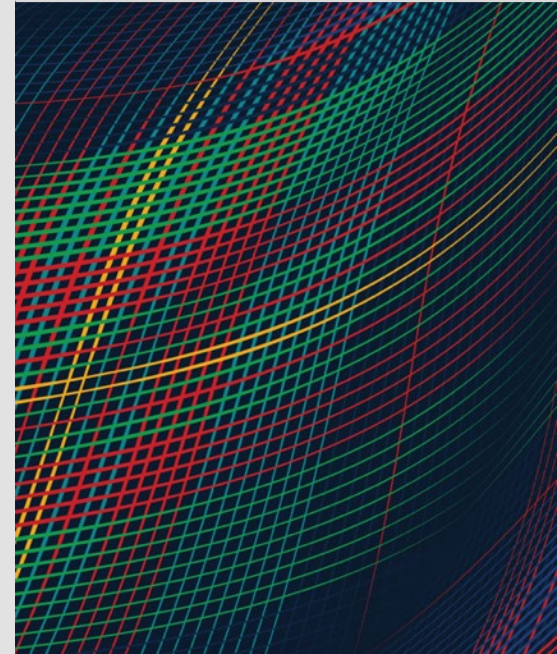


# The Critical Pathway to Insider Risk

**MARCH 6, 2024**

William R. Claycomb, Ph.D.  
Principal Researcher



# Document Markings

Copyright 2024 Carnegie Mellon University.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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 was prepared for the exclusive use of Participants of the 2nd International Symposium on Insider Threat Mitigation and may not be used for any other purpose without the written consent of [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-0227

# Short Distribution Statements

## Statement in Document Markings System

## Short Statement You Can Use

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

[INTERNAL SEI-USE ONLY] Further dissemination requires re-submittal through DM-RRO.

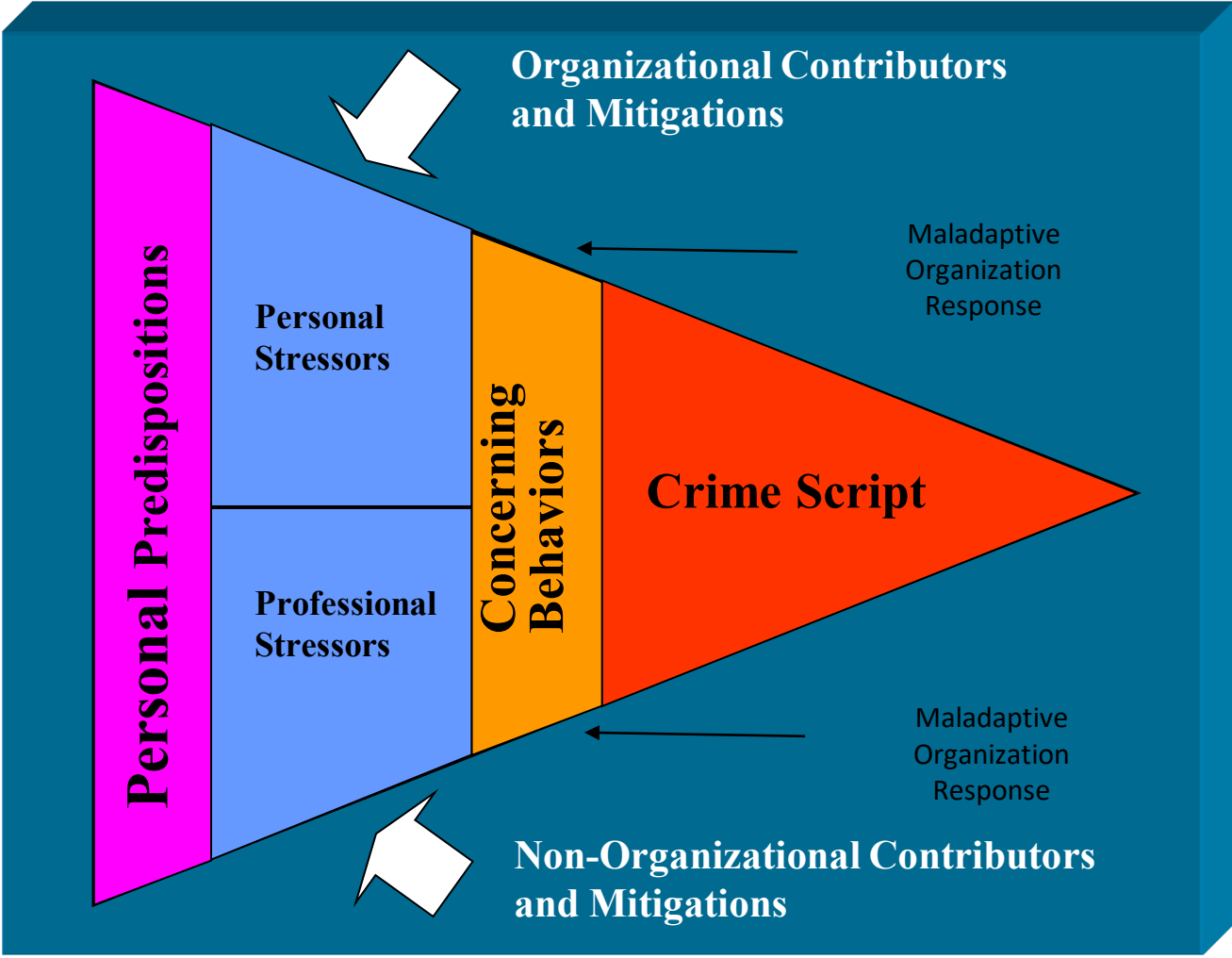
[INTERNAL SEI-USE ONLY] DM-RRO REQUIRED.

