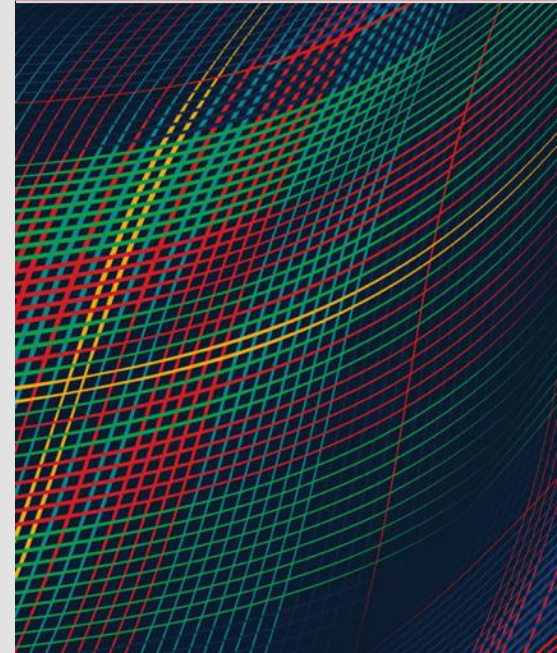


The Critical Pathway to Insider Risk: Introduction and Origins

DECEMBER 11, 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 Public webinar organized by DOE Insider Threat Group and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

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

DM24-1659

Agenda

- **What is The Critical Pathway to Insider Risk?**
- **Origins**
- **Research**
- **Visual representations through the years**
- **Use in practice**

Presentation Name

What is “The Critical Pathway to Insider Risk”?

The Critical Pathway to Insider Risk



Lenzenweger, Mark F., and Eric D. Shaw. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." *Counter-Insider Threat Research and Practice* 1, no. 1 (2022).

The Critical Pathway to Insider Risk

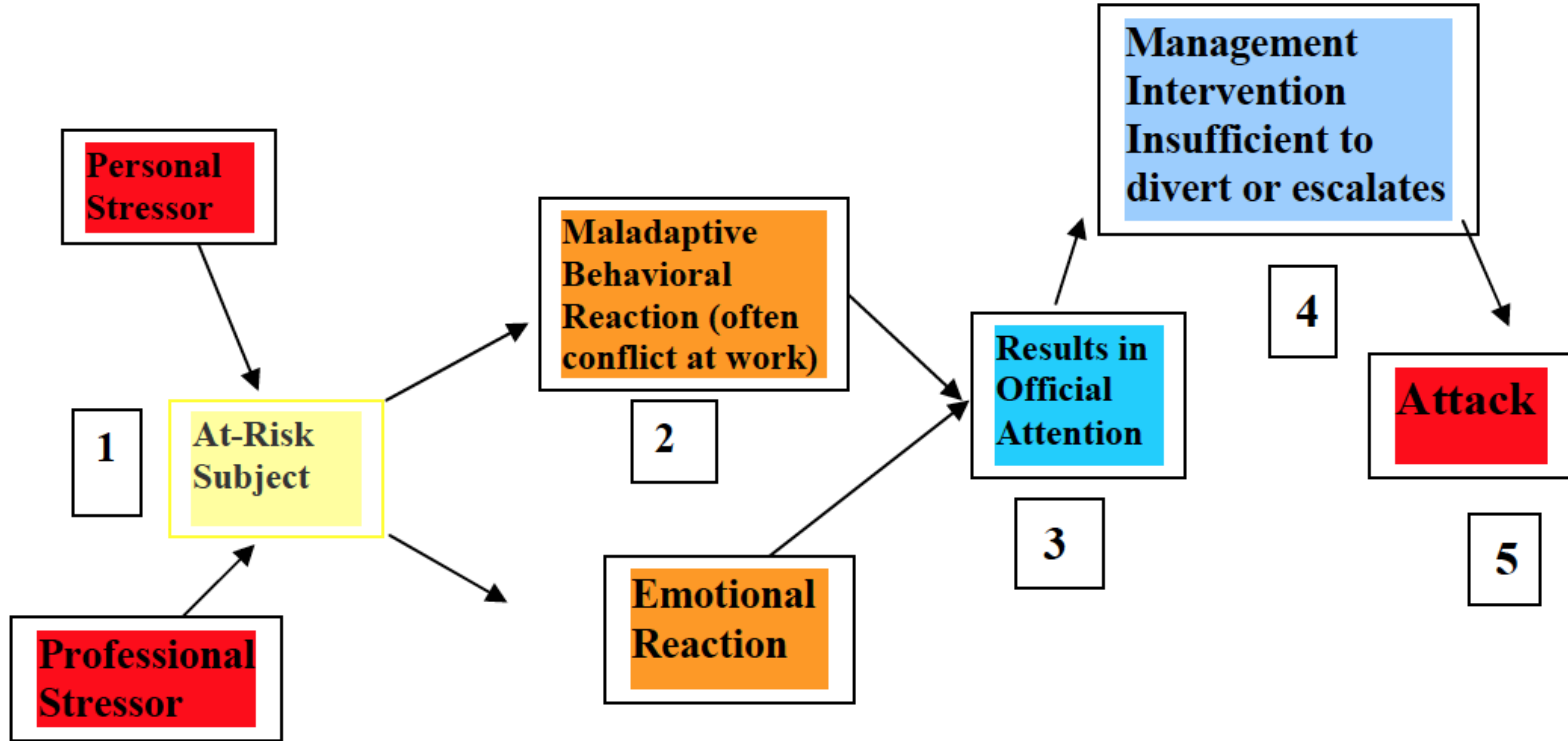
Origins

“The Critical Pathway in Insider Espionage” (1998)

- Predisposing Personal Traits
- An Acute Situational Stressor
- Emotional Fallout
- Biased Decision-making or Judgment Failures
- Failure of Peers and Supervisors to Intervene Effectively

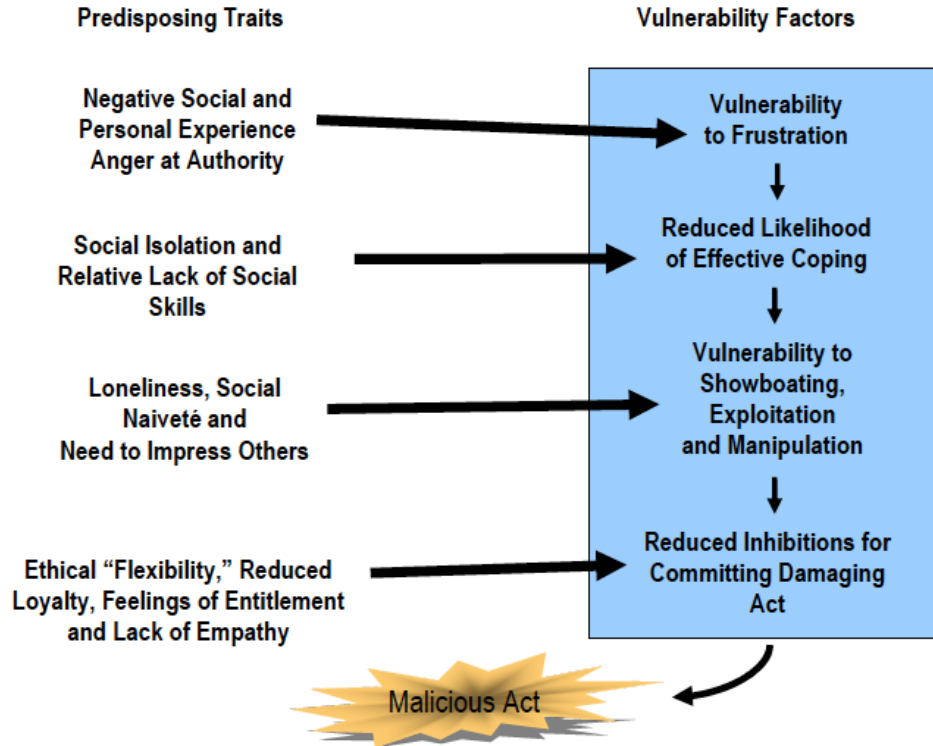
Shaw, Eric D., Keven G. Ruby, and Jerrold M. Post. "The insider threat to information systems." *Security Awareness Bulletin* 2, no. 98 (1998): 1-10.

