



Defense and Response Against Insider Threats & User Errors

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2020 Carnegie Mellon University.

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.

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.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

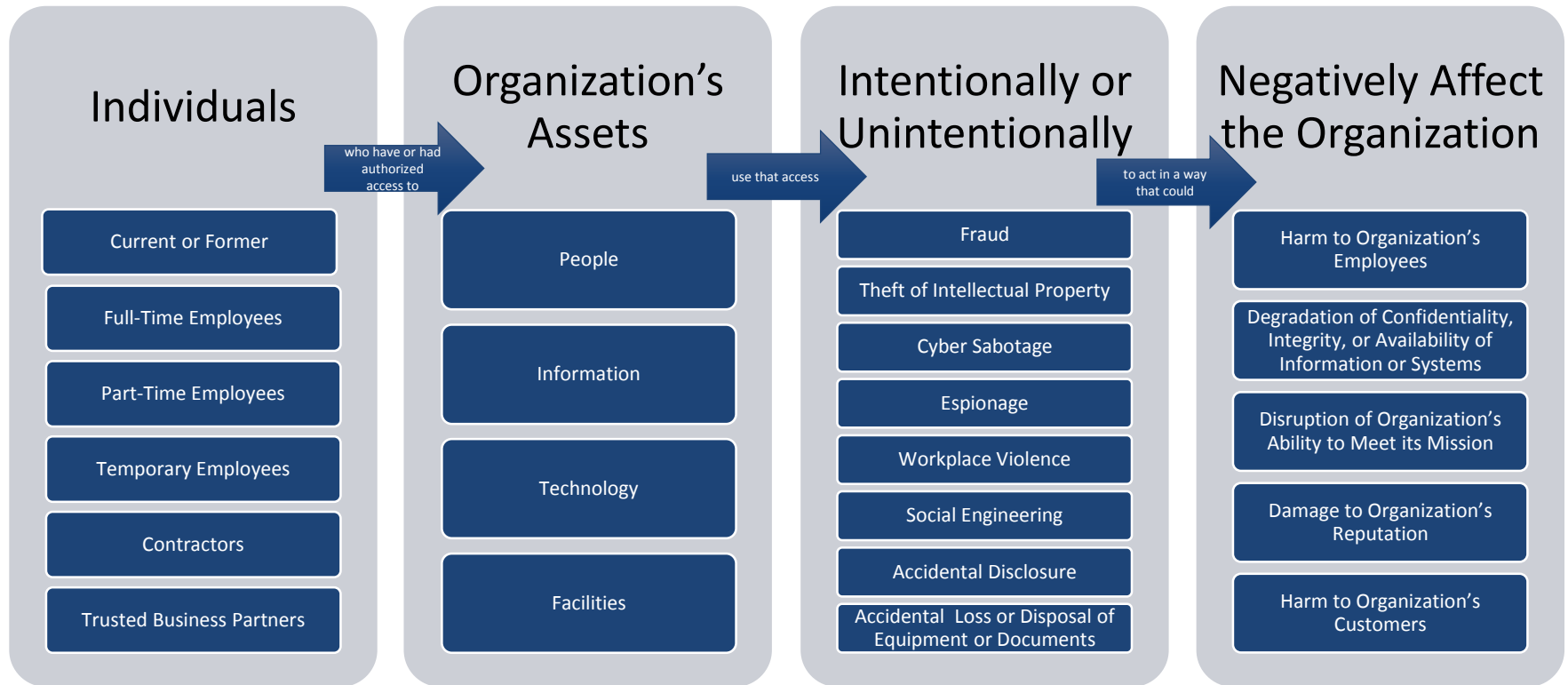
Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-1154