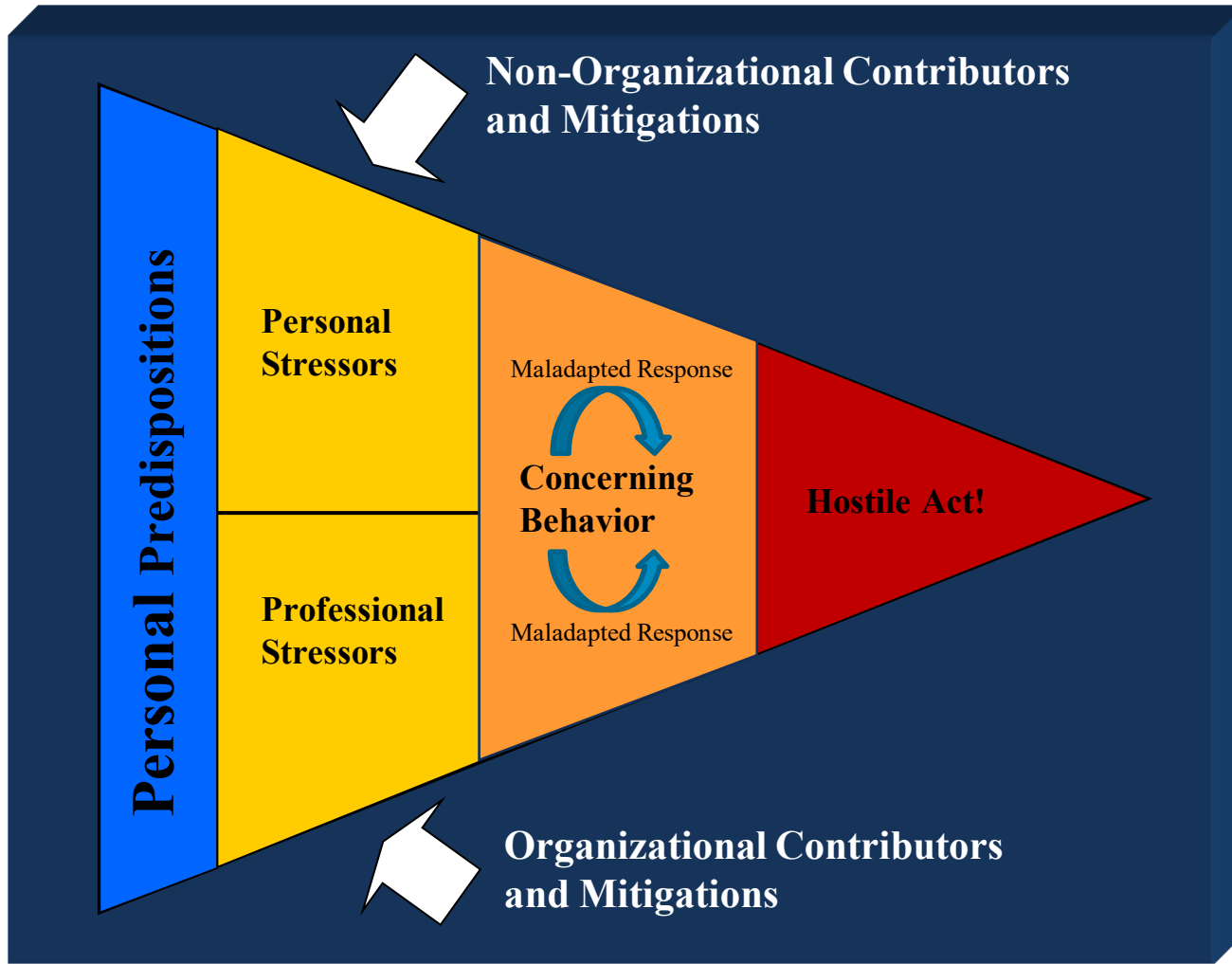
# Agenda

- **What is The Critical Pathway to Insider Risk?**
- **Origins**
- **Research**
- **Use in practice**

