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

Presenter: Michael C. Theis

Notices

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.

DM-0004065

Research Objective and Approach

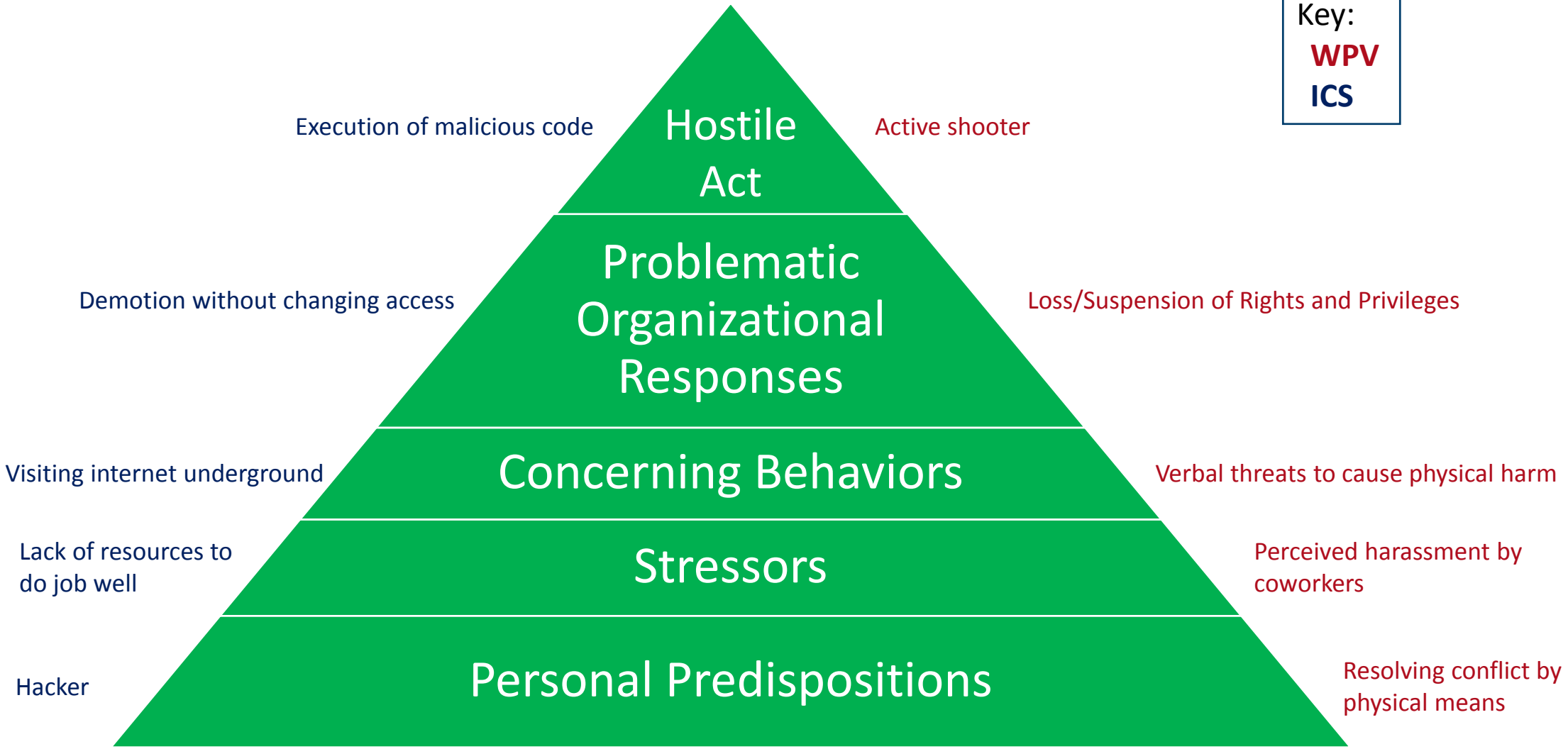
Objective: Determine if coherent, integrated, and validated indicators for Insider Workplace Violence (WPV) and Insider Cyber Sabotage (ICS) can be identified.

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.