"Events Along the Critical Pathway" (2005)



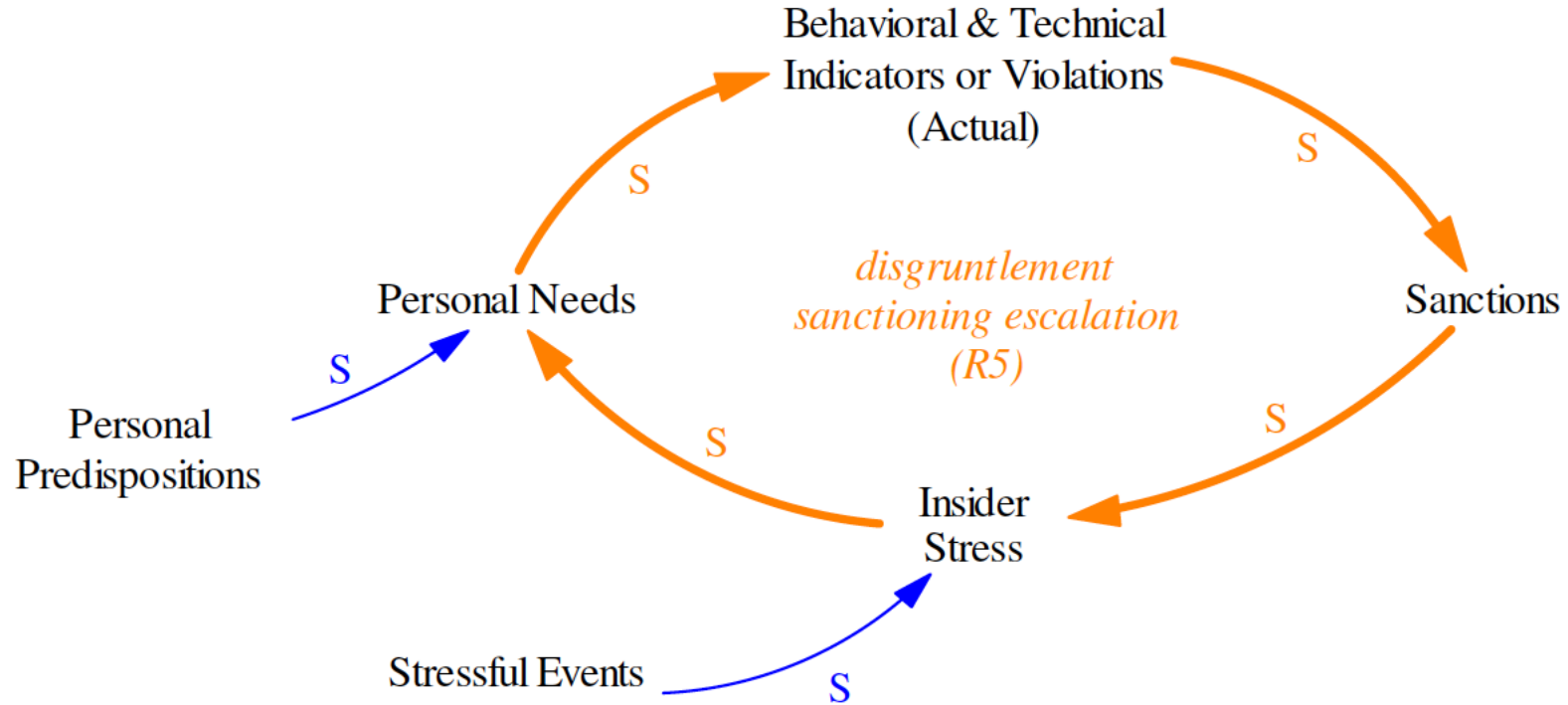
Shaw, Eric D., and Lynn F. Fischer. "Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations." *Defense Personnel Security Research Center, Monterey, CA* (2005).

“Effects of Personal Risk Factors in the Workplace” (2005)



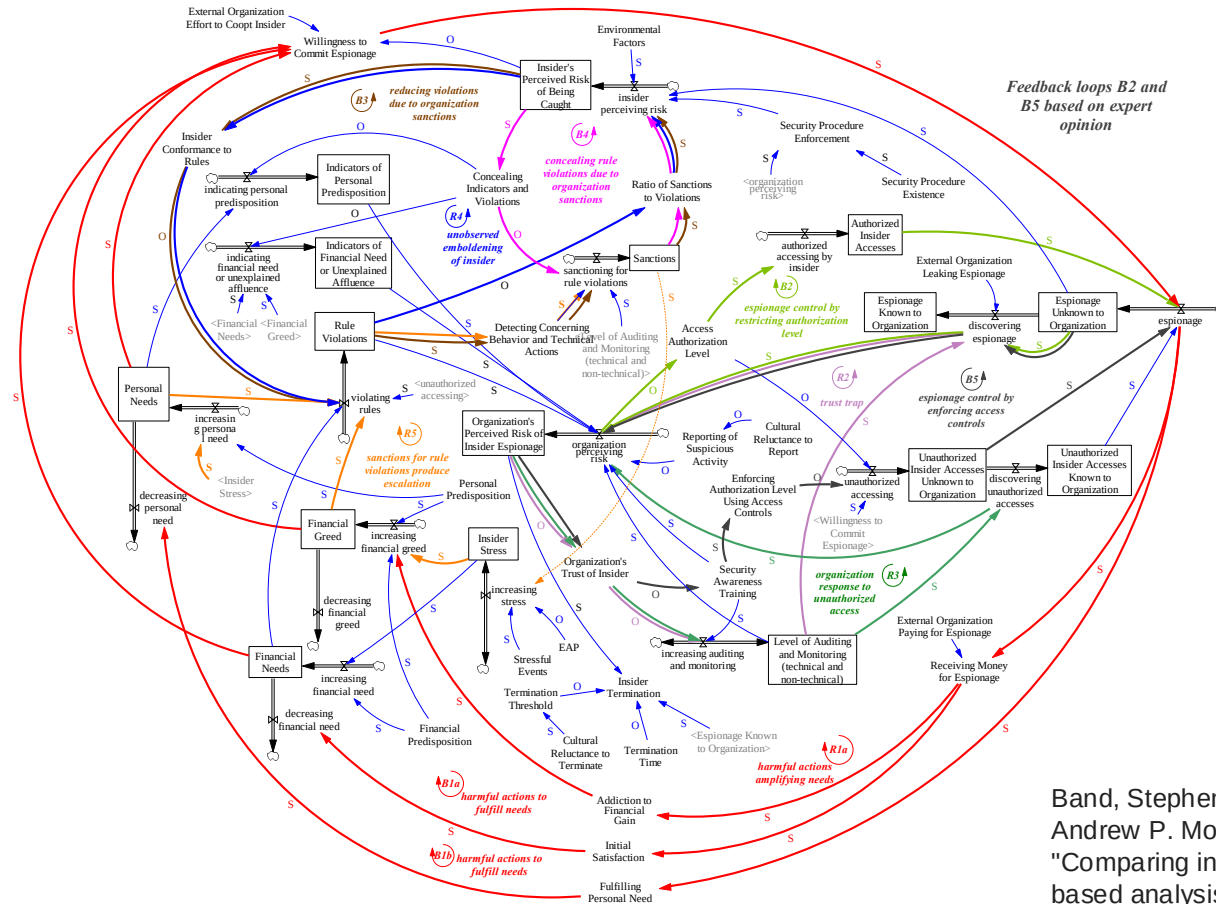
Shaw, Eric D., and Lynn F. Fischer. "Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations." *Defense Personnel Security Research Center, Monterey, CA* (2005).

