FISSEA 2009

LA Traffic:

Knowledge + Malice = Chaos

John G. O’Leary, CISSP
O’Leary Management Education

FISSEA 2009

LA Traffic:

Minor Internal Incident; Major External Possibilities

John G. O’Leary, CISSP
O’Leary Management Education

FISSEA 2009

LA Traffic:

When Awareness Doesn't Work

John G. O'Leary, CISSP
O'Leary Management Education

Abstract

- On Nov. 5, 2008, two Los Angeles traffic engineers pled guilty to illegally accessing a city computer. The pair, at work on Aug 21, 2006, hacked one of their traffic computers and sent commands to disconnect four signal control boxes at critical intersections. No one was killed, no accidents were even reported, but it took 4 days for LA traffic to get back to its usual semi-controlled, semi-chaotic state.
- The plea bargain doled out minimal penalties for this crime, but the mind boggles thinking about possible consequences of similar exploits in the future.
- We'll analyze the incident from a security awareness viewpoint and ask some questions

Speaker Bio

John O'Leary, CISSP, is President of O’Leary Management Education. His background spans four decades as an active practitioner in information systems, IT Security and contingency planning. He has designed, implemented and managed security and recovery for networks ranging from single site to multinational. John has trained tens of thousands of practitioners, and conducted on-site programs at major corporations and government facilities worldwide. He has also facilitated meetings of Working Peer Groups, where security professionals from diverse corporations share ideas, concerns and techniques. John was the recipient of the 2004 COSAC award and the 2006 EuroSec Prix de Fidelite.

He has never been convicted of anything really serious or run for public office

Agenda

- Basic Facts/Background
- Disruption
- Economic Reality
- Consequences(?)
- Questions Raised
- What If? …..
- Lessons for FISSEA

Basic Facts/Background

- Gabriel Murillo (39) and Kartik Patel (36)
  - Both employed as LA City Traffic Engineers
  - Automated Traffic Surveillance Center (ATSC)
  - 17 year employee and 12 year employee at time of incident
  - No previous criminal records

Basic Facts/Background

- ATSC is a union shop
- Both members of Engineers and Architects Association (Union)
- Computer system manages 3,200 of the city’s 4,300 traffic signals

Basic Facts/Background

- ATSC does have an information security program
- ATSC does have a security awareness program

- Unknown – Whether the awareness program stresses consequences to individuals for inappropriate actions

Basic Facts/Background

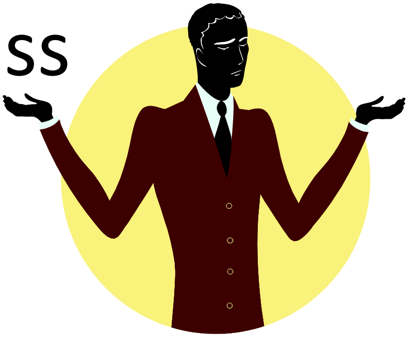
- Hack occurred Aug 21, 2006 between 9:10PM and 9:30PM
- A few hours before a job action by the Union
- Stolen supervisor credentials were used to:
  - disconnect signal control boxes at 4 targeted intersections
  - manipulate system so that other managers could not reconnect the lights

Facts/Background

- Statement from the union had said that on the day of their job action ***"Los Angeles is not going to be a fun place to drive."***
- City officials assumption was that the statement meant that in the event of a strike, union traffic engineers would not be available to monitor hotspots, fix outages, reroute traffic, adjust light timings, etc.
- Managers would have to do the actual work

Facts/Background

- Possible threat of intentional sabotage was downplayed, but …
- City officials, taking the threat seriously, blocked access for all engineers to the system and sent out a memo telling them so
- Murillo said he was on paternity leave and didn’t get the memo about no access
- Patel originally denied everything

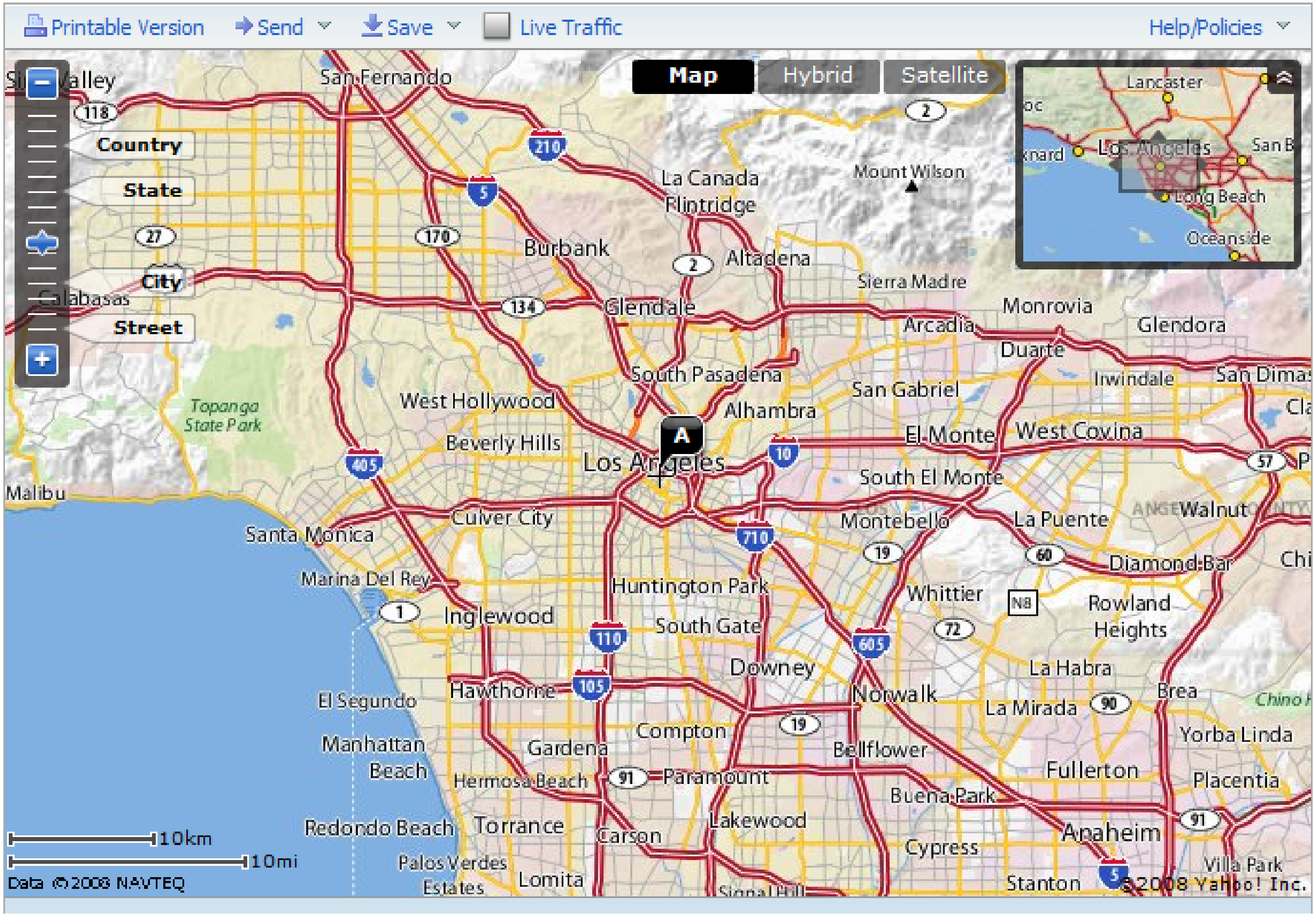


Intersections Targeted

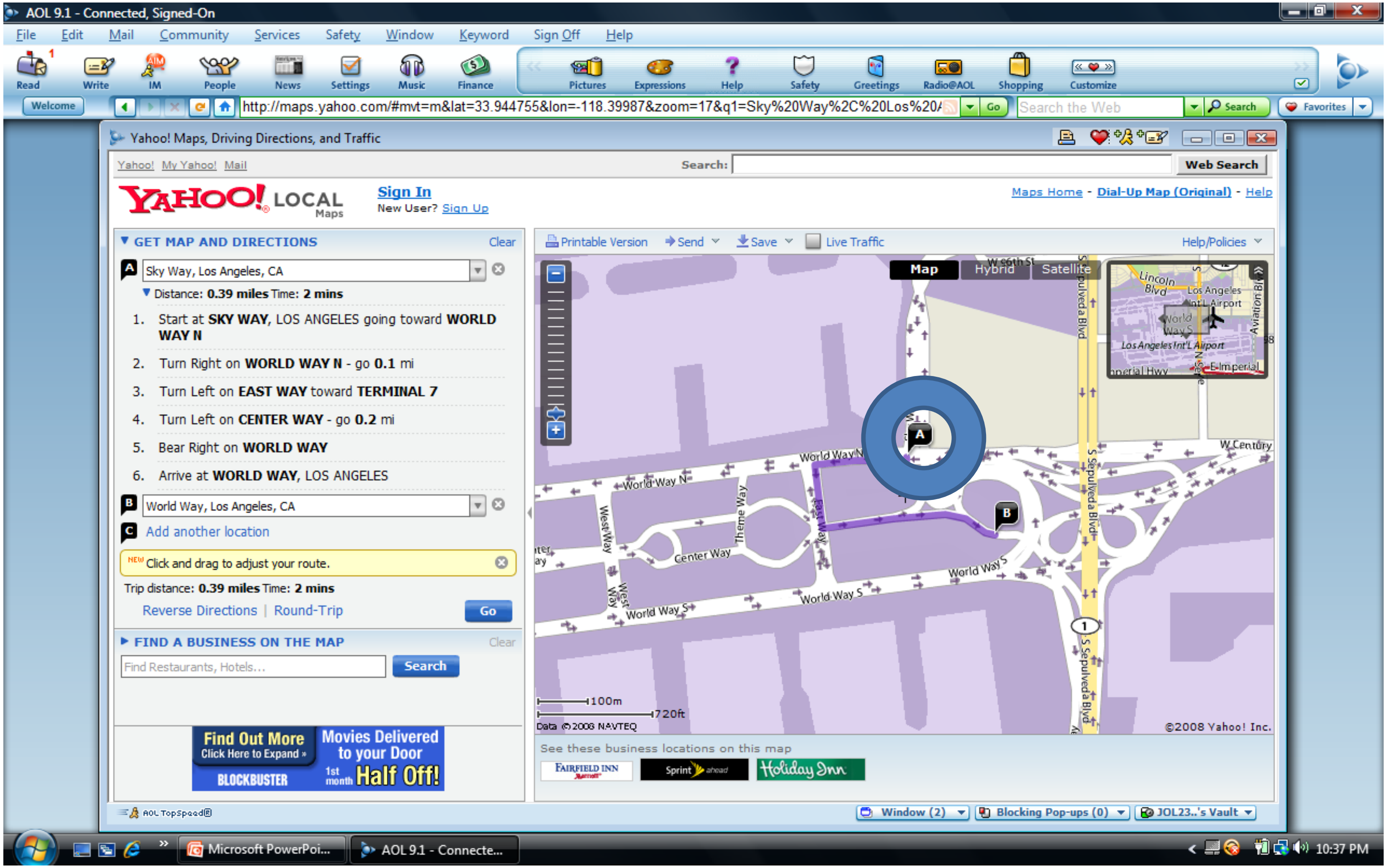
- Sky Way and World Way at LAX
- Coldwater Canyon Avenue and Riverside Drive in the San Fernando Valley
- Alvarado Street and Glendale Boulevard at Berkeley Avenue in Echo Park
- 1st and Alameda Streets downtown

- ***Airport, Studios, Little Tokyo, Downtown***

Los Angeles, CA



World Way and Sky Way (LAX)



AOL 9.1 - Connected, Signed-On

http://maps.yahoo.com/#mvt=m&lat=33.944755&lon=-118.39987&zoom=17&q1=Sky%20Way%2C%20Los%20/

Yahoo! Maps, Driving Directions, and Traffic

GET MAP AND DIRECTIONS

A Sky Way, Los Angeles, CA

Distance: **0.39 miles** Time: **2 mins**

1. Start at **SKY WAY,** LOS ANGELES going toward **WORLD WAY N**
2. Turn Right on **WORLD WAY N** - go **0.1** mi
3. Turn Left on **EAST WAY** toward **TERMINAL 7**
4. Turn Left on **CENTER WAY** - go **0.2** mi
5. Bear Right on **WORLD WAY**
6. Arrive at **WORLD WAY,** LOS ANGELES

B World Way, Los Angeles, CA

C Add another location

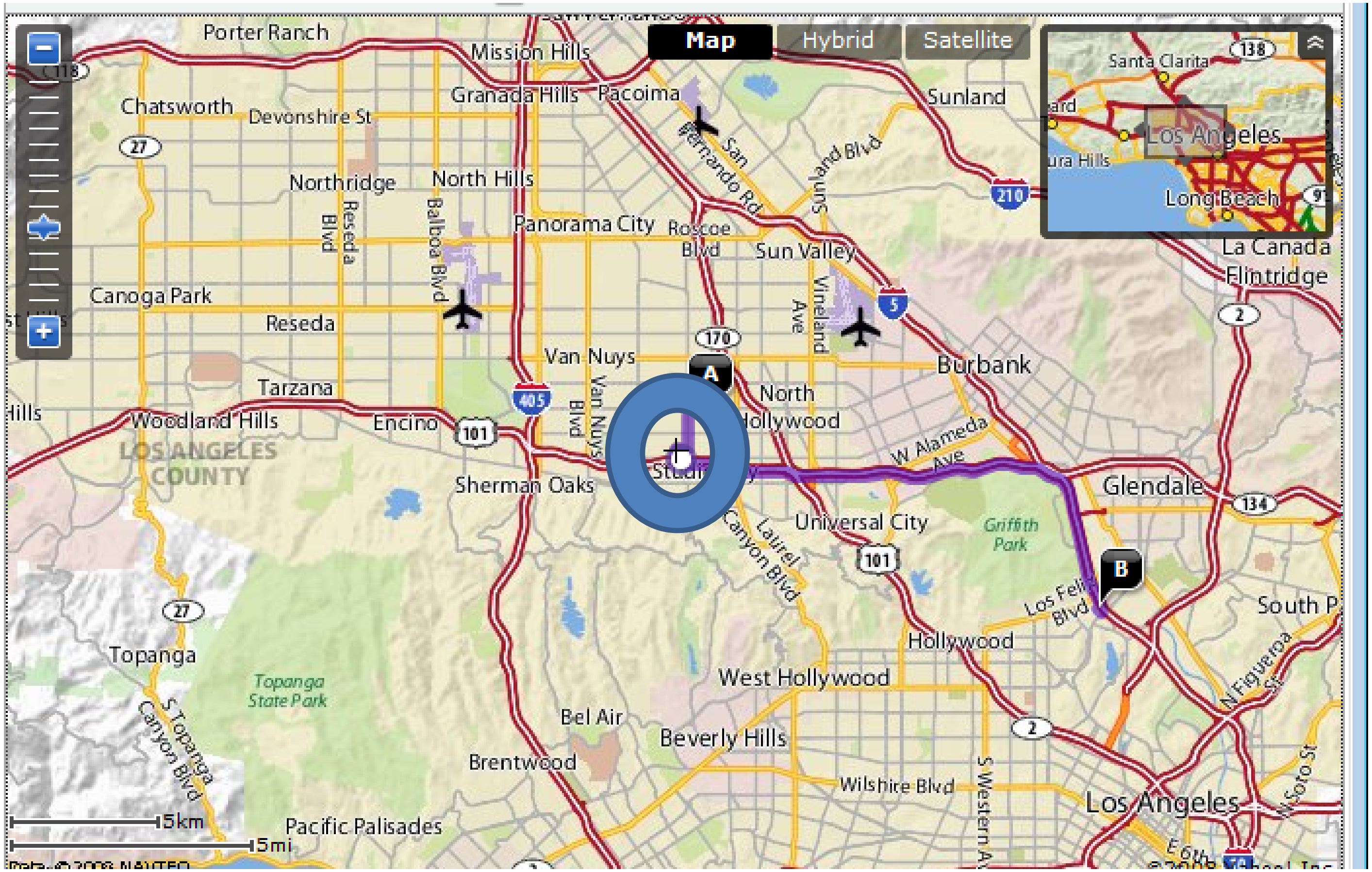
NEW Click and drag to adjust your route.

Trip distance: **0.39 miles** Time: **2 mins**

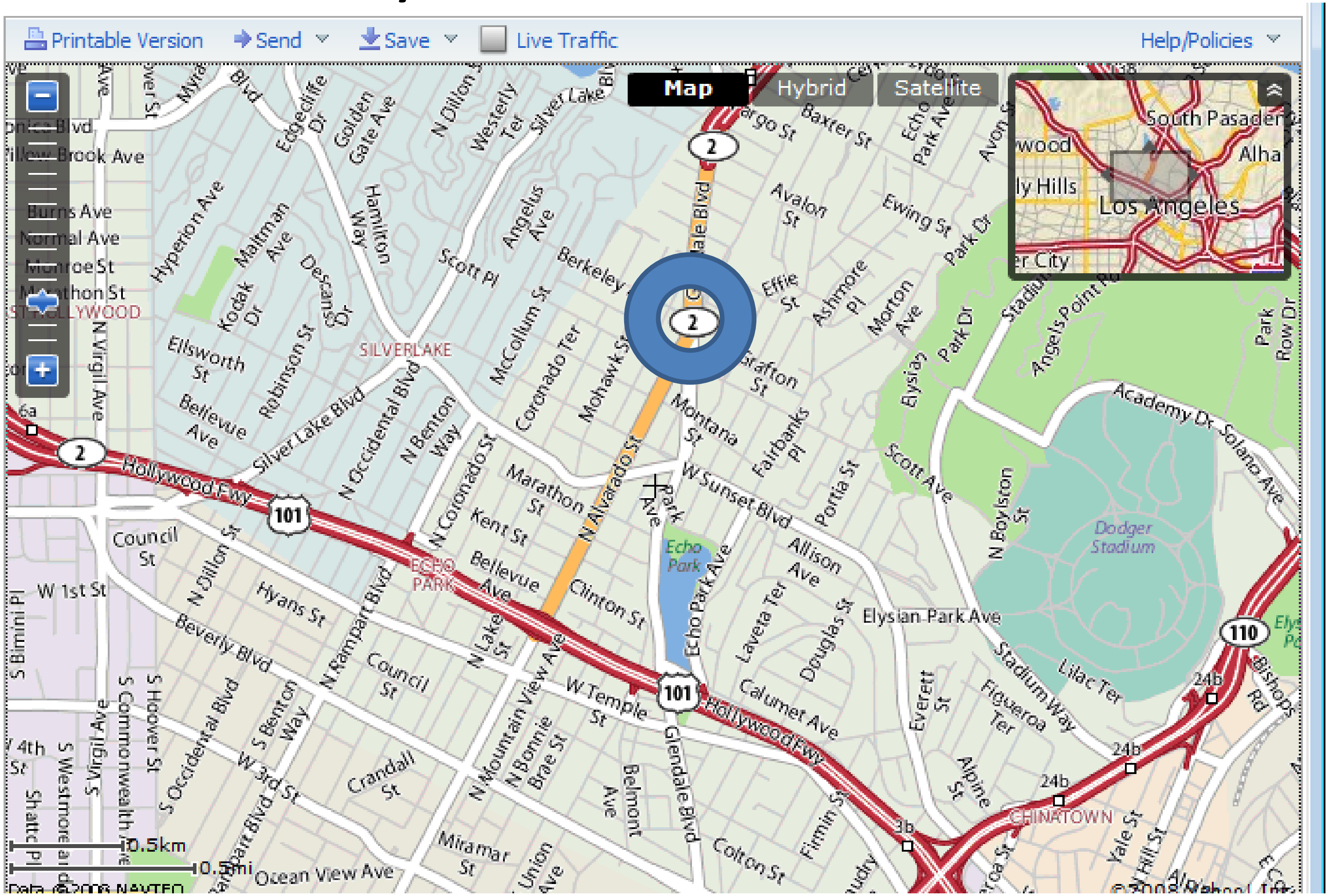
Reverse Directions | Round-Trip Go

FIND A BUSINESS ON THE MAP

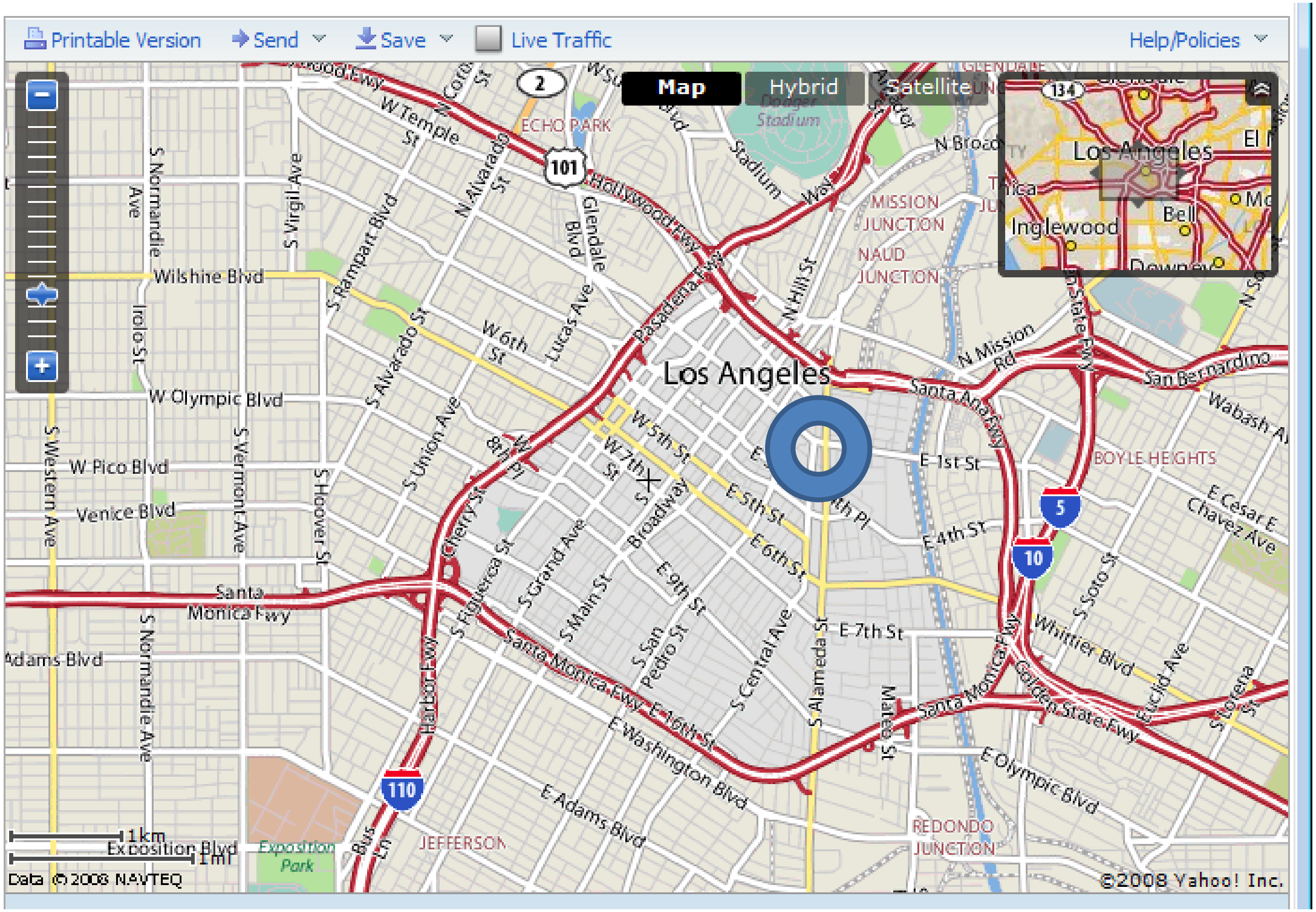
Coldwater Canyon Drive & Riverside

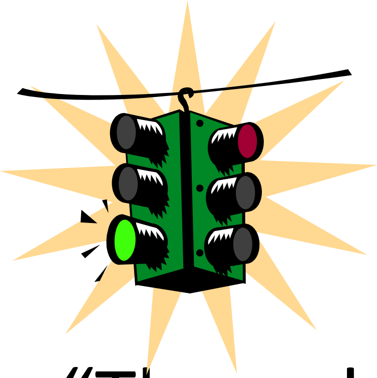


Alvarado Street and Glendale Boulevard at Berkeley Avenue in Echo Park



First & Alameda Streets





Traffic Disruption

- "The red signal would be on too long for the critical approach and the green signal would be on too long for the noncritical approach, thus resulting in long backups into the airport and other key intersections around the city," said one source in the traffic department, who spoke on condition of anonymity.

Note

- You can’t make all the lights green in all directions. There are physical relays and switches embedded in the actual traffic lights that make this impossible
- So please let your terrorist brains settle down just a little bit
- And hold off on writing that screenplay

Traffic Disruption

- Prosecutors argued that the pair picked intersections they knew would cause significant backups because they were close to freeways and major destinations. They said the red lights would be extremely long on the most congested approaches to the intersections, causing gridlock for several days.

Déjà Vu All Over Again

- Where have you seen this before?
- Of course, … Hollywood
- *The Italian Job*
- In the movie, the good bad-guys manipulate the street lights to confuse cops and bad bad-guys
- At least here, the street didn’t collapse sending a target truck down into the sewers

Who us?? No Way!!

- Jan 8, 2007 – both Patel and Murillo plead not guilty
- Free on their own recognizance – 2 conditions
  - No access to city computers
  - No physical access to DOT facilities without their attorneys
- Large number of co-workers on hand to support their two union colleagues
- Virtual receiving line outside the courtroom

Economic Reality

- Clifford Neuman, a computer security expert and the director of the USC Center for Computer Systems Security, said there are two primary ways to design computers to guard against malicious activity by insiders, but each can interfere with employees’ ability to do their tasks and would probab prohibitively expensive for the city.

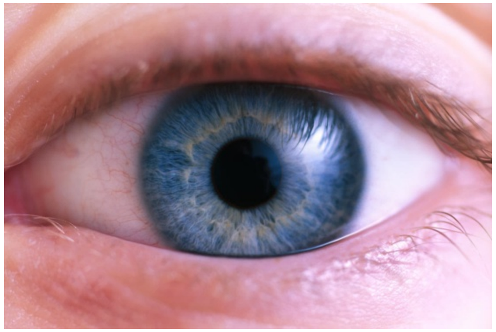
Economic Reality

- Neuman was really saying that utility trumps security in management’s eyes
- Probably true, but it also makes internal bad guys even more dangerous

- And both of these statements accentuate the necessity and value of an effective awareness program – one that stresses the probability of being caught and the consequences

Plea Deal

- Both must pay restitution
- Serve 120 days in jail or 240 hours of community service
- Submit to having their home and work computer user monitored



- Despite pleading guilty to a felony, both men would be sentenced to one misdemeanor count and, after a brief period of probation, the count would be dismissed and their criminal records expunged

Why So Lenient?

- Book *Traffic* details how they do similar things as part of the job, especially on Oscar night, when they have to try to make sure that stars' limousines arrive at the theater on time in spite of LA Monday night rush hour traffic and gawkers trying to get there to see their favorite stars.
- Both Murillo and Patel are reportedly very good at managing traffic

- LA wants the stars to get to the red carpet on time
- Brad and Angelina should NOT be stuck in traffic

Defense Counsel’s Perspective

- Murillo’s attorney, James Blatt
- "This was an emotional collective-bargaining strike situation," Blatt said. "This should have been handled administratively. Mr. Murillo and Mr. Patel are outstanding citizens and have devoted a significant part of their professional lives to transportation safety in Los Angeles County.”

Questions

- How did they so easily get access to manager ID’s?
- Can these ID’s be accessed remotely?
- What kind of protection is on them?
- How come no firecall ID for instant fix?
- Is there a backup site?
- Where?
- Immediate failover or switchover?
- Four days to recover?

Questions

- Could a Security Awareness Program have prevented this incident?
- Is any shop with a union subject to this type of “coercion?”
- What punishment do you think would be appropriate for this action?
- What steps would you have taken to minimize the damage?
- Whose fault was this?
  - Perpetrators? Union? Managers? Mayor? Governator?

What if ???

- One (or both) of them was not an “outstanding citizen”
- They really wanted to cause mayhem
- They had premeditated this attack and destroyed backups and recovery capabilities
- The city had taken a hard stance against the union
- The disgruntled employees had been security professionals at ATSC

What if ???

- This had been Oscar night, not the end of August
- Another emergency had hit the city while this was going on:
  - Earthquake
  - Fires
  - Smog alert
  - ???

What if ???

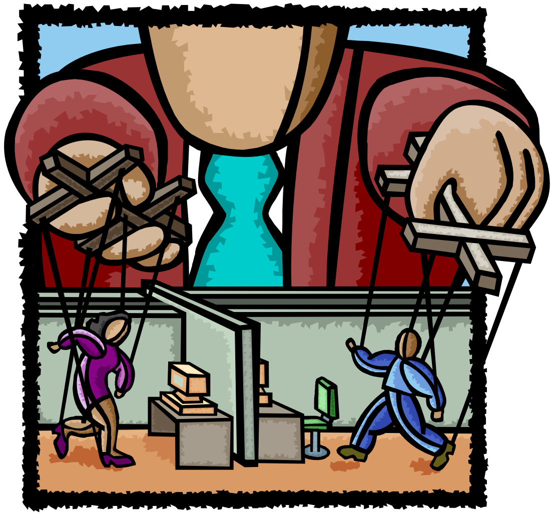
- It was an outsider who broke into the system and he didn’t know how to effect disruption without damage
- The knowledgeable employees were being blackmailed or otherwise coerced
- It was an outside agency who wanted to cause maximum carnage and disruption
- They hadn’t been able to recover in 4 days

Lessons for FISSEA

- The insider threat is real and potentially disastrous
  - The more they know, the more responsibility they have, the more damage they can do
- It's not always easy to predict the culprits
  - Both Patel and Murillo were long-term employees with excellent records
  - Patel was cited in *Traffic* for his legerdemain at Oscar time

Lessons for FISSEA

- Management will often give higher priority to operational items than to our security concerns
  - We can whine all we want, but that’s a fact of life, and it’s not going to change
  - They’re paid to manage and live with risk
  - Not all risk is information security-related



Lessons for FISSEA

- Awareness efforts should mostly stress the good things, but consequences for violations are an important element
  - Employees need to know that there are detection and logging controls, but not where they are, how they operate and how they differentiate between normal and malicious activity
  - They also need to know the policy basis for consequences and any history of enforcement

Lessons for FISSEA

- Sometimes, in spite of our best efforts and meticulously engineered and delivered awareness programs, some people either don’t get the message or choose to ignore it
  - We still need all those other controls, too

Epilogue

- Oct 2007 – LA reaches agreement with unions for 22,000 workers on 5-year contract
- Very little acrimony
- Used facilitators to keep emotion out of the talks
- “I think we did get most of what we wanted,” said Efren Corall, who drives a city truck that picks up recyclable trash. “Not to get too specific, but there were a few things that we thought better to wait for in terms of benefits. What we really wanted, too, was to be able to contribute ideas.”

- The last contract agreement with a city union came after a period of discord. In August 2006, about 7,500 members of the Engineers and Architects Assn. staged a two-day walkout; in January they received a 9% raise over three years in a new contract.

Sources

- LA Times reports by
  - Sharon Bernstein
  - Andrew Blankstein
  - Steve Hymon
- Cbs2.com
- Postings by Darren Murph
- Story by John Leyden in *Enterprise Security*
- Book – *Traffic* by Tom Vanderbilt

Summary

- We've covered:
  - Basic Facts/Background
  - Disruption
  - Economic Reality
  - Consequences(?)
  - Questions Raised
  - What If? .....
  - Lessons for FISSEA

Final Words

- Thank you for your
  - Patience
  - Attention
  - Comprehension

- Please keep up your good work and the good work of FISSEA