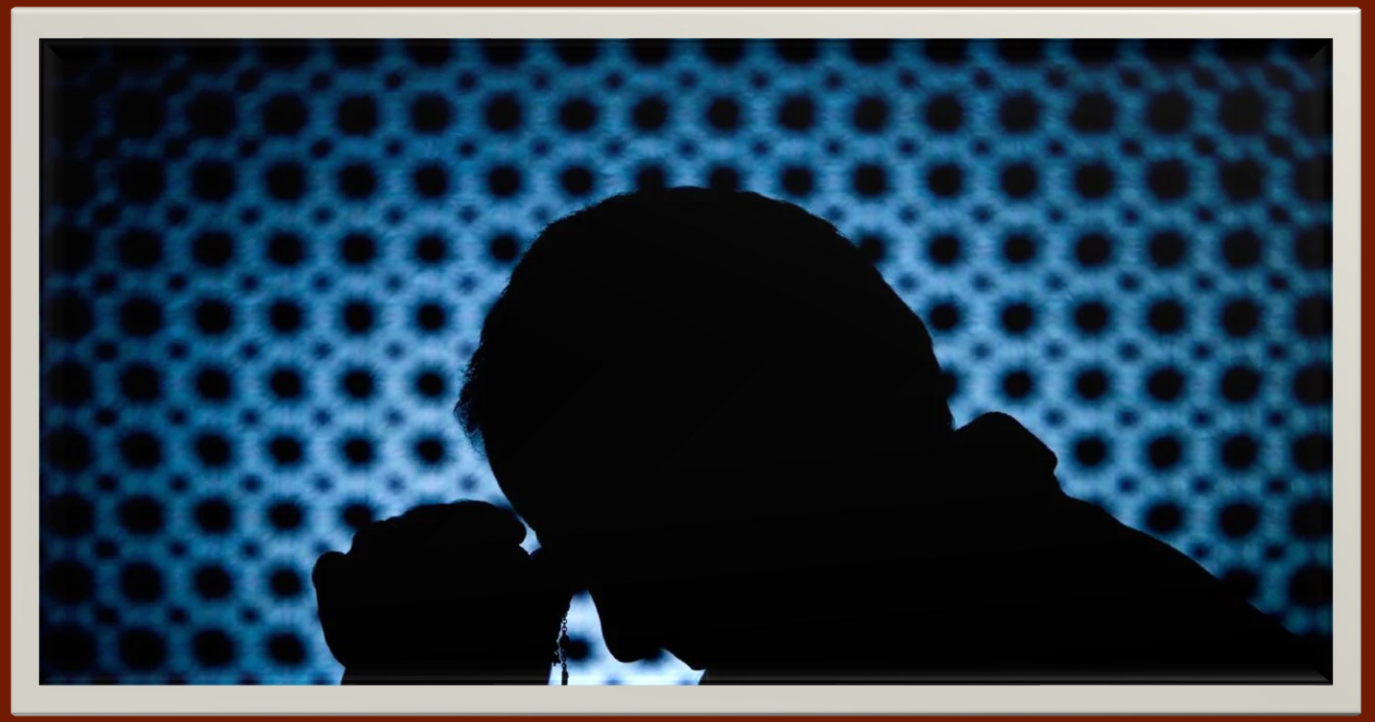
CONFESSIONS OF A SPY

HUMAN HACKING - IDENTIFYING THREATS AND BEST PRACTICES



Seminar for ACFE Heartland Chapter
May 7, 2022

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



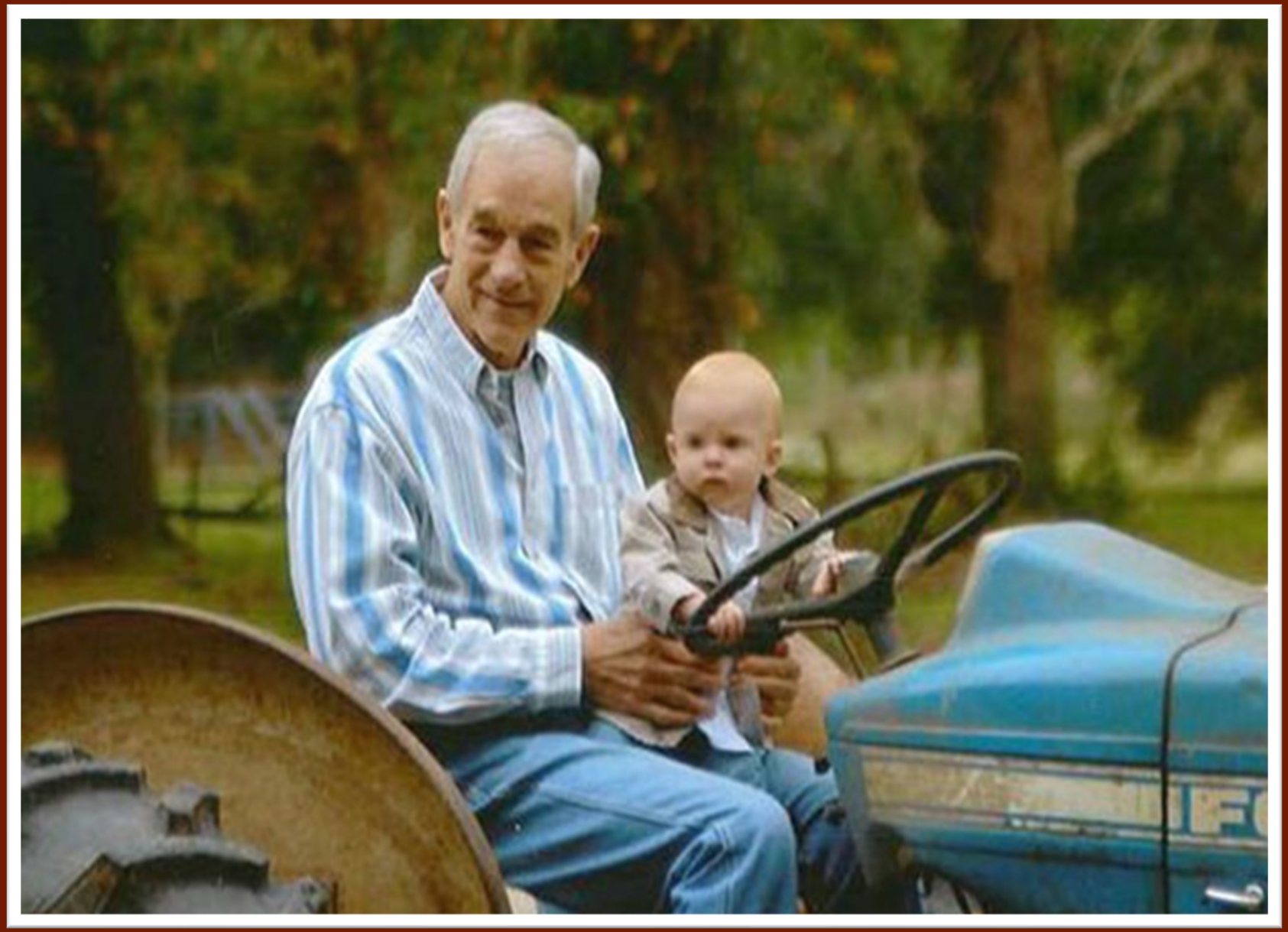
© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



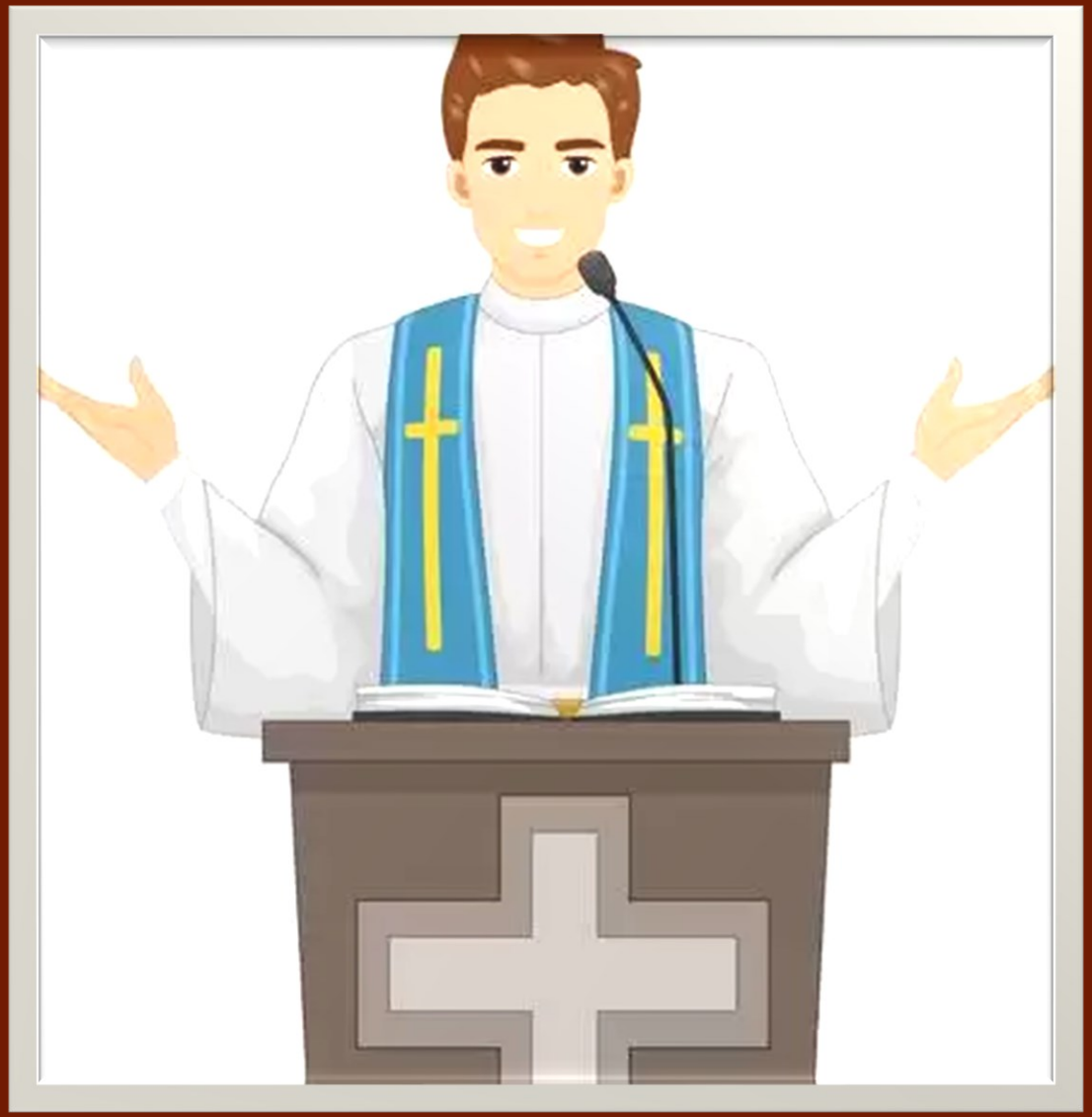
© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



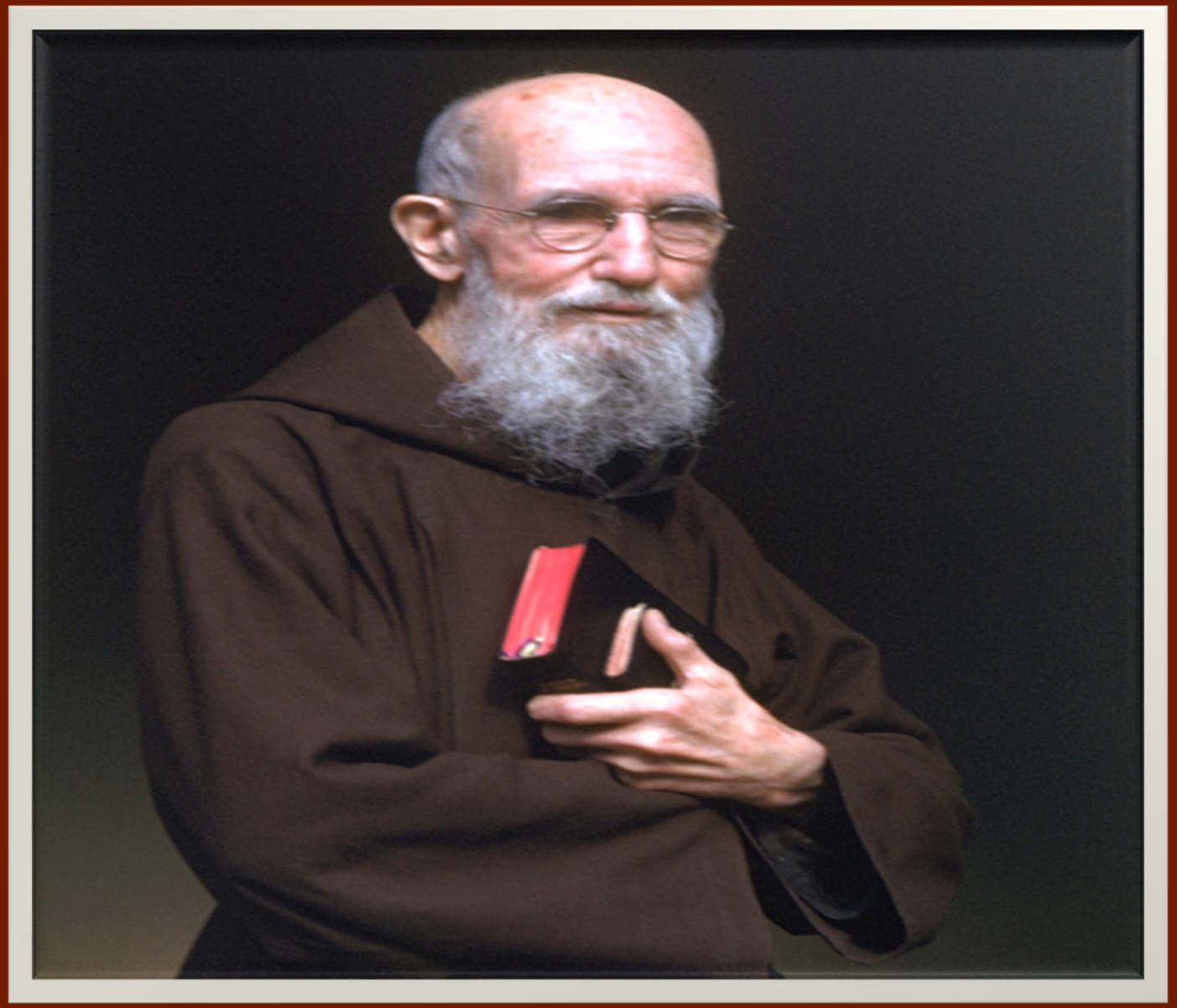
© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