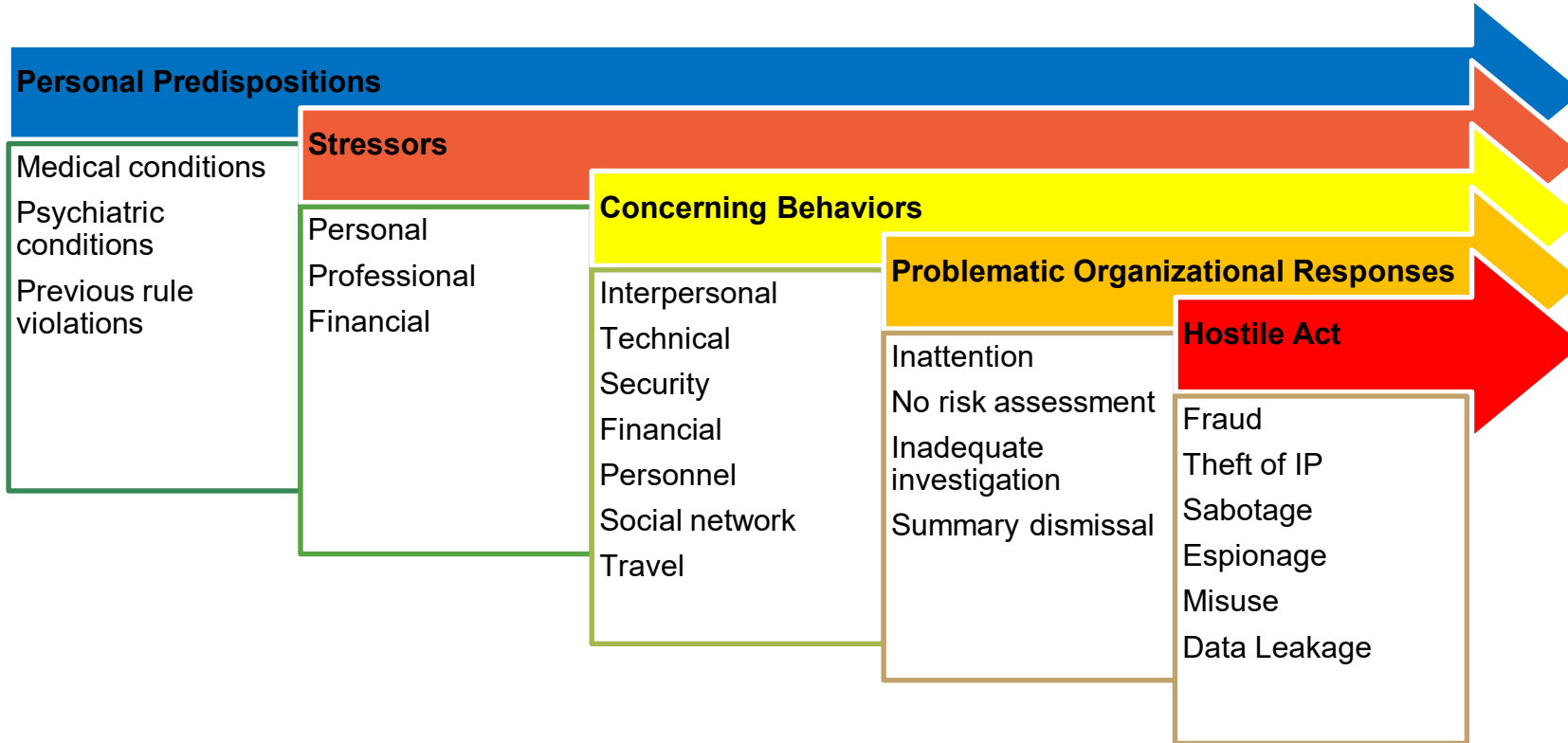
Presentation Name

# What is “The Critical Pathway to Insider Risk”





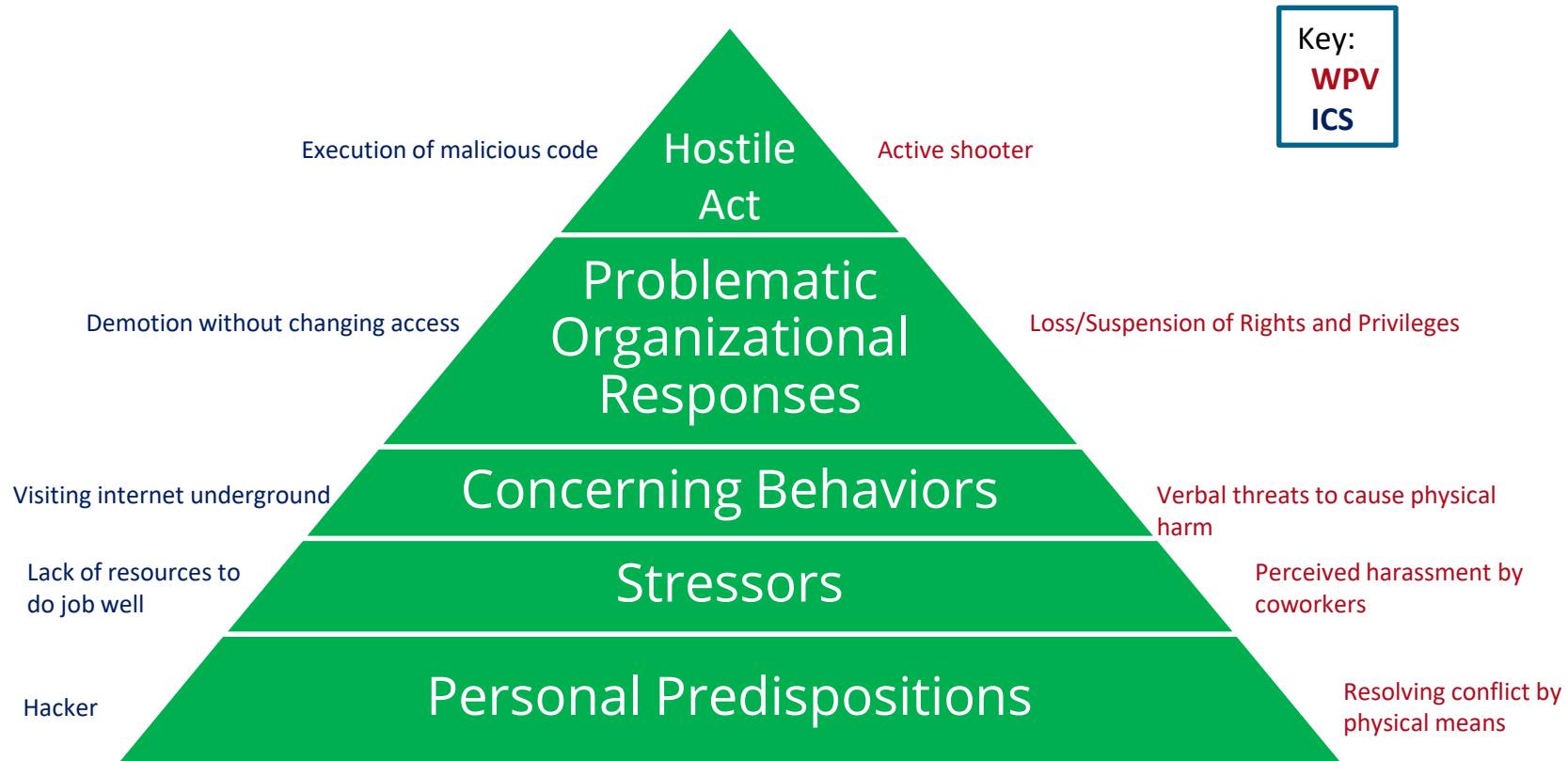
# “Critical Pathway to Insider Risk”







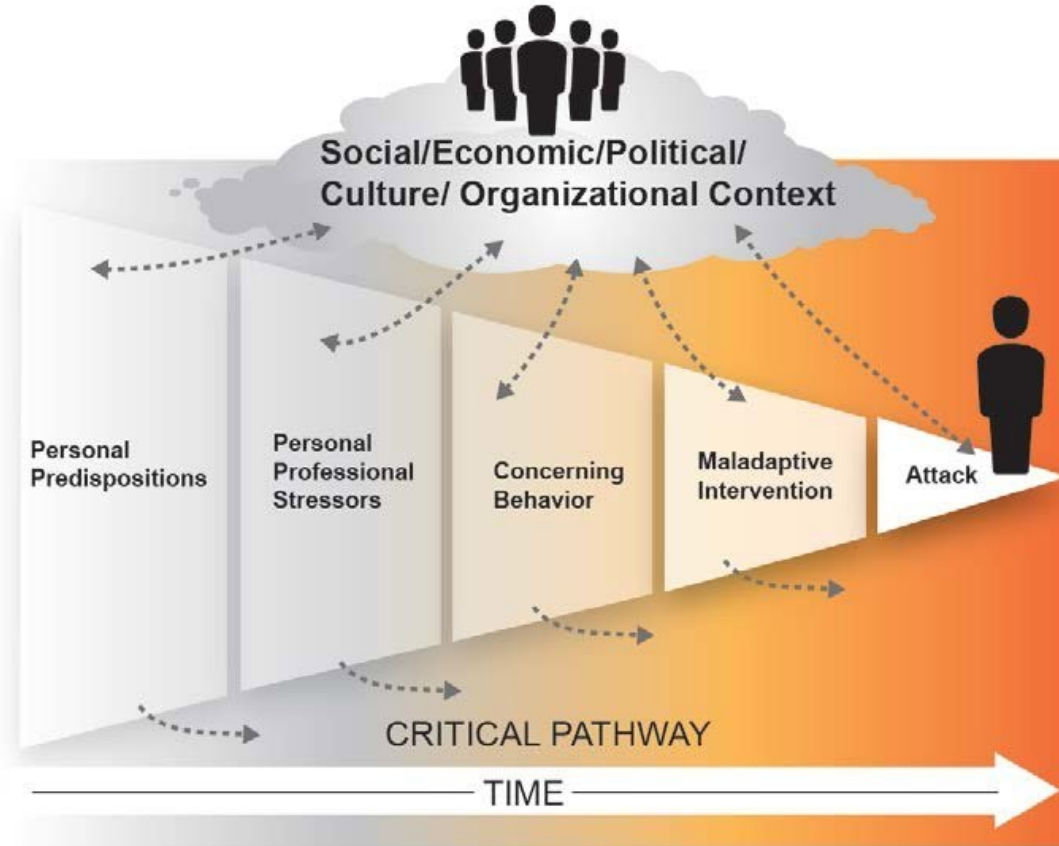
# “Critical Pathway to Insider Risk”



