# Insider Threat Mitigation

William R. Claycomb, PhD

Andrew Moore, M.A.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA  15213

**Software Engineering Institute** | **Carnegie Mellon University**

**Software Engineering Institute** | **Carnegie Mellon University**

**SEI Research Review 2015**
**October 7–8, 2015**
© 2015 Carnegie Mellon University
Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

**2**

# CERT Insider Threat Mitigation to Date

**2001**
First empirical studies of insider crime

**2007**
Interactive training simulation and workshop developed

**2009-current**
Insider Threat Vulnerability Assessment applied

**2012**
The CERT Guide to Insider Threats published (Theft, Fraud, Sabotage)

**2014-current**
Insider threat mitigation patterns applied in industry (OSIT group)

**2014-current**
Assist all DoD military branches to develop ITPs

**2015**
ITPM, ITVA, ITPE certificates offered

**2006-13**
Espionage model developed for DoD

**2009-current**
Insider Threat Workshops

**2011-current**
Insider threat mitigation patterns developed and tested in DoD, DOE, DHS

**2014**
Develop linguistic clues of insider risk

**2014-current**
Insider sociotechnical network modeling and analysis

**2015-current**
Transition tools to DoD/IC customers

To date, 33 workshops presented to over 550 students

*ITPM = Insider Threat Program Manager; ITVA = Insider Threat Vulnerability Assessor; ITPE = Insider Threat Program Evaluator*
*OSIT = Open Source Insider Threat Information Sharing Working Group*

Software Engineering Institute | Carnegie Mellon University

# What is the Insider Threat?



SEI Research Review 2015
October 7–8, 2015

**Software Engineering Institute** | **Carnegie Mellon University**

© 2015 Carnegie Mellon University
Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

**4**

# The Insider Threat



**"When you're in positions of privileged access like a systems administrator … you're exposed to a lot more information on a broader scale than the average employee"**

**Edward Snowden**

# The Insider Threat
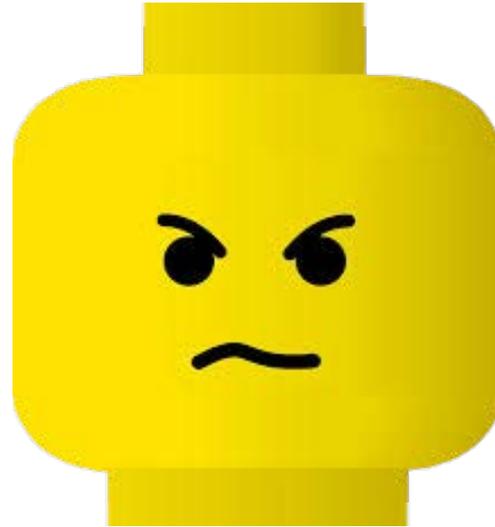
**"We're trying to locate the fugitive, but his face is so generic it matches every other face in our database."**

*- The LEGO® Movie*

# Where to Look
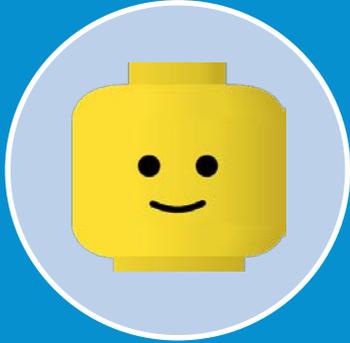
**Person**

Psychological factors, previous experience, etc.

**Environment**

Stress (professional, financial, medical, personal, etc.), social pressures, etc.

**Actions**

Use of information technology, engaging with others

**Software Engineering Institute** | **Carnegie Mellon University**

**SEI Research Review 2015**
**October 7–8, 2015**

7

© 2015 Carnegie Mellon University
Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

