Workplace Violence/IT Sabotage: Two Sides of the Same Coin?

Presenter: Michael C. Theis
Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0004065
Research Objective and Approach

**Objective:** Determine if coherent, integrated, and validated indicators for Insider Workplace Violence (WPV) and Insider Cyber Sabotage (ICS) can be identified.

**Reason:** If there are common indicators organizations may be able to develop socio-technical controls that prevent, detect, and help respond to both threats without identifying which crime will eventually be committed.

**Approach:** Collect, code, and analyze cases of WPV and compare them to cases of ICS in the CERT Insider Threat Center’s corpus.
WPV and ICS Incident Pathway

Hostile Act

Problematic Organizational Responses

Concerning Behaviors

Stressors

Personal Predispositions

Hostile Act

Execution of malicious code

Active shooter

Demotion without changing access

Loss/Suspension of Rights and Privileges

Visiting internet underground

Verbal threats to cause physical harm

Lack of resources to do job well

Perceived harassment by coworkers

Hacker

Resolving conflict by physical means

CERT, 2006

Key:

WPV
ICS

CERT, 2006

WPV and ICS Incident Pathway

Hostile Act

Problematic Organizational Responses

Concerning Behaviors

Stressors

Personal Predispositions

Hostile Act

Execution of malicious code

Active shooter

Demotion without changing access

Loss/Suspension of Rights and Privileges

Visiting internet underground

Verbal threats to cause physical harm

Lack of resources to do job well

Perceived harassment by coworkers

Hacker

Resolving conflict by physical means

CERT, 2006

Key:

WPV
ICS

CERT, 2006
Hypothesis: Common Path Before Divergence

Prevalence of Physical Manifestation

Incident Timeline

Average behavior
Range of behavior

Prevalence of Cyber Manifestation

Violence

Cyber Sabotage

Hiring
Aggregation of Stressors

- Personal: 19%
- Work: 16%
- Financial: 10%
- Relationship: 7%
- Mental Health: 9%
- Work Relationship: 39%
Stressors by ICS and WPV

**Stressors for ICS**
- Personal: 12%
- Work: 31%
- Financial: 51%
- Relationship: 0%
- Mental Health: 5%

**Stressors for WPV**
- Personal: 12%
- Work: 21%
- Financial: 13%
- Relationship: 8%
- Mental Health: 10%
- Work Relationship: 36%
Distinguishing the WPV and ICS Pathways

Prevalence of Physical Manifestation
- Predispositions
  - Conflict resolution using physical means
  - Hiring
- Member of hacking community

Prevalence of Cyber Manifestation
- Average behavior
- Range of behavior

Stressors
- Perceived harassment by coworkers

Concerning Behaviors
- Verbal threats of physical harm

Attack Execution
- Unauthorized weapons at work

Incident Timeline
- Potential measure to distinguish attack type

Workplace Violence/IT Sabotage: Two Sides of the Same Coin?
26 October 2016
© 2016 Carnegie Mellon University
Backups
A Cyber-Physical Scale for Assessing Observables*

Examples:
Execution of malicious code to delete critical files
Disabling the code that creates the backup tapes
Not submitting online reports in a timely manner
Other observables that do not reach the level of aggression
Not coming to meetings scheduled
Spreading false rumors
Verbal assault, bullying, shooting coworkers

* Note: combined cyber-physical observables may be broken down into their constituent components for measurement. See the Reality-Virtuality Continuum for a loosely related construct applied to virtual reality technologies. [https://en.wikipedia.org/wiki/Reality%E2%80%93virtuality_continuum](https://en.wikipedia.org/wiki/Reality%E2%80%93virtuality_continuum)
Operational Definitions (from Buss and Parrot)

**Aggression** – intentional behaviors that can cause significant harm to a victim (person or organization) who wishes to *avoid* the act. (note: definition excludes desired harm (sadomasochism, going to dentist) and unintentional harm (stepping on foot))

- **Direct Aggression** – person-to-person interactions (but not necessarily face-to-face) in which the perpetrator is easily identifiable by the victim (e.g., Active: Shooting, email a threat; Passive: intentionally not write a letter of recommendation and harming victim’s application for new job).

- **Indirect Aggression** – circuitous interactions in which the perpetrator may remain unidentified, possibly to avoid accusation, direct confrontation, and/or counterattack by the victim (e.g., Active: (anonymously) spreading false rumors; Passive (rare): (anonymously) not coming to the defense of someone being criticized).

- **Active Aggression** – an act of commission by the perpetrator, which involves active engagement in harming the victim (e.g., Direct: shooting; Indirect: (anonymously) spreading harmful rumors)

- **Passive Aggression** – an act of omission by the perpetrator, which involves a lack of active responding that causes harm to the victim (e.g., Direct: intentionally not write a letter of recommendation and harming victim’s application for new job; Indirect (rare): (anonymously) not coming to the defense of someone being criticized)

**Physical** - intentional acts involving personal or interpersonal interaction that does not involve cyber

**Cyber** - intentional acts involving interaction with computers, computer networks, or electronic media
## Hasan, Fort Hood – 2009: Concerning Behaviors

<table>
<thead>
<tr>
<th>Major Period</th>
<th>Sub-Period</th>
<th>Direct-Active Cyber Aggression (-3)</th>
<th>Indirect Active Cyber Aggression (-2)</th>
<th>Passive Cyber (Indirect or Direct) (-1)</th>
<th>Center of Scale (0)</th>
<th>Passive Physical (Indirect or Direct) (+1)</th>
<th>Indirect Active Physical Aggression (+2)</th>
<th>Direct Active Physical Aggression (+3)</th>
<th>Sub-Period Concerning Behaviors (non-zero)</th>
<th>Major Period Concerning Behaviors (non-zero)</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘92-97</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>‘98-03</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>‘04-09</td>
<td></td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>Sub-Periods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of Last Major</td>
<td>‘04-05</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Period</td>
<td>‘06-07</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>‘08-09</td>
<td></td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Major Period Totals</td>
<td></td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>18</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>Major Period</td>
<td>Sub-Period</td>
<td>Direct Active Cyber Aggression (-3)</td>
<td>Indirect Active Cyber Aggression (-2)</td>
<td>Passive Cyber (Indirect or Direct) (-1)</td>
<td>Center of Scale (0)</td>
<td>Passive Physical (Indirect or Direct) (+1)</td>
<td>Indirect Active Physical Aggression (+2)</td>
<td>Direct Active Physical Aggression (+3)</td>
<td>Sub-Period Concerning Behaviors (non-zero)</td>
<td>Major Period Concerning Behaviors (non-zero)</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>3/04-3/07</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/07-12/10</td>
<td></td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>'1/11-9/13</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-Periods of Last Major Period</td>
<td>2011</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2012</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2013</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Period Totals</td>
<td></td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>
7-Point Scale Analysis of Results

Key:
WPV: 
ICS:

Cyber Aggression

Physical Aggression

ICS1
ICS3
ICS4
ICS2
ICS5

Hasan
Alexis
Wells
Lopez

Physical Aggression

Cyber Aggression

WPV: Hasan, Alexis, Wells, Lopez
ICS: ICS1, ICS2, ICS3, ICS4, ICS5