CERT, 2006

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

# “Critical Pathway to Insider Risk”



# “Critical Pathway to Insider Risk”

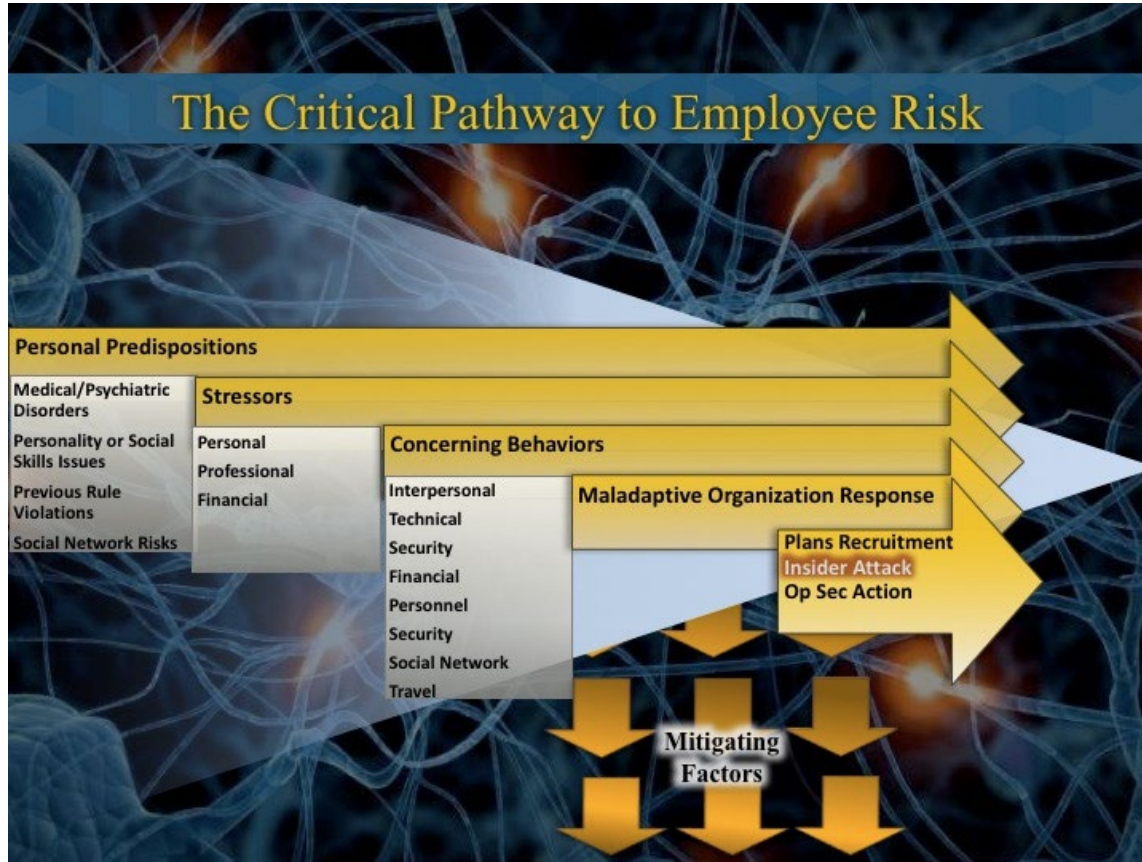
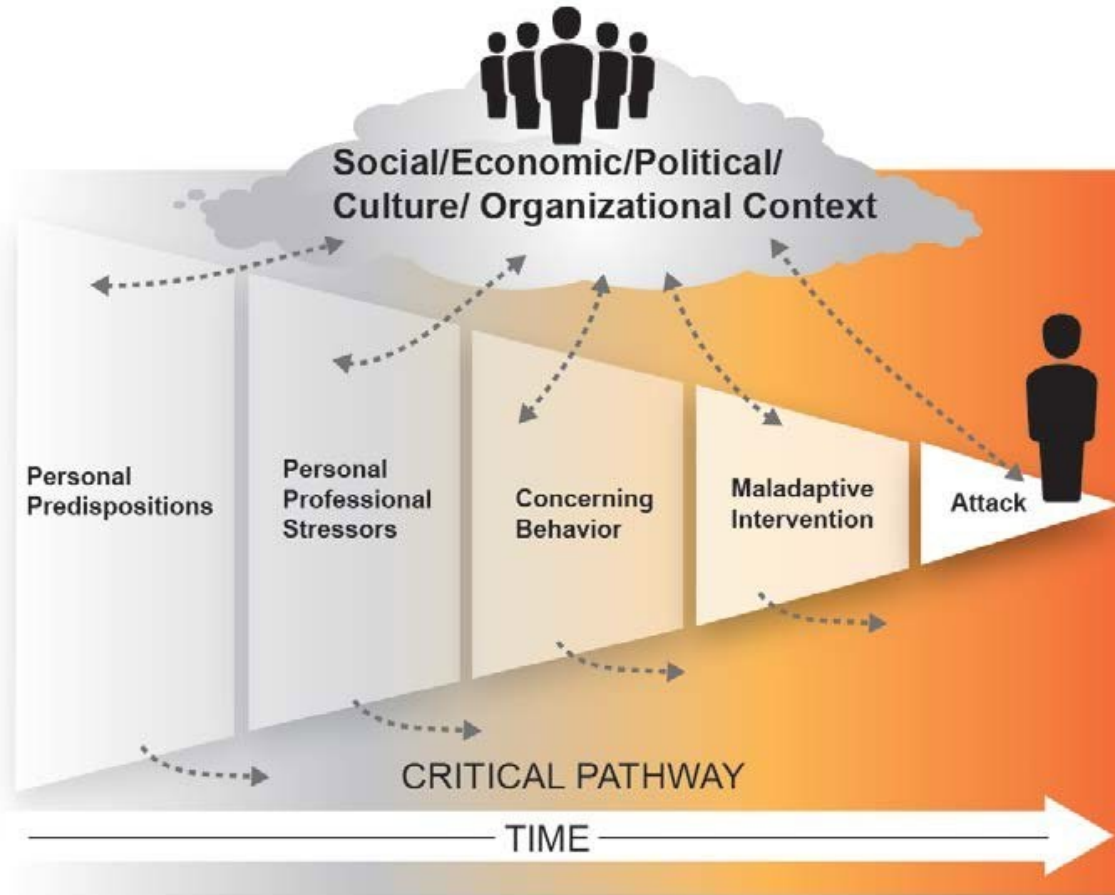
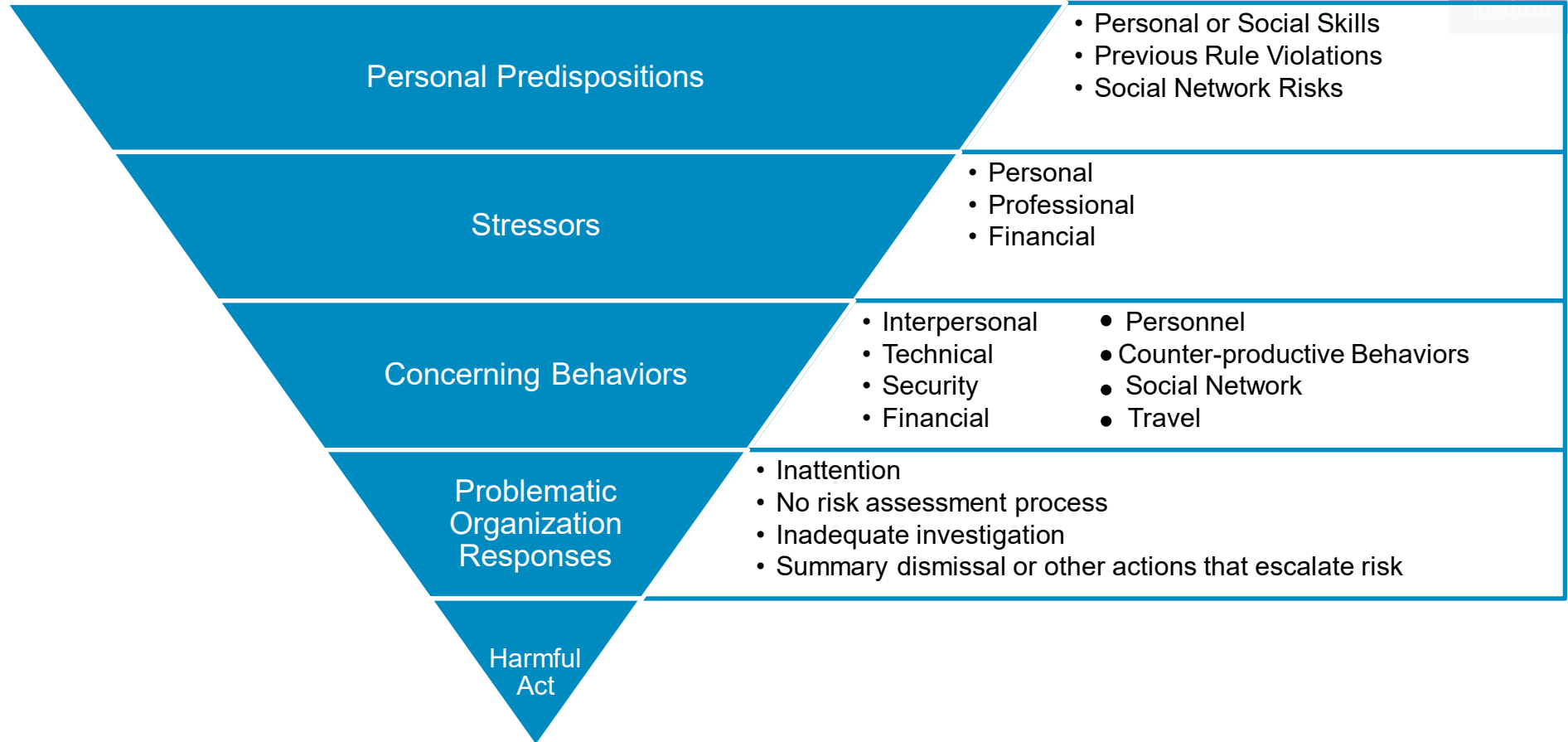