SOCIAL ENGINEERING HUMAN HACKING MANIPULATION



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



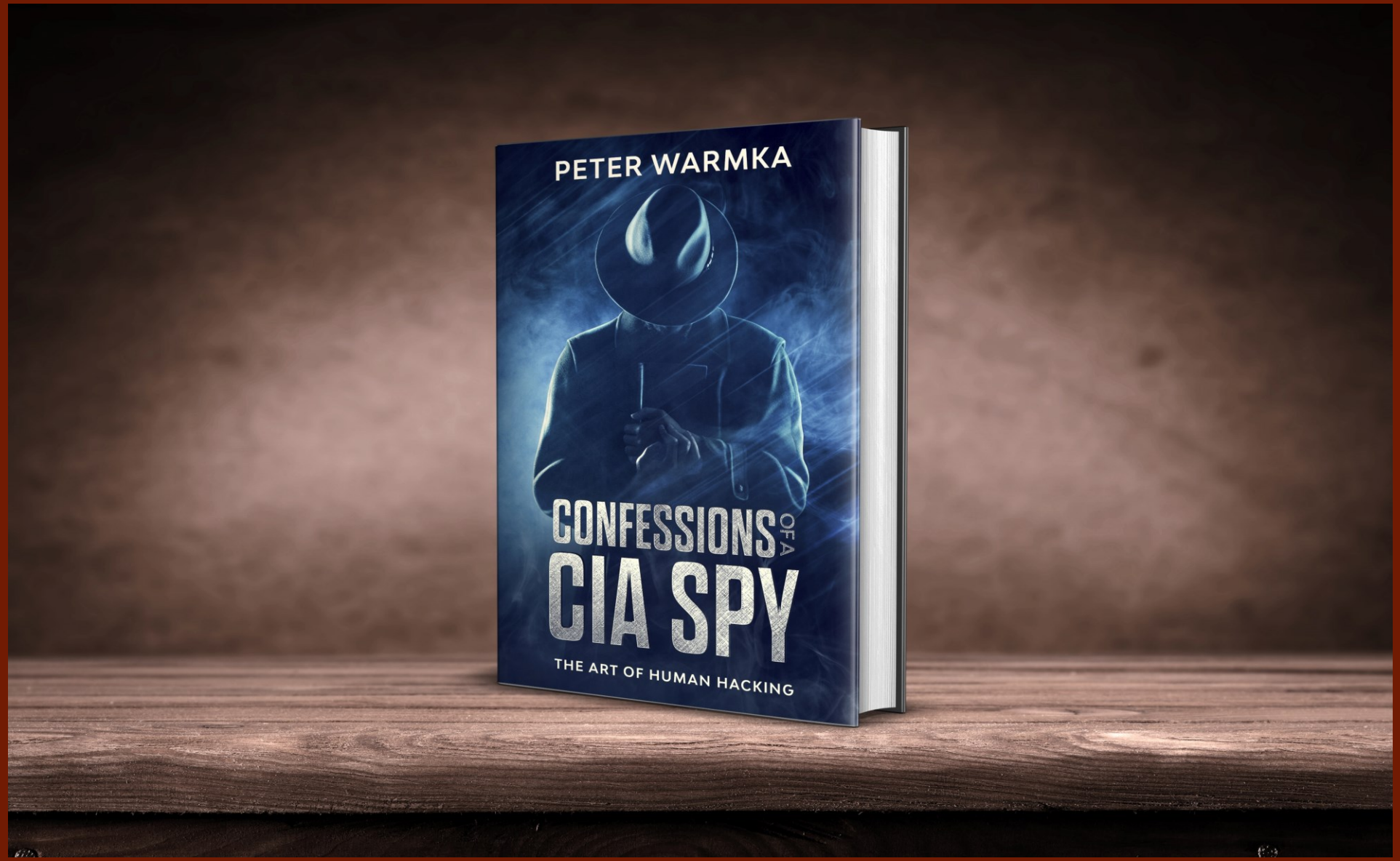
© COUNTERINTELLIGENCE INSTITUTE, LLC



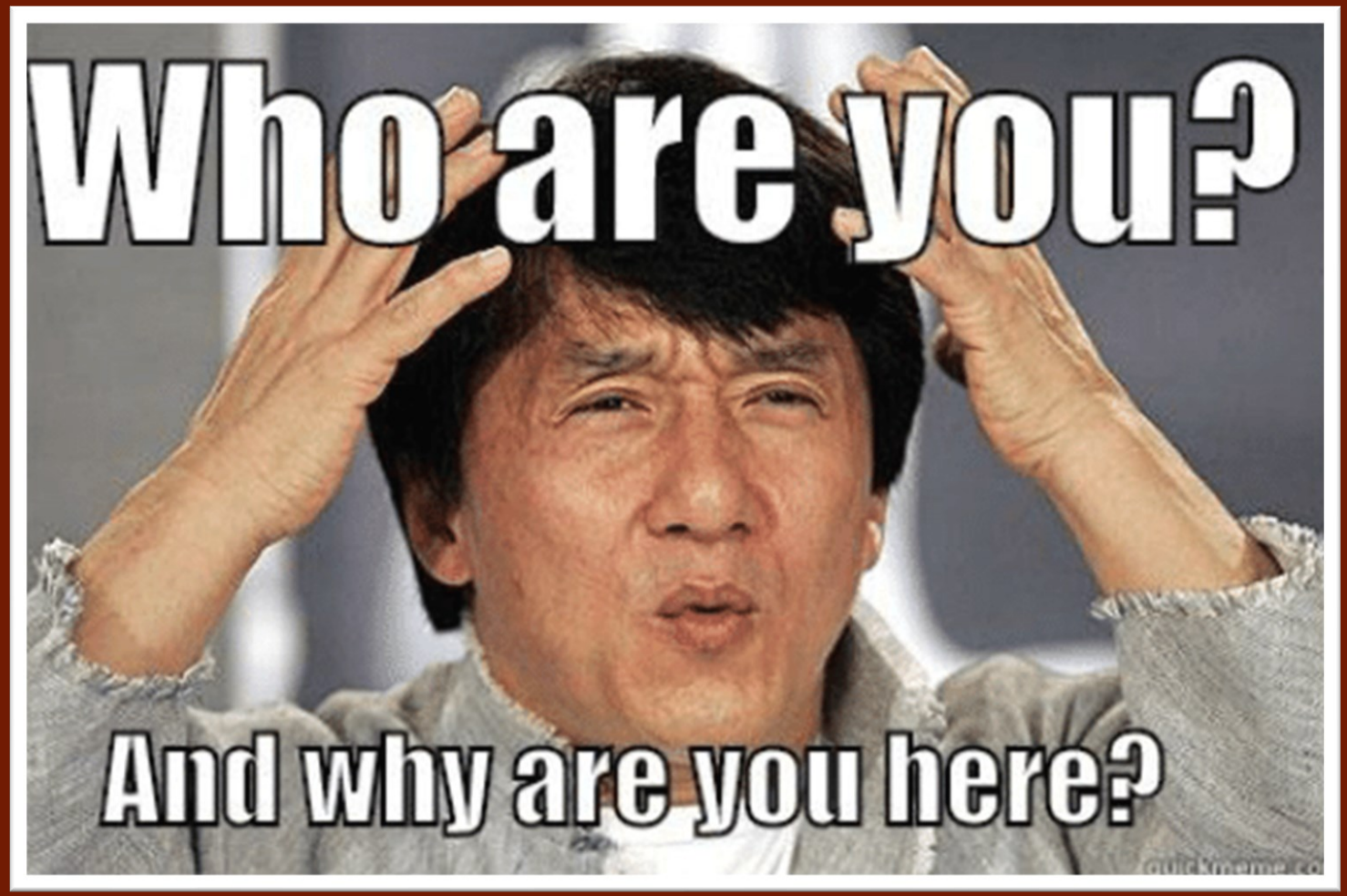
© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

AGENDA

- Introduction to Data Breaches
- Threat Actors
- Organizational Targeting
- Identification and Assessment of Insiders
- The Art of Elicitation
- Trust and Social Engineering (SE) Influence Techniques
- SE Attack Vectors – Spear Phishing, Smishing, Vishing and Face-to-Face
- Conclusion

© COUNTERINTELLIGENCE INSTITUTE, LLC

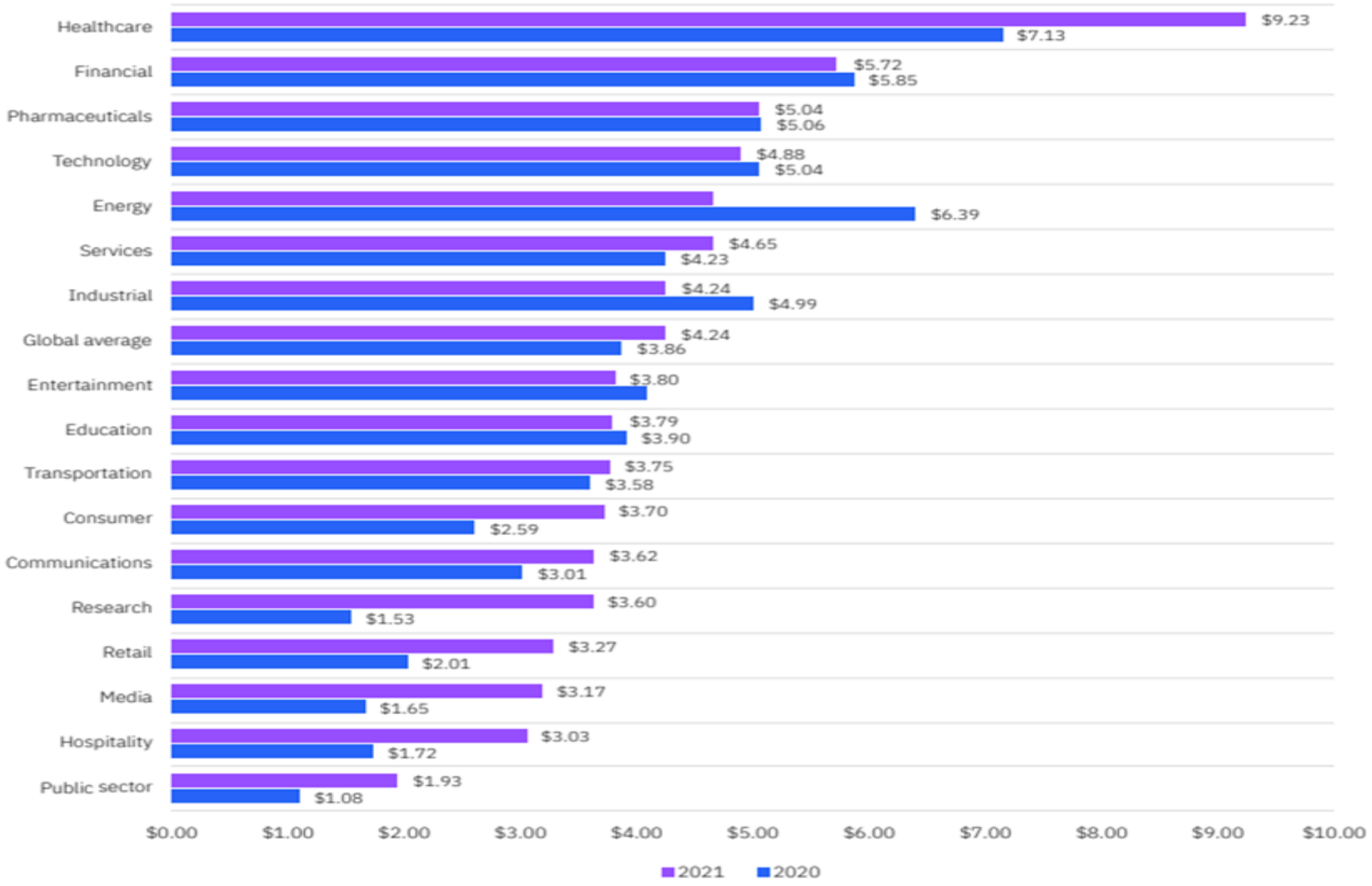
MAGNITUDE OF THE PROBLEM

- 2021 was a costly year for data breaches and we are still climbing the hill. (IBM Security)
- Average cost of a data breach worldwide in 2021: $4.24 million. (IBM Security)
- Average cost of data breach in U.S. during 2021: $9 million. (IBM Security)
- During 2021 there were more than 1,862 ***publicly disclosed*** breaches exposing 25 billion compromised records. (Security Magazine)
- Over 90 percent of successful data breaches are initiated by social engineering (Verizon)

© COUNTERINTELLIGENCE INSTITUTE, LLC

Average total cost of a data breach by industry

Measured in US$ millions



© COUNTERINTELLIGENCE INSTITUTE, LLC

IBM Security

- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

© COUNTERINTELLIGENCE INSTITUTE, LLC

- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

© COUNTERINTELLIGENCE INSTITUTE, LLC



WHO IS RESPONSIBLE WITHIN AN ORGANIZATION?

- Chief Information Security Officer
- Director of Security
- HR Director
- General Counsel
- CFO
- CEO
- Board of Directors
- The CFE practitioner

© COUNTERINTELLIGENCE INSTITUTE, LLC

THREAT ACTORS

Who are they and what do they want with your organization?

© COUNTERINTELLIGENCE INSTITUTE, LLC



Threat Actor

Criminal Group

Intelligence Service

Industrial Competitor

Activist Group

Lone Wolf

Objective

Proprietary Information

Customer Data

Employee Data

Ransomware

Business Email Compromise

Sabotage

Damage to Reputation

Insider

Employee

Contractor

Associated Business

SE Technique

Phishing

Smishing

Vishing

Face-to-Face

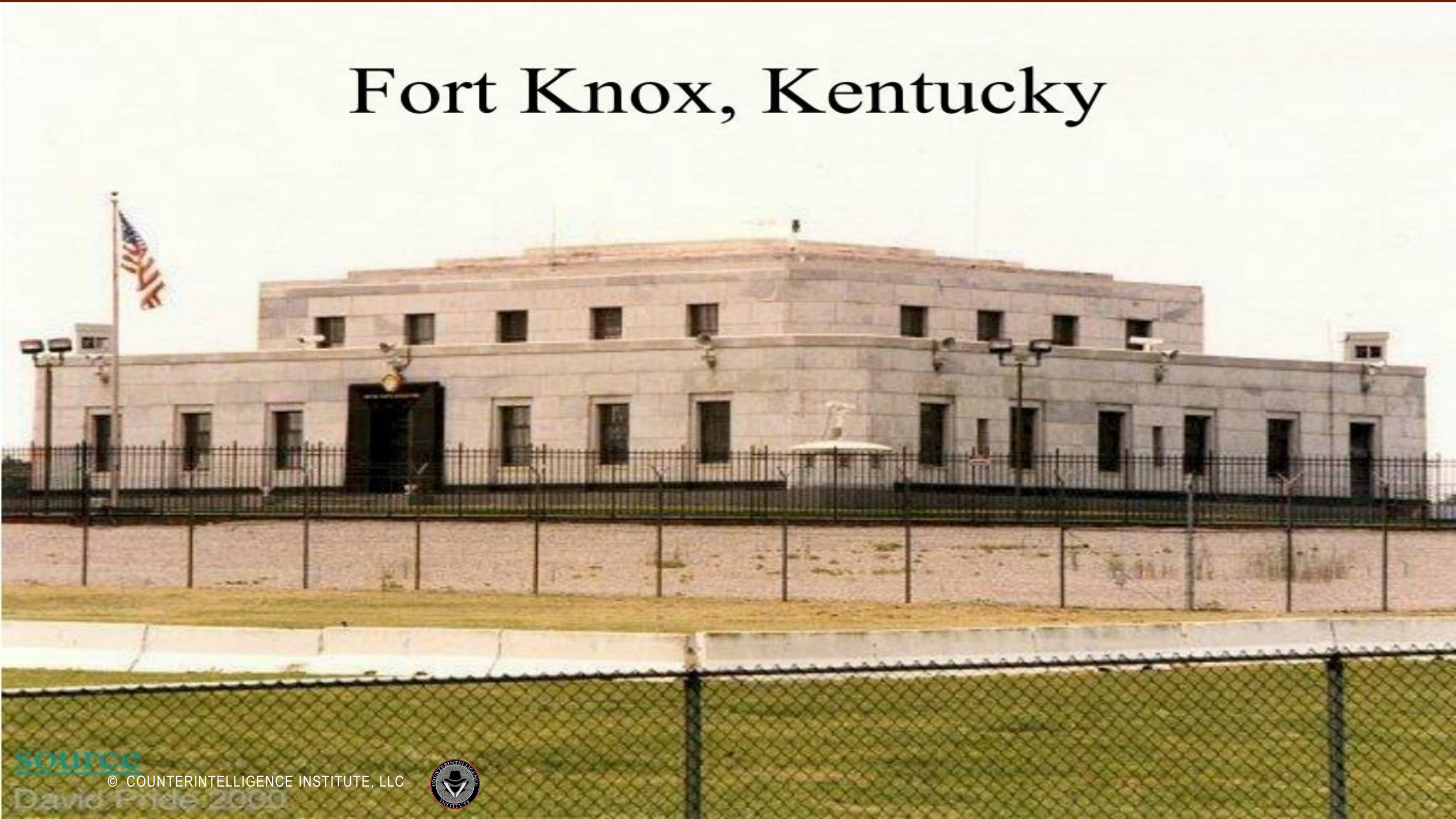
© COUNTERINTELLIGENCE INSTITUTE, LLC

Hah! My firm would never be a target!!!