Personal Predispositions (2006)



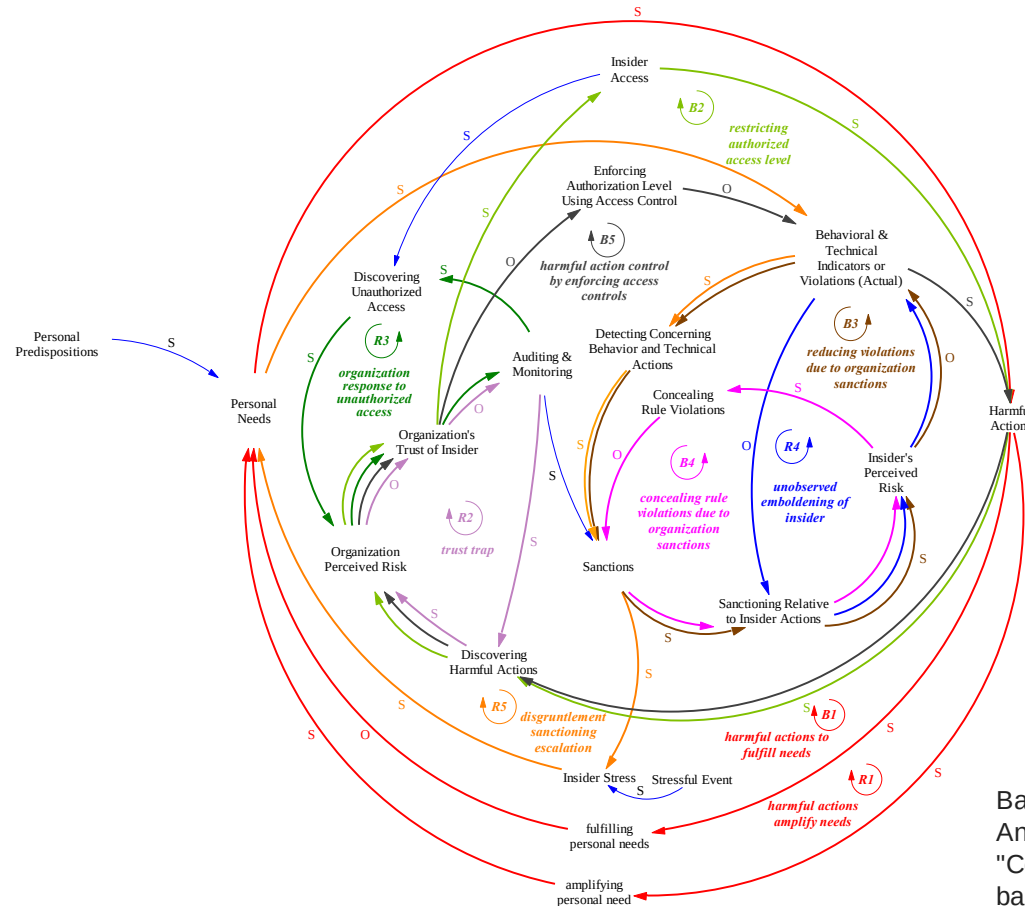
Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis." *CMU-CERT Program, Tech. Rep* (2006).

2006 PERSEREC-CERT Espionage Model



Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis." *CMU-CERT Program, Tech. Rep* (2006).

Abstracted Common (Espionage) Model



Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis." *CMU-CERT Program, Tech. Rep* (2006).

“Conceptual Framework” (2007)



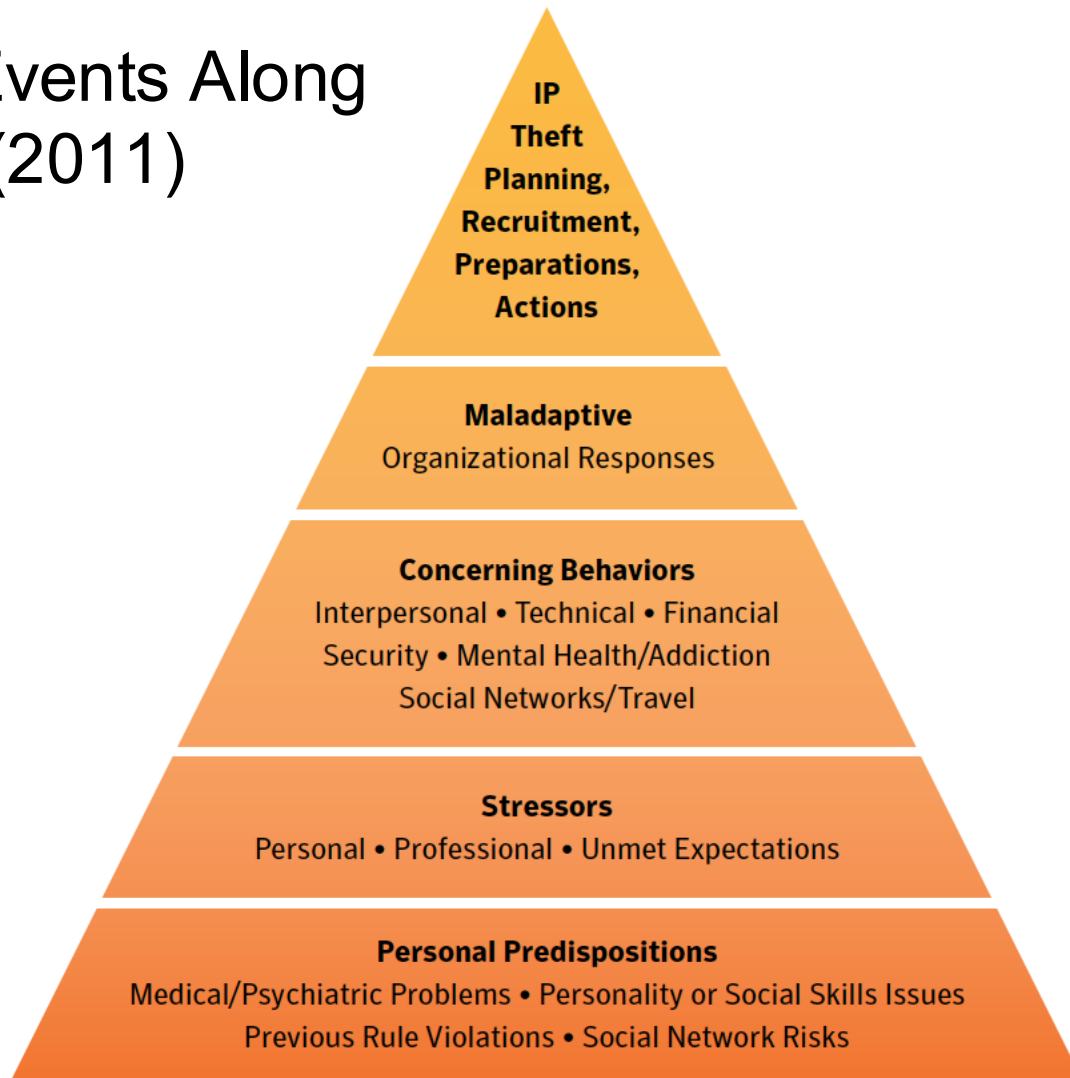
Dawn M. Cappelli, Andrew P. Moore, Daniel C. Phelps, Eric Shaw, and Randall F. Trzeciak, "Preliminary Analysis Results and Decision Rules for the CERT Insider Threat Project: Modeling Human Behavior in Cyberspace" *SEI Special Report* (2007).

