

# Insider Risk Control Validation

Dan Costa

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2021 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.

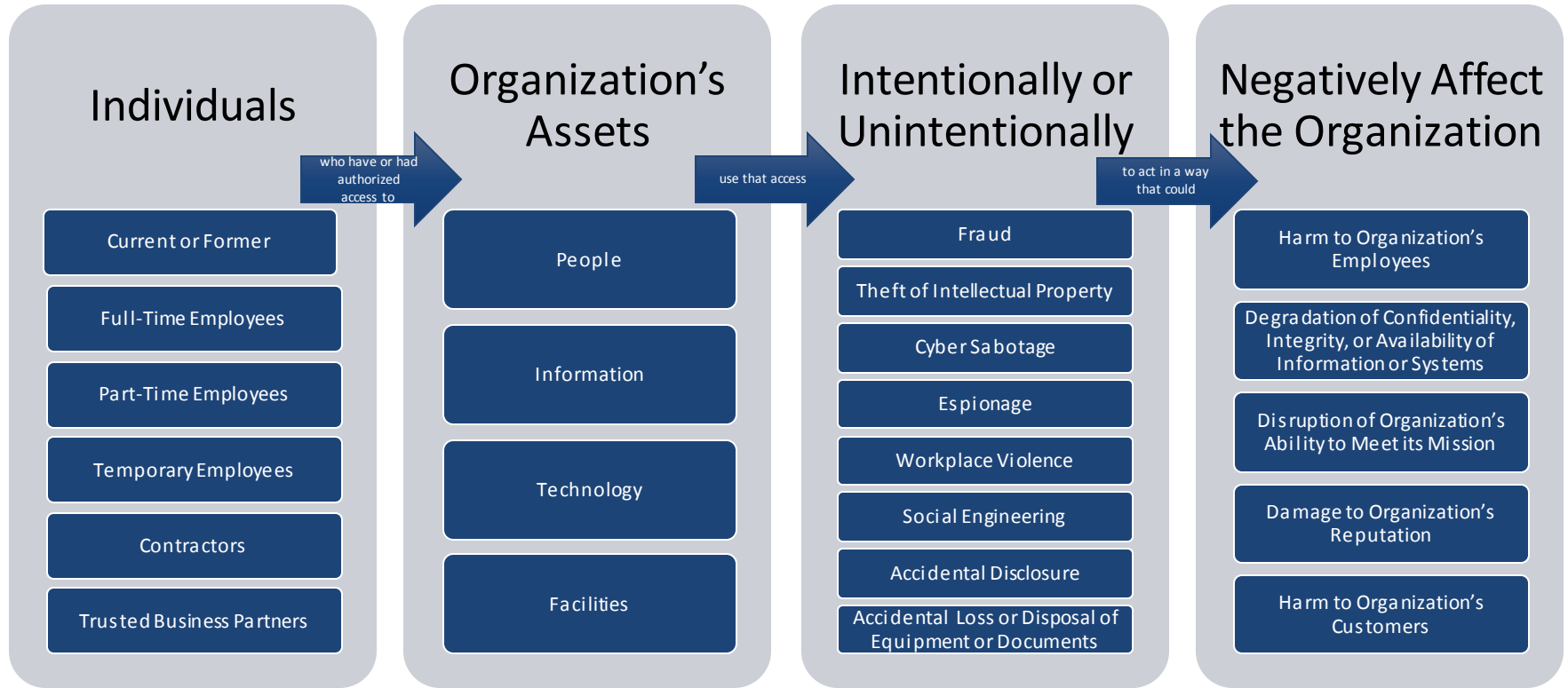
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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](mailto:permission@sei.cmu.edu).