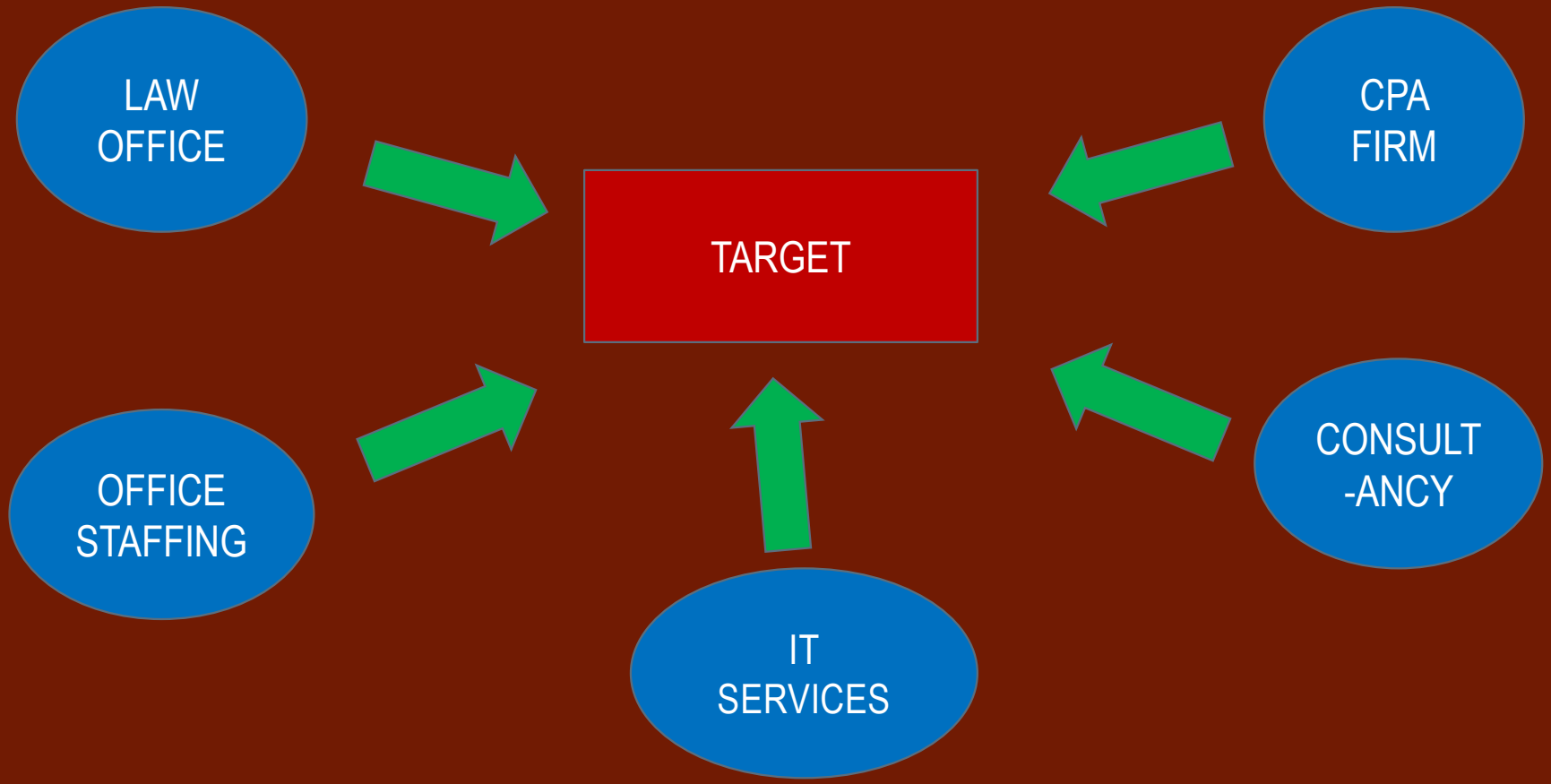
© COUNTERINTELLIGENCE INSTITUTE, LLC

Fort Knox, Kentucky



© COUNTERINTELLIGENCE INSTITUTE, LLC

LEVERAGING BACK DOOR ACCESS



© COUNTERINTELLIGENCE INSTITUTE, LLC

HANDOUT #1

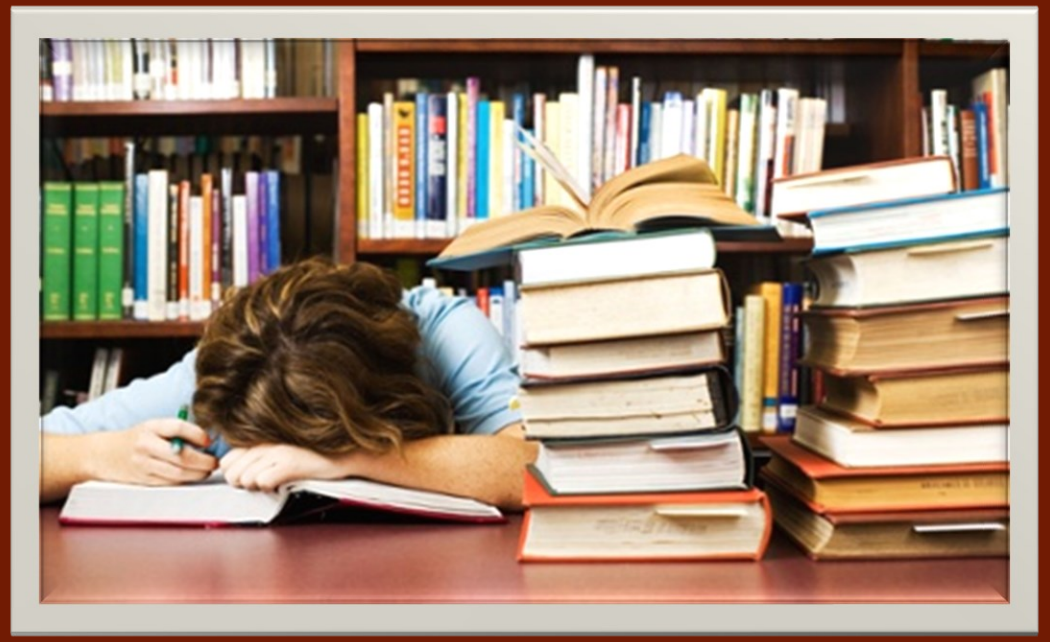
© COUNTERINTELLIGENCE INSTITUTE, LLC

TARGET ANALYSIS

OSINT COLLECTION

© COUNTERINTELLIGENCE INSTITUTE, LLC

COLLECTING INFORMATION ON YOUR ORGANIZATION





© COUNTERINTELLIGENCE INSTITUTE, LLC

COLLECTION ON THE ORGANIZATION

- Organization's Website
- Job Postings
- Glassdoor.com
- Pictures Uploaded by Employees to Social Media

© COUNTERINTELLIGENCE INSTITUTE, LLC

JOB POSTINGS

AWS Data Architect - Kansas City - 140K+

Technical Requirements

Experience implementing AWS Data Services in production
Redshift, EMR, EC2, S3, Athena, RDS, DynamoDB, Kinesis, Glue, etc.
Experience developing distributed data platforms using Spark
Scala, PySpark, Spark-SQL
Experience leveraging Big Data Technologies in Hadoop
Hive, HBase, HDFS, Cassandra, Kafka, Sqoop, etc.
Proficiency in Python, Scala, and/or Java
Proficiency in SQL
Experience with designing and implementing RDBMS
Oracle, PostgreSQL, MySQL, MS SQL Server, etc.

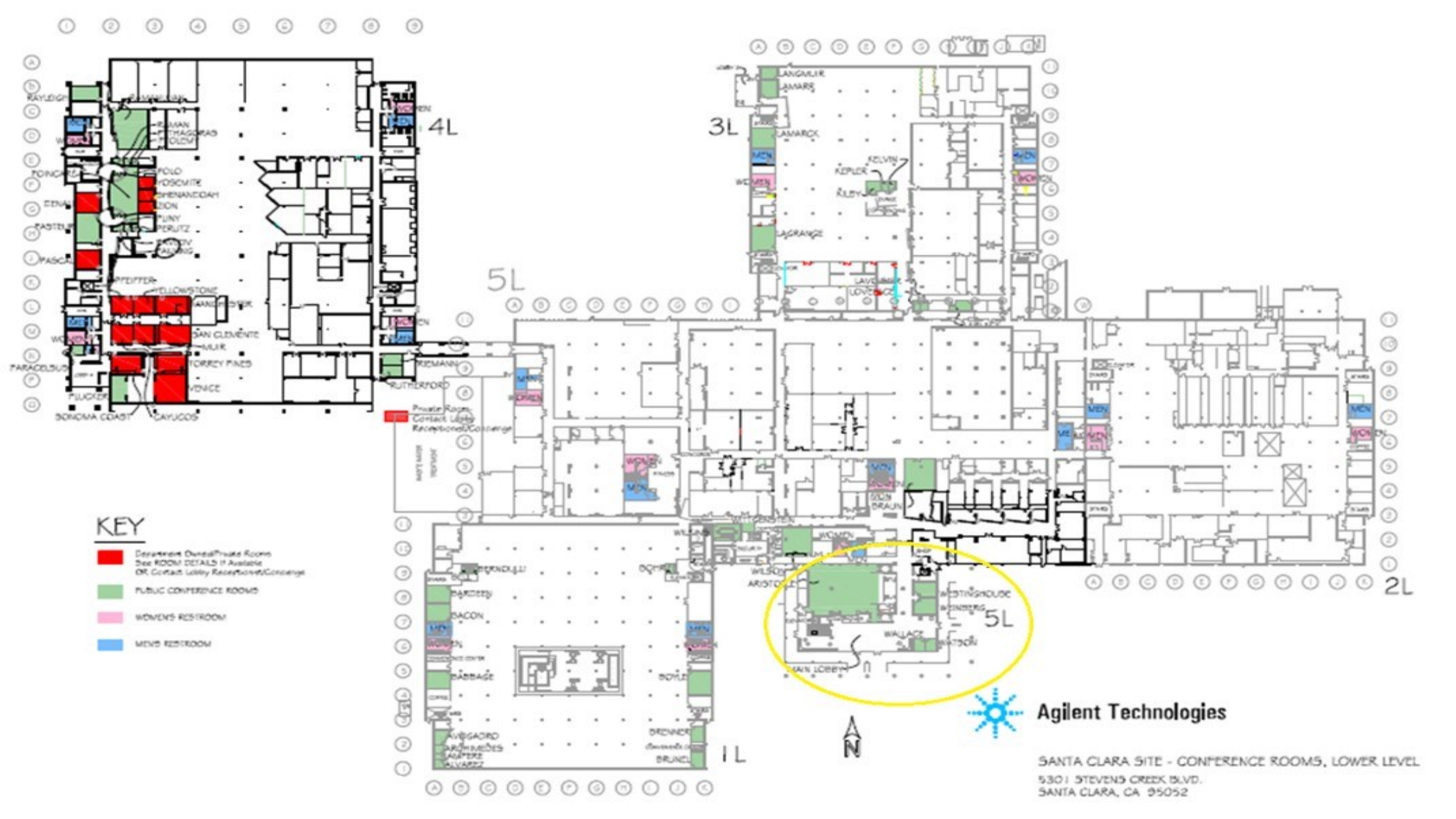
Source: Indeed.com

© COUNTERINTELLIGENCE INSTITUTE, LLC

COLLECTION ON THE ORGANIZATION

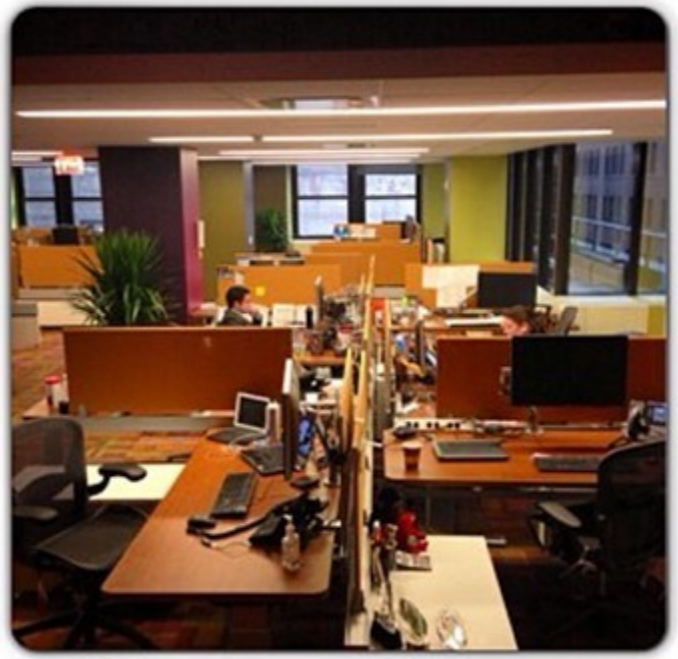
- Organization's Website
- Job Postings
- Glassdoor.com
- Pictures Uploaded by Employees to Social Media

© COUNTERINTELLIGENCE INSTITUTE, LLC


4L
3L
5L
2L
1L
KEY
Private Room
Contact Lobby Receptionist/Concierge
PUBLIC CONFERENCE ROOMS
WOMENS RESTROOM
MENS RESTROOM
Agilent Technologies
SANTA CLARA SITE - CONFERENCE ROOMS, LOWER LEVEL
5301 STEVENS CREEK BLVD.
SANTA CLARA, CA 95052











Example of office layouts

© COUNTERINTELLIGENCE INSTITUTE, LLC





Employee badges.

