Insider Risk Control Validation

Dan Costa

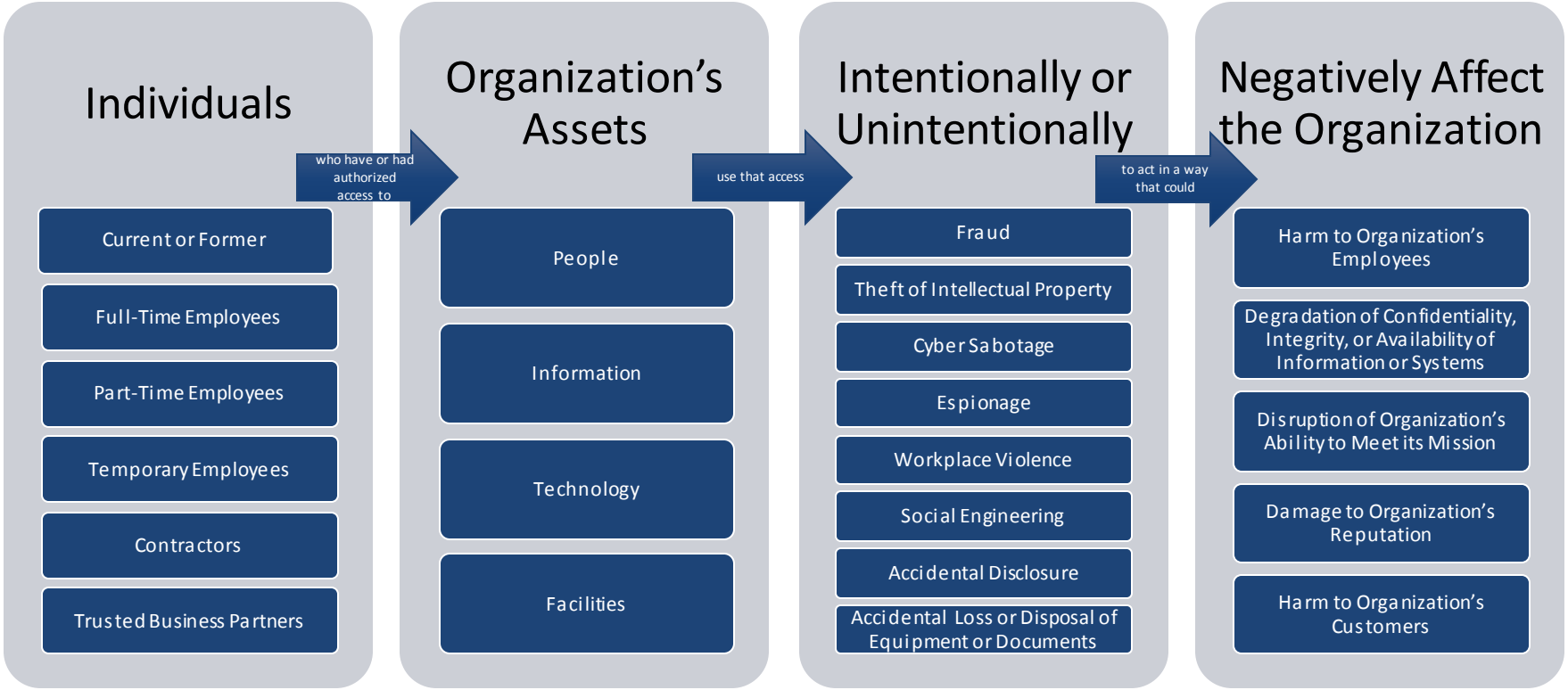
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

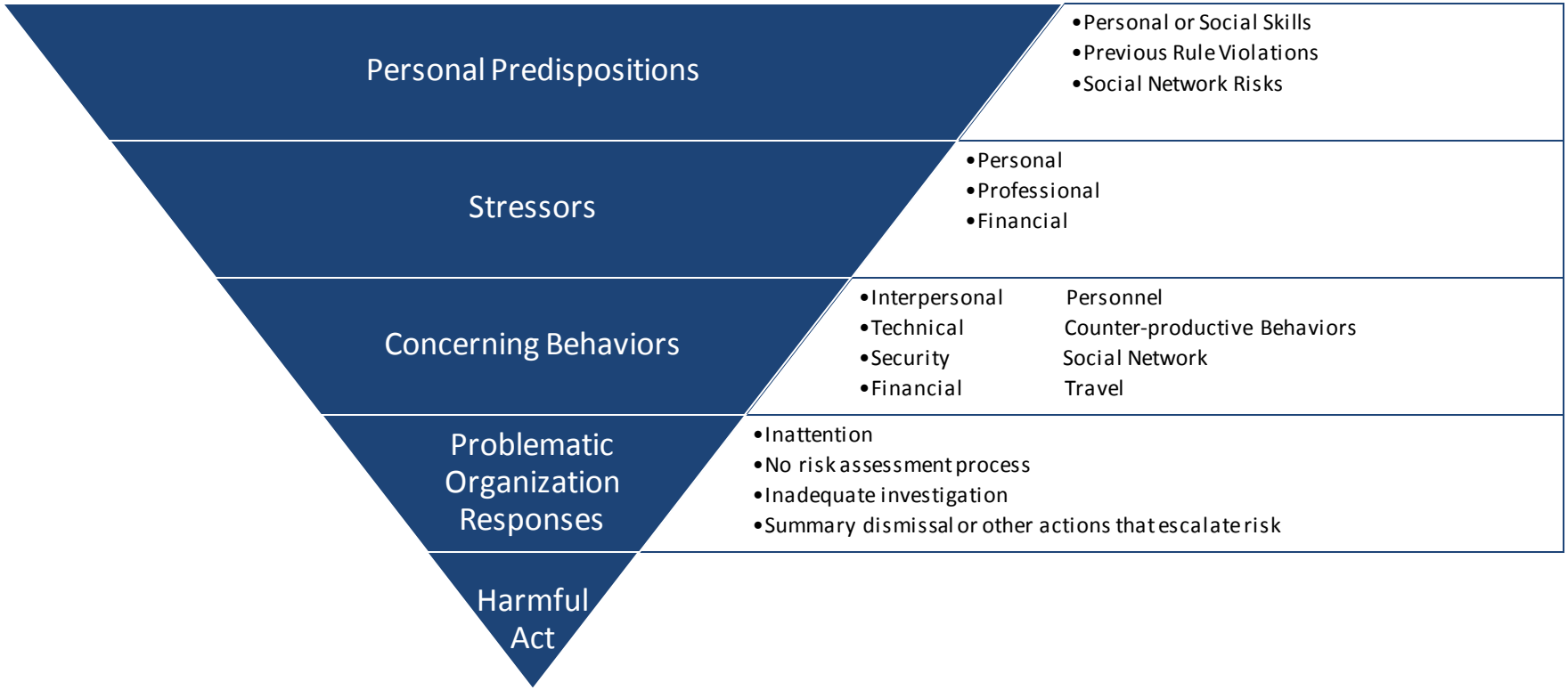
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0885

