Defense and Response Against Insider Threats & User Errors

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

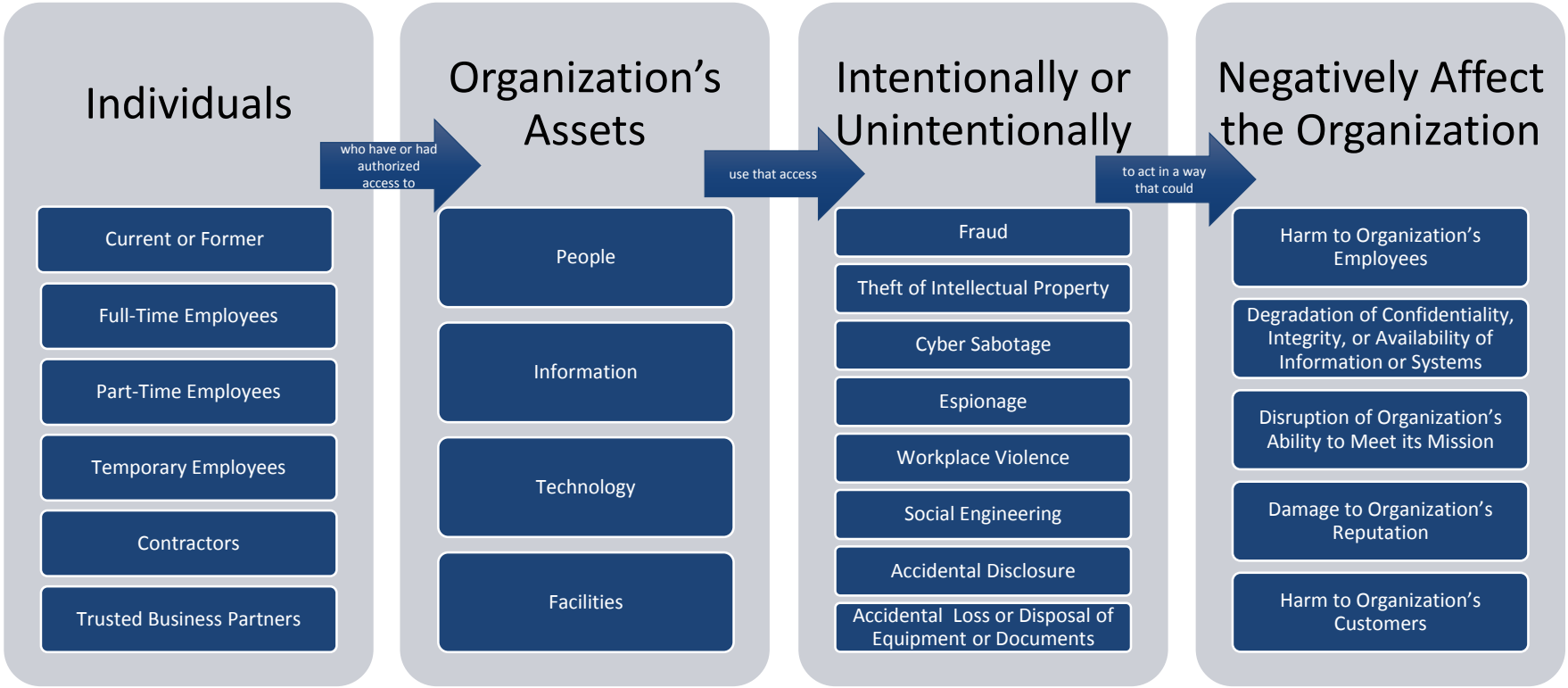
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-1154