Insider Threat Conceptual Framework: Groupings and Definitions (2010)



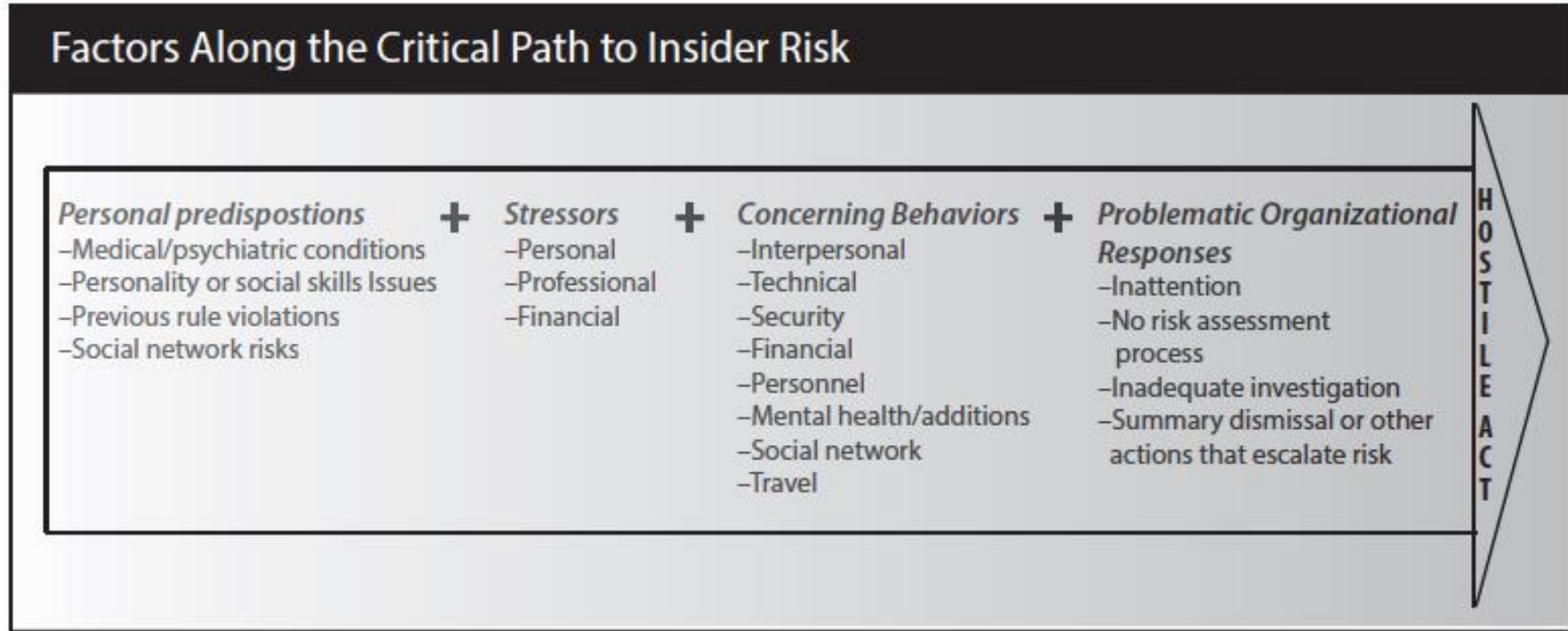
Eric Shaw, Adam Cummings, Michael Hanley, Andrew Moore, Derrick Spooner, Jaime Tupino, Randall Trzeciak. "Insider Threat Conceptual Framework: Groupings and Definitions " *SEI Special Report* (2010).

“The Progression of Events Along the Critical Pathway” (2011)



Shaw, Eric D., and Harley V. Stock. "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall." *White Paper*, Symantec, Mountain View, CA (2011).

