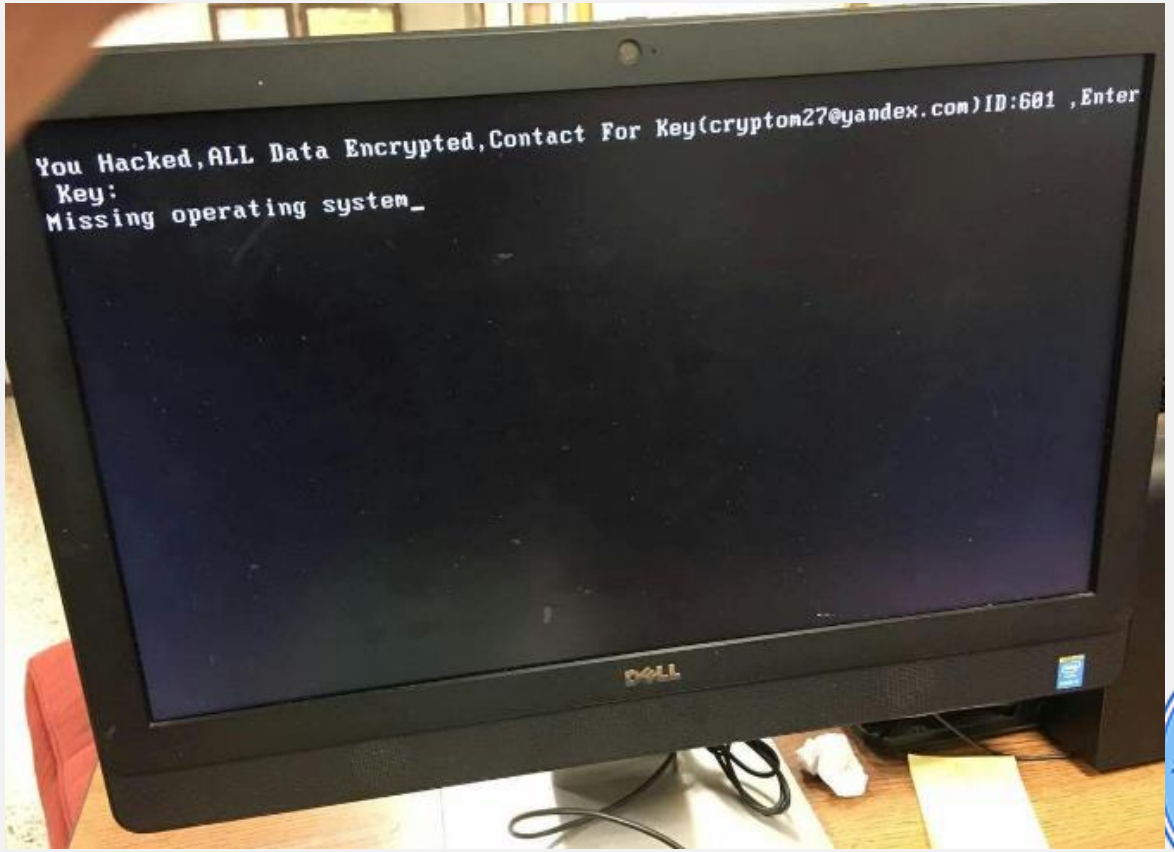
FEBRUARY 26, 2018

SFMTA
Municipal
Transportation
Agency

Part 1: What happened?

SFMTA
Municipal
Transportation
Agency

November 25, 2016



SFMTA
Municipal
Transportation
Agency

SFMTA
Municipal
Transportation
Agency

What is a Ransomware attack?

- Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. Ransomware often infiltrates a PC as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. (Webopedia)

SFMTA Took Following Actions

- Immediately shut down the payment systems
- Opened the fare gates
- Posted handwritten “Free Muni” signs on the ticket machines
- Updated blog posts

SFMTA
Municipal
Transportation
Agency

Press Quote

A San Francisco MTA spokesperson declined to comment beyond saying: "There's no impact to the transit service, but we have opened the fare gates as a precaution to minimize customer impact."

SFMTA
Municipal
Transportation
Agency

CITY ATTORNEY
THE CITY AND COUNTY OF SAN FRANCISCO
SEAL OF
SAN FRANCISCO

SFMTA
Municipal
Transportation
Agency

SFMTA Took the Following Actions (con't)

- IT immediately started analyzing situation
  - Determined attack did not compromise transit systems
  - Determined had back ups
  - Could repair affected computers with back up
- Security informed Department of Homeland Security, FBI, etc.

SFMTA
Municipal
Transportation
Agency

Part 2: Legal Issues

CITY ATTORNEY
SAN FRANCISCO

SFMTA
Municipal
Transportation
Agency

Overview of Legal Issues

What do you do as an attorney when your Agency's system has suffered an attack of some sort?

- Protect PII/PCI at all costs; if can't or didn't know legal oblgiations to dislcose
- What are the protocols in place? Technological and organizational?
- What are subsidiary issues to check on;
  - Documents compromised?
  - Who has liabililty/responsibility?