Image courtesy of “The Insider Risk Group,” <https://www.insiderriskgroup.com/>

# “Critical Pathway to Insider Risk”



# CERT's Critical Path to Insider Risk

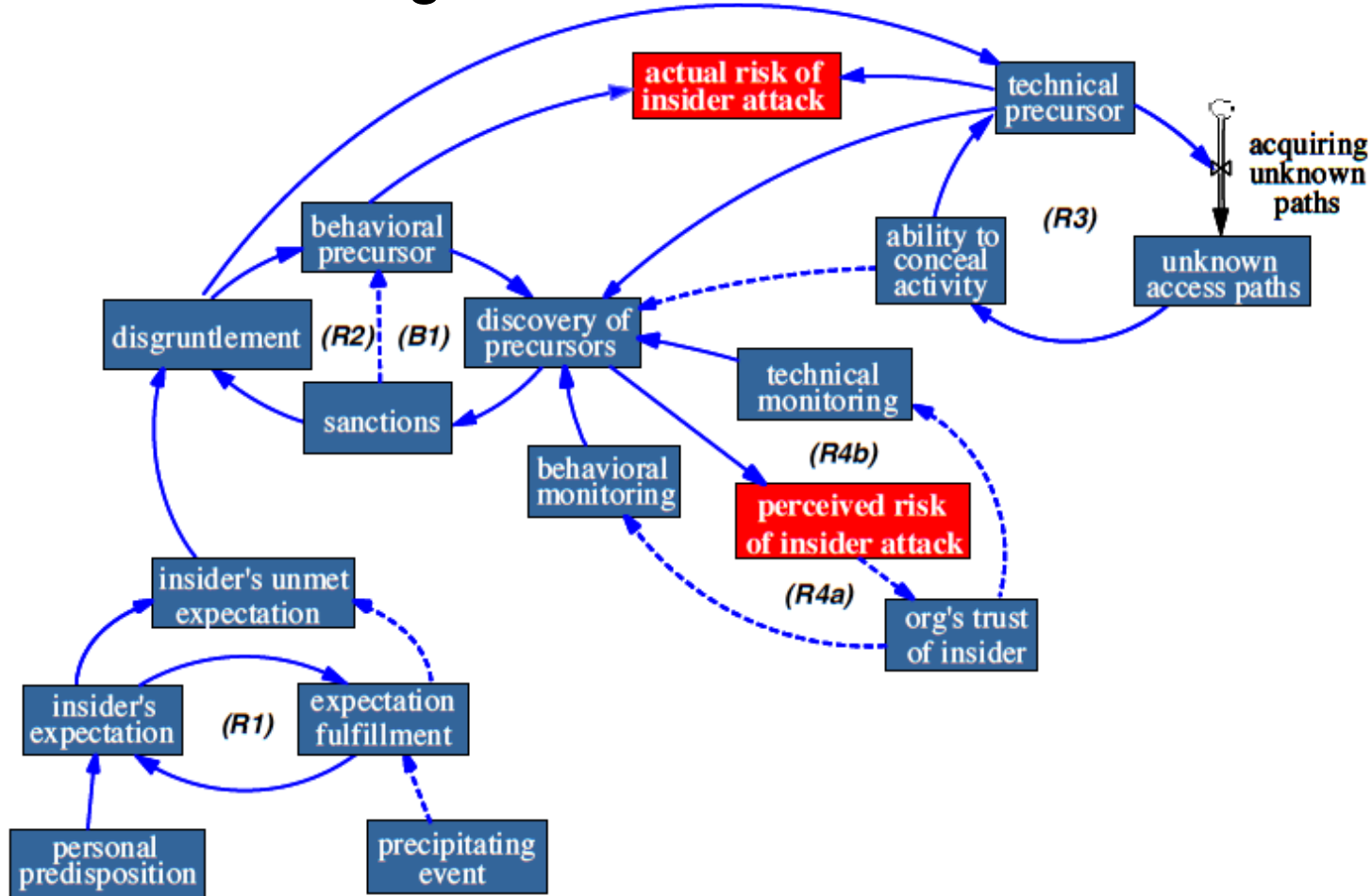


Adapted from Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)