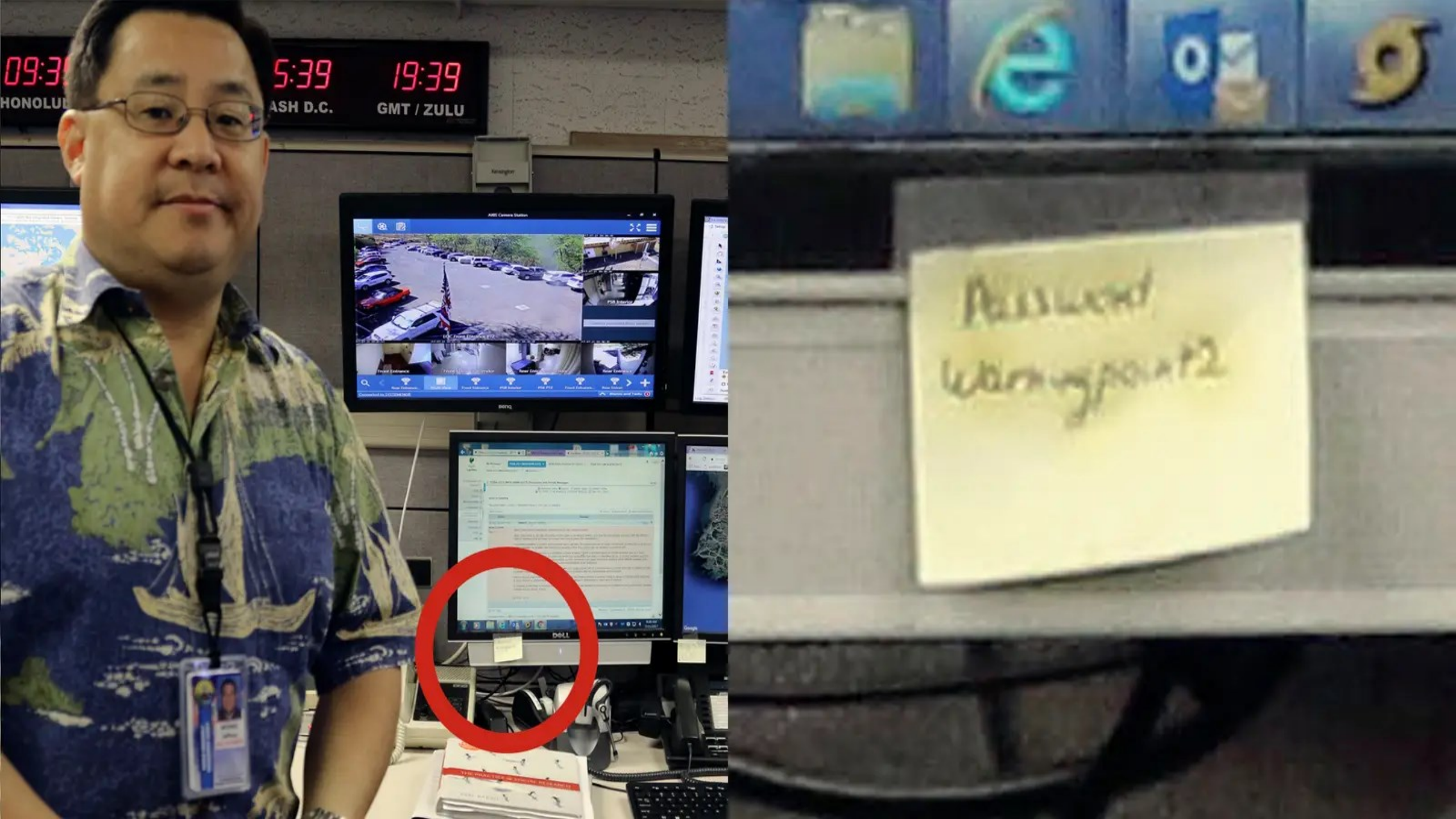
© COUNTERINTELLIGENCE INSTITUTE, LLC

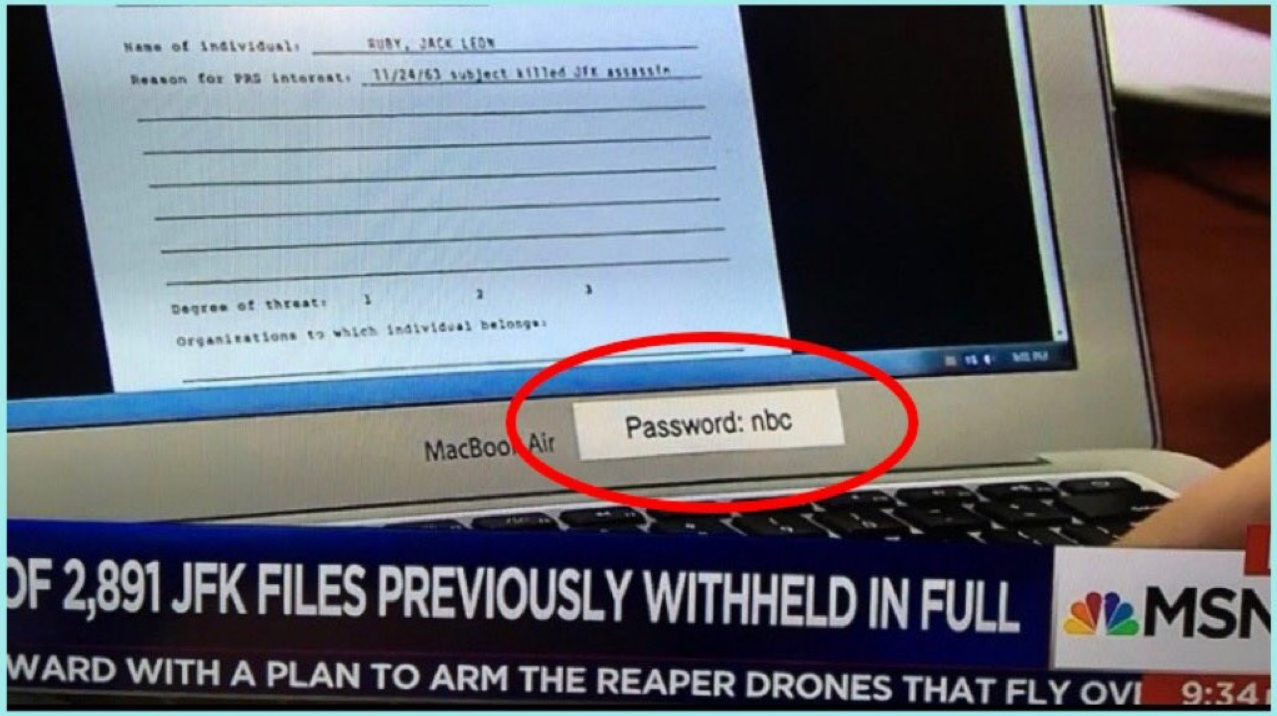


© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC


5:39
ASH D.C.
19:39
GMT / ZULU

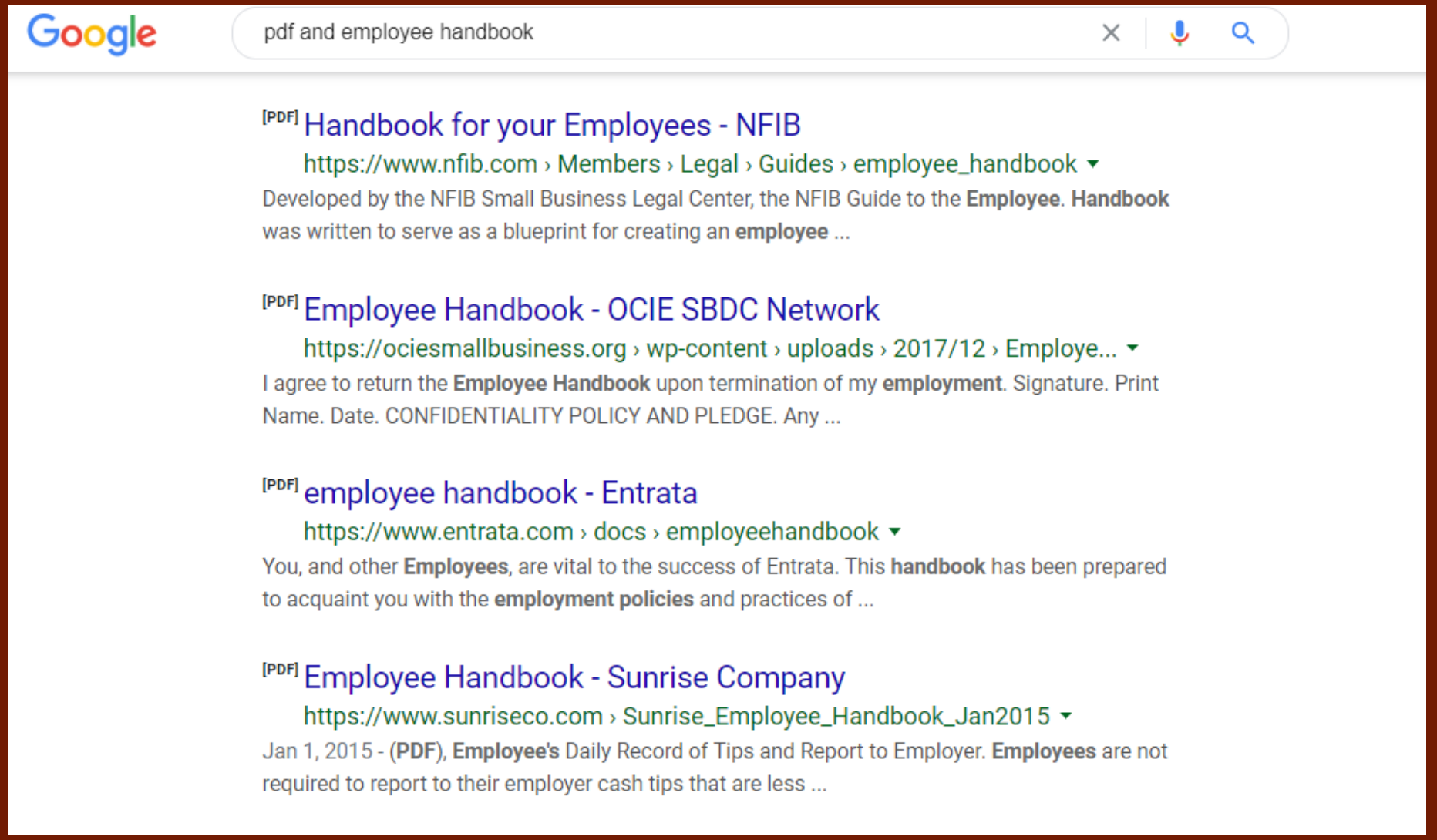

Name of individual: RUBY, JACK LEON
Reason for PRS interest: 11/24/63 subject killed JFK assassin
Degree of threat: 1 2 3
Organizations to which individual belongs:
Password: nbc
OF 2,891 JFK FILES PREVIOUSLY WITHHELD IN FULL
MSN
WARD WITH A PLAN TO ARM THE REAPER DRONES THAT FLY OVI
9:34


Wi-Fi Access
marko
w3Lc0m3!!HERE
case-sensitive
"Forget" or "Remove"
CBS THIS MORNING
SUPER BOWL SECURITY
INSIDE SECRET, FIRST-OF-ITS-KIND COM


2
© COUNTERINTELLIGENCE INSTITUTE, LLC


Username: EmergencyPlanning
Password: Winter14
USE ONLY THE DRY WIPE PENS PROVIDED
ME WEATHER
Flood
PLANNER SIMON PARKER
3 mins
NEWS ALERT
EXTREME WEATHER: FULL WEATHER AND TRAVI

Confidential Documents – Employee Manuals, Employee Benefits, Contracts, NDA's



© COUNTERINTELLIGENCE INSTITUTE, LLC

Press Releases



© COUNTERINTELLIGENCE INSTITUTE, LLC

PRESS RELEASES

Below is an email sent to Uber employees from the company's Board of Directors this evening:

Team,

We are delighted to announce that Uber's Board has voted unanimously to appoint Dara Khosrowshahi to be our new CEO.

Dara came to America at nine years old when his family escaped Iran on the eve of the Iranian Revolution. He grew up in Tarrytown, N.Y., trained as an engineer at Brown, and spent many years at IAC serving as Chief Financial Officer and in various operational and strategic roles.

In 2005, he became CEO of Expedia, which he built into one of the world's leading travel and technology companies, now operating in more than 60 countries. He has four children and not surprisingly loves to travel, one of his favorite trips being to the Angkor Wat temples in Cambodia where his wife Sydney said yes to marrying him……..

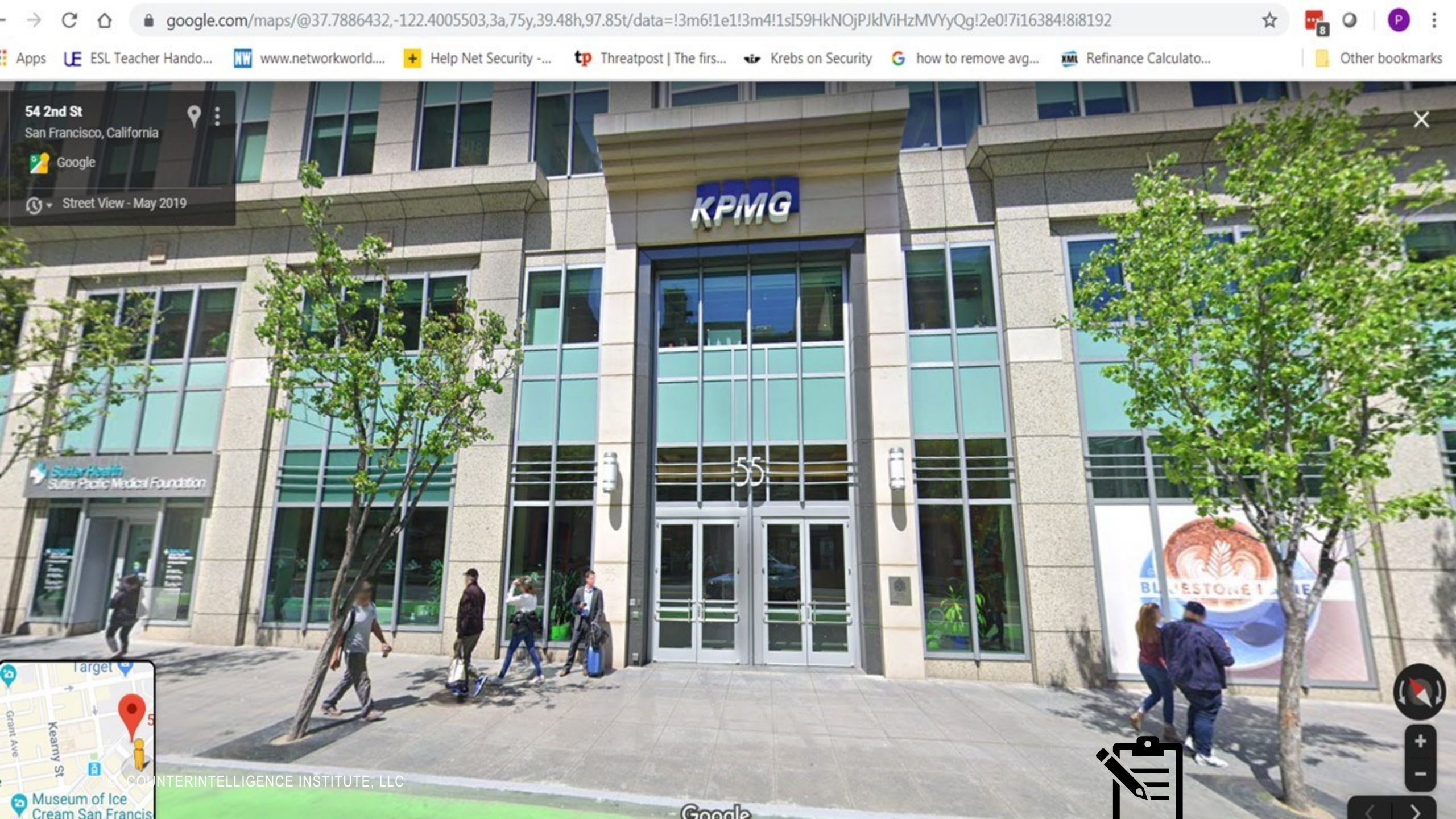
© COUNTERINTELLIGENCE INSTITUTE, LLC

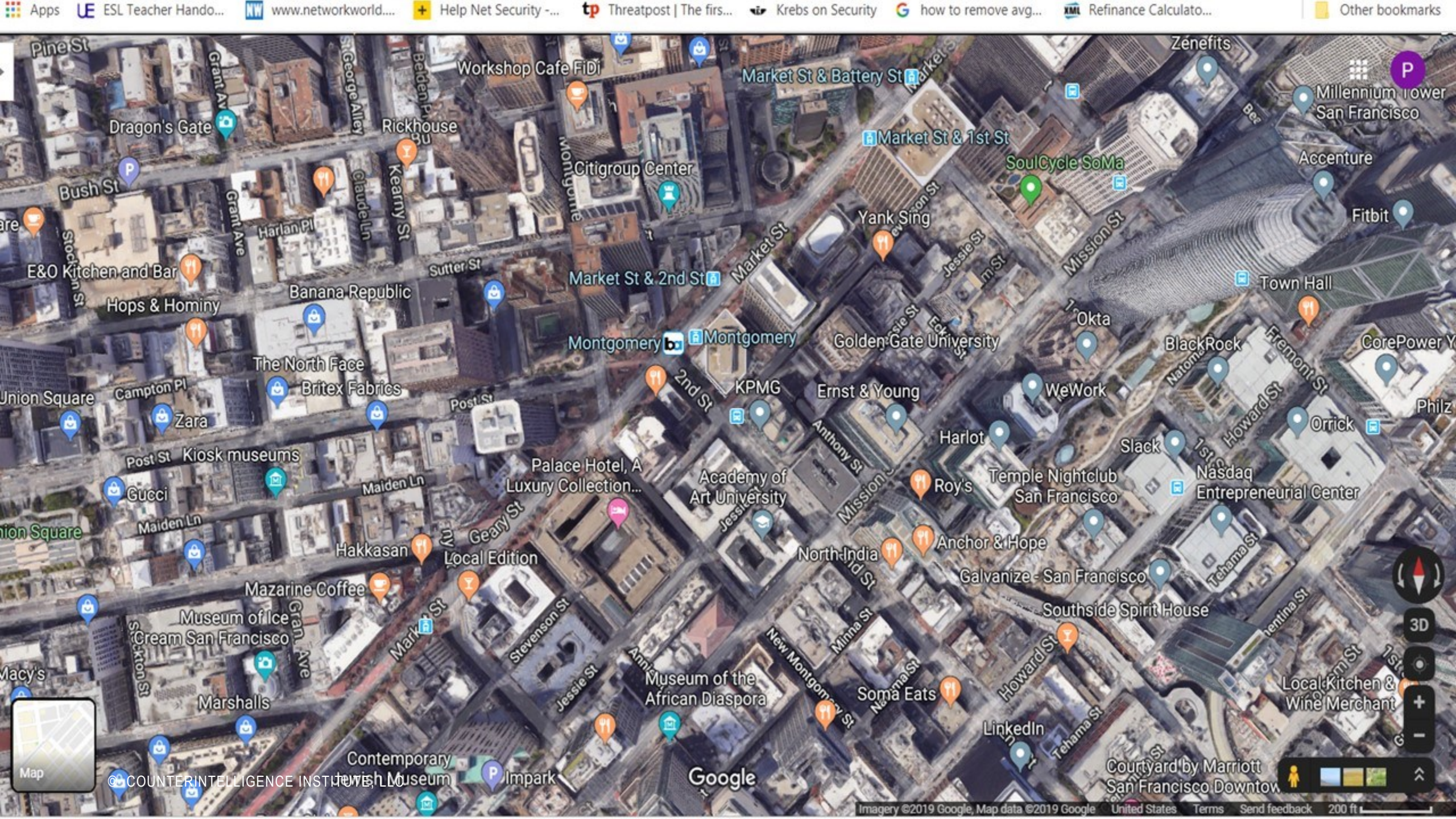


© COUNTERINTELLIGENCE INSTITUTE, LLC

RECONNAISSANCE




google.com/maps/@37.7886432,-122.4005503,3a,75y,39.48h,97.85t/data=!3m6!1e1!3m4!1sI59HkNOjPJklViHzMVYyQg!2e0!7i16384!8i8192
Apps
ESL Teacher Hando...
www.networkworld....
Help Net Security -...
Threatpost | The firs...
Krebs on Security
how to remove avg...
Refinance Calculato...
Other bookmarks
54 2nd St
San Francisco, California
Google
Street View - May 2019
KPMG
55
Sutter Health
Sutter Pacific Medical Foundation
Target
Grant Ave
Kearny St
Museum of Ice Cream San Francis
© COUNTERINTELLIGENCE INSTITUTE, LLC
Google