Insider Threat Mitigation
# **Social Network Dynamics**
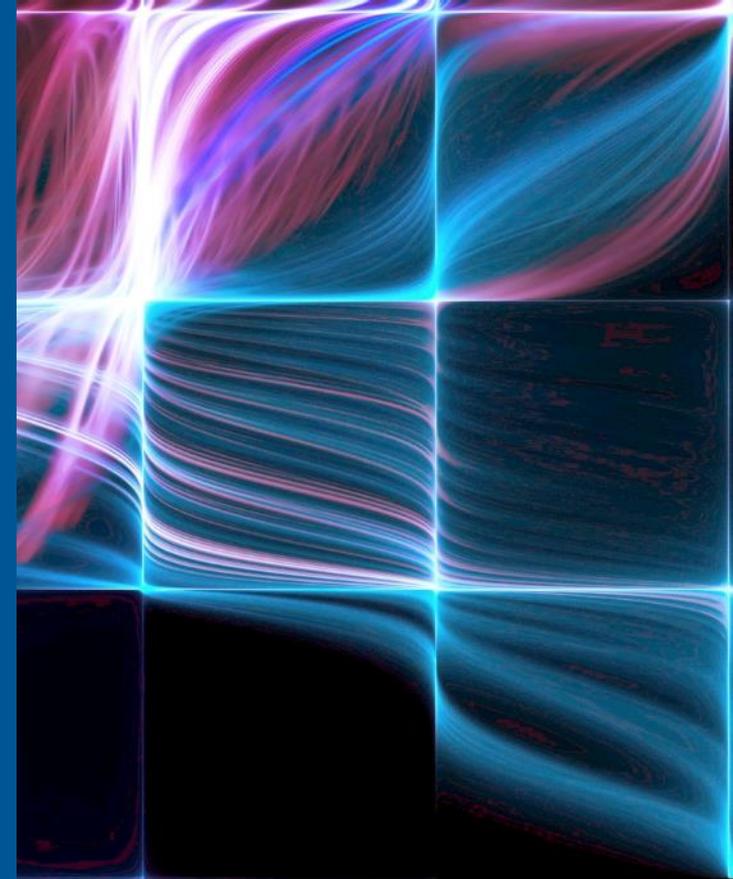
# Social Network Dynamics of Convicted Spies

## Overview

- **Hypothesis:** Over time, insider social networks exhibit weakening of internal connections, AND the strengthening of external connections to adversaries

- **Data:** ~140 insider espionage incidents: court docs, media, …

- **Data Analysis method:** Measure connection strength over time between insider and family/coworkers/adversaries - Organizational Risk Analyzer (ORA)

- **Connection strength measures:** communication frequency, affect positivity

# Social Network Dynamics of Convicted Spies

**Progress:** Hypothesis supported but is more complex than framed

- Analyzed dynamic, multidimensional networks of 9 espionage incidents (ORA)

  - Connections with family weaken; Connections with coworkers weaken or strengthen

    - Networks need to distinguish job activity from a spy gathering intel

  - Connections with adversary strengthen, including connections with any colluders

- Distinguished Enron "insiders" using machine learning (WEKA tool)

  - ROC curve identified 50% of insiders with a 18% false positive rate

- Developed simulation model of *physics* of job engagement and espionage

  - Shows how the flow of disengagement within organization translates to espionage

# Sociotechnical Network Analysis

**Sociotechnical network (STN) = social network + info flow network**

**Key Ideas**

- Combine analysis of information flow networks with social network analysis
  - earlier detection with lower false positive rates
- Focus not on insider access rights
  - but movement and trajectory of info flow

**Compare baseline document flows with actuals (Gemini tool)\***

- Identify document (expected) workflows as baseline (up front)
- Compare actual document flows with expected; identify anomalies (real time)
- Requires comparing *documents to documents* and *flows to flows*
- *Proposed Measures*
  - *Document Similarity :* hashing, plagiarism detection, keyword matching
  - *Flow Similarity :* graph matching algorithms – eg, using GED measures

\* Ard, et.al., "Information Behaving Badly," NSPW '13

**Software Engineering Institute** | **Carnegie Mellon University**

**SEI Research Review 2015**
**October 7–8, 2015**
© 2015 Carnegie Mellon University
Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

