Complexities in Investigating Cases of Social Engineering:
How reverse engineering and profiling can assist in the collection of evidence.

Christina Lekati
Cyber Risk GmbH
“The art and science, of skillfully maneuvering human beings to take action in some aspect of their lives …that may or may not be in the ‘target’s’ best interest.”

-Christopher Hadnagy
Social Engineering
The Typical Backbone of the Attack Strategy

Preparation:

Information Gathering → Identifying Targets & Victims → Pretexting the Approach

Execution:

Approach & Gain Trust → Drive Desired Behavior → Achieve & Disappear

Christina Lekati | Cyber Risk GmbH
Challenges in Handling Social Engineering Cases
Case Study: Medidata

How Medidata got tricked

$4.8 million loss from a Social Engineering attack.
Social Engineering: Quality of Evidence

Leaves mainly weak or non-admissible evidence

- Alleged/ Oral evidence
- Hearsay evidence
- Can manipulation be proved beyond reasonable doubt?
- Many plausible scenarios and interpretations
- ...and more
Case Study: Medidata $4.8 million Social Engineering loss

Other Plausible Interpretations

- Attackers manipulate Medidata and employees for monetary theft
- Medidata manipulates Insurance company for monetary benefits/embezzlement
- Employee manipulates Medidata and Insurance company for monetary theft
Social Engineering: Quality of Evidence

Courts still face difficulties on how to judge and evaluate cases involving mainly Social Engineering.

*Providing evidence “beyond reasonable doubt” seems to be the biggest challenge.*
But how does one find evidence in Social Engineering cases?

Supporting evidence & leads; tracing back the steps of the offender
Reverse engineer the suspect’s actions?

Traces left through the planning & preparation phase?

- Information used in the attack that were available only through certain sources.
- Did social media assist the attack?
- Forgotten blog posts, forum questions, email addresses and usernames, etc.
- Geolocations, stalking, cyberstalking.
Case Study: Silk Road
Collecting evidence from the preparation phase

When digital traces are well covered, look for behavioral mistakes.
Social Engineering
The Typical Backbone of the Attack Strategy

Preparation:

Attacker still feels “invisible” and secure. Potentially has not decided whether to attack or not. Potentially is still an amateur, learning how to protect his actions.

Exploitation of Vulnerabilities:

Has prepared and planned for most of his actions. Has already prepared and strategized into covering his tracks and misleading investigators.

Phase of Sloppy Mistakes

Phase of Careful Action.
Remember…

Sometimes, the fastest way from A to B…

...is the unpredicted one.
How do offenders select their victims?

Connecting the Dots

Tracing back an attack:

- The phase of **information gathering, targeting, and planning**.

- Reconnaissance: The attack strategy of the attacker can reveal the steps he took through his **preparation** and reveal **sloppy mistakes**.

- Offenders are still humans: look for **logical possible mistakes**.

- The way a victim was profiled leaves traces in profiling the attacker.
Insights on Targeting:

How offenders scan for Targets and Vulnerabilities online.
Demonstration
Finding Weaknesses and Vulnerabilities

Vulnerability Exposure Posts

Will not bother protecting the workplace
Manipulation to feed addictions
Send romance fraudster

Exploit need

WARNING
Insights on Profiling:

How offenders profile potential targets online.
How Key Traits are Being Assessed

• The overall representation or “Personal Brand”
• Selection of words
• Selection of interests & activities
• Work responsibilities
• Social life indications
• Vulnerabilities
An Example…
Demonstration
Tom's Profile - What is the overall personal brand?

- Body Language
- Variety of face expressions
- Content (activities)
- Colors
- Locations
- Other people
<table>
<thead>
<tr>
<th>Self Image</th>
<th>Personality Traits</th>
<th>Interests</th>
<th>Wants</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confident</td>
<td>Fitness</td>
<td>???</td>
<td>???</td>
</tr>
<tr>
<td></td>
<td>Expressive</td>
<td>Exploration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sharing</td>
<td>Adventure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Euphoric</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enthusiastic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Life</td>
<td>Social /Open</td>
<td>Travel</td>
<td>???</td>
<td>???</td>
</tr>
<tr>
<td></td>
<td>Extraverted</td>
<td>Social Events</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wide social circle</td>
<td>(mostly outdoors)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional Life</td>
<td>???</td>
<td>???</td>
<td>???</td>
<td>???</td>
</tr>
</tbody>
</table>
Words. Patterns. Expressiveness Style.
Demonstration
Tom’s Profile - A closer look & verbal expressions

- Ambition.
- Determination.
- Influence.
- Adventure.
- Extraversion.