Apps
ESL Teacher Hando...
www.networkworld....
Help Net Security -...
Threatpost | The firs...
Krebs on Security
how to remove avg...
Refinance Calculato...
Other bookmarks
Pine St
Grant Ave
St George Alley
Belden Pl
Workshop Cafe FiDi
Market St & Battery St
Zenefits
Millennium Tower San Francisco
Dragon's Gate
Rickhouse
Bush St
Harlan Pl
Claude Ln
Kearny St
Montgomery
Citigroup Center
Market St & 1st St
SoulCycle SoMa
Accenture
Fitbit
Yank Sing
Mission St
Stockton St
E&O Kitchen and Bar
Sutter St
Market St & 2nd St
Market St
Banana Republic
Hops & Hominy
Town Hall
Montgomery
Golden Gate University
Okta
BlackRock
Fremont St
CorePower Y
The North Face
Britex Fabrics
KPMG
Ernst & Young
WeWork
Howard St
Philz
Union Square
Campton Pl
Zara
Post St
Kiosk museums
Gucci
Palace Hotel, A Luxury Collection...
Academy of Art University
Harlot
Slack
Orrick
Temple Nightclub San Francisco
Roy's
Nasdaq Entrepreneurial Center
Maiden Ln
Geary St
Hakkasan
Local Edition
Anchor & Hope
North India
Galvanize - San Francisco
Mazarine Coffee
Museum of Ice Cream San Francisco
Stevenson St
Minna St
Southside Spirit House
Tehama St
Macy's
Marshalls
Jessie St
Museum of the African Diaspora
Soma Eats
Howard St
LinkedIn
Local Kitchen & Wine Merchant
Contemporary Jewish Museum
Impark
Courtyard by Marriott San Francisco Downtow
Google
Map
3D
© COUNTERINTELLIGENCE INSTITUTE, LLC
Imagery ©2019 Google, Map data ©2019 Google
United States
Terms
Send feedback
200 ft

HANDOUT #2

© COUNTERINTELLIGENCE INSTITUTE, LLC

Conduct your research with Handout #2



© COUNTERINTELLIGENCE INSTITUTE, LLC

INSIDERS

Selection and Assessment

© COUNTERINTELLIGENCE INSTITUTE, LLC







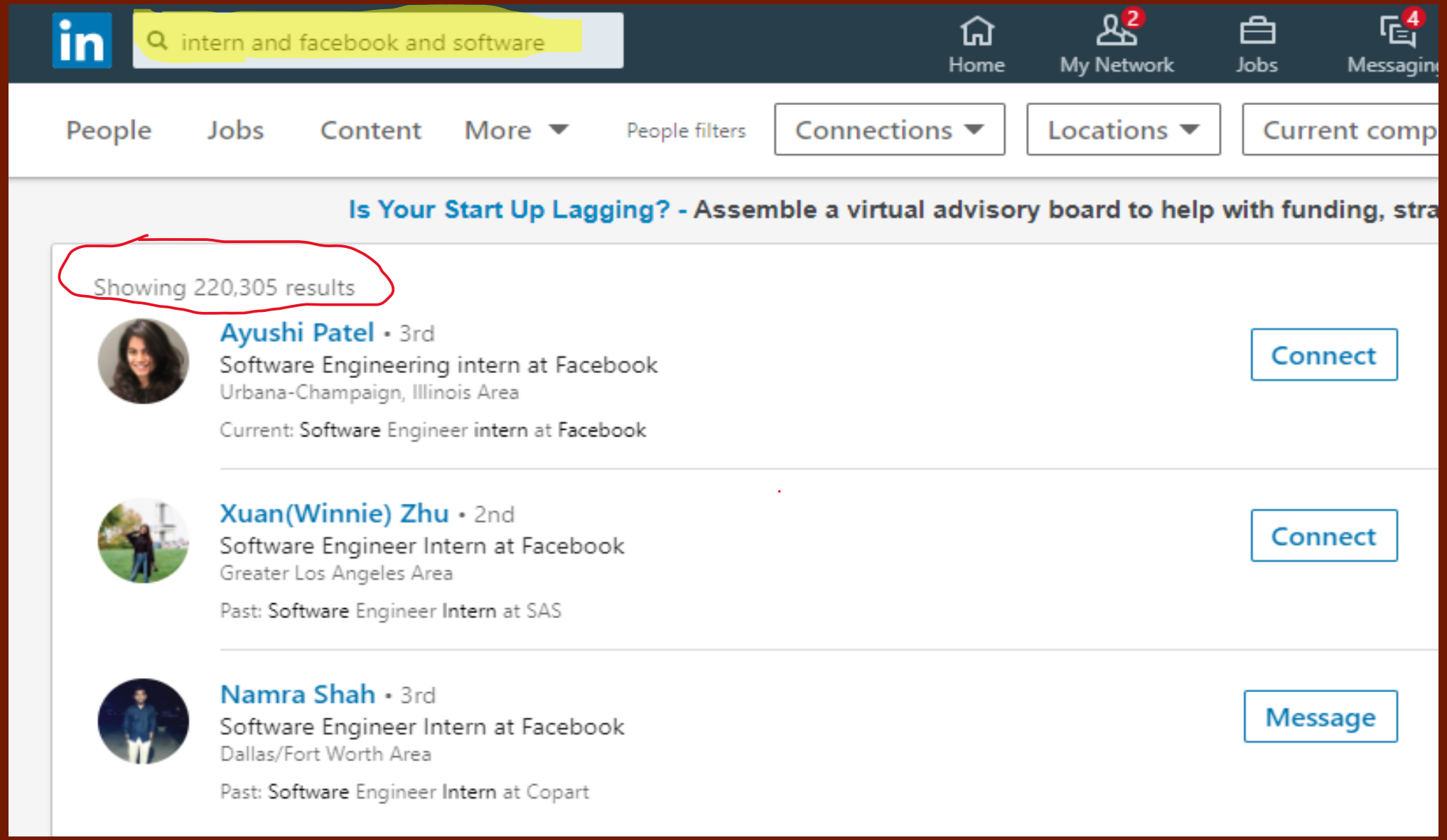
THE INSIDERS







© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

“TIME ON TARGET”



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTER[illegible]E INSTITUTE, LLC

RESEARCH INSIDERS ON SOCIAL MEDIA

- LinkedIn: academic and work experience, career aspirations (from about them as well as influencers), certifications and licenses, affiliations with associations, volunteer work, network of contacts

- Facebook: hobbies, interests, sports teams, music genre, favorite foods, travel, social economic status, close friends and family members, etc.

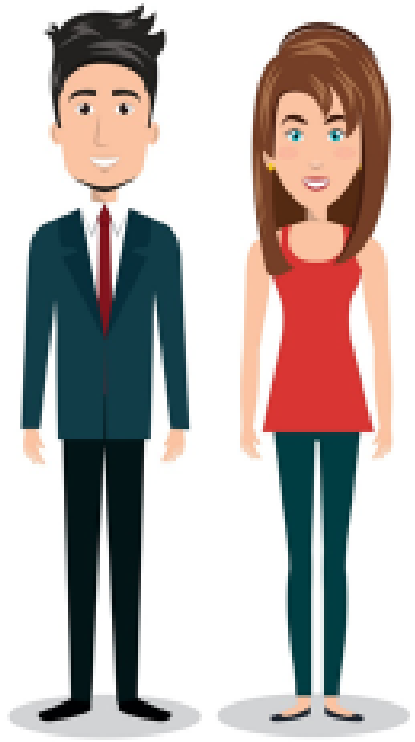
- Twitter: opinions, political leanings, ideology, religion, pet peeves, etc.

- Instagram: Pattern of Life

© COUNTERINTELLIGENCE INSTITUTE, LLC

Human Motivations

- Family
- Money
- Education
- Career
- Better home
- Luxury goods
- Desires/wants
- Ideology
- Religion
- Politics
- Excitement



Human Vulnerabilities

- Money
- Gambling
- Drinking to excess
- Drug addiction
- Sex
- Greed
- Hate/Revenge
- Jealousy
- Guilt
- Ego
- Low self-esteem

HANDOUT #3

© COUNTERINTELLIGENCE INSTITUTE, LLC

THE ART OF ELICITATION



© COUNTERINTELLIGENCE INSTITUTE, LLC

HANDOUT #4

© COUNTERINTELLIGENCE INSTITUTE, LLC

SOCIAL ENGINEERING OPERATIONS



© COUNTERINTELLIGENCE INSTITUTE, LLC

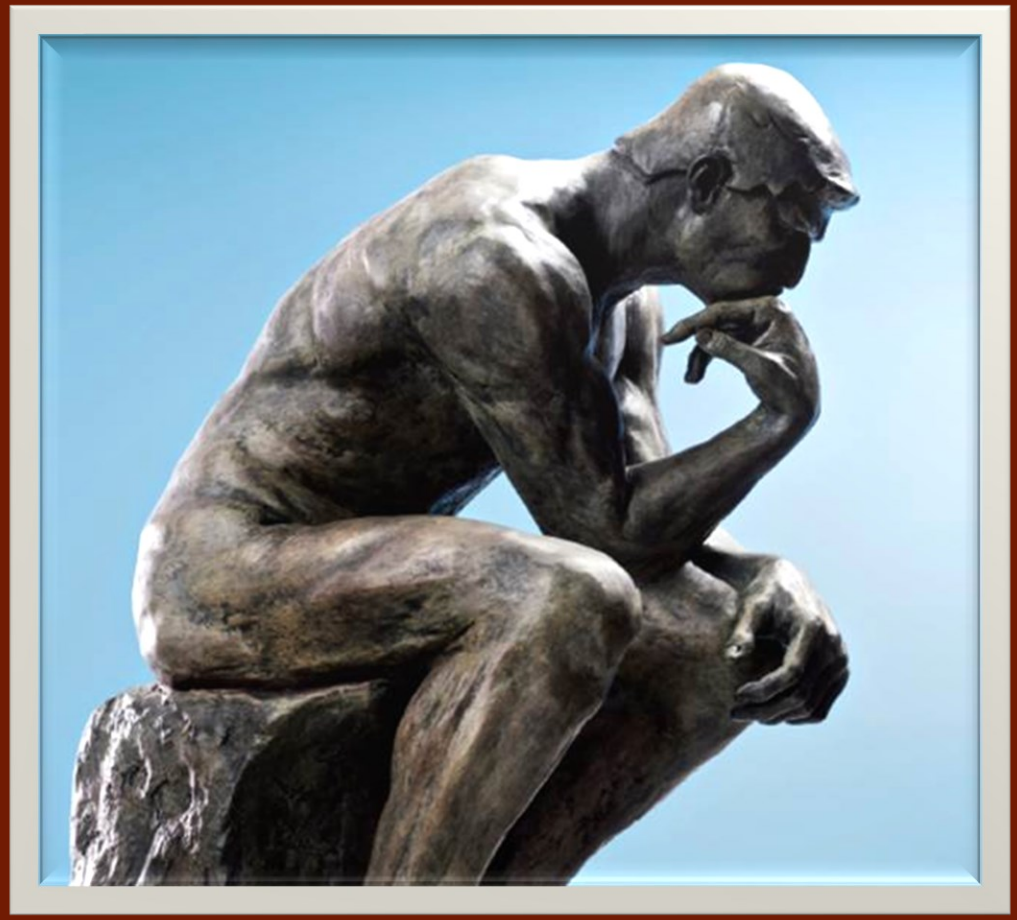
TRUST

&

INFLUENCE TECHNIQUES

© COUNTERINTELLIGENCE INSTITUTE, LLC

WHY ARE HUMANS SO SUSCEPTIBLE TO SOCIAL ENGINEERING?



© COUNTERINTELLIGENCE INSTITUTE, LLC

TRUST



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

BLIND TRUST CAN BE FATAL



© COUNTERINTELLIGENCE INSTITUTE, LLC









© COUNTERINTELLIGENCE INSTITUTE, LLC

WE EXPLOIT TRUST FOR THE GRAND DECEPTION



© COUNTERINTELLIGENCE INSTITUTE, LLC

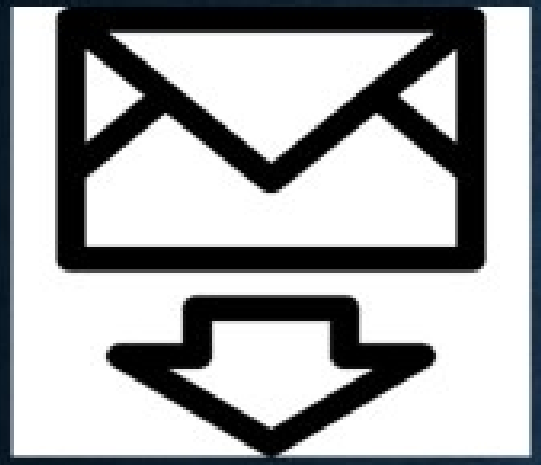
INFLUENCE TECHNIQUES

- Liking
- Scarcity
- Authority
- Reciprocity/Obligation
- Social Proof
- Consistency

© COUNTERINTELLIGENCE INSTITUTE, LLC

HANDOUT #5

© COUNTERINTELLIGENCE INSTITUTE, LLC



HELP!









© COUNTERINTELLIGENCE INSTITUTE, LLC

SE ATTACK VECTORS - 1

Phishing

© COUNTERINTELLIGENCE INSTITUTE, LLC





© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

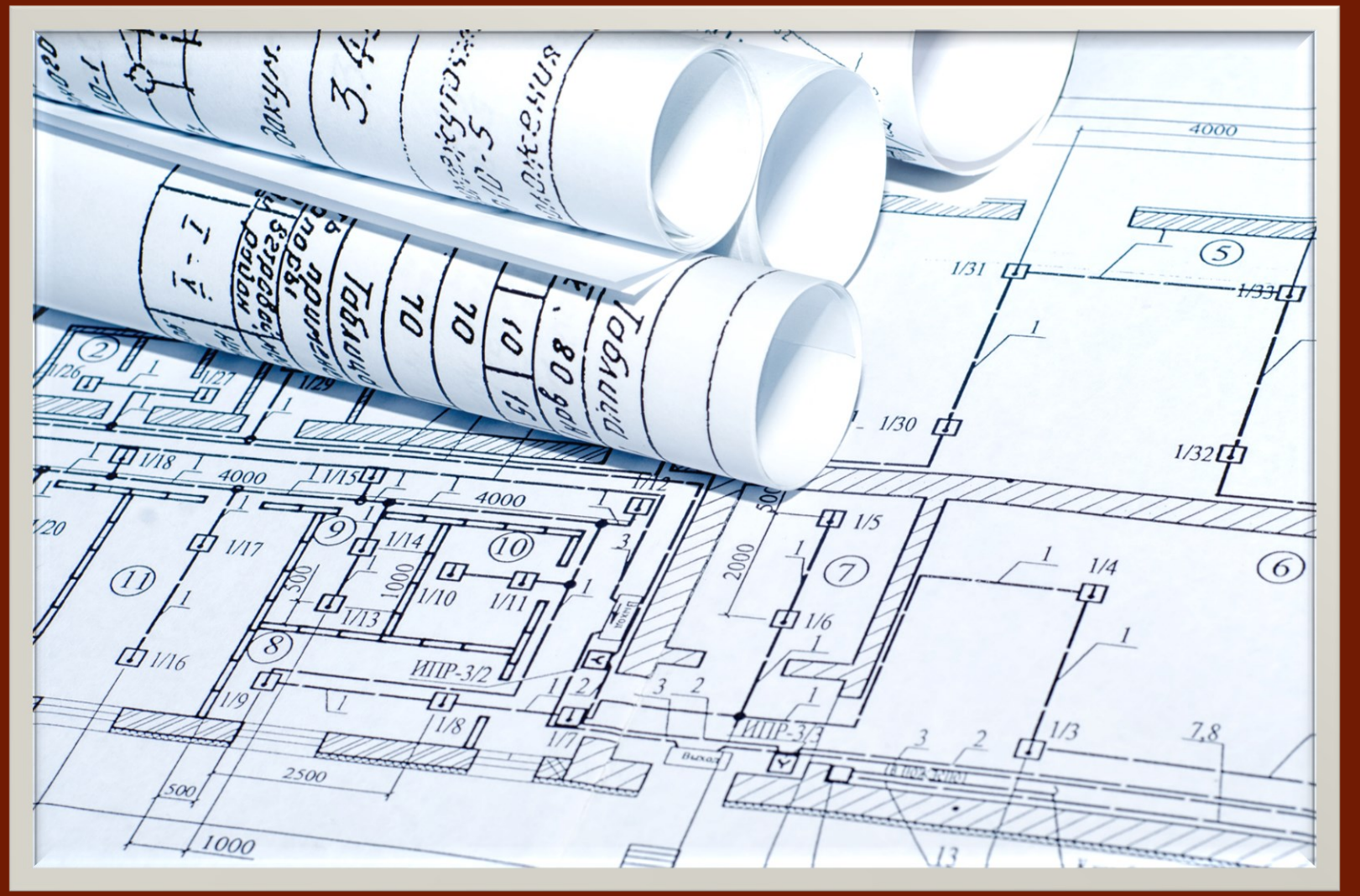


Robert Valencia
CEO
VLT Engineering, Inc.