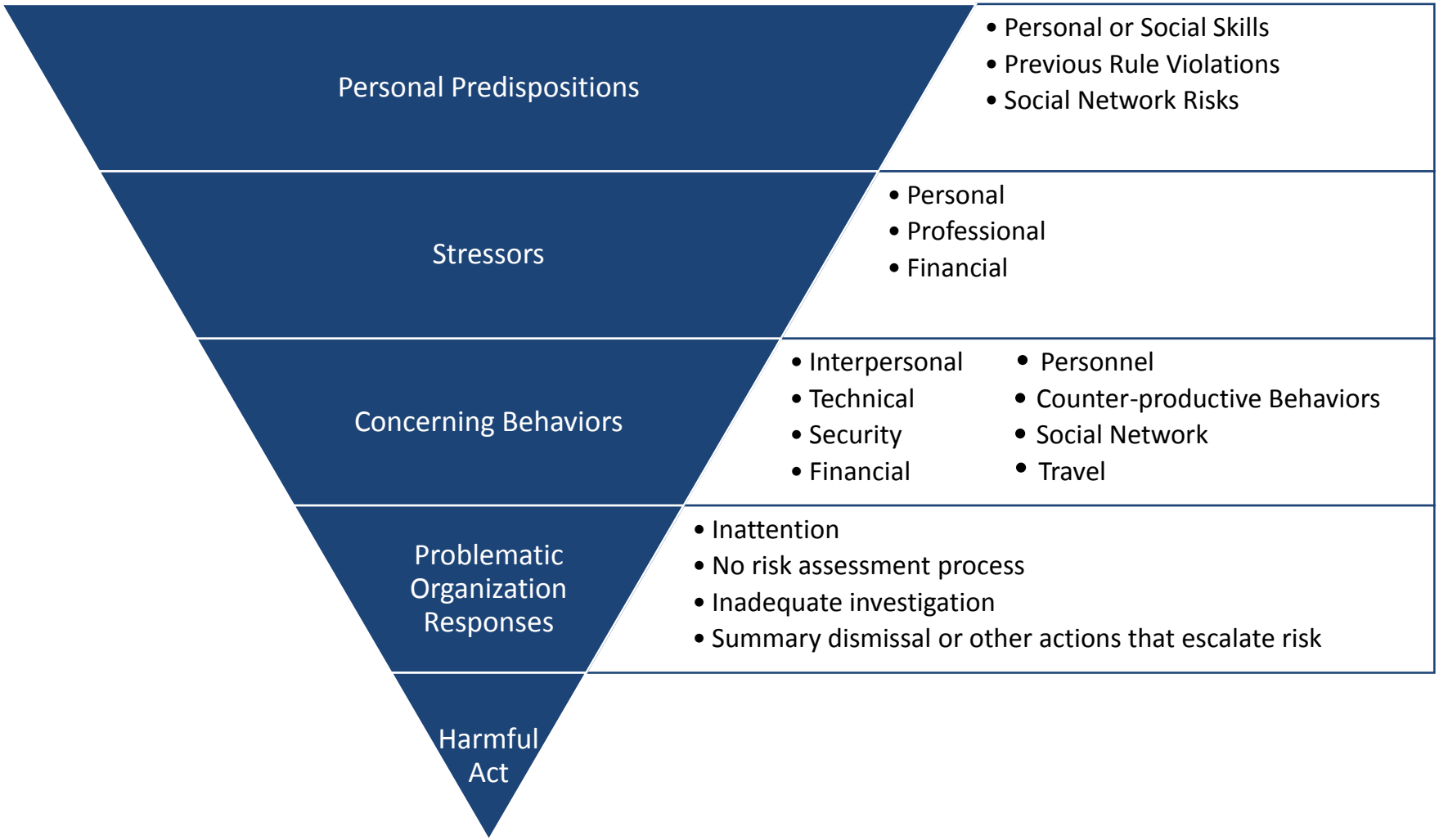
The Insider Threat Defined

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Scope of the Insider Threat

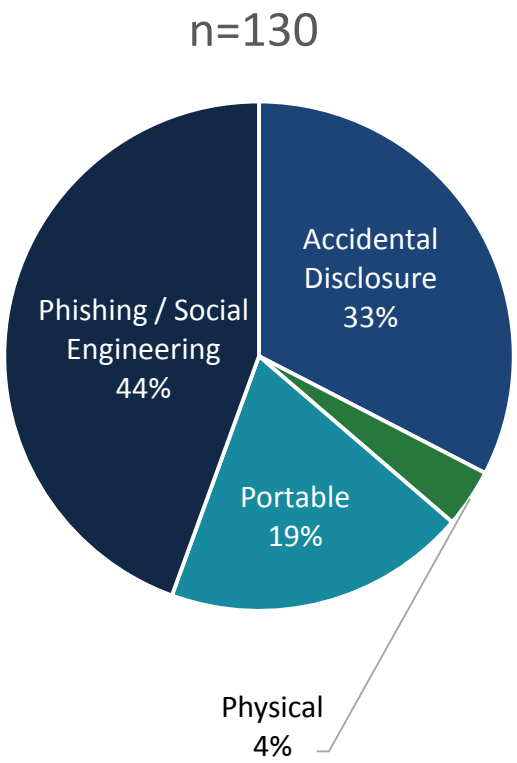


The Critical Path to Insider Risk



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)