Christina Lekati | Cyber Risk GmbH
## Demonstration
**Profiling Matrix**

<table>
<thead>
<tr>
<th>Personality Traits</th>
<th>Interests</th>
<th>Wants</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confident</td>
<td>• Fitness</td>
<td>• Inner peace &amp; happiness</td>
<td></td>
</tr>
<tr>
<td>• Expressive</td>
<td>• Exploration</td>
<td>• Recognition</td>
<td></td>
</tr>
<tr>
<td>• Sharing</td>
<td>• Adventure</td>
<td>• Admiration</td>
<td></td>
</tr>
<tr>
<td>• Euphoric</td>
<td>• Growth</td>
<td>• Advancement</td>
<td></td>
</tr>
<tr>
<td>• Enthusiastic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Determined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Hard worker</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Self Image

<table>
<thead>
<tr>
<th>Social Life</th>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Social /Open</td>
<td></td>
</tr>
<tr>
<td>• Extraverted</td>
<td></td>
</tr>
<tr>
<td>• Wide social circle</td>
<td></td>
</tr>
<tr>
<td>• Authoritative style</td>
<td></td>
</tr>
<tr>
<td>• of expression</td>
<td></td>
</tr>
<tr>
<td>• Travel</td>
<td></td>
</tr>
<tr>
<td>• Social Events (mostly outdoors)</td>
<td></td>
</tr>
<tr>
<td>• Others' well being</td>
<td></td>
</tr>
<tr>
<td>• To have positive influence</td>
<td></td>
</tr>
<tr>
<td>• To appeal authoritative</td>
<td></td>
</tr>
<tr>
<td>• To be asked for advice</td>
<td></td>
</tr>
</tbody>
</table>

### Social Life

<table>
<thead>
<tr>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Professional Life</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
Demonstration
What about the Professional life?? Deductive thinking and more assumptions

<table>
<thead>
<tr>
<th>Personality Traits</th>
<th>Interests</th>
<th>Wants</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confident</td>
<td>Fitness</td>
<td>Inner peace &amp; happiness</td>
<td>???</td>
</tr>
<tr>
<td>Expressive</td>
<td>Exploration</td>
<td>Recognition</td>
<td></td>
</tr>
<tr>
<td>Sharing</td>
<td>Adventure</td>
<td>Admiration</td>
<td></td>
</tr>
<tr>
<td>Euphoric</td>
<td>Growth</td>
<td>Advancement</td>
<td></td>
</tr>
<tr>
<td>Enthusiastic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard worker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expressive</td>
<td>Fitness</td>
<td>Inner peace &amp; happiness</td>
<td>???</td>
</tr>
<tr>
<td>Sharing</td>
<td>Exploration</td>
<td>Recognition</td>
<td></td>
</tr>
<tr>
<td>Euphoric</td>
<td>Adventure</td>
<td>Admiration</td>
<td></td>
</tr>
<tr>
<td>Enthusiastic</td>
<td>Growth</td>
<td>Advancement</td>
<td></td>
</tr>
<tr>
<td>Determined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard worker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social /Open</td>
<td>Travel</td>
<td>To have positive influence</td>
<td></td>
</tr>
<tr>
<td>Extraverted</td>
<td>Social Events (mostly outdoors)</td>
<td>To appeal authoritative</td>
<td></td>
</tr>
<tr>
<td>Wide social circle</td>
<td>Others’ well being</td>
<td>To be asked for advice</td>
<td></td>
</tr>
<tr>
<td>Authoritative style of expression</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Events (mostly outdoors)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others’ well being</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Self Image