The Critical Pathway to Insider Risk

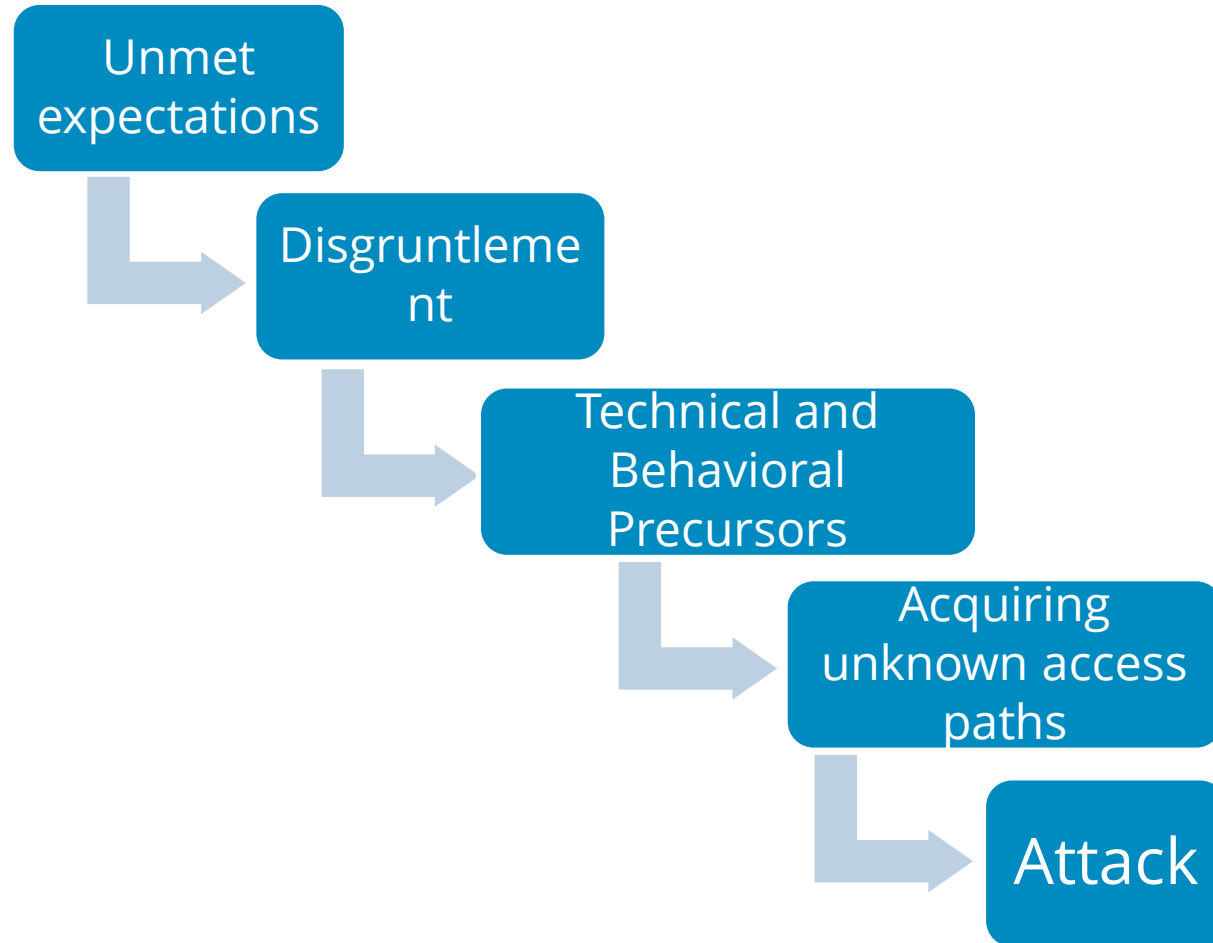
# Origins

# Model: Insider Sabotage

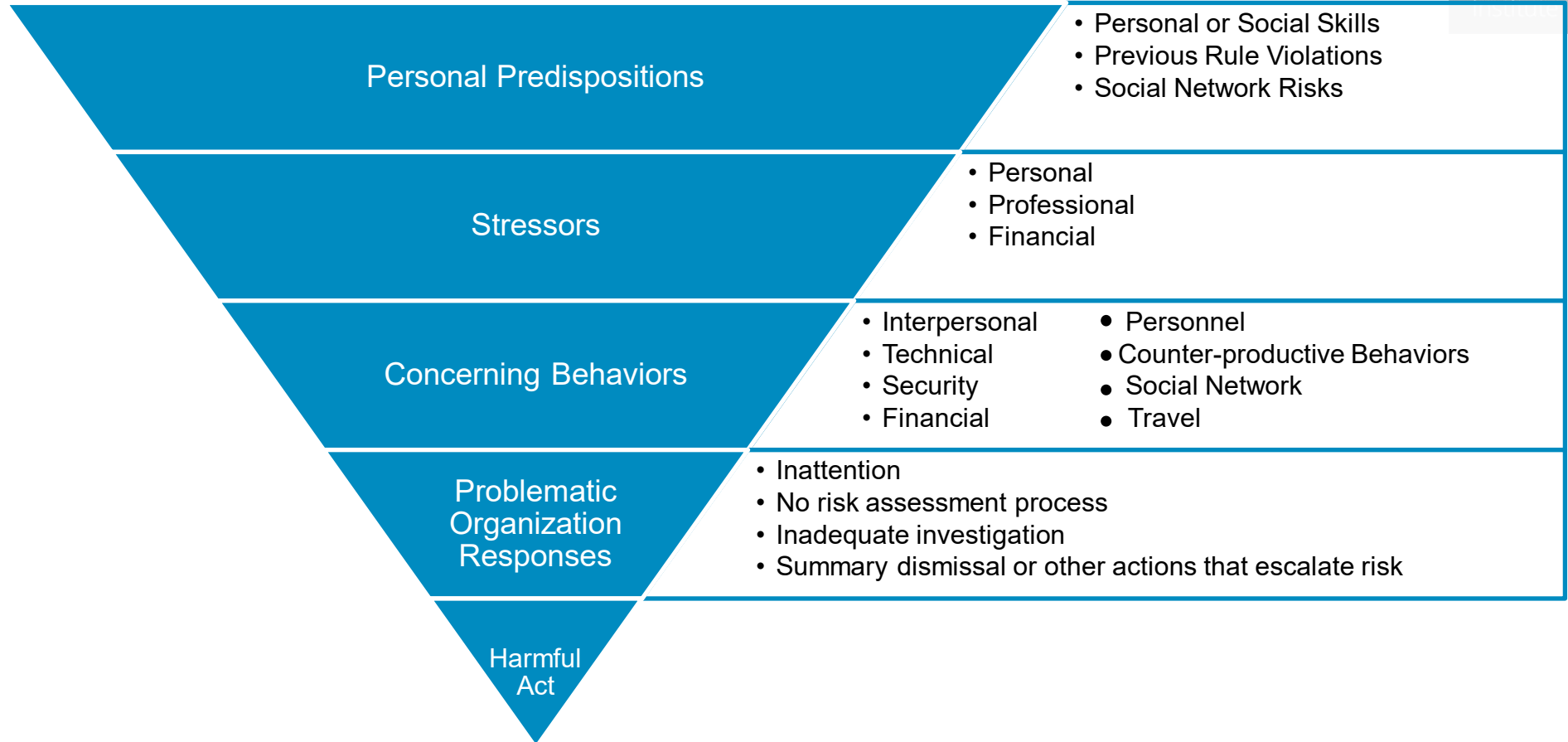




# Insider Sabotage Model Simplified



# CERT's Critical Path to Insider Risk



Adapted from Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)

# Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