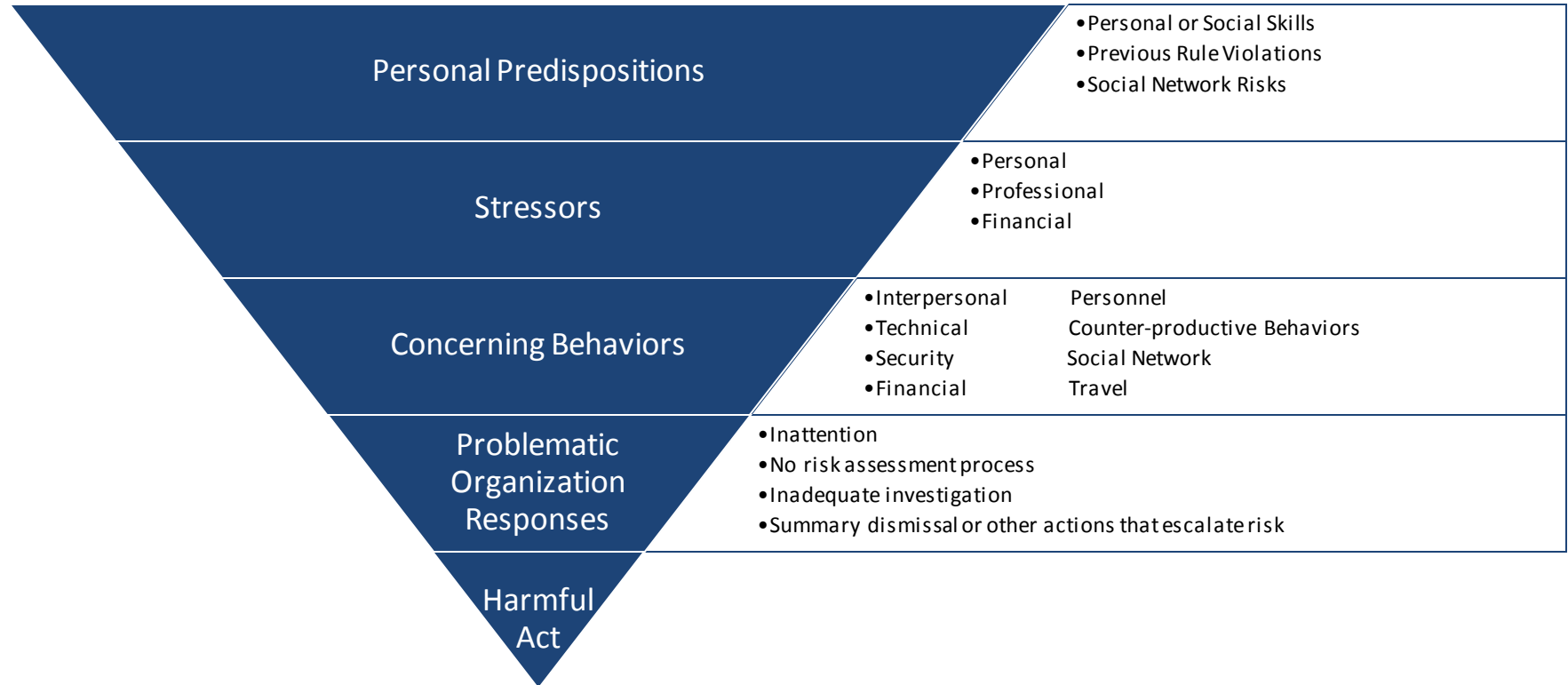
Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM21-0885

# Scope of the Insider Threat



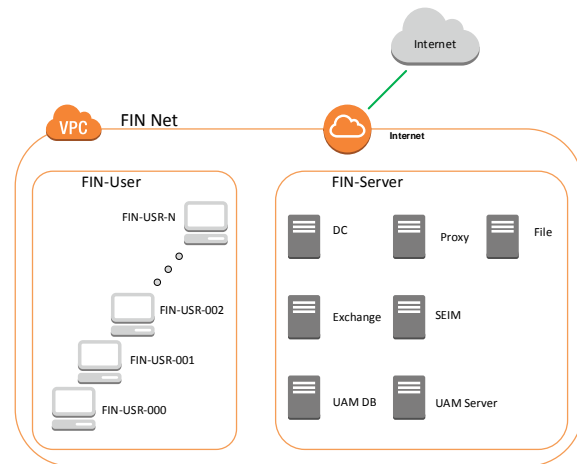
# Critical Path to Insider Threat



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)