**11**

# Information Flow Analysis



Business Data → Business Processes

Want to find this case

Personal Data → Personal Processes

Software Engineering Institute | Carnegie Mellon University
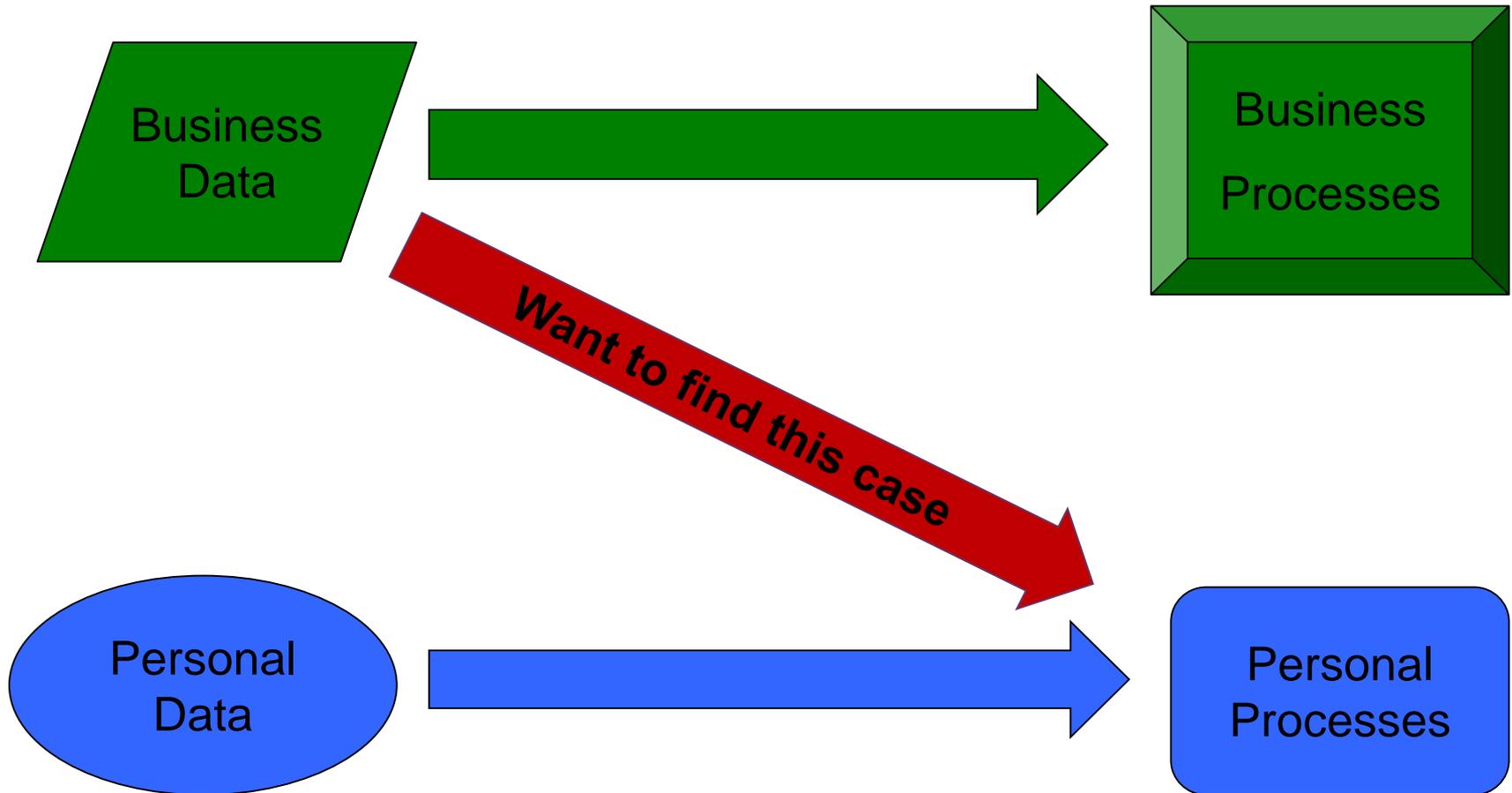
# New Paradigms for IF Net Analysis

- Moves the focal point of behavioral analysis from the user to the information we want to protect.

  - Anomalous information flows point back to a user.

  - Combine these flags with SNA flags for higher-value alerts.

- Document content similarity analysis

  - Progress in the Enron dataset:

    - Analyzed cases where the same filename can indicate dissimilar content (e.g., Resume.doc, Agenda.doc), and that the same content can be found under different filenames (renamed files)

    - File extension is incorrect for 24% of the files in the Enron dataset, which inhibits our ability to extract and compare raw text

**13**

# Similarity Metric Conclusions

- Bit-based forensic hashes
  - Successful in detecting file extension changes
  - Easily defeated by minor text changes
    - e.g .docx, due to xml encoding
- Text-based similarity measures
  - Similar to plagiarism detection
  - Successful at detecting minor text changes
  - Easily defeated when file extension is incorrect, for some tools