Critical Path to Insider Risk



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

Critical Pathway to Employee Risk

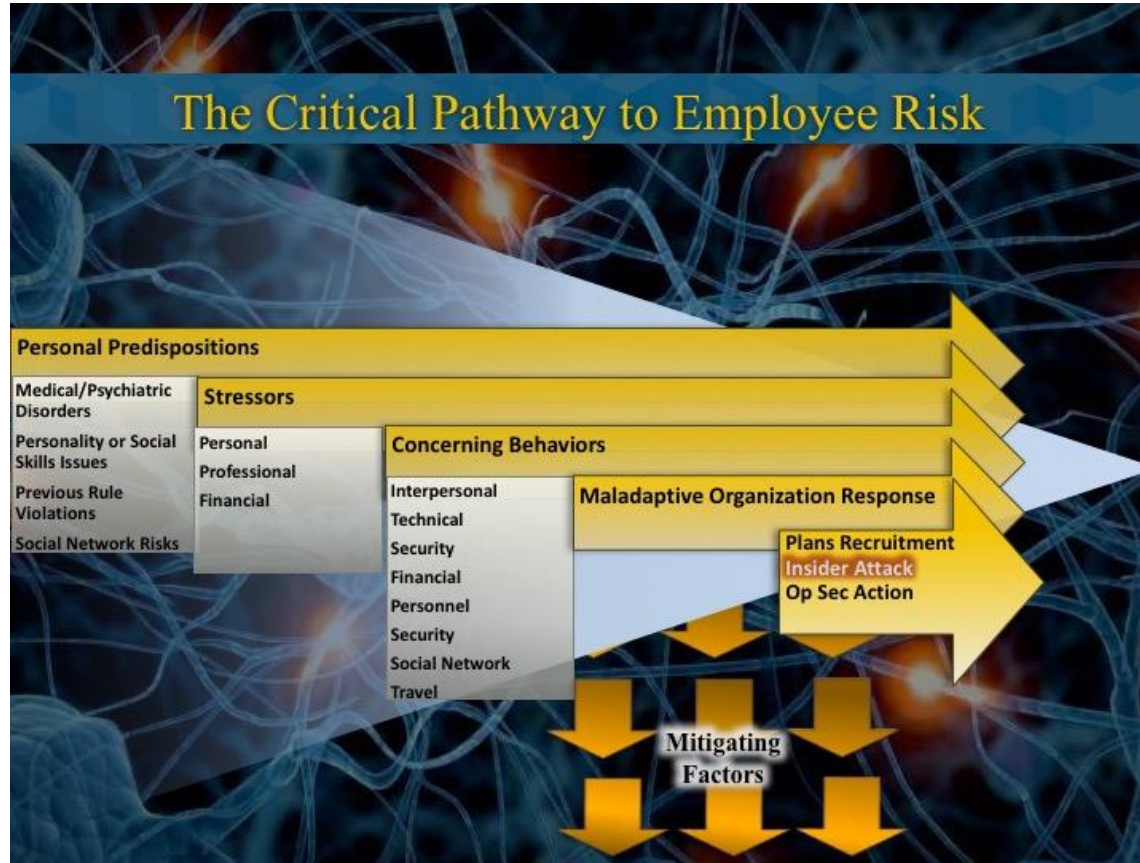


Image courtesy of "The Insider Risk Group," <https://www.insiderriskgroup.com/>

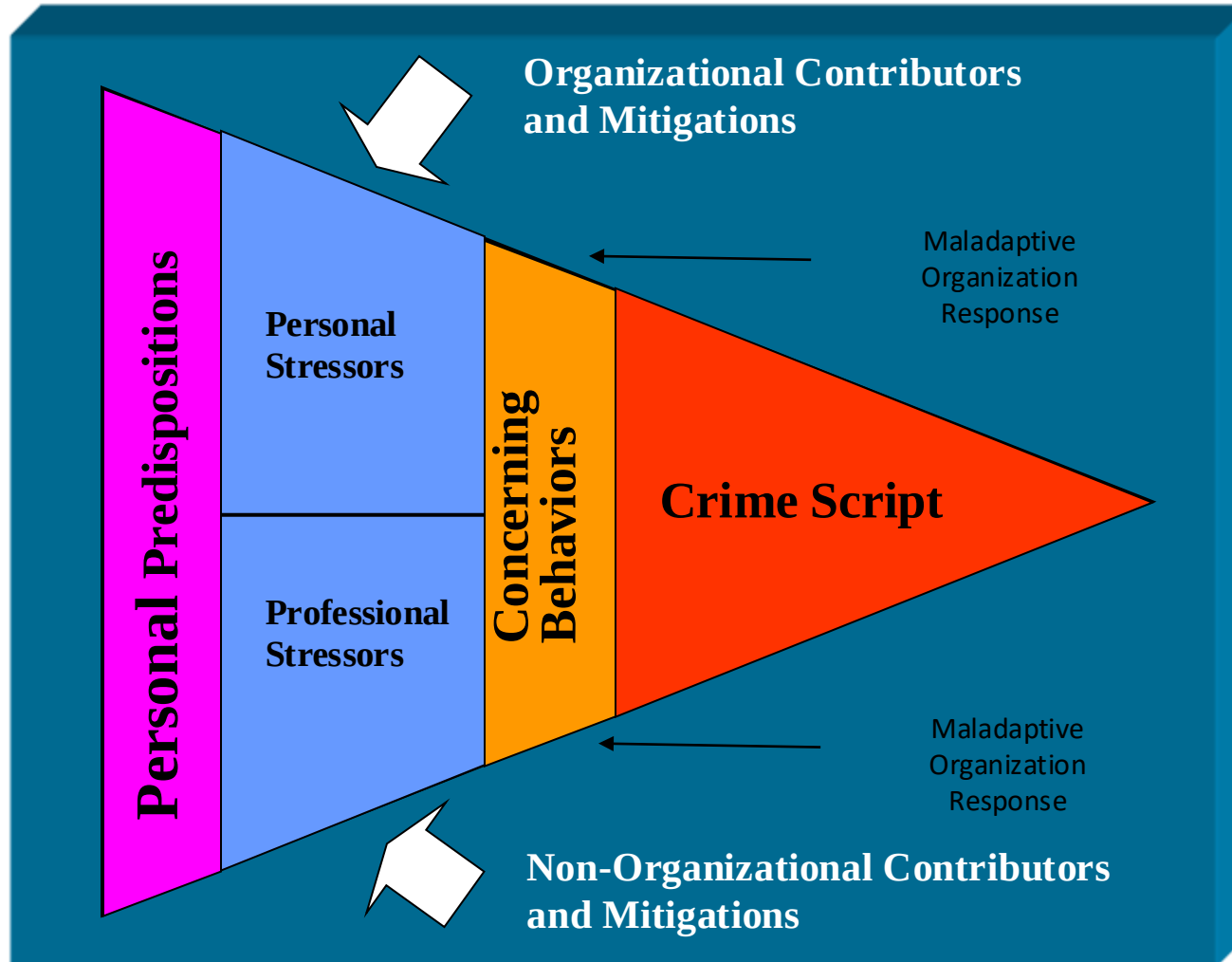
The Critical Pathway to Insider Risk

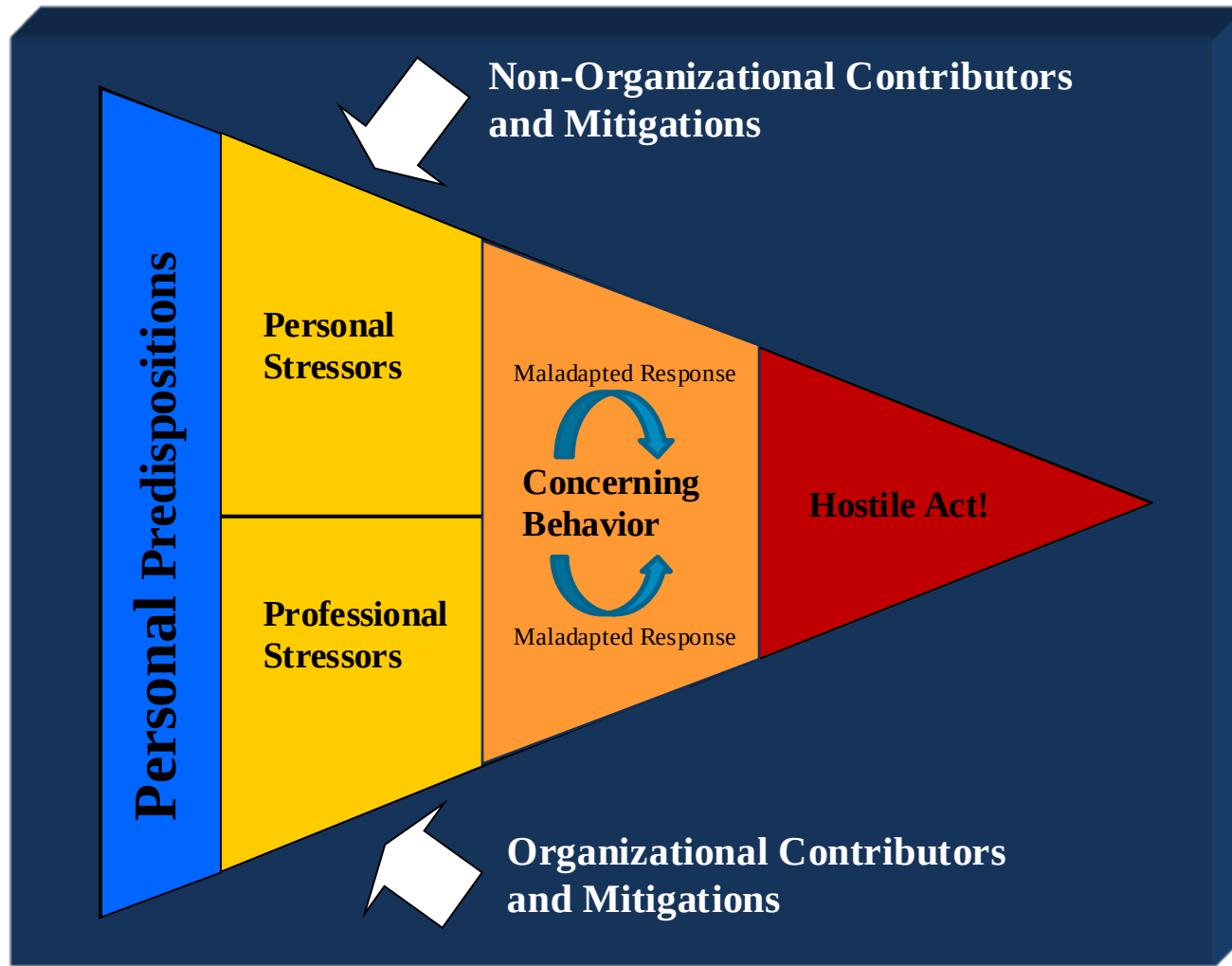
Supporting Research

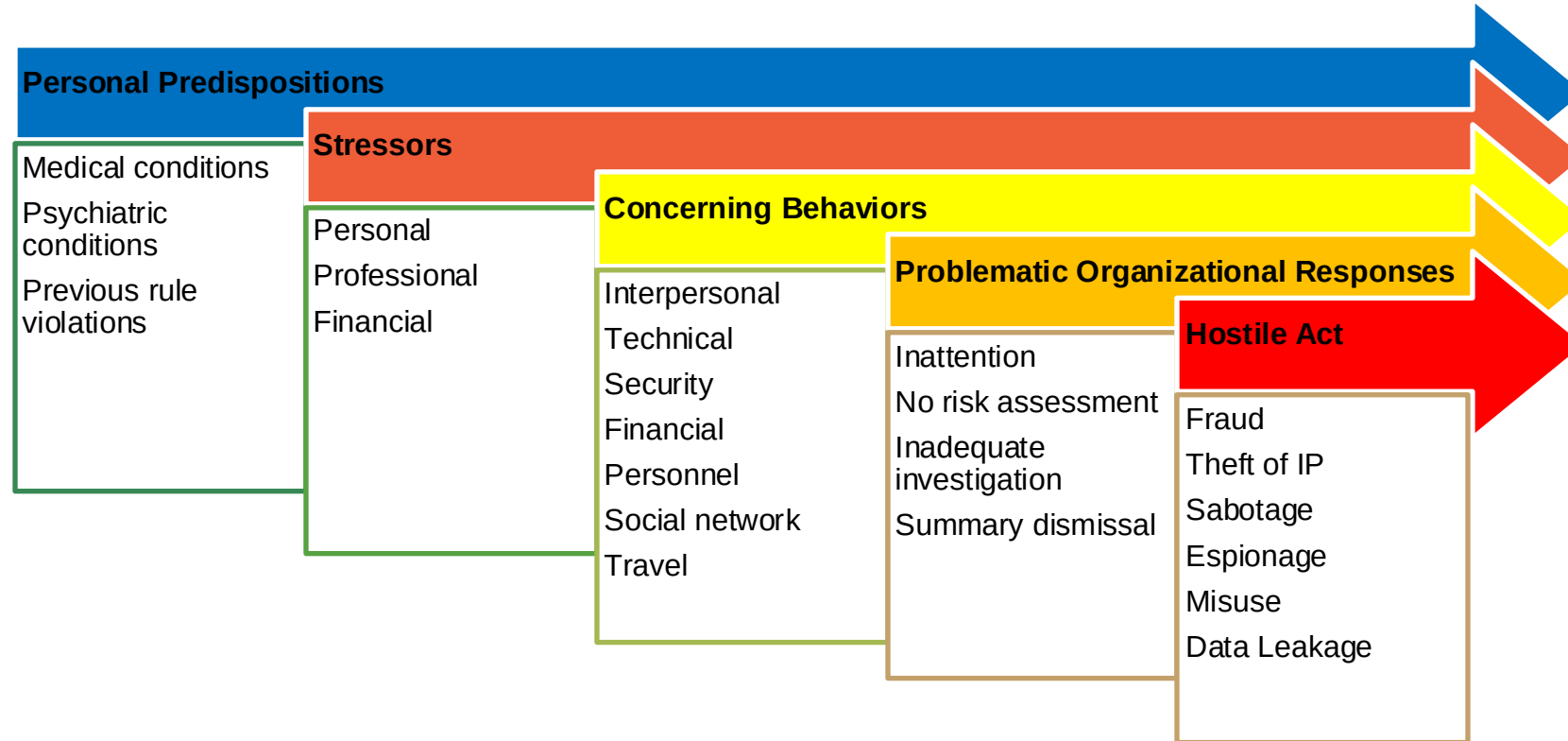
Related Research: Past and Present

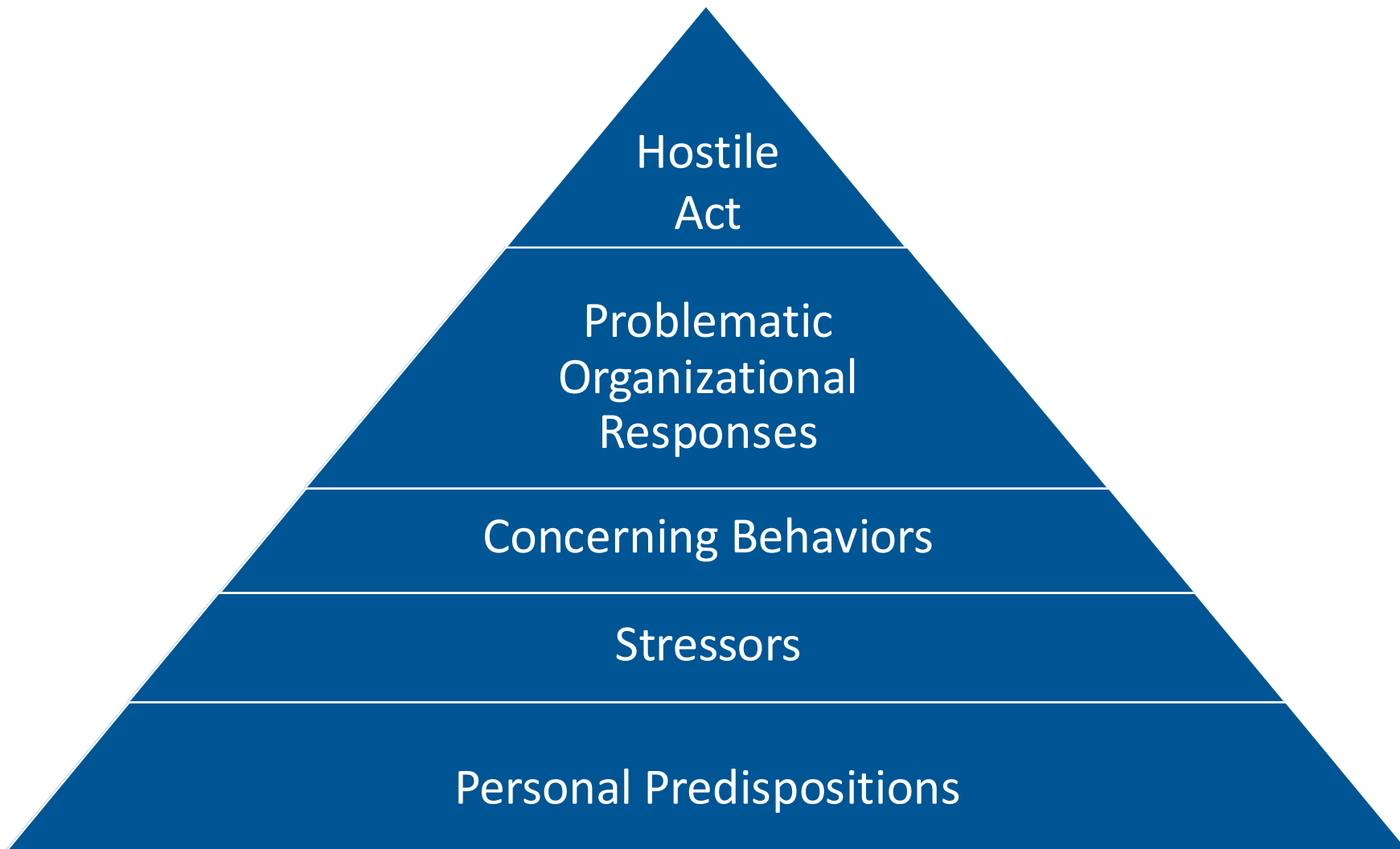
- Shaw, Eric D., Keven G. Ruby, and Jerrold M. Post. "The insider threat to information systems." *Security Awareness Bulletin* 2, no. 98 (1998): 1-10.
- Shaw, Eric D., and Lynn F. Fischer. "Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations." *Defense Personnel Security Research Center, Monterey, CA* (2005).
- Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis." *CMU-CERT Program, Tech. Rep* (2006).
- Shaw, Eric D. "The role of behavioral research and profiling in malicious cyber insider investigations." *Digital investigation* 3, no. 1 (2006): 20-31.
- Dawn M. Cappelli, Andrew P. Moore, Daniel C. Phelps, Eric Shaw, and Randall F. Trzeciak, "Preliminary Analysis Results and Decision Rules for the CERT Insider Threat Project: Modeling Human Behavior in Cyberspace" SEI Special Report (2007).