Scope of the Insider Threat



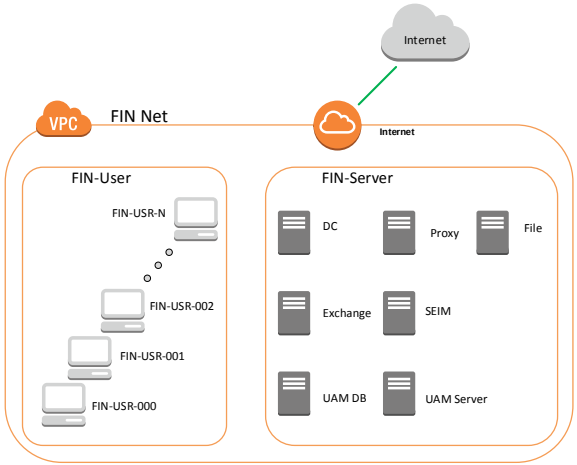
Critical Path to Insider Threat



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

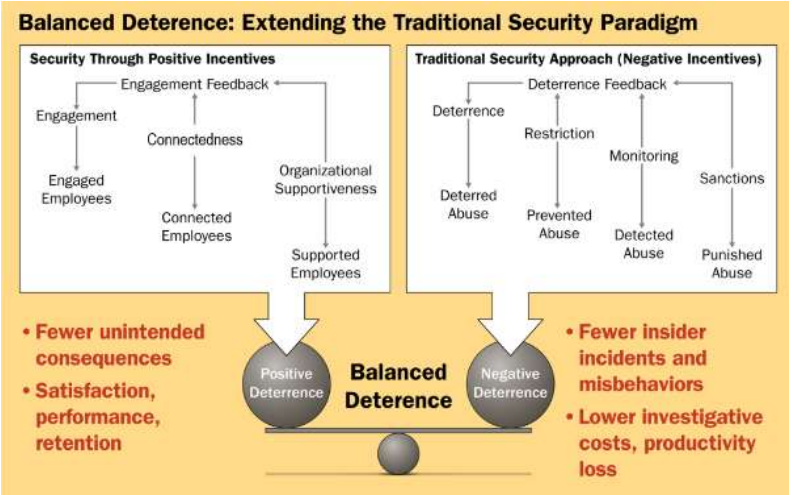


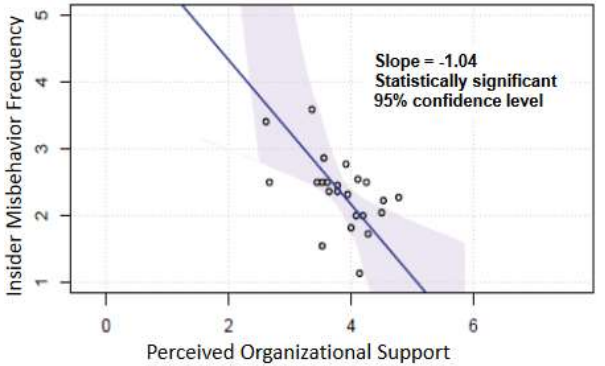

```
resource "aws_instance" "this" {
  ami                    = data.aws_ami.this.id
  instance_type          = var.dc_instance_type
  iam_instance_profile   = "FIN SSM Role"
  private_ip             = "10.0.40.20"
  subnet_id              = var.subnets
  vpc_security_group_ids = var.security_groups

  tags = {
    Terraform   = "true"
    Name        = "FIN DC"
    Environment = "FIN Test"
  }
}
```

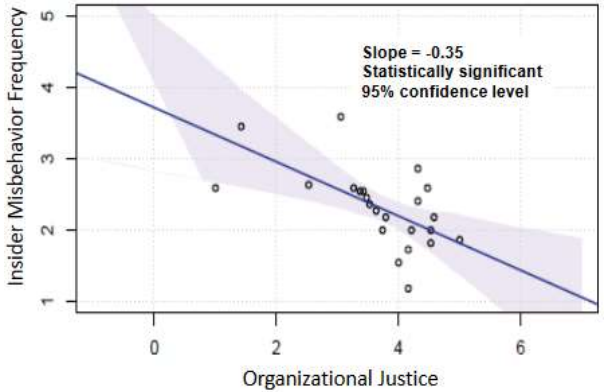
Non-Technical Control Validation

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

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