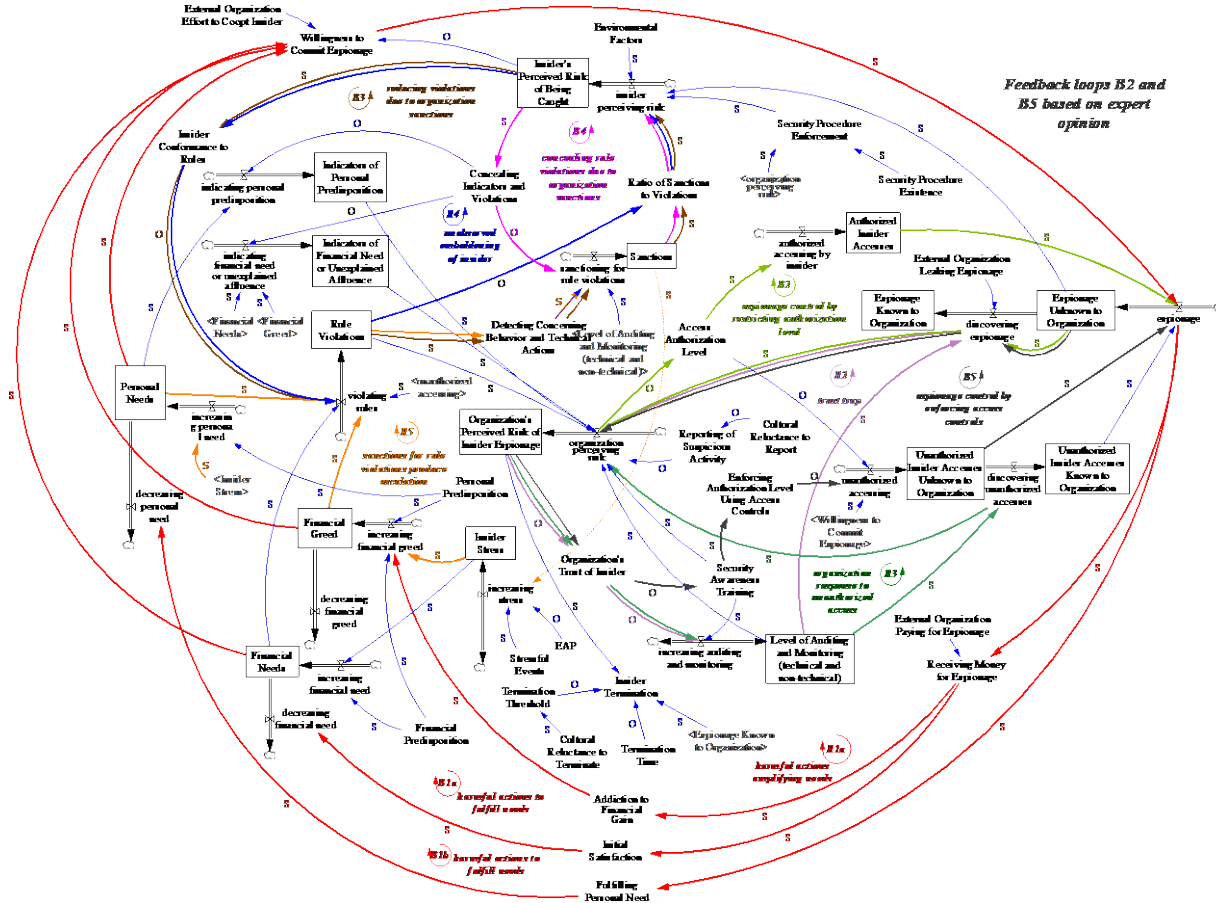
Stephen R. Band, Ph.D. (Counterintelligence Field Activity - Behavioral Science Directorate)  
Dawn M. Cappelli (CERT)  
Lynn F. Fischer, Ph.D. (DoD Personnel Security Research Center)  
Andrew P. Moore (CERT)  
Eric D. Shaw, Ph.D. (Consulting & Clinical Psychology, Ltd.)  
Randall F. Trzeciak (CERT)