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTER[illegible]E INSTITUTE, LLC

PROTECTING THEIR TRUE IDENTITY





© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

SOME PROSPECTIVE ON LINKEDIN'S REPORTING ON FAKE PROFILES

- "Between January and June 2019, we took action on 21.6 million fake accounts. This includes:

- Preventing 19.5 million fake accounts from being created at registration.

- Restricting 2 million fake accounts before members reported them and 67,000 following member reports.

- 98% of all fake accounts we prevented or took down were done so through our automated defenses, including artificial intelligence and machine learning. The rest were captured through manual review."

© COUNTERINTELLIGENCE INSTITUTE, LLC



Accept | Ignore | More...

Dave Mitchel · 2nd

Emerging Technology Specialist

Sydney, Australia · 500+ connections · Contact info

Customers btob

Highlights

42 mutual connections

You and Dave both know Paulo Müller, Fausto Tucci, and 40 others

Experience

Business Development Manager

Customers btob

Oct 2003 – Jul 2007 · 3 yrs 10 mos

Sydney, Australia

I was tasked in this role to develop business to business relationships with set targets and KPI's that were exceeded.

I was required to find and nurture my own leads and grow them into strong repeat business that increased over time to grow the key areas of the business and report and interact with key stake holders.

Business Manager

DiNG DiNG

May 1999 – Oct 2003 · 4 yrs 6 mos

Beijing City, China

I manage chinese operation.

Skills & Endorsements

New Business Development · 48

Michelle Elyn Hogan and 47 connections have given endorsements for this skill

Business Strategy · 47

Endorsed by Wilmar Gomes . ' . (mutual connection)

Cloud Computing · 46

Endorsed by Kavit Munshi, who is highly skilled at this

Endorsed by Wilmar Gomes . ' . (mutual connection)

Show more

Interests

On Startups - The Community For ...
626,986 members

FreeMason Networking
16,567 members

Masonic Network
9,715 members

US Government Accountability Offi...
53,301 followers

Innovative Uses of HPC
1,285 members

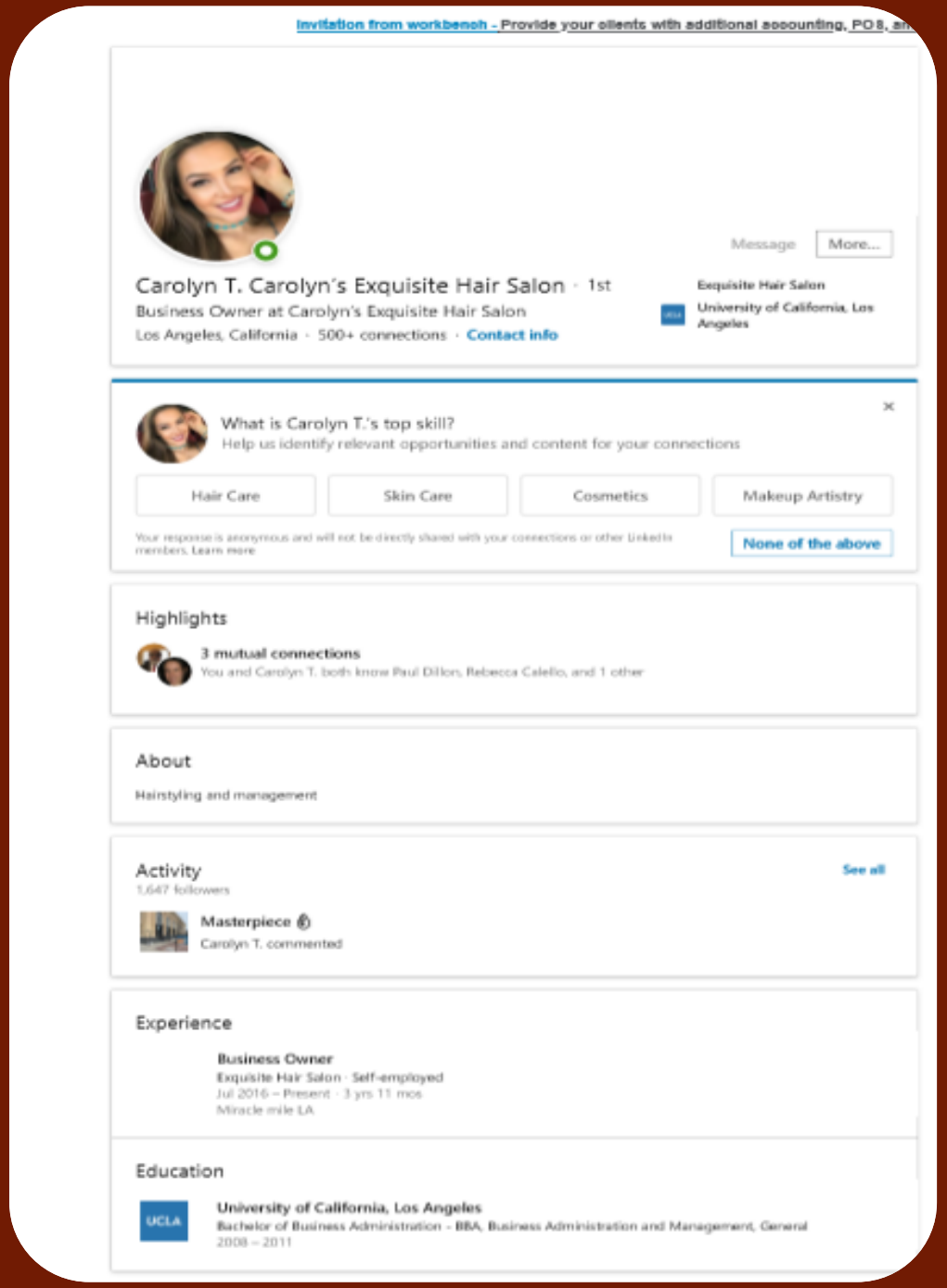
LION Network
19,541 members

See all

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC


Invitation from workbench - Provide your clients with additional accounting, POS, an
Message
More...
Carolyn T. Carolyn's Exquisite Hair Salon · 1st
Business Owner at Carolyn's Exquisite Hair Salon
Los Angeles, California · 500+ connections · Contact info
Exquisite Hair Salon
University of California, Los Angeles
What is Carolyn T.'s top skill?
Help us identify relevant opportunities and content for your connections
Hair Care
Skin Care
Cosmetics
Makeup Artistry
None of the above
Highlights
3 mutual connections
You and Carolyn T. both know Paul Dillon, Rebecca Calello, and 1 other
About
Hairstyling and management
Activity
1,647 followers
See all
Masterpiece
Carolyn T. commented
Experience
Business Owner
Exquisite Hair Salon · Self-employed
Jul 2016 – Present · 3 yrs 11 mos
Miracle mile LA
Education
University of California, Los Angeles
Bachelor of Business Administration - BBA, Business Administration and Management, General
2008 – 2011


Baile
Féach thart
Fógraí
Teachtaireachtaí
Leabharmharc...
Liostaí
Próifíl
Tuilleadh
Tweet
Samantha Per...
@Perkins12S
Vanessa
6,605 6605 Tweet
Lean
Vanessa
@VanessaWilsonDC
A proud #Resist American Proudly followed by @RoKhanna,@funder, @joncoopertweets"I want to have fun. It's a beautiful life. You win,u lose,but you get up"
Cláraithe Nollaig 2018
3,286 3286 Á leanúint
2,945 2945 Leantóir
Not followed by anyone you're following
Tweetanna
Tweetanna & freagraí
Meáin
Thaitin siad seo le
Pinned Tweet
Vanessa
14 Márta
Mitch McConnell just helped his major donor by lifting Russian sanctions. Listen to @Funder's podcast episode about it below. #WheresMitch



Accept | Ignore | More...

James Brian · 2nd

Grand master illuminati

Freemasonry

United States · 104 connections · Contact info

Highlights

2 mutual connections
You and James both know Evert van der Veen /G\ and william mclean

Activity

See all

104 followers

Join the Freemason and better your life
James shared this
1 Reaction

***About Illuminati* *We are the sell of the new world order. we are known a...**
James commented

***About Illuminati* *We are the sell of the new world order. we are known as the...**
James commented

***About Illuminati* *We are the sell of the new world order. we are known a...**
James commented

Experience

freemason
Grand master illuminati
Jan 2002 – Present · 18 yrs 5 mos

illuminati
Member of the freemasonary · Full-time
Apr 2020 · 1 mo
USA colorado

Interests

Narendra Modi
Prime Minister of India
3,482,823 followers

Netflix
4,745,475 followers

Masonic Medical Research Institute
1,482 followers

Jeff Weiner
CEO at LinkedIn
10,509,881 followers

Robert Herjavec
Founder of Herjavec Group | Shark on AB...
2,122,199 followers

Forbes
13,699,125 followers

Google | JPG | alone musk

All | Images | Maps | Shopping | More | Settings | Tools

About 28,270,000,000 results (1.12 seconds)



Image size: 736 × 736

Find other sizes of this image: All sizes - Small - Medium

Possible related search: alone musk

Elon Musk - Wikipedia
https://en.wikipedia.org › wiki › Elon_Musk
Elon Reeve Musk FRS is an engineer, industrial designer, technology entrepreneur, and philanthropist. He is a citizen of South Africa, the United States (where ...

alone musk | Elon Musk | Know Your Meme
https://knowyourmeme.com › photos › 1463009-alon-musk
Elon Musk - alone musk. Like us on Facebook! Save · Shop the Meme · PROTIP: Press the ... and ... keys to navigate the gallery. 'g' to view the gallery, or 'r' to ...
all results for »

Visually similar images



Report images

Pages that include matching images

Elon Musk Gets a Theme Song From Weezer's Old Bassist ...
https://www.wired.com › 2017/10 › elon-musk-rents-a-song
2264 × 1200 - Oct 4, 2017 - Elon Musk finally has his, even if his more melancholy fable than rahrah rousers. The band in question is Matt Sharp, vocalist and frontman for ...

Elon Musk Has Trump's Ear, and Wall Street Takes Note - The ...
https://www.nytimes.com › business › elon-musk-donald-trump-wall-street
1237 × 2048 - Jan 24, 2017 - The entrepreneur Elon Musk last month. In the runup to the presidential election, Mr. Musk openly criticized Donald J. Trump's candidacy, but ...

Elon Musk's tweet on Tesla going private was a surprise to ...
https://www.seattletimes.com › business › elon-musks-tweet-on-tesla-going-p...
300 × 400 - Aug 19, 2018 - Elon Musk, the electric car company's chief executive, is said to have written his Twitter post last week in haste, even though he said on Monday ...

The 20 Truths - ELON MUSK MOTIVATIONAL SPEECH ...
https://www.youtube.com › watch
168 × 94 - Dec 20, 2017 - [GET MOTIVATION] https://www.multigenbrother.com MAIN CHANNEL - SUBSCRIBE FOR MORE MOTIVATIONAL VIDEOS ...

Ford Motor Co. executive ribs Tesla CEO Elon Musk over ...
https://www.bizjournals.com › news › teslermodel3-5000-target-musk-ford
1024 × 574 - Jun 28, 2018 - Spread thin and sleeping again on the factory floor, Elon Musk tried to put a positive spin on Tesla's sprint to build 5000 Model 3 sedans per ...



Connect | Message | More...

Matthew P. CPP, PSP, PCI, CFE, CFI · 2nd

Senior Regional Program Manager, APAC

Singapore · 500+ connections · Contact info

Microsoft

Loyola University New Orleans

© COUNTERINTELLIGENCE INSTITUTE, LLC

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

About

Top-performing, ASIS, ACFE, and IAI Board Certified, Security Executive with extensive experience and advanced education geared towards contribution of long-range operational objectives. Tested, proven leadership abilities; extensive field experience in key global markets. Excel at navigating complex challenges. Honored with numerous awards for service, distinguished results and effectiveness.

• Subject Matter Expertise: Physical security solutions, intelligence risk analysis, incident investigation management, and crisis response for high-profile organizations.

• Investigative Assets: Extensive investigative management experience involving crimes, cybercrimes, forensics, and intelligence.

• Security Continuity: Excel at identifying potential security risks. Extensive experience in defining, establishing, and managing security risk metrics and tracking effectiveness.

• Risk Mitigation: Affinity for balancing risk mitigation with organizational needs. Effective at identifying and controlling vulnerabilities.

• Team Leadership: Talent for implementing enterprise-wide programs, and managing cross-functional, high-performing teams. Highly collaborative, with the ability to build and maintain effective working relationships.

• Key Strengths: Finely tuned analytical skills with a dedication to continually streamlining and improving work processes. Effectively interface with executive leadership to collaborate on issues and resolve problems. Results focused; achieves maximum impact with minimal cost.

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Experience

Senior Regional Program Manager, APAC

Microsoft · Full-time
Feb 2020 – Present · 6 mos
Singapore

Senior Regional Program Manager (Security), APAC

Program Management of Data Center Physical Security in the Asia Pacific Region, responsible for identifying, evaluating, and quantifying physical security issues at proposed critical infrastructure sites, including corollary policies, procedures, guidelines, technical defenses & preemptive measures.

Selected Contributions:
• Conduct ongoing risk assessments & site security analysis, recommending mitigation and remediation as necessary to protect staff, equipment and operational continuity, while monitoring corporate & geopolitical threat levels globally.

• Supervise protective programs and new vendor tender processes, and provide vendor oversight, and visitor, executives, staff & contractor threat assessments.

• Investigate breaches and ancillary incidents, concurrent with providing thorough security staff training.

• Foster & cultivate quick-reaction relationships with host-nation policing authorities, security branches and private sector security firms, while ensuring bank compliance with relevant jurisdictional regulations and reporting requirements.

• Identify, target and optimize security vendor cost efficiencies, including reviewing contractual terms and issuing recommendations to corporate management.

see less

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Regional Security Manager, APAC
CBRE · Full-time
Apr 2017 – Feb 2020 · 2 yrs 11 mos
Singapore

Regional Security Manager, APAC

Leader of corporate security delivery in Asia Pacific Region, primarily tasked with security operations, including policies, procedures, guidelines, technical defenses & protective measures, and for safeguarding principle Security Operations Center complex.

see less

Senior Special Agent
Naval Criminal Investigative Service (NCIS) · Full-time
Sep 2002 – Apr 2017 · 14 yrs 8 mos
Worldwide

Senior Special Agent, National Security Division, Proactive Operations.