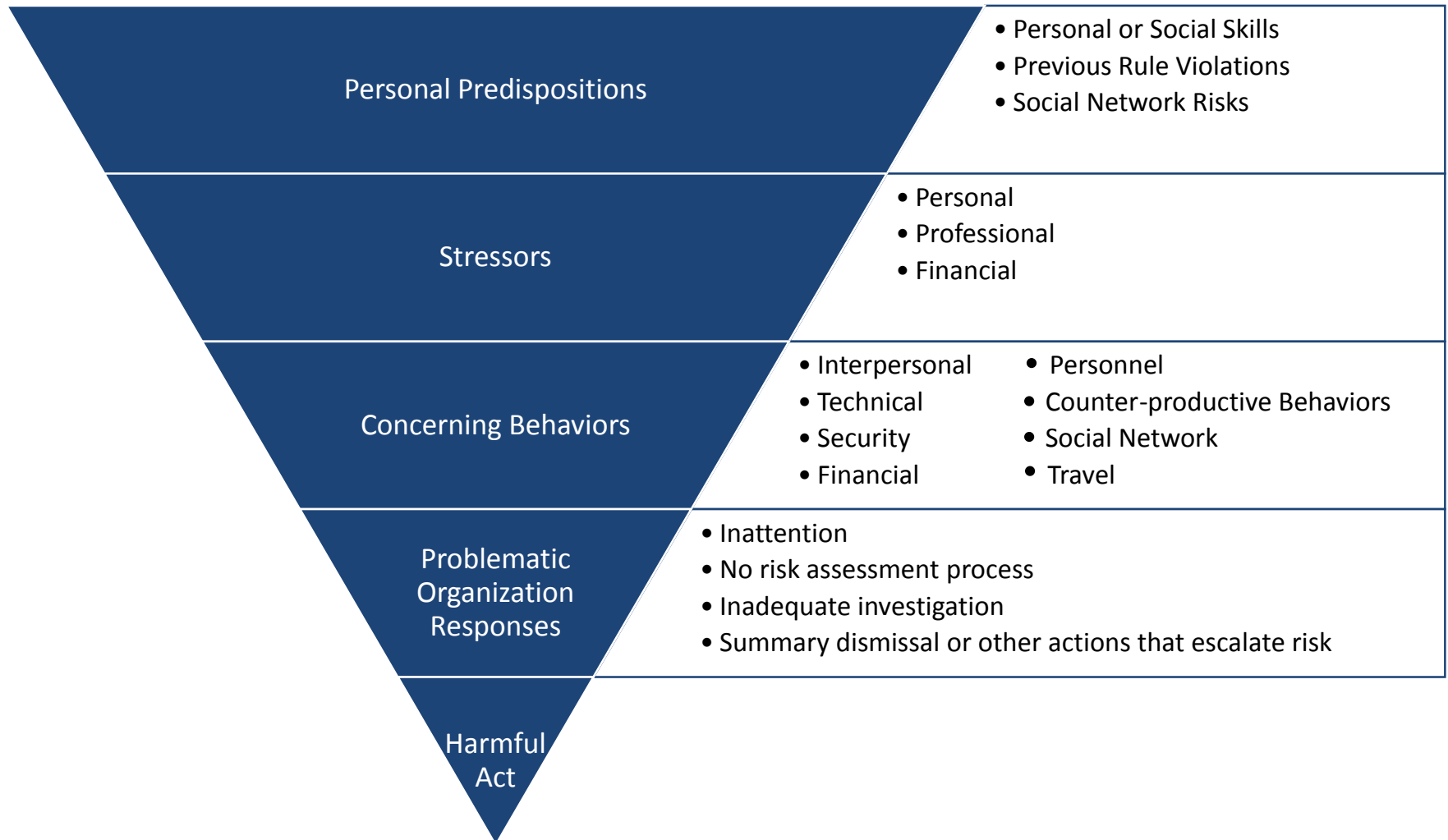
The Insider Threat Defined

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

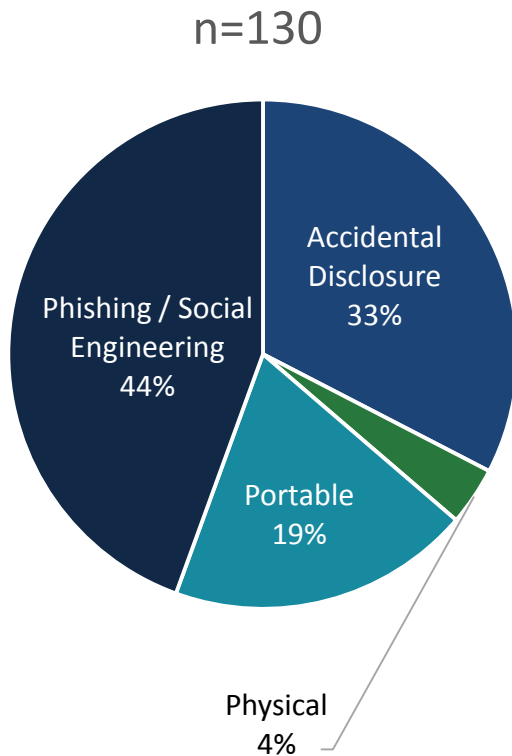