**Software Engineering Institute** | **Carnegie Mellon University**

**SEI Research Review 2015**
**October 7–8, 2015**

**14**
© 2015 Carnegie Mellon University
Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

Insider Threat Mitigation
**Detecting Stress**

Software Engineering Institute | Carnegie Mellon University
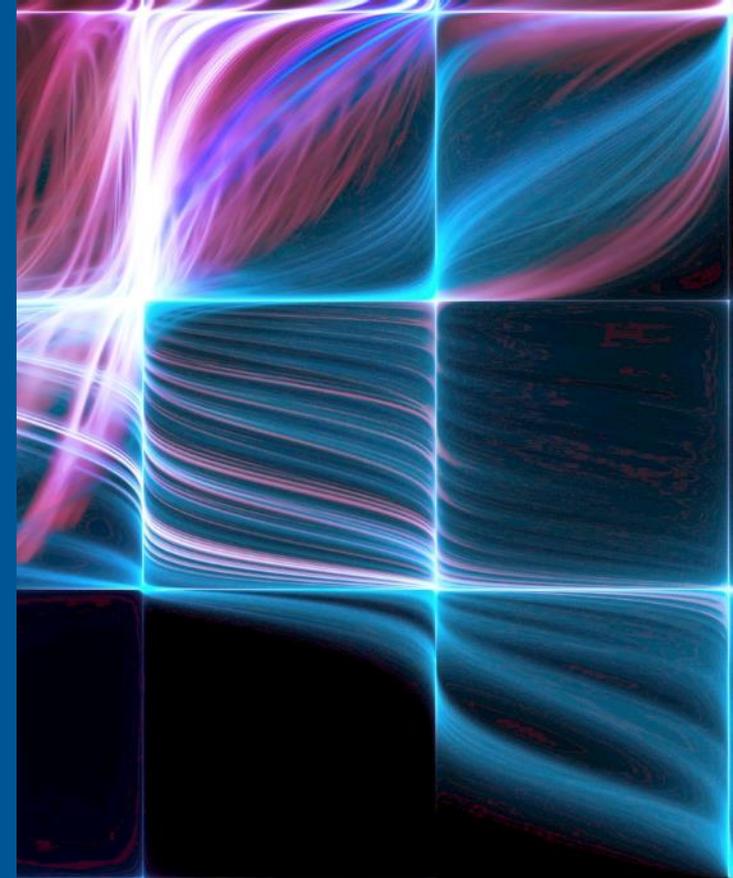
# Stress Detection

- Key ideas
  - Personality is reflected in language
  - Emotion and sentiment is also reflected in language
- Open question
  - Are temporary states such as stress also reflected in language?
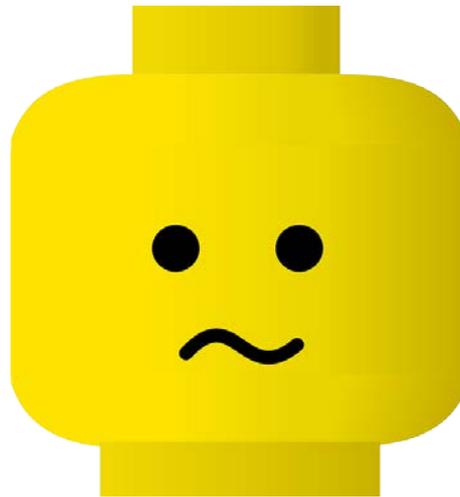
# Linguistic Metrics During Periods of Stress - Verb Use