Unintentional Insider Threats



Accidental Disclosure (e.g., via the internet)

- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

Malicious Code (e.g., hacking, malware/spyware)

- an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

Improper/accidental disposal of physical records

- lost, discarded, or stolen non-electronic records, such as paper documents

Portable equipment no longer in possession

- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

Source: Unintentional Insider Threats: A Foundational Study, Available Online at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58744

Contributing Factors to Human Error

Fatigue

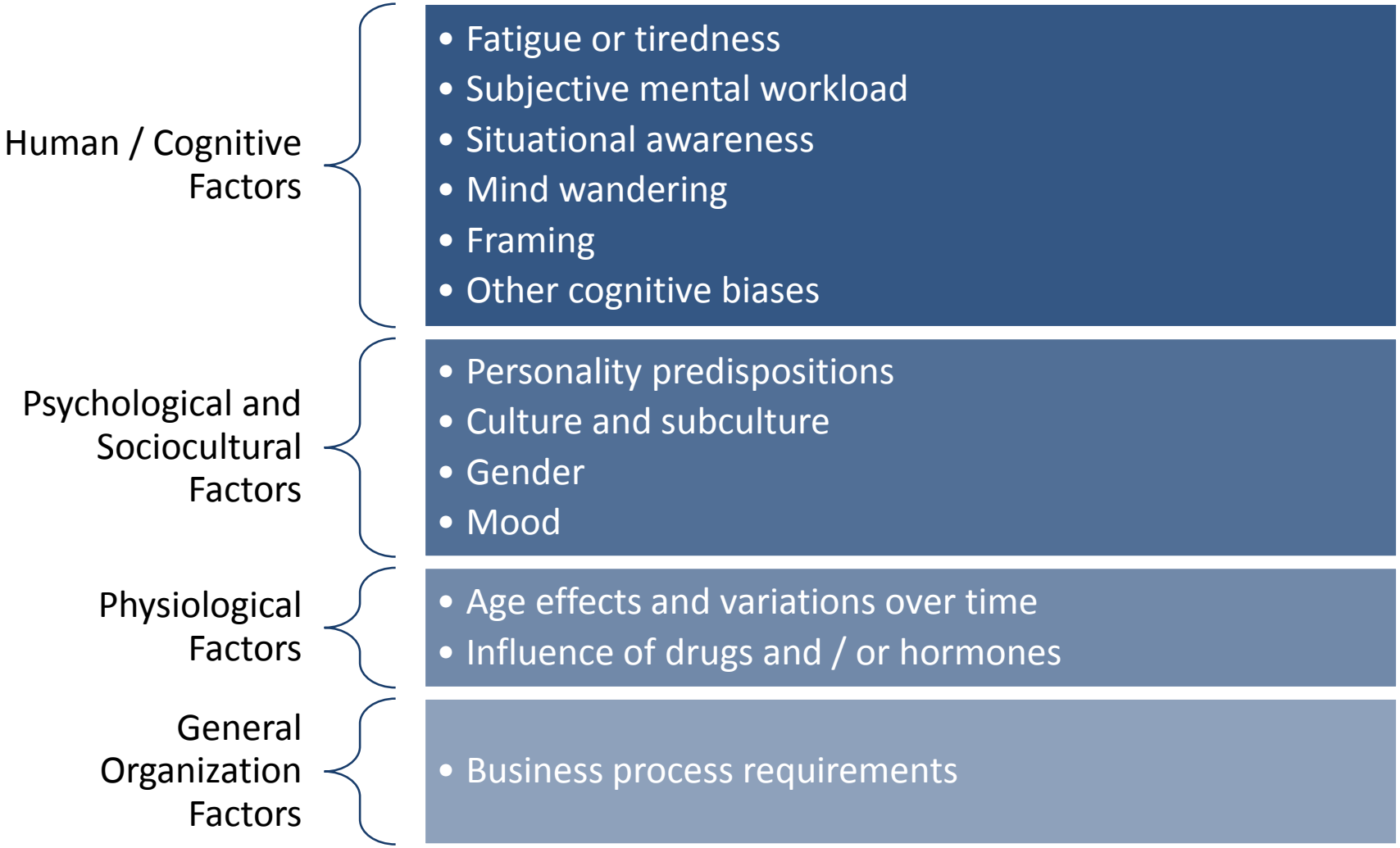
High Subjective Mental Workload

Lack of / Loss of Situational Awareness

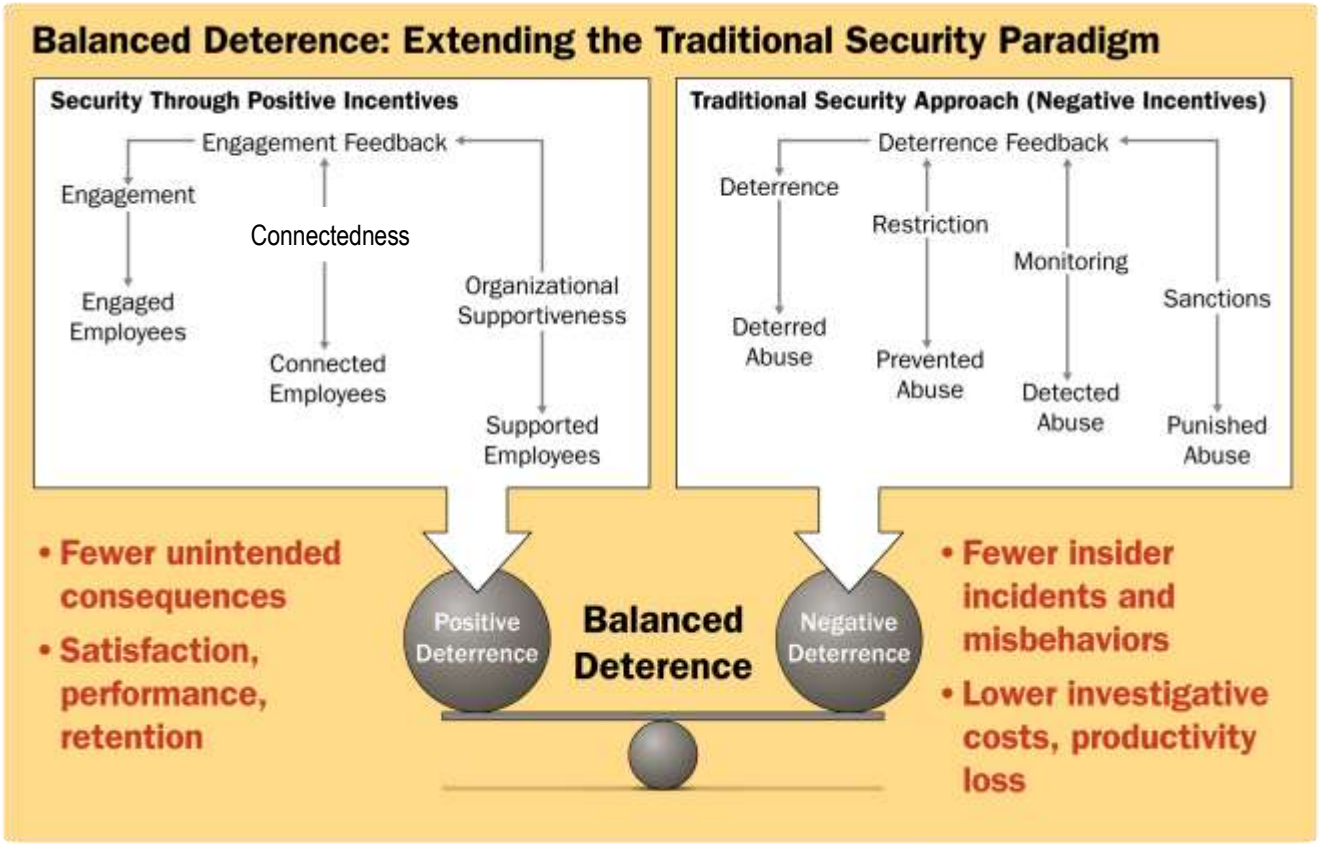
Mind Wandering

Risk Perception and Risky Decision Making

Contributing Factors in Risk Perception



Extending the Traditional Security Paradigm



Source: The Critical Role of Positive Incentives for Reducing Insider Threats, Available Online at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484917

Presenter Contact Information

Dan Costa, CISSP, PSEM

Deputy Director, CERT National Insider Threat Center

dlcosta@cert.org

www.cert.org/insider-threat