Social Life

Professional Life

- Front line person
- Team leader
- Management

Ideally he would have: Challenging job position with a variety of responsibilities and room for growth

Consultant?
Instructor?
Manager?
etc
Demonstration
What about the Vulnerabilities?? More deductive thinking and assumptions

<table>
<thead>
<tr>
<th>Personality Traits</th>
<th>Interests</th>
<th>Wants</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confident</td>
<td>• Fitness</td>
<td>• Inner peace &amp; happiness</td>
<td>• Failure</td>
</tr>
<tr>
<td>• Expressive</td>
<td>• Exploration</td>
<td>• Recognition</td>
<td>• Ineffectiveness</td>
</tr>
<tr>
<td>• Sharing</td>
<td>• Adventure</td>
<td>• Admiration</td>
<td>• Idleness</td>
</tr>
<tr>
<td>• Euphoric</td>
<td>• Growth</td>
<td>• Advancement</td>
<td>• Triviality</td>
</tr>
<tr>
<td>• Enthusiastic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Determined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Hard worker</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Self Image

- Social /Open
- Extraverted
- Wide social circle
- Authoritative style of expression

Social Life

- Travel
- Social Events (mostly outdoors)
- Others’ well being

- To have positive influence
- To appeal authoritative
- To be asked for advice

- Rejection
- Low impact
- Ignoring

Professional Life

- Front line person
- Team leader
- Management

Ideally he would have: Challenging job position with a variety of responsibilities and room for growth

Consultant? Instructor? Manager? etc
Profiling the Victim
How does a social engineer use all that???

• “Interests” and “Wants” columns: provide fruitful ground to start a conversation and engage the target…Attacker builds rapport, then starts building trust.

• “Vulnerabilities” column: strategically used when likeability cannot drive the desired action or for blackmailing.

• The attacker will adjust his approach according to how the target responds. He has a lot of information to work with.

• Knows the patterns of lifestyle, locations, motives, and best time to approach or attack.

• Profiling information help the attacker tailor his pretext to the victim’s personality.
Case study: Targeting victims through social media

- Throughout 2010, a kidnapping ring was targeting victims by scouting through social media.
- Wealthy individuals were preferred: Ransom would be tailored to each victim’s perceived wealth.

**Gang’s attack strategy:**
- Scouting through social media.
- Profiling targets and selecting vulnerable victims.
- Studying routines and finding patterns to determine best place & method of kidnapping.

**Tracing back:**
- Information tracing that the target was at place X at time X. (schedule availability, other people, social media, online available information?)
Case study: Targeting victims through social media

Attackers look for patterns, but they operate in patterns, too.
The case of “J-Dirt”: Persuading into Juvenile Prostitution

Underground Gangster Crips: Justin Strom’s plan of action:

• Socially engineering juveniles found through social media.

• Turning victims into prostitutes and gang members through “flattery, manipulation and when needed, force”.

• The gang recruited 10 underaged girls online and operated the prostitution ring for 6 years.

Law Enforcement Case Resolution:

• From allege and hearsay – to digital traces and evidence.

• Uncovered: Social media evidence, location evidence, payment traces, surveillance footage and more.

• Enough to connect the dots and provide strong evidence?
Reverse Engineering the Attacks

Learnings for Law Enforcement
By knowing how a victim was profiled, investigators can...

- Pinpoint the channels and sources of information used by criminals.

- Link the unique information used in an attack with the sources through which they were available.

- Predict potential future targets.

- Narrow down leads and suspects.

- ...and more
Profiling the Suspect?

• Patterns in behavior and attack strategies
• Character evidence in intend, motive or opportunity.
• Narrowing down possible suspects
• Acquisition of supportive evidence and leads
• Profile the suspect’s tendencies: better predict future behavior
• Use profiling information for more effective questioning and interrogation
• Use profiling in interrogation to lead to confession
Contact Details:

Thank you.

Christina Lekati
Social Engineering Expert
Cyber Risk GmbH

Contact Details:

Christina.lekati@cyber-risk-gmbh.com
Christina Lekati
@ChristinaLekati