- Shaw, Eric D., Lynn F. Fischer, and Andrée E. Rose. "Insider risk evaluation and audit." *Defense Personnel Security Research Center, Monterey, CA* (2009).
- Eric Shaw, Adam Cummings, Michael Hanley, Andrew Moore, Derrick Spooner, Jaime Tupino, Randall Trzeciak. "Insider Threat Conceptual Framework: Groupings and Definitions " SEI Special Report (2010).
- Shaw, Eric D., and Harley V. Stock. "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall." *White Paper, Symantec, Mountain View, CA* (2011).
- Claycomb, William R., Carly L. Huth, Lori Flynn, David M. McIntire, Todd B. Lewellen, and CERT Insider Threat Center. "Chronological examination of insider threat sabotage: Preliminary observations." *Journal of Wireless and Mobile Networks & Ubiquitous Computing and Dependable Applications* 3, no. 4 (2012): 4-20.
- Claycomb, William R., and Carly L. Huth. "CERT® Series on Chronological Analysis of Spy Behavior Prior to Attack: Overview." *SEI Special Report*. (2013).
- Shaw, Eric, and Laura Sellers. "Application of the critical-path method to evaluate insider risks." *Studies in Intelligence Vol* 59, no. 2 (2015).
- Noonan, Christine F. 2018. "Spy the Lie: Detecting Malicious Insiders". Pacific Northwest National Laboratories. PNNL-SA-122655, March 2018. <https://doi.org/10.2172/1452870>.
- Lenzenweger, Mark F., and Eric D. Shaw. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." *Counter-Insider Threat Research and Practice* 1, no. 1 (2022).