PII/PCI

Certain obligations to ascertain whether Personally Identifiable Information (PII) or Payment and Credit Information (PCI) has been breached

SFMTA
Municipal
Transportation
Agency

What is PII? (Cal. Civl Code 1798.3(a))

- Any information that is maintained by an agency that identifies or describes an individual, including but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

For purposes of breach notification:

For unencrypted data: First name or initial and last name in combination with any one or more of the following data elements:

- SSN
- Driver's license #/California ID card umber
- Account No., credit or debit #, in combination with required security code or password
- medical information
- Health Insurance info
- Automated license plate recognition system information
- User name or e-mail address in combination with password or security question/answer that permits access to an on-line account

SFMTA
Municipal Transportation Agency

What is PII (cont'd)

For encrypted data : PII and the encryption key or security credential (the key) has been acquired or reasonably believed to have been acquired by an unauthorized person and the agency that has the key has a reasonable belief that the key could render the PII readable or useable.

Cal. Civ. Code § 1798.29

SFMTA
Municipal
Transportation
Agency

What is a breach of PII?

Unauthorized acquisition or "reasonable belief" of unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. (Good faith acquisition by an employee of the agency is not a breach).

Cal. Civ. Code § 1798.29(a) & (f)

SFMTA
Municipal
Transportation
Agency

What do you have to do if there is a breach?

1. Call your Attorney.

2. You have to notify affected individuals in "the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."

Cal. Civ. Code § 1798.29(a)

SFMTA
Municipal
Transportation
Agency

Who do you notify?

The subjects of the breach and if over 500 California residents affected by the breach, the California Attorney General. *Cal. Civ. Code § 1798.29(f)*

What is the penalty?

Private right of action which means each person whose data is breached can sue you. *Cal. Civ. Code § 1798.84(b)*

Conclusion PII/PCI – No Breach

MTA Blog – 3 days post-attack

In coordination with our partners at Cubic Transportation Systems, who operate Clipper®, we took the precaution of turning off the ticket machines and faregates in the Muni Metro subway stations, starting Friday until 9 a.m., Sunday. This action was to minimize any potential risk or inconvenience to Muni customers.

The primary impact of the attack was to approximately 900 office computers. The SFMTA's payroll system remained operational, but access to it was temporarily affected. There will be no impact to employees' pay.

SFMTA
Municipal
Transportation
Agency

Further Recommendation

Conduct post-incident review to ascertain and document no PII/PCI breach ("White Hat" hackers)

SFMTA
Municipal
Transportation
Agency

Protocols

CITY ATTORNEY
SAN FRANCISCO

SFMTA
Municipal
Transportation
Agency

Broader Security Threats?

- Confirm your agency is working with other authorities (Department of Homeland Security, FBI, etc.)
- Here: no impact to transit systems, perpetrator identified as likely repeat ransomware attacker looking for monetary payouts.

SFMTA
Municipal
Transportation
Agency

Negotiation

- Attacker demanded 100 bit coins ($73,000)
- Promise “code” to restore systems.
- DOT: Did not want to negotiate
- Risks:
  - Political/PR risks
  - Practical: How get Bitcoin from City Controller?

Result – No Payment, Restored System

SFMTA Statement

The SFMTA has never considered paying the ransom. We have an information technology team in place that can restore our systems, and that is what they are doing.

Existing backup systems allowed us to get most affected computers up and running this morning, and our information technology team anticipates having the remaining computers functional in the next day or two.

SFMTA
Municipal
Transportation
Agency

Documents

CITY ATTORNEY
SAN FRANCISCO

Discovery/Litigation Holds

- Legal obligation of City to preserve information for litigation;
- Determine nature/extent of data loss
- Any loss could raise legal issues and liability for the City.
- Result: Ascertained that all data was restored via systems back up. All data intact.

SFMTA
Municipal
Transportation
Agency

Contractors

CITY ATTORNEY
SAN FRANCISCO

SFMTA
Municipal
Transportation
Agency

Third Party Contractors:

- Recommended reviewing whether any contractor involved with the breach or with the installation of systems that did not act as planned during the incident.
- If yes, recommend reviewing contract to see if pursuing insurance or othe remedies provided under the contract is appropriate.
- Here: No issues with contractors.

SFMTA
Municipal
Transportation
Agency

Conclusion

SF'S TRANSIT HACK COULD'VE BEEN WAY WORSE—AND CITIES MUST PREPARE

Wired magazine, November 28, 2016

Resources

California Civil Code, Sections 1798 et seq.

APTA Standards Development Program, Cybersecurity Considerations for Public Transit
http://www.apta.com/resources/standards/2014%20Q2%20Public%20Comment/RP_cyber_security_considerations_%20PUB_COMMENTS_V10%2012%2019%2013.pdf

Cyberattacks against Intelligent Transportation Systems, Assessing Future Threats to ITS, Trendlabs Research paperhttps://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf