Pretending to Be a Terrorist
كيف تكون إرهابي

"The Jihadist Adventures of Tyler & Steve"

Infidels!
The Target

Something East
Why Test Security?

- Considerable Increase in Digital & Physical Threats
- False Sense of Security
- Complacency About Security
- Executive Leadership Needed to Understand the Risks
Goals

Collect As Much Intelligence As Possible
Use Digital and Analog Tactics for Entry
Gain Access to Facilities 1 & 2
Photograph an Ethernet Jack
Leave Something As Your Mark

I’d Come Out Of The Bottle For This Job.
The Target

Location 1
The Target

Location 2
The Target

Get Inside!

I’m Not a Terrorist?
Methods of Intelligence Gathering

COMMUNICATIONS INTELLIGENCE - COMINT

ELECTRONIC INTELLIGENCE - ELINT

SIGNAL INTELLIGENCE - SIGINT

HUMAN INTELLIGENCE - HUMINT

Intelligence?
Methods of Intelligence Gathering

OSINT
Anything Publically Available
OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD), as "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."
Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy."
PROCESS OSINT
Other Business Uses
FOR THESE BUSINESS PURPOSES

These are not allowed:

- Pretexting
- Phishing
- Collaboration
- Any Communication

These are not allowed.
Reconnaissance for Defeating Security
FOR TESTING SECURITY

These are allowed:

- Pretexting
- Phishing
- Collaboration
- Any Communication
- Deception
Forbidden

- Call in Bomb Threat, Pulling Fire Alarms
- Hostage Taking, Bribery or Insider Collusion
- Posing as a State, Local or Federal Employee

Rosie O'Donnell
Khalid Shaikh Mohammed
OSINT Process For People Intelligence

Attaching the Person to a Digital Entity

Email
Username
Phone Number
Anchor Points
OSINT Process For Business Intelligence

Attaching the Business to a Digital Entity

- Domain
- Employee Emails
- Phone Numbers
- Anchor Points
OSINT Process

Attaching the Person/Business to a Digital Entity

Attaching the Target to Digital Content or Analog Data
Sources of Intelligence

OSINT
1000+ Social Networking / Media Sites

200 Million+

Blog Sites

Any Public Data
What Do We Look For?

Anything ...

- Social Networking Sites
- Blog Sites
- Property Information
- Email Addresses
- Login User Names
- Domain Ownership
- Phone Numbers
- Vendor Information

Anything Publically Visible on the Internet
Things We Learned

- Who They Used As Approved Vendors
- Identified Phone Numbers
- Property Maps and Building Details
- Employees and Upper Management Names
- News and Media Content About Facilities
Things We Learned

Who They Used As Approved Vendors

Construction Contractors

Technology Vendors

Delivery Services

Local Police

Security Services
Things We Learned

Identified Phone Numbers

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Site</th>
<th>Department</th>
<th>Pager Number</th>
<th>Work Phone 1</th>
<th>Work Phone 2</th>
<th>Work Ext.</th>
<th>Job Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Brown</td>
<td>Phoenix, AZ</td>
<td>Human Resources</td>
<td>N/A</td>
<td>602-555-5555</td>
<td>N/A</td>
<td>555-5555</td>
<td>Manager</td>
</tr>
<tr>
<td>Jane Johnson</td>
<td>Salt Lake City, UT</td>
<td>IT Management</td>
<td>N/A</td>
<td>801-222-2222</td>
<td>N/A</td>
<td>222-2222</td>
<td>IT Specialist</td>
</tr>
<tr>
<td>Michael Smith</td>
<td>Bradenton, FL</td>
<td>Payroll</td>
<td>N/A</td>
<td>941-333-3333</td>
<td>N/A</td>
<td>333-3333</td>
<td>Payroll Manager</td>
</tr>
<tr>
<td>Sarah Miller</td>
<td>Beaverton, OR</td>
<td>Human Resources</td>
<td>N/A</td>
<td>503-444-4444</td>
<td>N/A</td>
<td>444-4444</td>
<td>Customer Service Representative</td>
</tr>
<tr>
<td>Jason Garcia</td>
<td>Bradenton, FL</td>
<td>Operations</td>
<td>N/A</td>
<td>941-555-5555</td>
<td>N/A</td>
<td>555-5555</td>
<td>Operations Manager</td>
</tr>
<tr>
<td>Emily Lee</td>
<td>Sioux Falls, SD</td>
<td>Human Resources</td>
<td>N/A</td>
<td>605-777-7777</td>
<td>N/A</td>
<td>777-7777</td>
<td>Benefits Specialist</td>
</tr>
<tr>
<td>Mark Harris</td>
<td>Bradenton, FL</td>
<td>Benefits</td>
<td>N/A</td>
<td>941-666-6666</td>
<td>N/A</td>
<td>666-6666</td>
<td>Benefits Coordinator</td>
</tr>
<tr>
<td>John Davis</td>
<td>Bradenton, FL</td>
<td>IT</td>
<td>N/A</td>
<td>941-777-7777</td>
<td>N/A</td>
<td>777-7777</td>
<td>IT Technical Support</td>
</tr>
<tr>
<td>_CFG_INCO</td>
<td>Bradenton, FL</td>
<td>Sales</td>
<td>N/A</td>
<td>941-888-8888</td>
<td>N/A</td>
<td>888-8888</td>
<td>Sales Representative</td>
</tr>
<tr>
<td>Lisa Jordan</td>
<td>Bradenton, FL</td>
<td>Payroll</td>
<td>N/A</td>
<td>941-999-9999</td>
<td>N/A</td>
<td>999-9999</td>
<td>Payroll Specialist</td>
</tr>
<tr>
<td>Amy Sanchez</td>
<td>Bradenton, FL</td>
<td>New Client Team</td>
<td>N/A</td>
<td>941-777-7777</td>
<td>N/A</td>
<td>777-7777</td>
<td>New Client Team Coordinator</td>
</tr>
<tr>
<td>Rachel Evans</td>
<td>Bradenton, FL</td>
<td>New Client Team</td>
<td>N/A</td>
<td>941-666-6666</td>
<td>N/A</td>
<td>666-6666</td>
<td>New Client Team Manager</td>
</tr>
<tr>
<td>Maria Smith</td>
<td>Costa Mesa, CA</td>
<td>Benefits</td>
<td>N/A</td>
<td>714-555-5555</td>
<td>N/A</td>
<td>555-5555</td>
<td>Benefits Coordinator</td>
</tr>
<tr>
<td>Ryan White</td>
<td>Newport Beach, CA</td>
<td>Benefits</td>
<td>N/A</td>
<td>305-333-3333</td>
<td>N/A</td>
<td>333-3333</td>
<td>Benefits Specialist</td>
</tr>
<tr>
<td>Mark Wilson</td>
<td>Sarasota, FL</td>
<td>Sales</td>
<td>N/A</td>
<td>941-777-7777</td>
<td>N/A</td>
<td>777-7777</td>
<td>Sales Manager</td>
</tr>
<tr>
<td>Sarah Brown</td>
<td>Sarasota, FL</td>
<td>Payroll</td>
<td>N/A</td>
<td>941-888-8888</td>
<td>N/A</td>
<td>888-8888</td>
<td>Payroll Coordinator</td>
</tr>
<tr>
<td>David Lee</td>
<td>Bradenton, FL</td>
<td>Finance</td>
<td>N/A</td>
<td>941-999-9999</td>
<td>N/A</td>
<td>999-9999</td>
<td>Finance Manager</td>
</tr>
<tr>
<td>Emily Brown</td>
<td>Bradenton, FL</td>
<td>Payroll</td>
<td>N/A</td>
<td>941-777-7777</td>
<td>N/A</td>
<td>777-7777</td>
<td>Payroll Specialist</td>
</tr>
</tbody>
</table>

Security
Accounts Payable
Human Resources
Info Tech.
Shipping.
Things We Learned

Property Maps and Building Details

Property Maps

Schematics

Building Layout
Things We Learned

Employees and Upper Management Names

Org Charts
Senior Mgmt.
Important People
Things We Learned

News and Media Content About Facilities

- Announcements
- Partnerships
- Technologies
- Public Service
- Anything
Other Sources of Intelligence
OSINT in Inspire

I READ THIS!
Open Source Jihad

A resource manual for those who loathe the tyrants; includes bomb making techniques, security measures, guerrilla tactics, weapons training and all other jihad related activities.

Informal A disaster for the repressive imperialistic nations: *The open source jihād is America’s worst nightmare.*

It allows Muslims to train at home instead of risking a dangerous travel abroad: *Look no further, the open source jihād is now at hands reach.*

“Open Source Jihad”

*It’s Almost Like My Name!*

“Infidel!”

Terrorists Adopted the Methodology
“Terrorist Recognition Handbook”

Same Tools and Techniques

- Night-vision equipment.
- Cameras.
- Video cameras.
- Vehicles for drop-off and pickup.
- Payment for informers or insiders.
- Computers.
- Darkroom with photo-processing chemicals.
- Digital systems printer for photo enhancement.

Tactical Operations Cells
- Rifles, pistols, and machine guns.
- Explosives and grenades.
- Chemicals.
- Weapons of mass destruction components.
- False identity documents.
- Vehicles.

Methods of Acquiring Supplies

Legally: Terrorists use themselves or supporters to acquire materials and supplies legally on the open market.

Illegally: Terrorists steal the equipment they need themselves or purchase it on the black market.

- Amateur crime: Terrorists may use low-level criminal methods such as robbery or theft as a way to acquire equipment, systems, and weapons or their components.
- Professional crime: Terrorists may use highly involved and developed criminal pathways, pipelines, and institutions to covertly acquire materials. This includes international gun smuggling, illicit commercial transactions, and false bank transfers.

Detecting Terrorist Logistics Cells

Logistics cells have a higher probability of being...
Reconnaissance
Things We Learned

- Guard Shack Requires Everyone to Check In
- Everyone is Badged and use RFID Card Access
- Cameras Positioned Throughout Entire Property
- Area is Fenced and Topped with Razor Wire
- Fence is Tied to Motion and Heat Sensors
- Guards are Armed
- Guards Have Guns

I'd Come Out Of The Bottle For This.
Attack Plans
Plan 1-Hail Mary Plan

Drop Tyler Off at Obscure Point

X

Location 1
Plan 1-Hail Mary Plan

Climb Fence and Throw Car Mat Over Razor Wire
Plan 1-Hail Mary Plan

Run Across Parking Lot

Location 1
Plan 1-Hail Mary Plan

Wait By Door to Tail Gate In

Location 1
Plan 1-Hail Mary Plan

Location 2 is far more difficult
Plan 1-Hail Mary Plan

PLAN WAS SCRAPPED

Cameras
Fence Sensors
Being Seen
Doors Locked
Guns
Plan 2- Special Delivery

Pose as a Trusted and Approved Vendors
Plan 2- Special Delivery

- Pose as a Trusted and Approved Vendors
- Leverage Identified Phone Numbers
- Deliver Something Big and Special
- Create a Diversion
Plan 2 - Special Delivery

Active Jobs

<table>
<thead>
<tr>
<th>ID</th>
<th>Range</th>
<th>CallerID</th>
<th>Seconds</th>
<th>Lines</th>
<th>Status</th>
<th>Progress</th>
<th>Start Time</th>
<th>Stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>XXXX</td>
<td>XXXX</td>
<td>53</td>
<td>1</td>
<td>active</td>
<td>7%</td>
<td>2009-04-05 13:06:45 EDT</td>
<td></td>
</tr>
</tbody>
</table>

Submit a New Job

The target telephone range (1-123-456-XXXX)
Plan 2 - Special Delivery

Attack Vector - War Dial

WARVOX

BRILLIANT!

Need This To Name Drop
Plan 2- Special Delivery

STINKIN BADGES!
Plan 2- Special Delivery

Ahhh!!!... I Like The Red Coat!
Plan 2- Special Delivery
Plan 2- Special Delivery

THE PHONE IS THIS BIG!
First Attempt
Location 2
Plan 2-Special Delivery

LOCATION 2 IS FAR MORE DIFFICULT
First Attempt- Building 2

Logic For Hitting The Tougher Location First

- IF BREACHED THE OTHER SHOULD BE EASY
- MINIMIZE EXPOSURE IF CAUGHT
- POSSIBLE TO STILL BREACH OTHER BUILDING
First Attempt - Building 2
First Attempt- Building 2
He Has a Whistle and a GUN!!!
First Attempt - Building 2
First Attempt - Building 2

DANGER

Arc flash and Shock Hazard
Appropriate PPE Required

______ Inch Flash Hazard Boundary
cal/cm² Flash Hazard at ____ inches

Class 1 PPE Level: Cotton Underwear, FR Shirt & Pants, Hard Hat,
Safety Glasses, Hearing Protection, Rubber/Leather Gloves,
Leather Work Shoes

______ VAC Shock Hazard with cover removed
__ Inch Limited Approach
__ Inch Restricted Approach
__ Inch Prohibited Approach
How Long Are You Going to Be In There?
First Attempt - Building 2

Mission Accomplished
I'm Not Wearing a Santa Hat!!!
Second Attempt
Location 2
Second Attempt-Building 2

BUILDING 2 USES ACTUAL POLICE AS GUARDS

FEDEX...YOU’RE ON THE LIST.
Second Attempt-Building 2

OSINT DATA PAID OFF
Second Attempt-Building 2

WAITED FOR 30 - 40 MINUTES
Second Attempt-Building 2

WAITED FOR 30 - 40 MINUTES
Second Attempt-Building 2

He Waited
Second Attempt - Building 2

PARTIAL SUCCESS
I Like Chocolate Bunny!

Second Attempt-Building 2
Thank You.