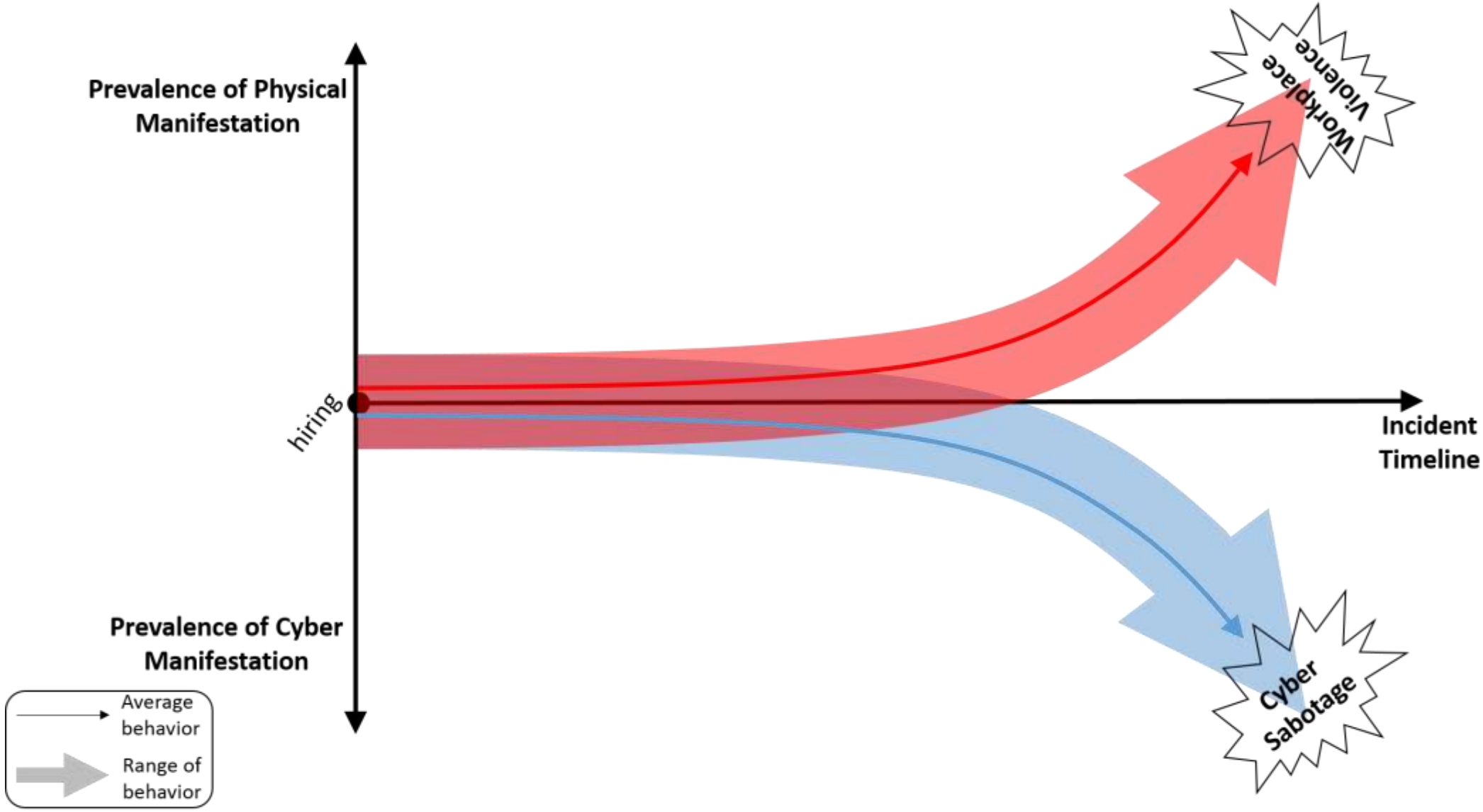
WPV and ICS Incident Pathway

Key:
WPV
ICS

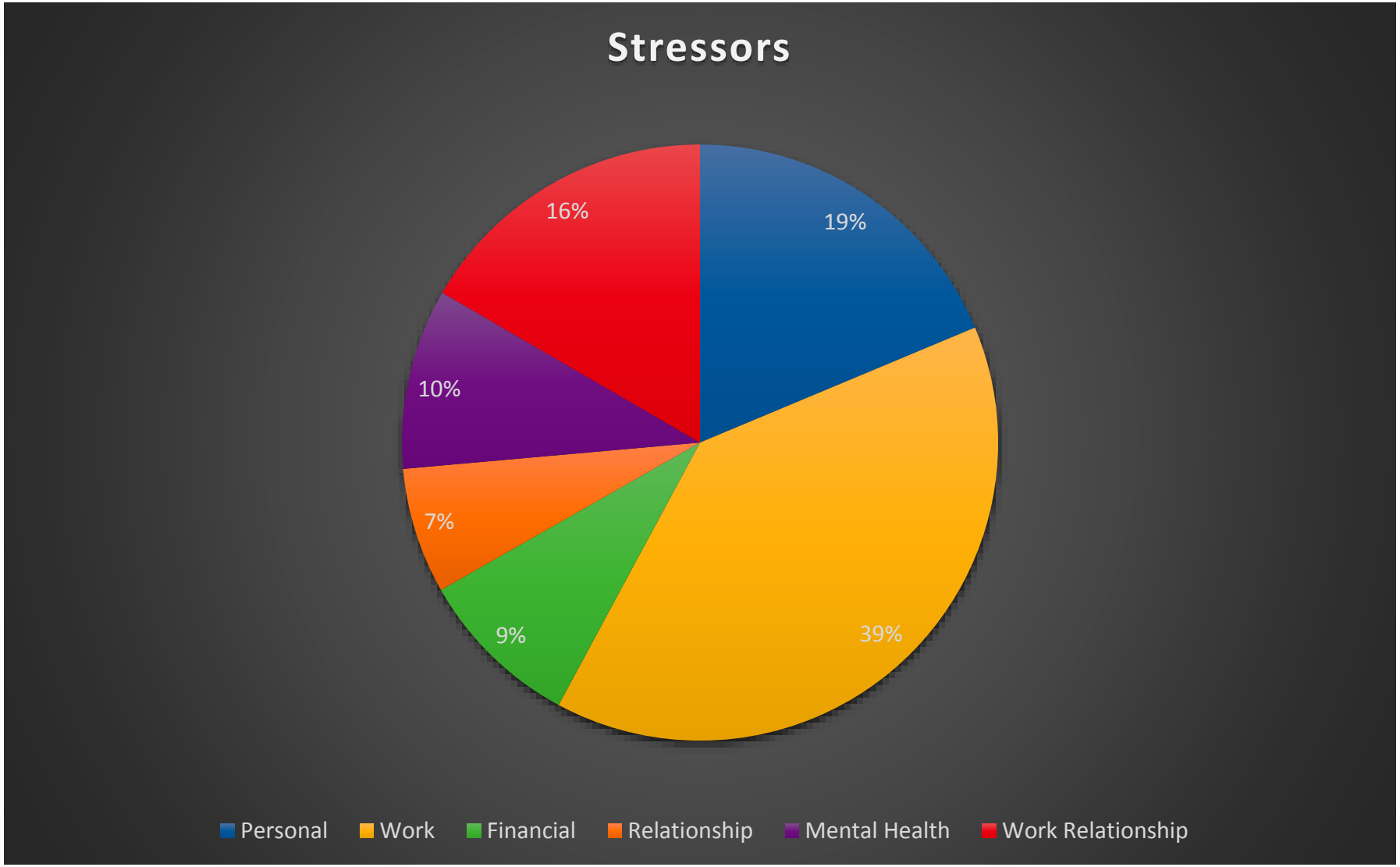