The Critical Path to Insider Risk



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

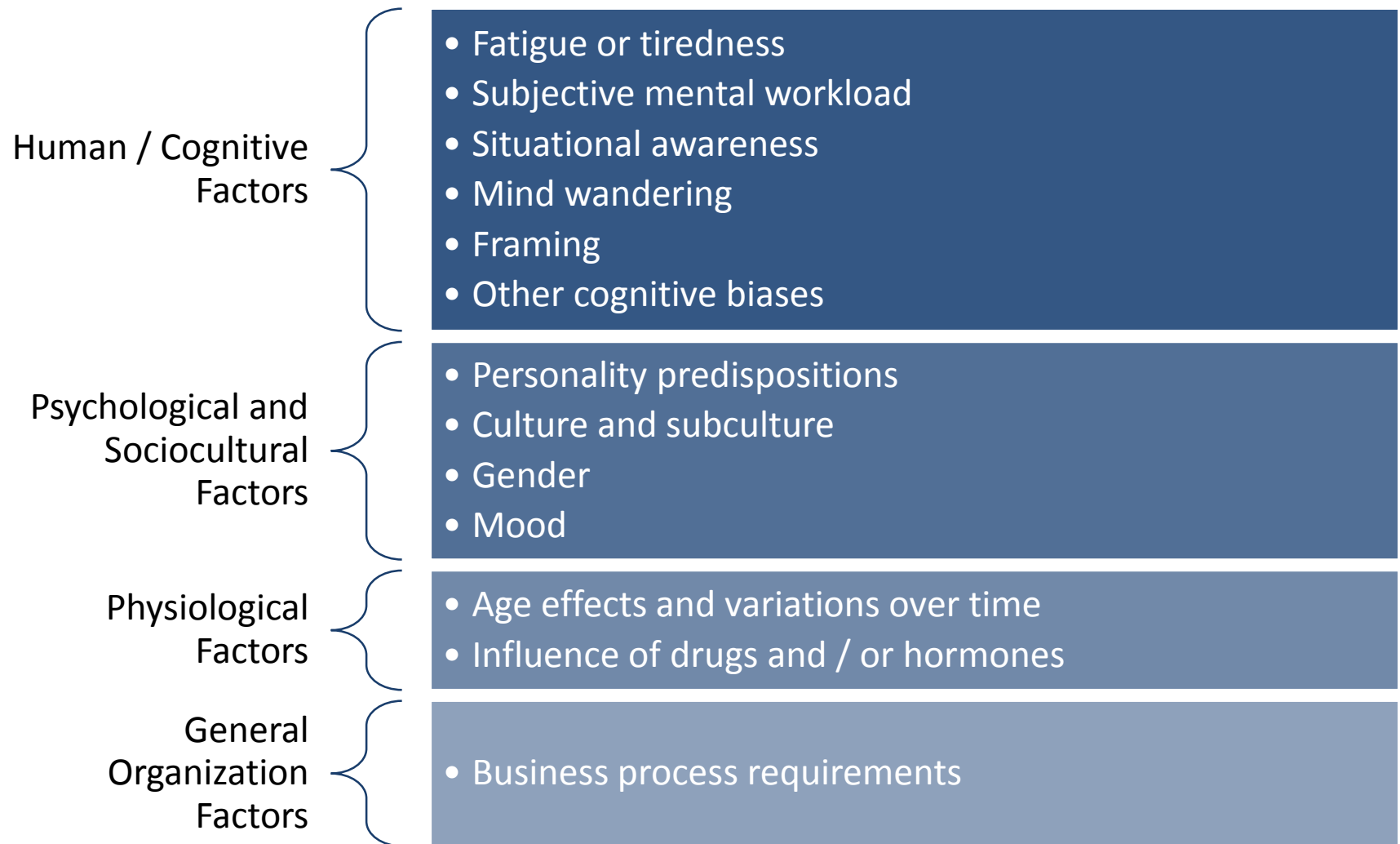
High Subjective
Mental