Lead investigative teams in sensitive and complex national security intelligence operations and programs around the world. Accountable for developing detailed operational plans for asset protection, threat mitigation, proprietary technology protection, and exploitation of intelligence information in support of organizational objectives.

see less

Patrol Sergeant
Folsom Police Department · Full-time
May 1998 – Sep 2002 · 4 yrs 5 mos
Folsom, Louisiana

Patrol Sergeant

Supervision of sworn law enforcement officers and staff involved in traffic, field patrol, investigations, crime prevention, and community relations. Participated in shift activities including enforcing federal, sate, and local laws, issuing citations, making arrests, and court testimony.

see less

© COUNTERINTELLIGENCE INST

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Education

Loyola University New Orleans
Master of Arts (MA), Criminal Justice/Police Science
2001 – 2002

Media (1)



Loyola University New Orleans

Southeastern Louisiana University
Bachelor's Degree (BA), Criminal Justice/Police Science
1992 – 1996

Media (1)



Southeastern has been ranked No. 1 in Louisiana and No. 15 in the nation

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Licenses & Certifications

Executive Protection Certificate
ASIS International
Issued 2019 · No Expiration Date

Rescue Diver
PADI
Issued 1999 · No Expiration Date

Professional Certified Investigator (PCI)
ASIS International
Issued 2017 · Expires 2024

Certified Forensic Interviewer (CFI)
International Association of Interviewers
Issued 2019 · Expires 2022

Certified Protection Professional (CPP)
ASIS International
Issued 2019 · Expires 2022

Physical Security Professional (PSP)
ASIS International
Issued 2019 · Expires 2022

Certified Fraud Examiner (CFE)
Association of Certified Fraud Examiners (ACFE)
Issued 2019 · Expires 2021

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Active Shooter Instructor Trainer
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Automatic Weapons Instructor
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Firearms Instructor
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Non Lethal Weapons Instructor
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Physical Fitness Coordinator
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Reactive Firearms Instructor
FEDERAL LAW ENFORCEMENT TRAINING CENTER

Singapore Home Team Academy Firearms Instructor
Ministry of Home Affairs Singapore

Matthew P. CPP, PSP, PCI, CFE, CFI

Senior Regional Program Manager, APAC

Volunteer Experience



Volunteer

Audubon Nature Institute

May 1997 – May 1998 • 1 yr 1 mo

Education

© COUNTERINTELLIGENCE INSTITUTE, LLC

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Skills & Endorsements

Security Management · 15

Endorsed by **Samrendra Mohan Kumar and 5 others who are highly skilled at this**

Risk Management · 13

Endorsed by **Samrendra Mohan Kumar, who is highly skilled at this**

Risk Assessment · 12

Endorsed by **Adolfo Benages CPP CAS MBA and 1 other who is highly skilled at this**

Industry Knowledge

- **Crisis Management** · 8
- **Security Operations** · 7
- **Force Protection** · 7
- **Counterintelligence** · 5
- **Surveillance** · 5
- **Law Enforcement** · 6
- **Intelligence Analysis** · 5
- **Emergency Management** · 1
- **Fraud Investigations** · 1
- **Corporate Security** · 1
- **Auditing** · 1
- **Criminal Justice** · 1
- **Project Management** · 1
- **Physical Security** · 8
- **Business Continuity** · 6
- **Executive Protection** · 5
- **Counterterrorism** · 4
- **Investigation** · 7
- **Maritime Security** · 5
- **Criminal Investigations** · 5
- **Banking** · 1
- **Loss Prevention** · 1
- **Security** · 8
- **Public Safety** · 1
- **Private Investigations** · 5

Home My Network Jobs Messaging

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

Interpersonal Skills

- **Leadership** · 7
- **Team Leadership** · 5
- **Training** · 1
- **Interrogation** · 5
- **Management** · 1
- **Customer Service**

Other Skills

- **Operational Due Diligence** · 7
- **Threat Intelligence** · 7
- **Government Liasioning** · 6
- **Intelligence Collection** · 5
- **Counter Surveillance** · 5
- **Firearms Instruction** · 5
- **Maritime Domain Awareness** · 5
- **Federal Law Enforcement** · 5
- **Cross Cultural Management** · 6
- **Anti-counterfeiting** · 6
- **Brand Protection** · 6
- **Security Investigations** · 5
- **Anti-corruption** · 5
- **Cultural Diversity** · 5
- **Maritime Law Enforcement** · 5
- **Security Clearance** · 5

© COUNTERINTELLIGENCE INSTITUTE, LLC

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

40 **Courses**

Active Shooter Instructor Training Program
FLETC

Advanced Foreign Counterintelligence Operations Course
DoD

Advanced High Risk Operations Training Program
NCIS / FLETC

Automatic Weapons Instructor Training Program
NCIS / FLETC

BSR Evasive Driving Course
BSR

Clandestine Methamphetamine Laboratory Identification Training
LSP

Counter Surveillance and Surveillance Detection Course
DoD

Counter Terrorism Investigations and Operations Course
DoD

Counterintelligence Force Protection Course
DoD

Counterintelligence Interviewing Skills Course
DoD

Counterterrorism Asset Validation
CIC

Espionage Investigations and Interviewing Techniques
CIC

Senior Regional Program Manager, APAC

Federal Criminal Investigator Training Program
CITP / FLETC

Firearms Instructor Training Program
FLETC

Foreign Service Institute East & North Africa Regional Seminar
FSI

High Risk Operations Training Program
NCIS / FLETC

High Risk Port Support Operations Training Program
NCIS / FLETC

High Risk Protective Service Operations Training Program
NCIS / FLETC

ITI Evasive & Defensive Driving Course
ITI

Inland Boat Operator Training Program
FLETC

Intelligence Operations Familiarization Course
DoD

Intoxilyzer Certification Course
LSP

Louisiana State University P.O.S.T Certified
LSU

Maritime Counter-Improvised Explosive Device Awareness
CNIC

Military Counterintelligence Collections Course
DoD

National Security Investigations Course
DoD

Non-Lethal Weapons Instructor Training Program
FLETC

Senior Regional Program Manager, APAC

Physical Fitness Coordinator Training Program
FLECT

Protective Service Operations Course
ITI

Reactive Shooter Instructor Training Program
FLETC

SERE 225
DoD

SIG SAUER Armorer Course
SIG SAUER

Sig Arms DAK Transition Course
Sig Arms / NCIS

Singapore Home Team Academy Firearms Instructor Training Program
HTA

Special Agent Basic Training Program
NCIS / FLETC

Suicide Bomber Mitigation Training Program
FLETC

Surveillance Operations Course
DoD

Threat Country Intelligence Seminar
DoD

Threat Country Intelligence – Intelligence and Operations Methodologies
CIC

Threat Country Operations Course
DoD

Show less

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

10 **Organizations**

Association of Former Intelligence Officers (AFIO)
Jul 2017 – Present • Member

American Chambers of Commerce in Singapore
May 2017 – Present • Member

Asia Crisis & Security Group
2017 – Present • Member

Association of Certified Anti-Money Laundering Specialists (ACAMS)
2017 – Present • Member

Association of Certified Fraud Examiners (ACFE)
2017 – Present • Member

International Association of Emergency Managers
2017 – Present • Member

National Emergency Management Association
2017 – Present • Member

Overseas Security Advisory Council (OSAC)
2017 – Present • Member

ASIS International
2005 – Present • Member

Federal Law Enforcement Officers Association (FLEOA)
2002 – Present • Member

Show less

Matthew P. CPP, PSP, PCI, CFE, CFI
Senior Regional Program Manager, APAC

5 **Honors & Awards**

Department of State Meritorious Honor Award
2015 • United States Department of State (DoS)

Joint Civilian Service Commendation Award
2009 • United States Department of Defense (DoD)

Naval Criminal Investigative Service Expeditionary Medals (3)
2008 • Naval Criminal Investigative Service (NCIS)

Navy Meritorious Civilian Service Award
2003 • United States Department of Navy (DoN)

Master of Criminal Justice Scholar Award
2002 • Loyola University New Orleans

2 **Languages**
English • Thai

© COUNTERINTELLIGENCE INSTITUTE, LLC

Be fast. Be flexible. - Internet & Voice just $35 each/mo. when you buy both. Restrict

Media Lab Solutions



Featured In

BUSINESS INSIDER · CBS · yahoo! finance · FOX NEWS channel · NBC

Message · More...

Natalie Weinstein · 1st

Director of Podcast Relations at Media Lab Solutions

Tampa, Florida, United States · 194 connections · Contact info

Media Lab Solutions

The Johns Hopkins University

pinterest.com/mandymodgirl/professional-female-headshots-mandy-mcewen/

Today · Search

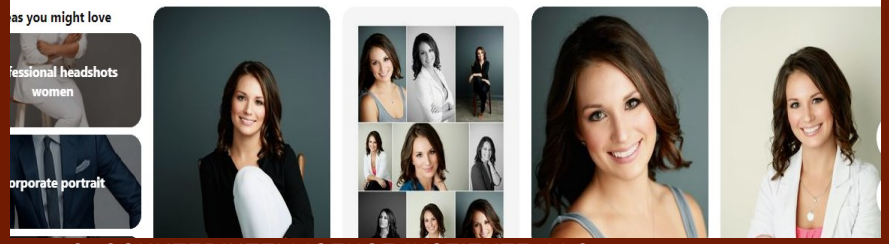
Headshots - Mandy McEwen

Mandy McEwen · My headshots for Mod Girl Marketing - taken by Sweet Jean Photography of Roseville, California.

419 followers

Share

as you might love



© COUNTERINTELLIGENCE INSTITUTE, LLC

unitedtrustinvestmentbank.com/about-us/

UTI BANK

Home · About Us · Our Services · Credit/Debit Cards · Contact Us · Internet Banking

Meet Our Team



Anthony Ridge
Legal Adviser

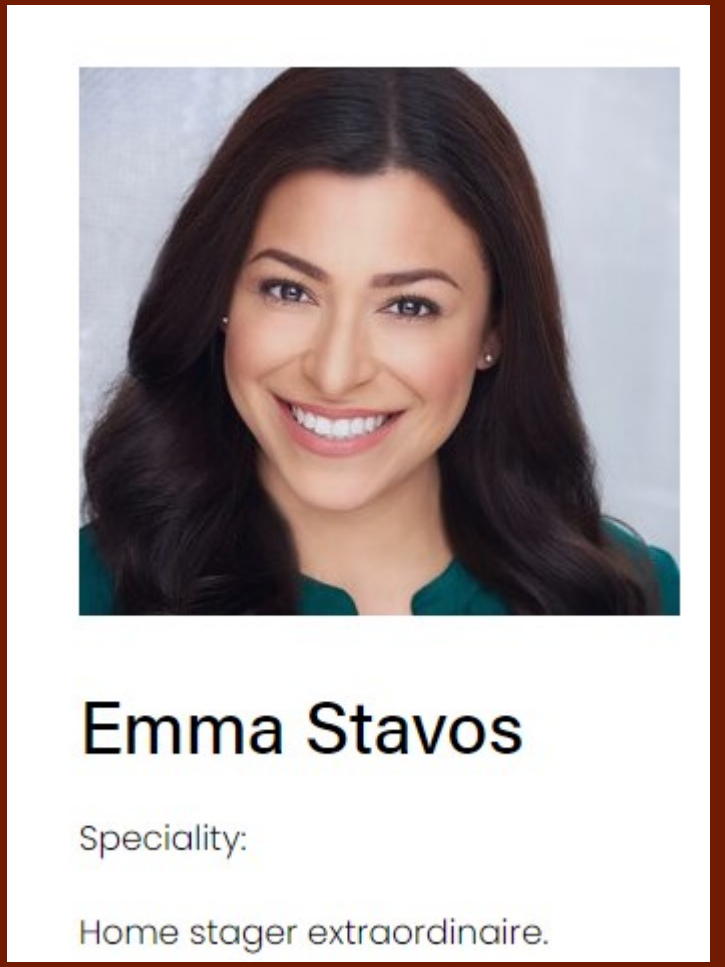


Keith Tunner
Investment Manager



Tiffany Hill
Remittance Manager





https://www.taylorjonesgroup.com/team

© COUNTERINTELLIGENCE INSTITUTE, LLC

POLL – WHAT CRITERIA DO YOU USE WHEN DECIDING WHETHER OR NOT TO ACCEPT LINKEDIN CONNECTION INVITATIONS?

1) No real criteria, I accept all invitations

2) More likely to accept if they have an attractive profile photo

3) Likely to accept if they have an impressive profile

4) I only accept invitations from people I know

5) I accept from known people or from people representing known organizations

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

Experience

Executive Recruiter
Self-employed
Mar 2014 – Present · 6 yrs 5 mos
Greater New York City Area

Leveraging extensive experience in business consulting, I specialize in working with Fortune 500 companies in the selection of executive management talent. This starts with a clear understanding of the client's needs and expectations and ends with the presentation of top candidates. While predominantly working out of the New York area, I utilize an extensive network of associated recruiters to fulfill global requirements.

Manager, Executive Recruiting
McKinsey & Company
Jan 2012 – Feb 2014 · 2 yrs 2 mos
Sao Paulo, Brazil

Deloitte Brasil
5 yrs 5 mos

Manager
Jan 2009 – Dec 2011 · 3 yrs
Sao Paulo, Brazil

Senior Consultant
Aug 2006 – Dec 2008 · 2 yrs 5 mos
Sao Paulo, Brazil

Education

Universidade Paulista
Master's Degree, Business Administration
2005 – 2007

Universidade Paulista
Bachelor's Degree, Public Relations/Image Management
2001 – 2004

© COUNTERINTELLIGENCE INSTITUTE, LLC

Accomplishments

3 **Languages**

English • Portuguese • Spanish

Interests



Arianna Huffington

Founder and CEO at Thrive Global

9,191,315 followers



Sramana Mitra

Founder and CEO of One Million by One ...

429,461 followers

"Recruiters and Consultants"

27,567 members

Zoran Pesic - Recruitment

15,063 followers

The New York Times

5,045,482 followers

UNIP - Universidade Paulista

11,302 members

See all

© COUNTERINTELLIGENCE INSTITUTE, LLC

SKILLS & ENDORSEMENTS

- **Executive Search** 145
- **Recruiting** – 138
- **Consulting** – 127
- **Management Consulting** - 56
- **Performance Management** - 52
- **Change Management** - 51
- **Public Relations** - 46
- **Strategy** - 46
- **Business Strategy** - 44
- **Strategic Planning** - 42
- **Start-ups** - 42
- **CRM** - 39
- **Customer Relationship Management (CRM)** – 2
- **Management** - 51
- **Talent Management** - 50
- **Leadership** - 49
- **Interviews** - 46
- **Executive Management** - 46
- **Executive Coaching** - 44
- **International Business Consulting** - 44

© COUNTERINTELLIGENCE INSTITUTE, LLC



Ana Maria [redacted] • 10:51 AM

Hi [redacted]

Thanks for accepting my connection request. My company is working with a top tier university along with several professionals within the fleet management industry to help identify whether or not there is a growing need for the development of university degrees and/or more specific certification programs which would enhance the expertise and professional stature of individuals working within this field.

I am attaching the results of our initial survey. I would really appreciate your review of the survey and any comments which you may like to provide.

As detailed in the attachment, we will be organizing a webinar early next year on this topic and hope you will be able to participate.

Respectfully,

Ana Maria

PDF **Fleet.Prof.Survey.pdf**
9 MB

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

HANDOUT #6

© COUNTERINTELLIGENCE INSTITUTE, LLC

SE ATTACK VECTORS - 2

Smishing

© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

Dear Employee,

So sorry to disrupt your well deserved memorial day weekend, but we just became aware of an issue which could significantly delay for most employees the processing of payroll for deposit this coming Friday. To advert this from happening in your particular case, we need you to log into our new HR Portal. Please use the following link PCHR.2020@PrestigeComm.net for login utilizing your current credentials. Once inside, confirm your hour submission for the previous pay period. Prior to logging out, establish a new password for your account. Please complete this requirement soon as possible.

Happy Memorial Day!