CERT, 2006

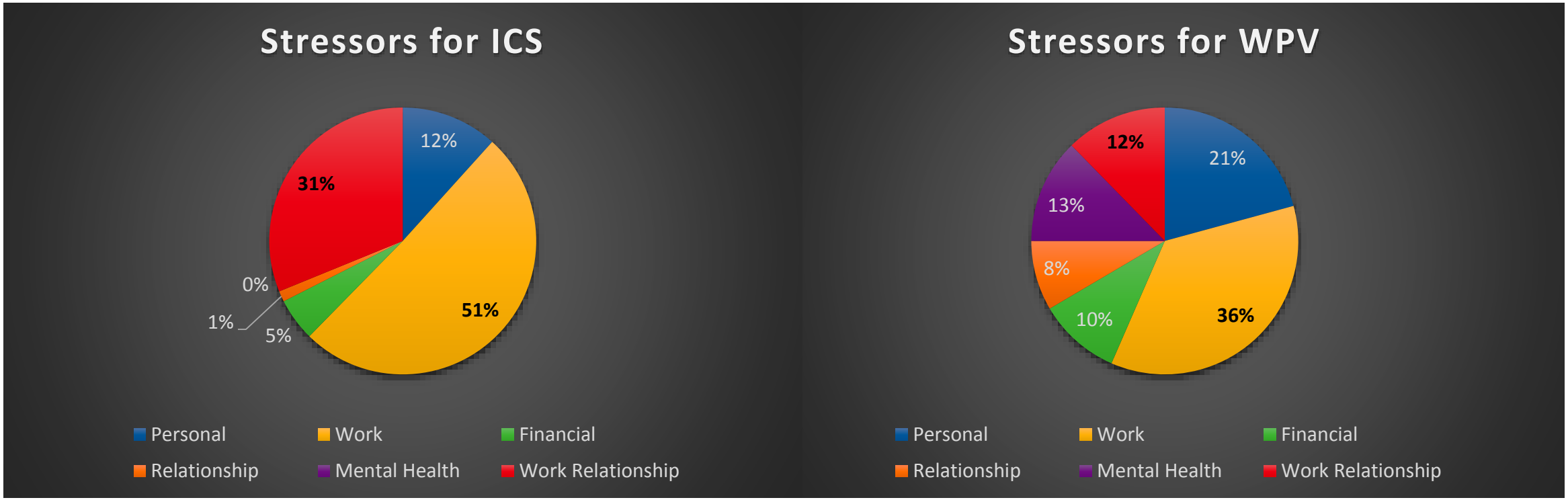
Hypothesis: Common Path Before Divergence