CPIR Visual Representations Through the Years

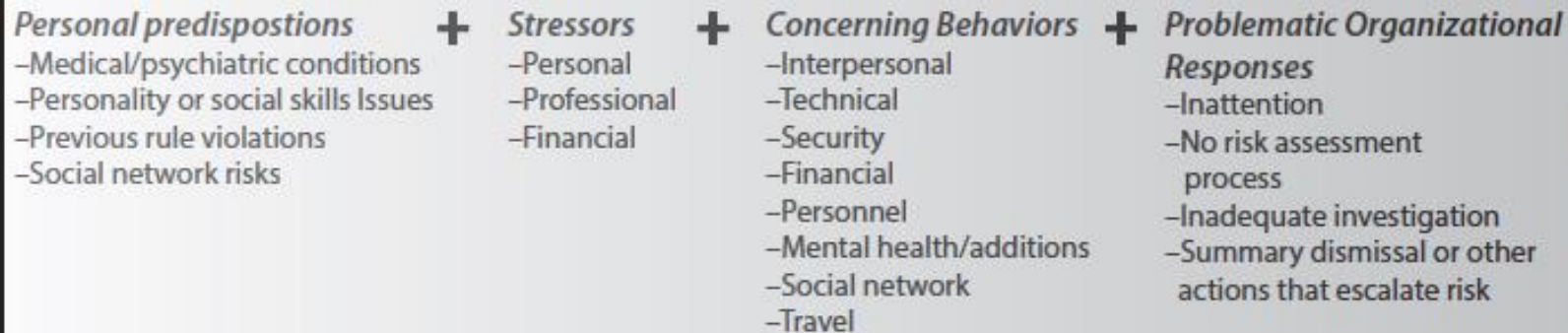




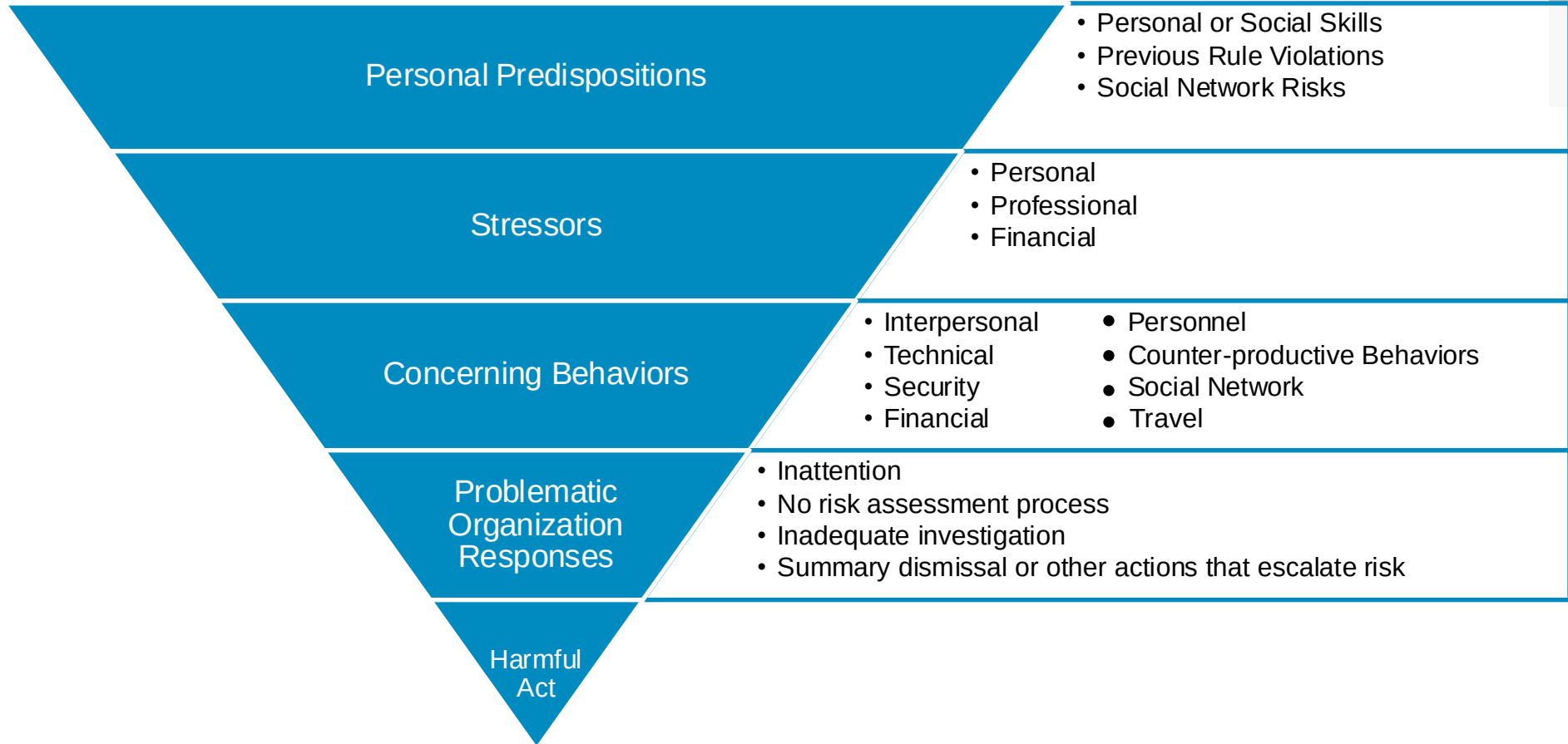




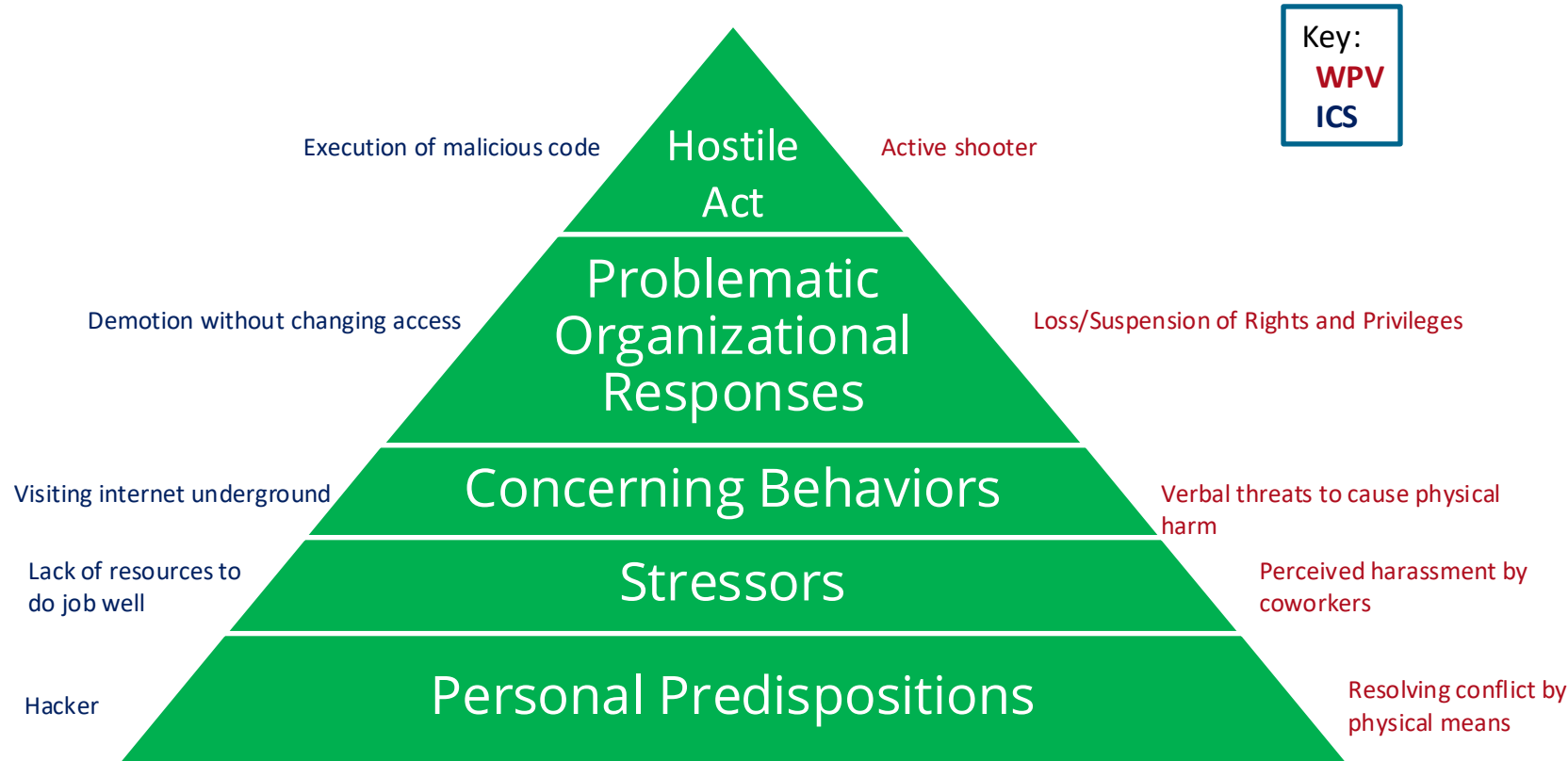
Factors Along the Critical Path to Insider Risk