# Technical Control Validation

- What's Needed:
  - Simulated infrastructure
    - Open-source tools such as [GreyBox](#) and [TopGen](#)
    - Infrastructure-as-code tools including [Terraform](#), [Ansible](#), and [Packer](#) facilitate reuse and automation
  - Simulated user activity
    - Open-source tools such as [GHOSTS](#)
  - Realism
    - Base rates of occurrence
    - Incident data

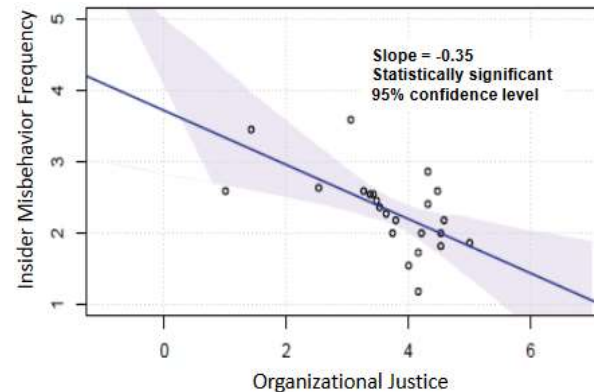
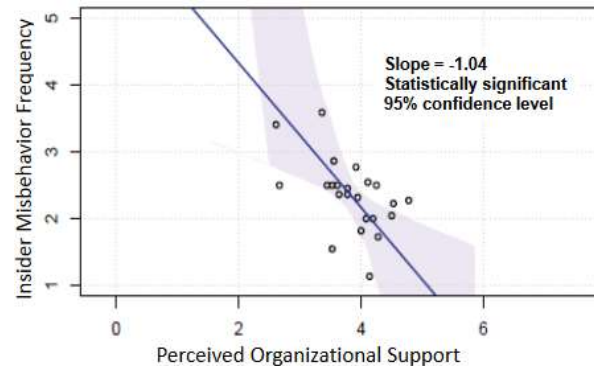
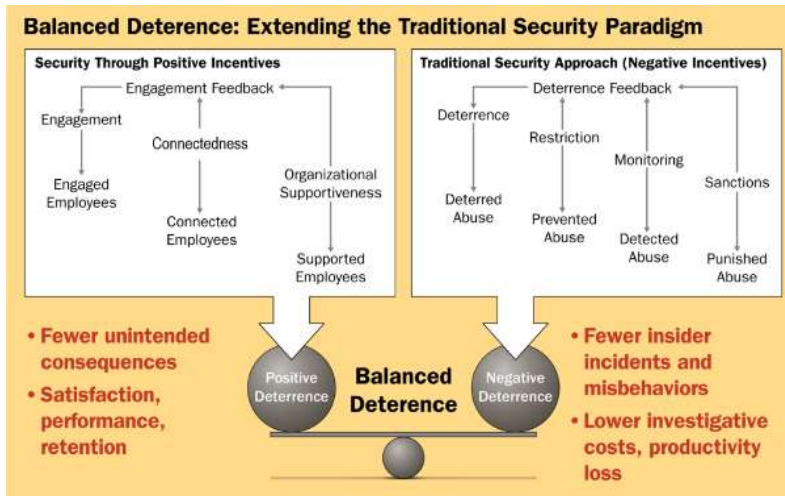


```
resource "aws_instance" "this" {  
  ami           = data.aws_ami.this.id  
  instance_type = var.dc.instance_type  
  iam_instance_profile = "FIN-USR-001"  
  private_ip    = "10.0.40.20"  
  subnet_id     = var.subnets  
  vpc_security_group_ids = var.security_groups  
  
  tags = {  
    Terraform = "true"  
    Name      = "FIN-DC"  
    Environment = "FIN-Test"  
  }  
}
```

# Non-Technical Control Validation

What's Needed:

- Modeling and simulation
- Proxy measures
- Pilots



# Presenter Contact Information / For More Information

Dan Costa

Technical Manager, Enterprise Threat and  
Vulnerability Management

CERT Division | Carnegie Mellon University  
Software Engineering Institute

[dlcosta@sei.cmu.edu](mailto:dlcosta@sei.cmu.edu)

<https://insights.sei.cmu.edu/blog/functional-requirements-for-insider-threat-tool-testing>

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484917>

<https://www.sei.cmu.edu/our-work/insider-threat/index.cfm>