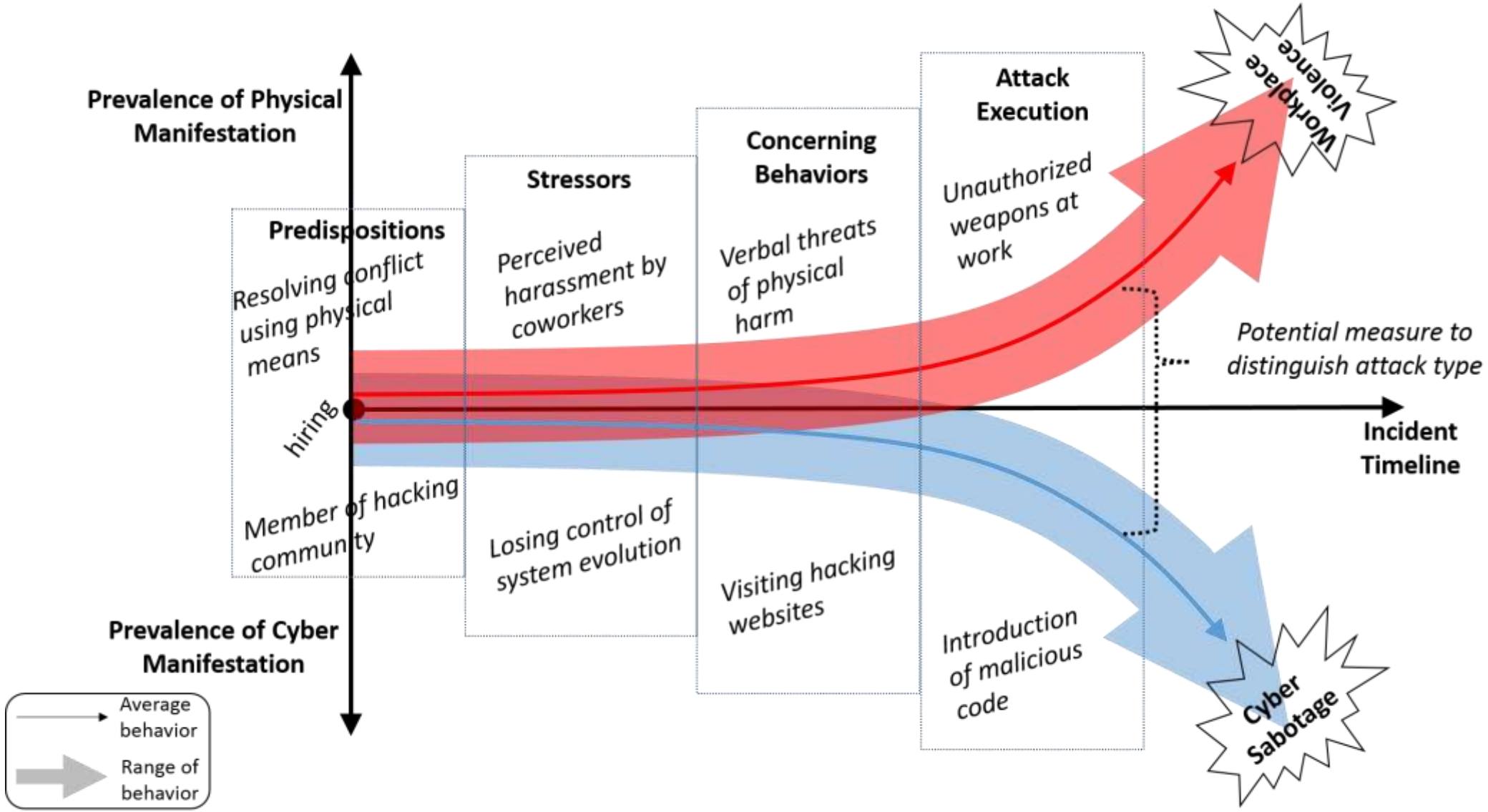
Aggregation of Stressors



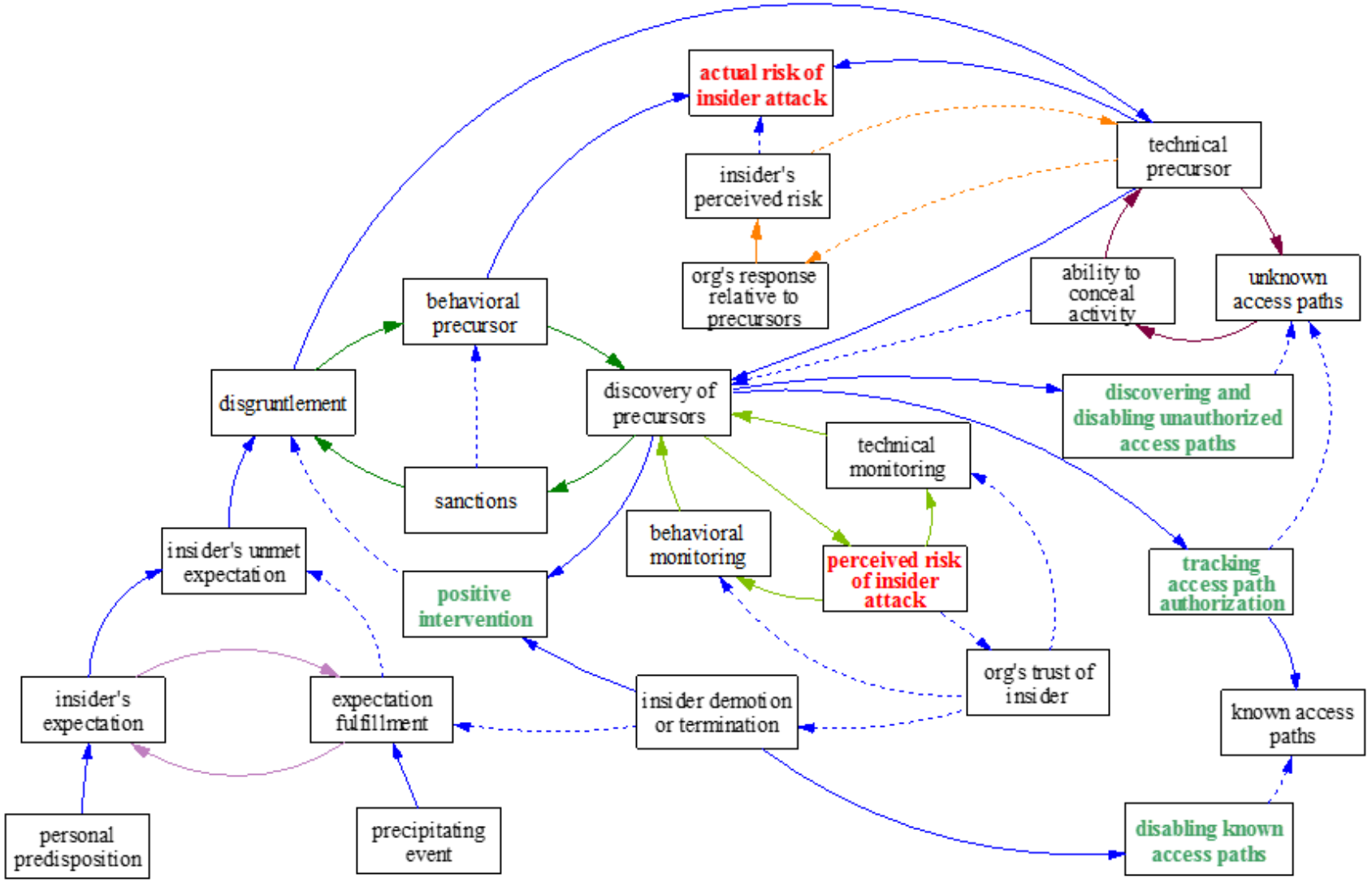
Stressors by ICS and WPV



Distinguishing the WPV and ICS Pathways

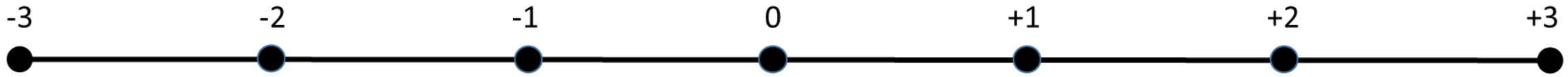


ICS Causal Loop Diagram



Backups

A Cyber-Physical Scale for Assessing Observables*



-3	-2	-1	0	+1	+2	+3
Direct, Active Cyber Aggression	Indirect, Active Cyber Aggression	Passive (Direct or Indirect) Cyber Aggression	Non-aggressive behaviors whether physical or cyber	Passive (Direct or Indirect) Physical Aggression	Indirect, Active Physical Aggression	Direct, Active Physical Aggression
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