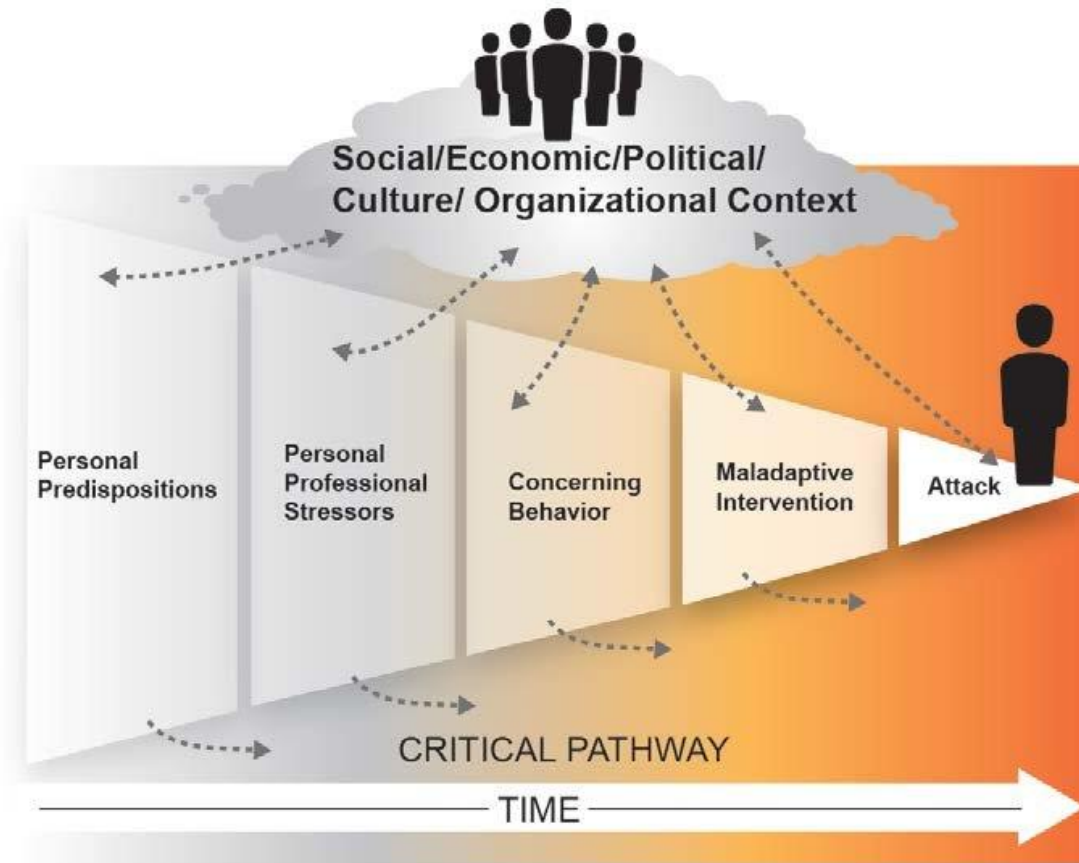
Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)



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)



SEI Research Review, 2016



Noonan, Christine F. 2018. "Spy the Lie: Detecting Malicious Insiders". Pacific Northwest National Laboratories. PNNL-SA-122655, March 2018. <https://doi.org/10.2172/1452870>.

The Critical Pathway to Employee Risk



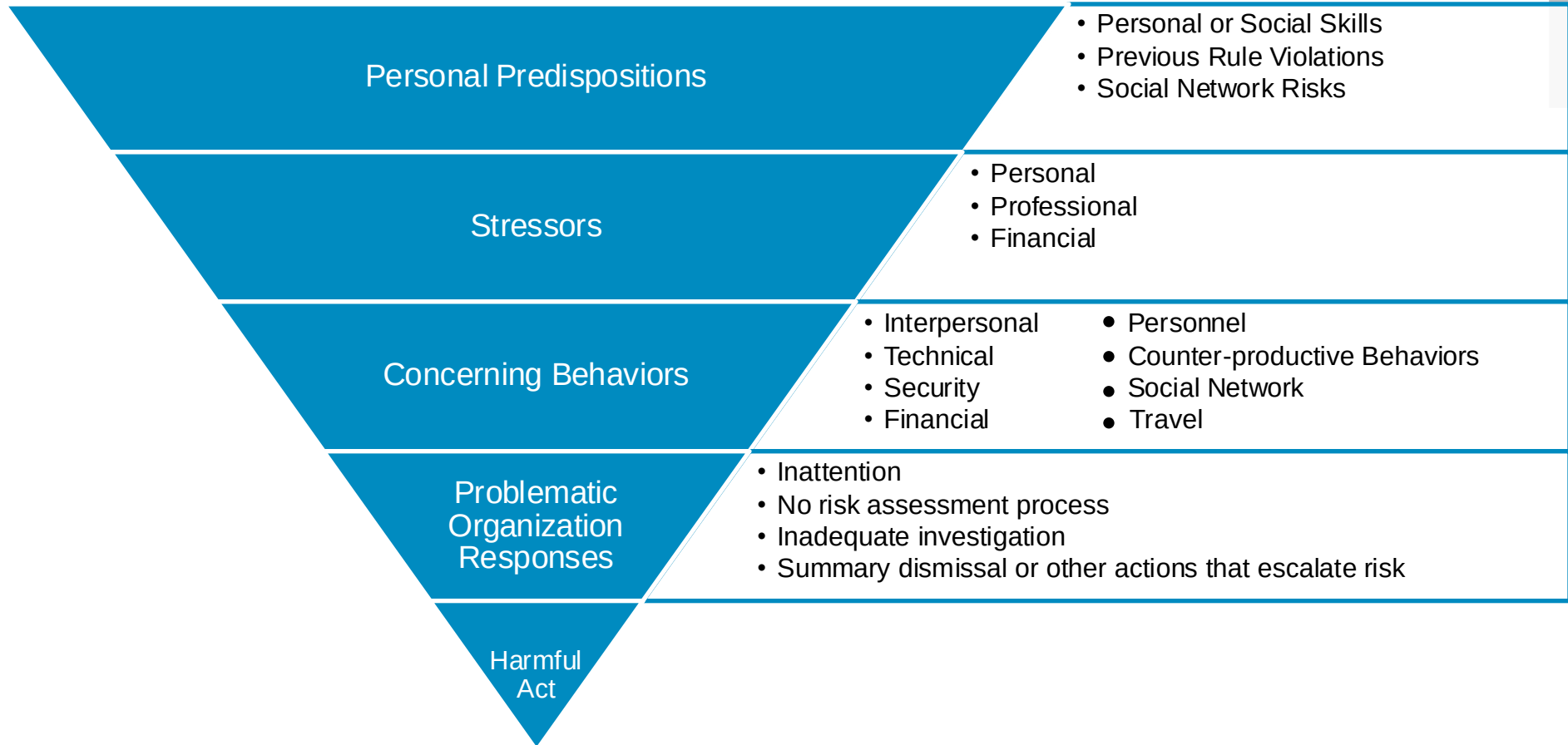
Image courtesy of "The Insider Risk Group," <https://www.insiderriskgroup.com/>

The Critical Pathway to Insider Risk

Use in Practice

In Practice





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

Questions

Contact: claycomb@cert.org