Workload

Lack of / Loss of
Situational
Awareness

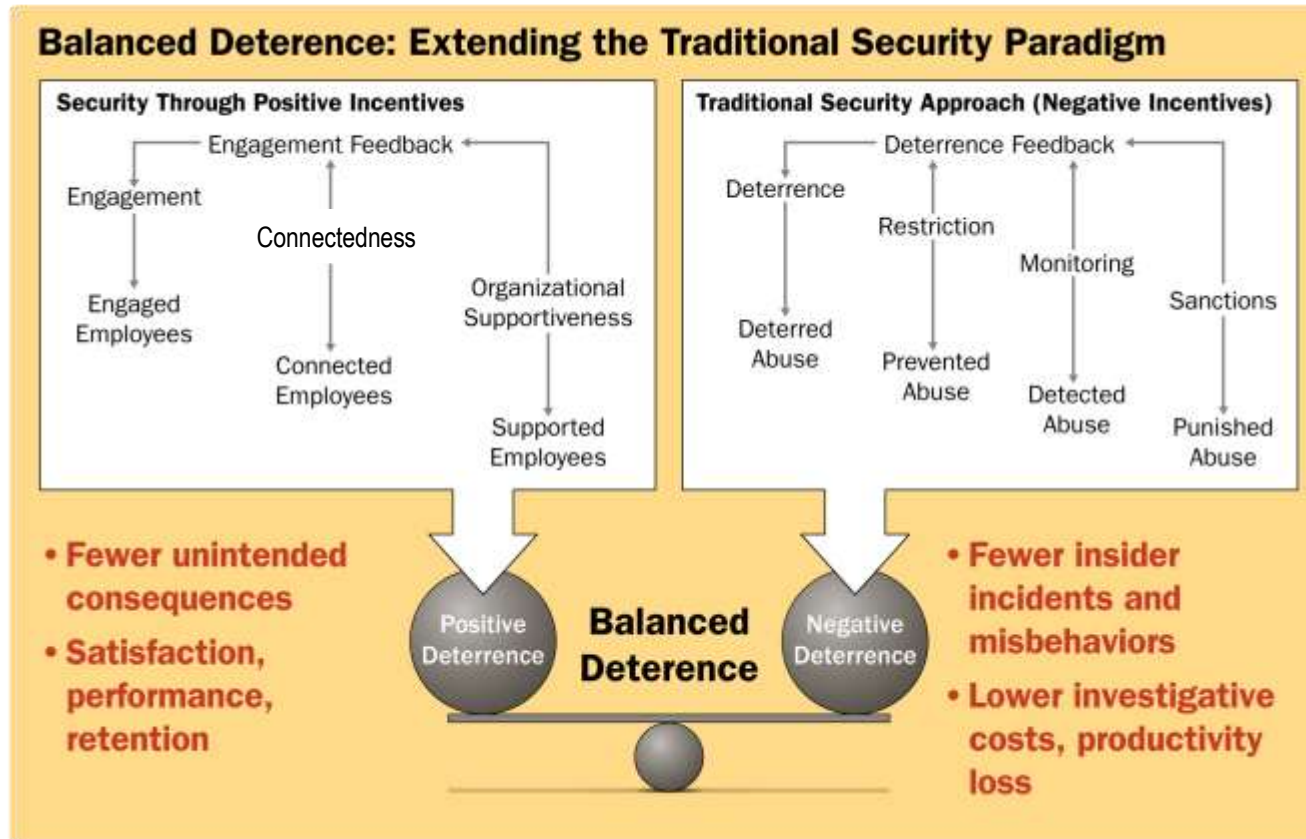
Mind Wandering

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