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

Major Period	Sub-Period	Direct-Active Cyber Aggression (-3)	Indirect Active Cyber Aggression (-2)	Passive Cyber (Indirect or Direct) (-1)	Center of Scale (0)	Passive Physical (Indirect or Direct) (+1)	Indirect Active Physical Aggression (+2)	Direct Active Physical Aggression (+3)	Sub-Period Concerning Behaviors (non-zero)	Major Period Concerning Behaviors (non-zero)
'92-97		0	0	0		1	2	0		3
'98-03		0	0	0		0	1	0		1
'04-09		2	3	0		1	5	3		14
Sub-Periods of Last Major Period	'04-05	0	0	0		0	2	0	2	
	'06-07	0	0	0		0	2	0	2	
	'08-09	2	3	0		1	1	3	10	
Major Period Totals		2	3	0		2	8	3		18

Alexis, WNY – 2013: Concerning Behaviors

Major Period	Sub-Period	Direct-Active Cyber Aggression (-3)	Indirect Active Cyber Aggression (-2)	Passive Cyber (Indirect or Direct) (-1)	Center of Scale (0)	Passive Physical (Indirect or Direct) (+1)	Indirect Active Physical Aggression (+2)	Direct Active Physical Aggression (+3)	Sub-Period Concerning Behaviors (non-zero)	Major Period Concerning Behaviors (non-zero)
3/04-3/07		0	0	0		1	0	2		3
4/07-12/10		0	0	2		1	0	1		4
’1/11-9/13		0	0	0		1	3	0		4
Sub-Periods of Last Major Period	2011	0	0	0		0	0	0		
	2012	0	0	0		0	0	0		
	2013	0	0	0		1	3	0	4	
Major Period Totals		0	0	2		3	3	3		11

7-Point Scale Analysis of Results