Software Engineering Institute | Carnegie Mellon University
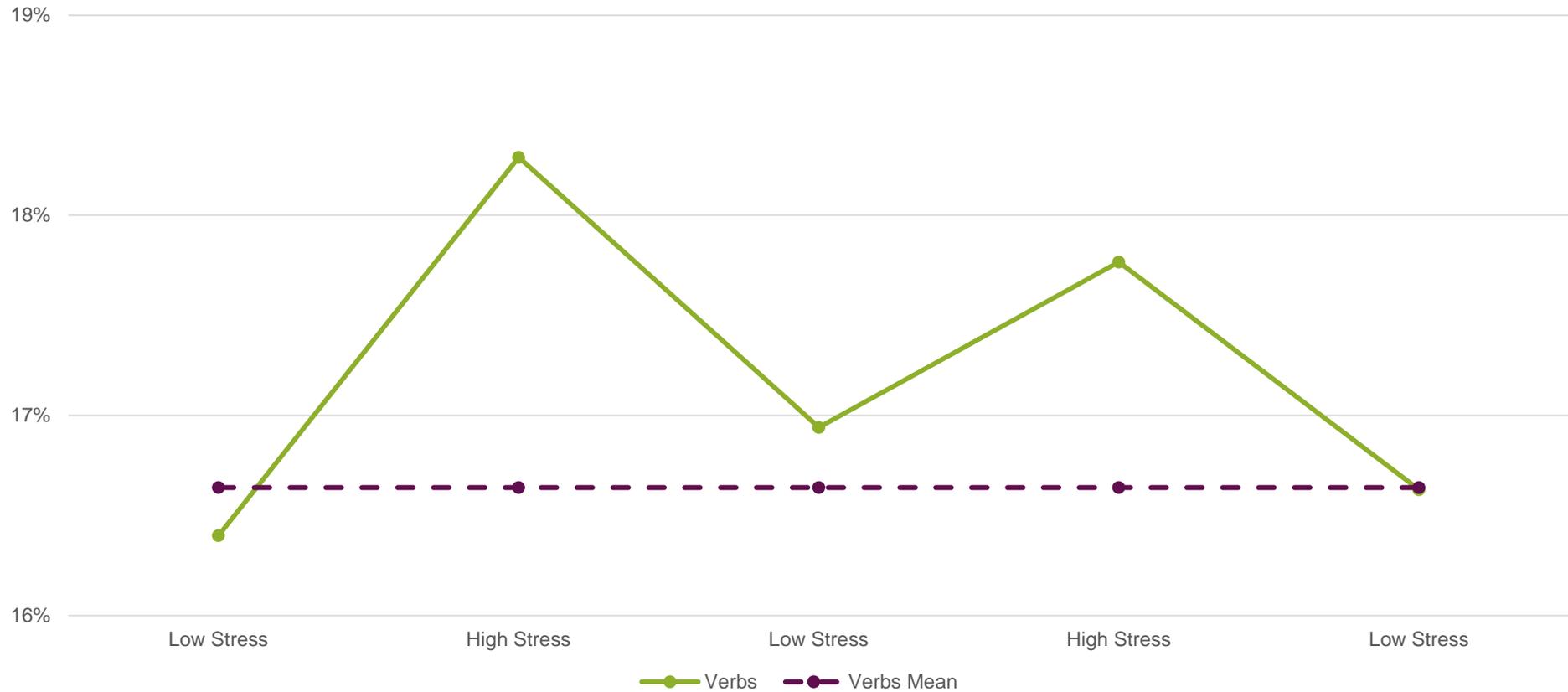
# Linguistic Metrics During Periods of Stress - Pronoun Use
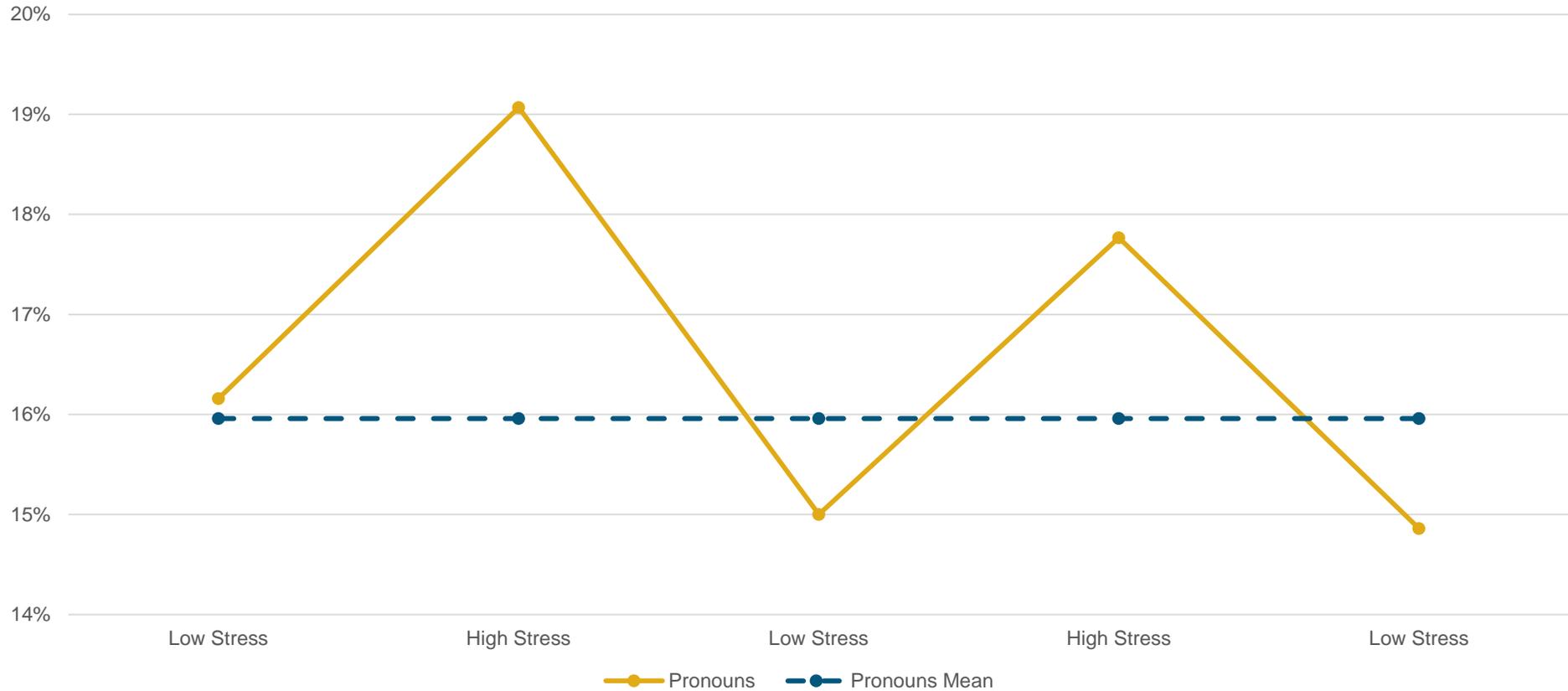
Insider Threat Mitigation
# But…