**December 2006**

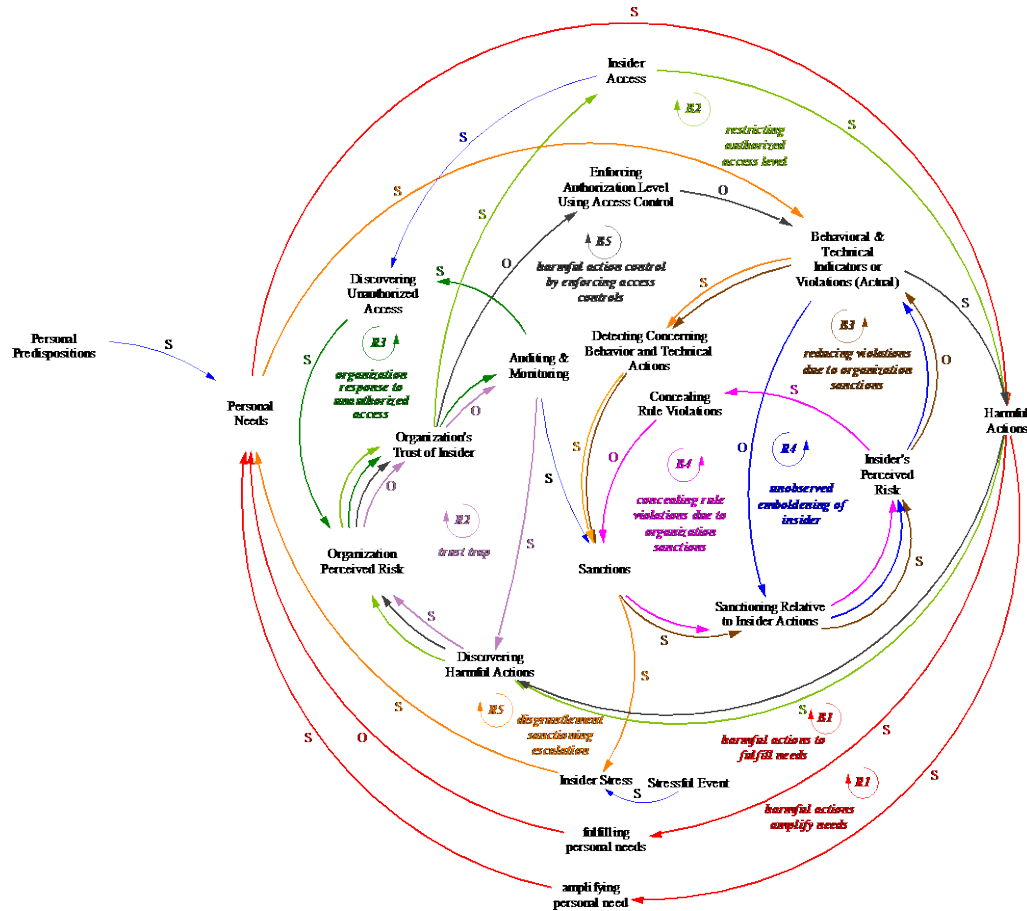
**TECHNICAL REPORT**  
CMU/SEI-2006-TR-026  
ESC-TR-2006-091

**CERT® Program**  
Unlimited distribution subject to the copyright.

# 2006 PERSEREC-CERT Espionage Model

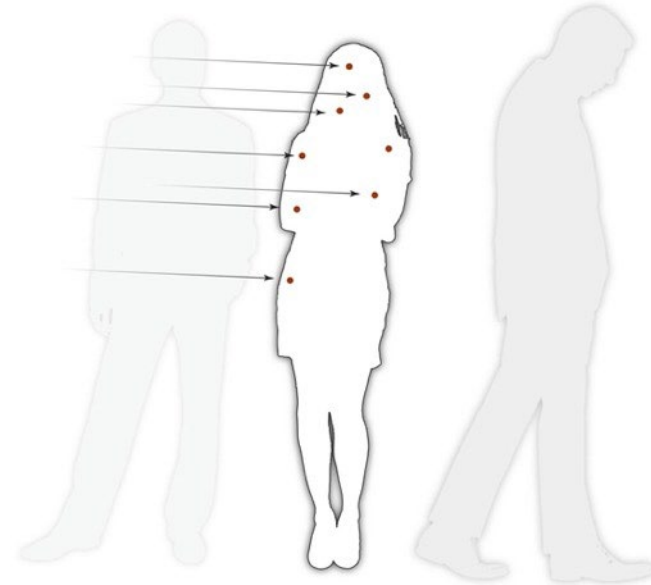


# Abstracted Common (Espionage) Model



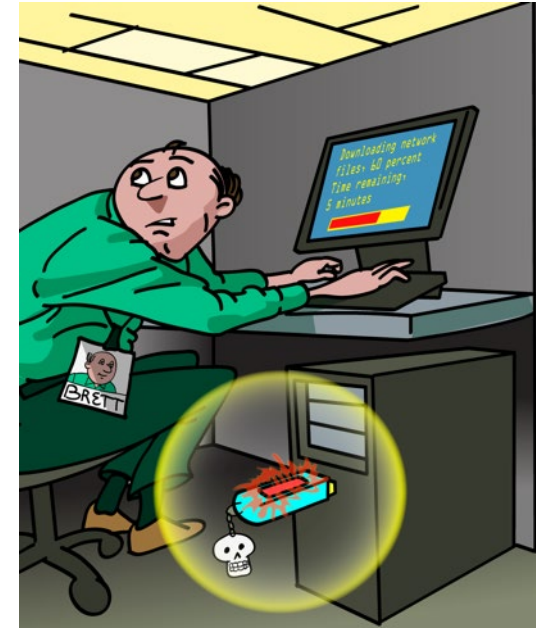
# Behavioral Precursors Observed in Cases

- Drug use
- Conflicts (coworkers, supervisor)
- Aggressive or violent behavior
- Web surfing, chat rooms at work
- Mood swings
- Bizarre behavior
- Used organization's computers for personal business
- Poor performance
- EEO complaint
- Absence/tardiness
- Sexual harassment
- Poor hygiene



# Technical Precursors Undetected in Cases

- Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers
- Failure to create backups as required
- Failure to document systems or software as required
- Unauthorized access of customers’ systems
- Unauthorized use of coworkers’ machines left logged in
- Sharing passwords with others & demanding passwords from subordinates
- System access following termination
- Refusal to swipe badge to record physical access
- Access of web sites prohibited by acceptable use policy
- Refusal to return laptop upon termination
- Use of backdoor accounts
- Use of organization’s system for game playing, violating acceptable use policy
- Set up every new computer for easy access remotely



The Critical Pathway to Insider Risk

# Supporting Research



# Research Through the Years

- **Shaw & Fischer, 2005**
- **Band et al., 2006**
- **Shaw, 2006**
- **Shaw, Fischer, & Rose, 2009**
- **Shaw & Strock, 2001**
- **Shaw & Sellars, 2015**
- **Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T. (2012). Chronological examination of insider threat sabotage: Preliminary observations. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3, 4–20.**

The Critical Pathway to Insider Risk

# Use in Practice

**Carnegie  
Mellon  
University**  
Software  
Engineering  
Institute

# In Practice



The Critical Pathway to Insider Risk

# Questions

Contact: [claycomb@cert.org](mailto:claycomb@cert.org)