Susan Jones

HR Director, Prestige Communications

© COUNTERINTELLIGENCE INSTITUTE, LLC

SE ATTACK VECTORS - 3

Vishing

© COUNTERINTELLIGENCE INSTITUTE, LLC

VISHING



SpoofCard



Easily Disguise Your Caller ID

© COUNTERINTELLIGENCE INSTITUTE, LLC

PRETEXT TO COLLECT SENSITIVE INFORMATION

- Academic Research
- Conducting a Survey
- Career Advice
- Future Employee
- Recommendations for Service Providers
- Potential Vendor
- Current Client
- Co-Worker from Another Area

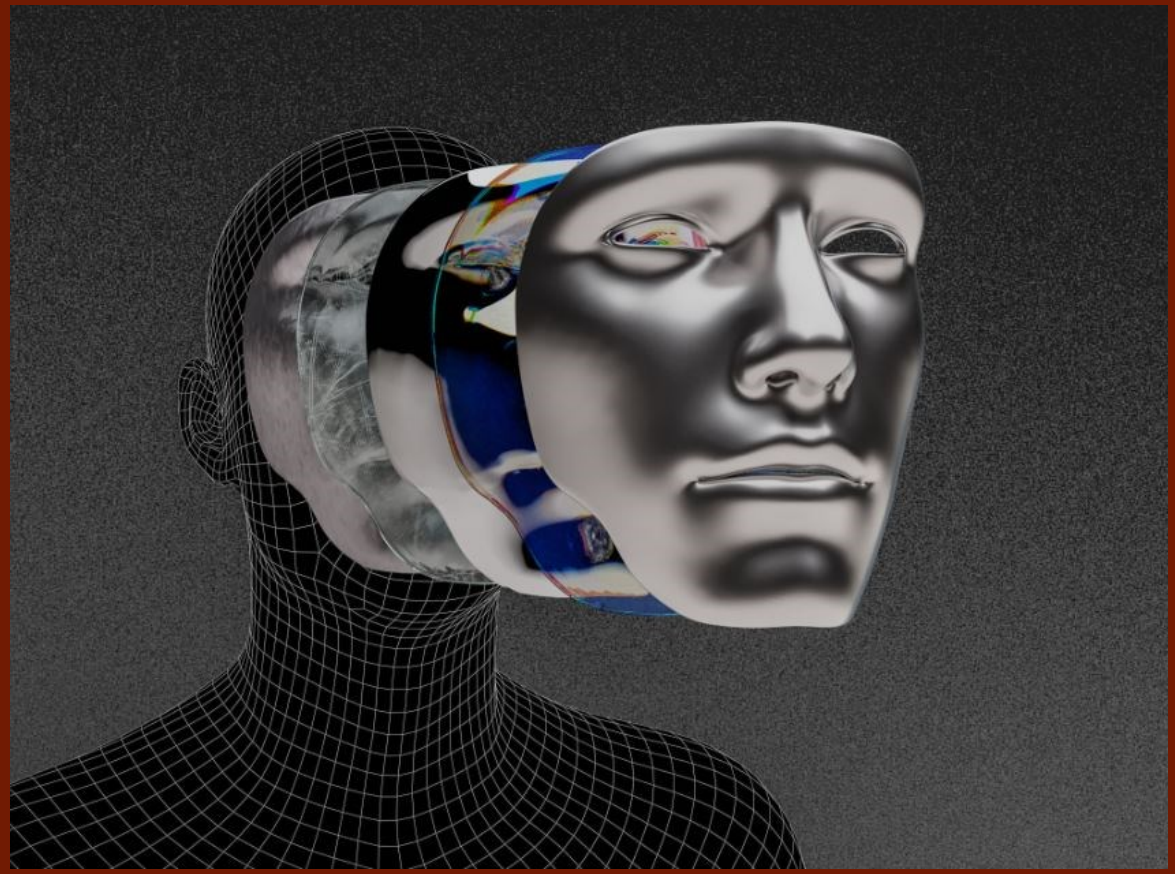
© COUNTERINTELLIGENCE INSTITUTE, LLC



Christine – The New Receptionist

© COUNTERINTELLIGENCE INSTITUTE, LLC

DEEPFAKES AND AI THREATS



© COUNTERINTELLIGENCE INSTITUTE, LLC

PAYMENT FRAUD

Case 1

- **2019**
- **CEO of unnamed UK-based energy firm**
- **Received instructions via phone call with boss from German parent**
- **Transfer of Euros220,000 to the bank account of Hungarian supplier**
- **Subsequent calls made, claimed that money was reimbursed**
- **Third call asking for same transfer; suspected as caller ID came from Australia**

© COUNTERINTELLIGENCE INSTITUTE, LLC

CASE 2

- 2020 bank manager in Hong Kong received call
- UAE based client requested transfers totaling $35 million to cover acquisitions
- Email received between client and lawyer substantiating transaction
- Transfer made
- U.A.E. conducting investigation
- Scheme appeared to involve at least 17 individuals
- Contacted U.S. authorities in effort to recover $400,000 wired to accounts held by Centennial Bank

© COUNTERINTELLIGENCE INSTITUTE, LLC

SE ATTACK VECTORS - 4

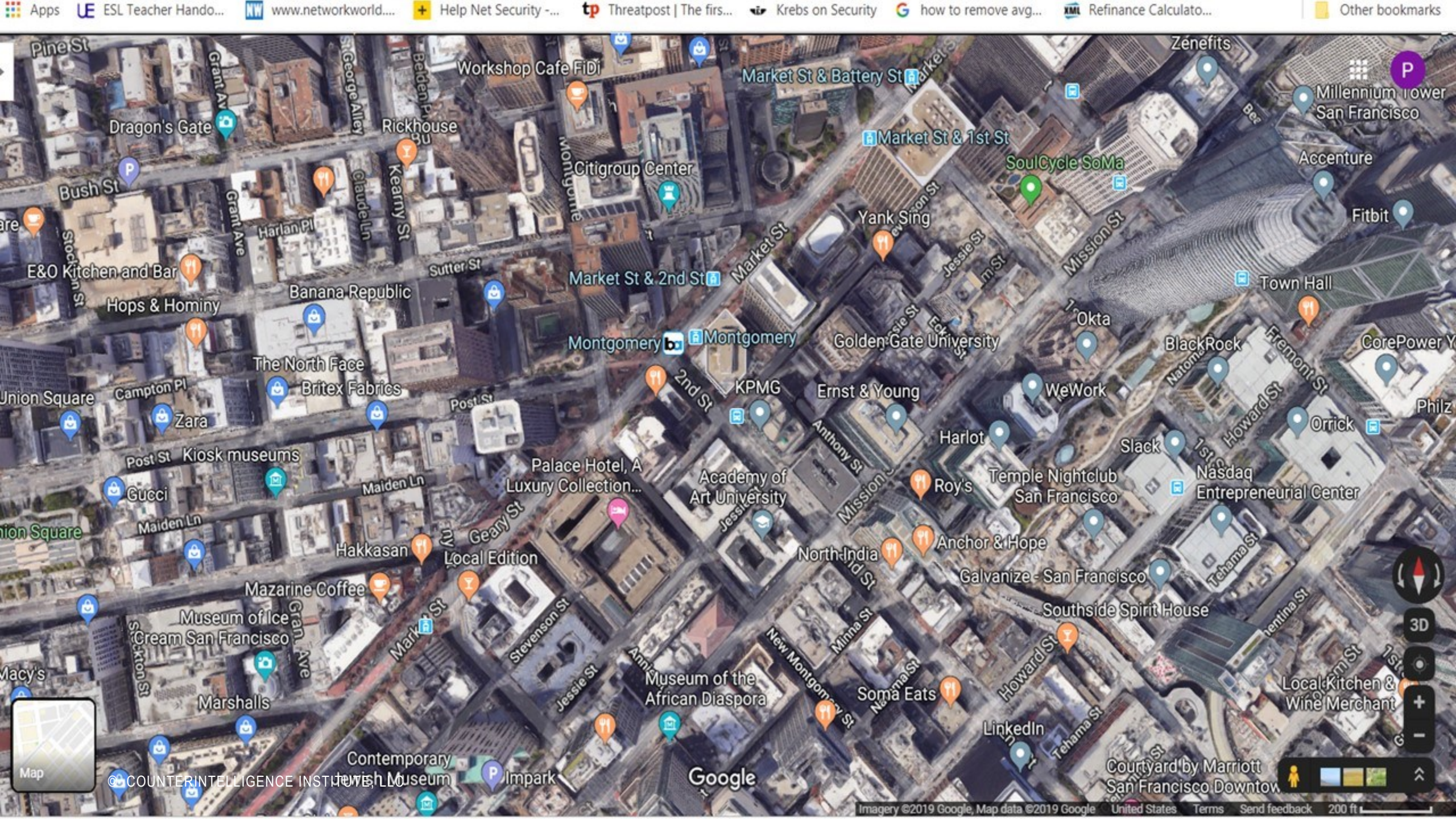
Face-to-Face Interaction

© COUNTERINTELLIGENCE INSTITUTE, LLC

FACE-TO-FACE ENCOUNTERS



© COUNTERINTELLIGENCE INSTITUTE, LLC


Apps
ESL Teacher Hando...
www.networkworld....
Help Net Security -...
Threatpost | The firs...
Krebs on Security
how to remove avg...
Refinance Calculato...
Other bookmarks
Pine St
Grant Ave
St George Alley
Belden Pl
Workshop Cafe FiDi
Market St & Battery St
Zenefits
Millennium Tower San Francisco
Dragon's Gate
Rickhouse
Bush St
Harlan Pl
Claude Ln
Kearny St
Montgomery
Citigroup Center
Market St & 1st St
SoulCycle SoMa
Accenture
Fitbit
Yank Sing
Mission St
Stockton St
E&O Kitchen and Bar
Sutter St
Market St & 2nd St
Market St
Banana Republic
Hops & Hominy
Town Hall
Montgomery
Golden Gate University
Okta
BlackRock
Fremont St
CorePower Y
The North Face
Britex Fabrics
KPMG
Ernst & Young
WeWork
Howard St
Philz
Union Square
Campton Pl
Zara
Post St
Kiosk museums
Gucci
Palace Hotel, A Luxury Collection...
Academy of Art University
Harlot
Slack
Orrick
Temple Nightclub San Francisco
Roy's
Nasdaq Entrepreneurial Center
Maiden Ln
Geary St
Hakkasan
Local Edition
Anchor & Hope
North India
Galvanize - San Francisco
Mazarine Coffee
Museum of Ice Cream San Francisco
Stevenson St
Minna St
Southside Spirit House
Tehama St
Macy's
Marshalls
Jessie St
Museum of the African Diaspora
Soma Eats
Howard St
LinkedIn
Local Kitchen & Wine Merchant
Contemporary Jewish Museum
Impark
Courtyard by Marriott San Francisco Downtow
Google
Map
3D
© COUNTERINTELLIGENCE INSTITUTE, LLC
Imagery ©2019 Google, Map data ©2019 Google
United States
Terms
Send feedback
200 ft



© COUNTERINTELLIGENCE INSTITUTE, LLC

How We Get in Front of You

- Bumps within pattern of life
- Conference and tradeshow targeting
- Targeted Invites

© COUNTERINTELLIGENCE INSTITUTE, LLC

Targeted Invites

- Interview for publication
- Nomination of an award
- Student conducting research
- Executive Headhunting Scheme

© COUNTERINTELLIGENCE INSTITUTE, LLC

THE ART OF ELICITATION



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC





Interview
or
Elicitation?

© COUNTERINTELLIGENCE INSTITUTE, LLC

TARGETING DURING FOREIGN TRAVEL



© COUNTERINTELLIGENCE INSTITUTE, LLC

CORPORATE ESPIONAGE – INDUSTRIAL ESPIONAGE

- Customer data
- Employee data
- Vendor information
- Pricing strategies
- Proprietary formulas and processes
- Technical components and plans
- Corporate strategies
- Corporate financial data
- Telephone directories
- Computer access protocols
- Computer network design
- Acquisition strategies
- Marketing strategies
- Investment data
- Negotiation strategies
- Passwords (computer, phone, accounts)

© COUNTERINTELLIGENCE INSTITUTE, LLC

HOW INFORMATION IS COLLECTED

- Visa Application
- Airports (WIFI, Electrical Outlets, Security Checks)
- Customs & Immigration
- Secondary
- Local Transport, Hotel Services, Translation Services, Bar (elicitation)

© COUNTERINTELLIGENCE INSTITUTE, LLC

NO EXPECTATION OF PRIVACY







© COUNTERINTELLIGENCE INSTITUTE, LLC

TECHNICAL VERSUS PHYSICAL COLLECTION RESOURCES

Technical

- Media Devices, Cameras, Audio, Key Control

Physical

- Informants, agents, physical surveillance

© COUNTERINTELLIGENCE INSTITUTE, LLC

MEDIA DEVICE EXPLOITATION







1. How they be accessed
2. Value of information contained on them
3. Opportunity to monitor future activity
4. Gateway to your company's network

© COUNTERINTELLIGENCE INSTITUTE, LLC

CAMERAS









© COUNTERINTELLIGENCE INSTITUTE, LLC

AUDIO







© COUNTERINTELLIGENCE INSTITUTE, LLC

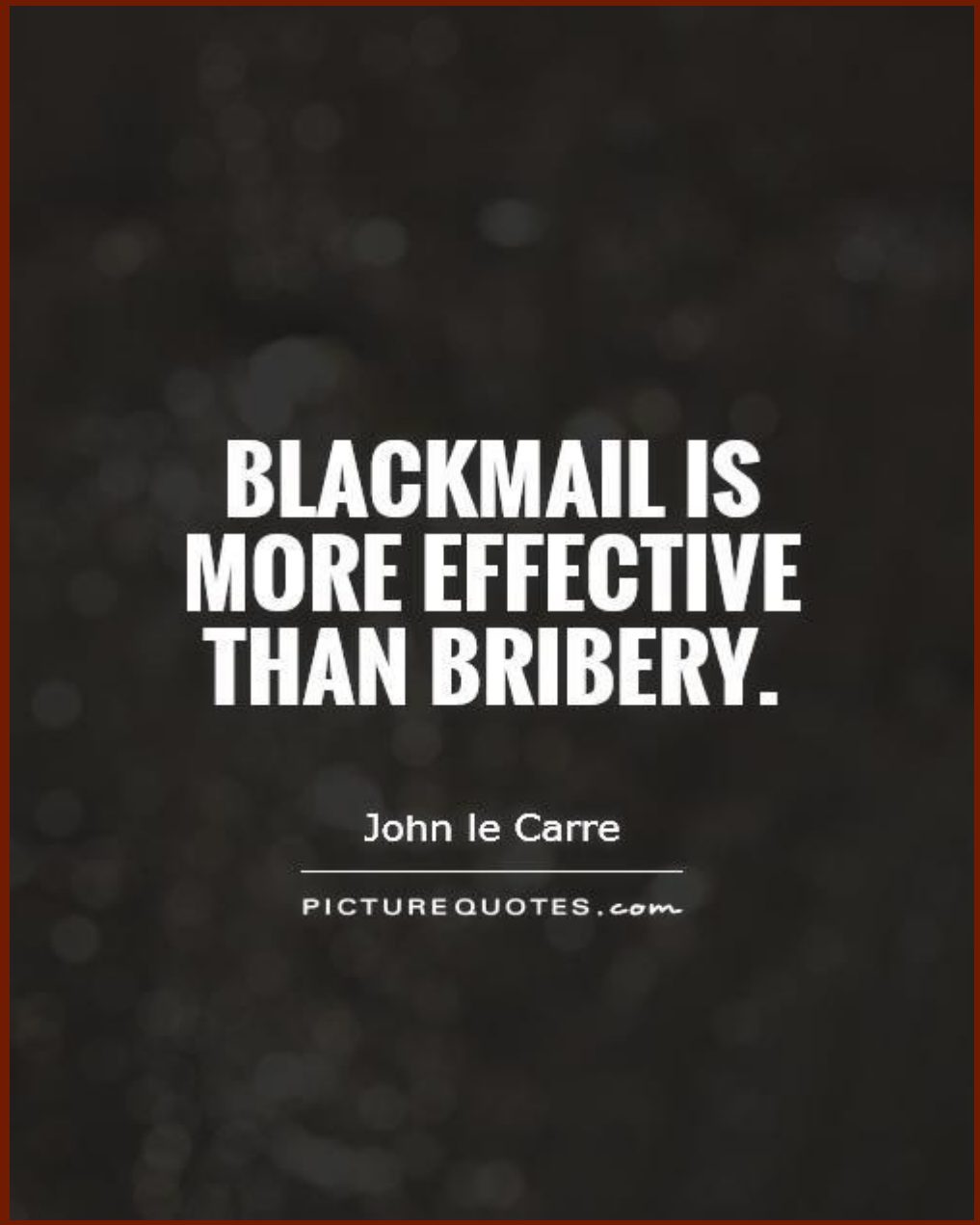
HONEY POT



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

HUMAN HACKING RISK MITIGATION



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC

HANDOUT #7

© COUNTERINTELLIGENCE INSTITUTE, LLC



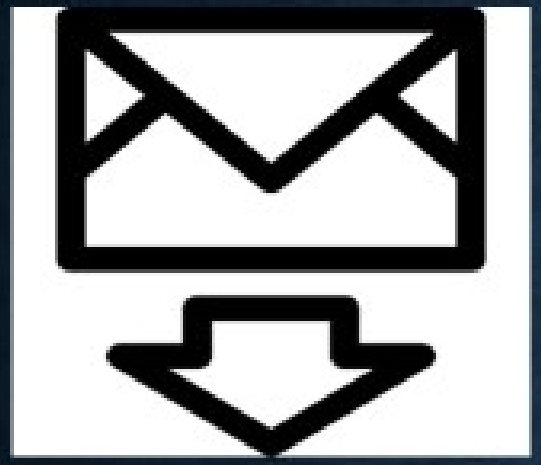
© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



© COUNTERINTELLIGENCE INSTITUTE, LLC



HELP!









© COUNTERINTELLIGENCE INSTITUTE, LLC

"VERIFY, THEN TRUST!!!"

© COUNTERINTELLIGENCE INSTITUTE, LLC

QUESTIONS?????



© COUNTERINTELLIGENCE INSTITUTE, LLC



PETER G. WARMKA

SPY & HUMAN HACKER

PGWARMKA@COUNTERINTELLIGENCE-INSTITUTE.COM

WWW.COUNTERINTELLIGENCE-INSTITUTE.COM



© COUNTERINTELLIGENCE INSTITUTE, LLC