# the threat just changed

**Software Engineering Institute** | **Carnegie Mellon University**
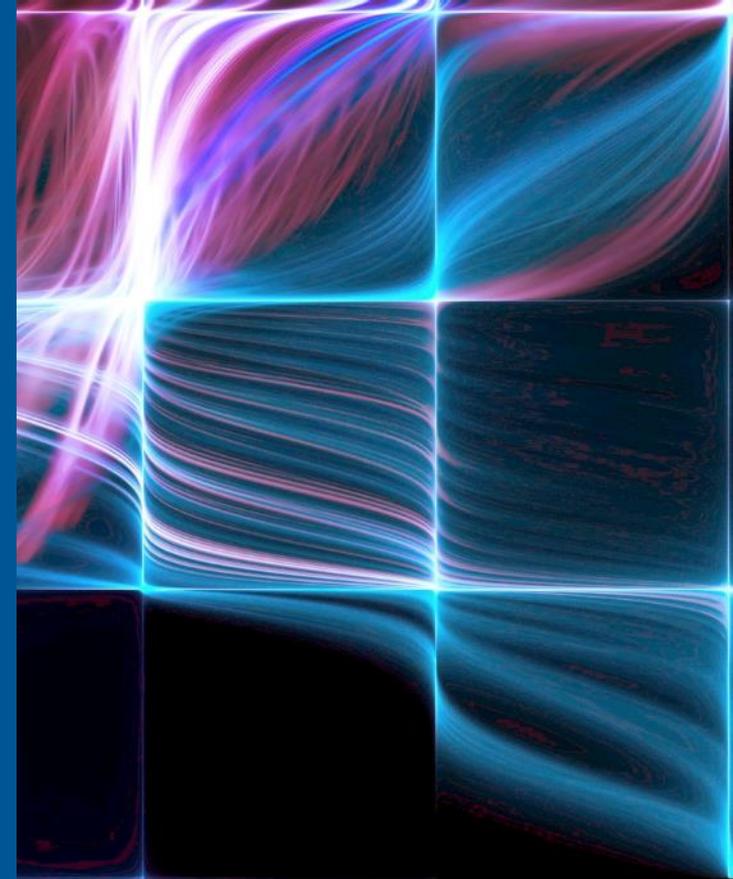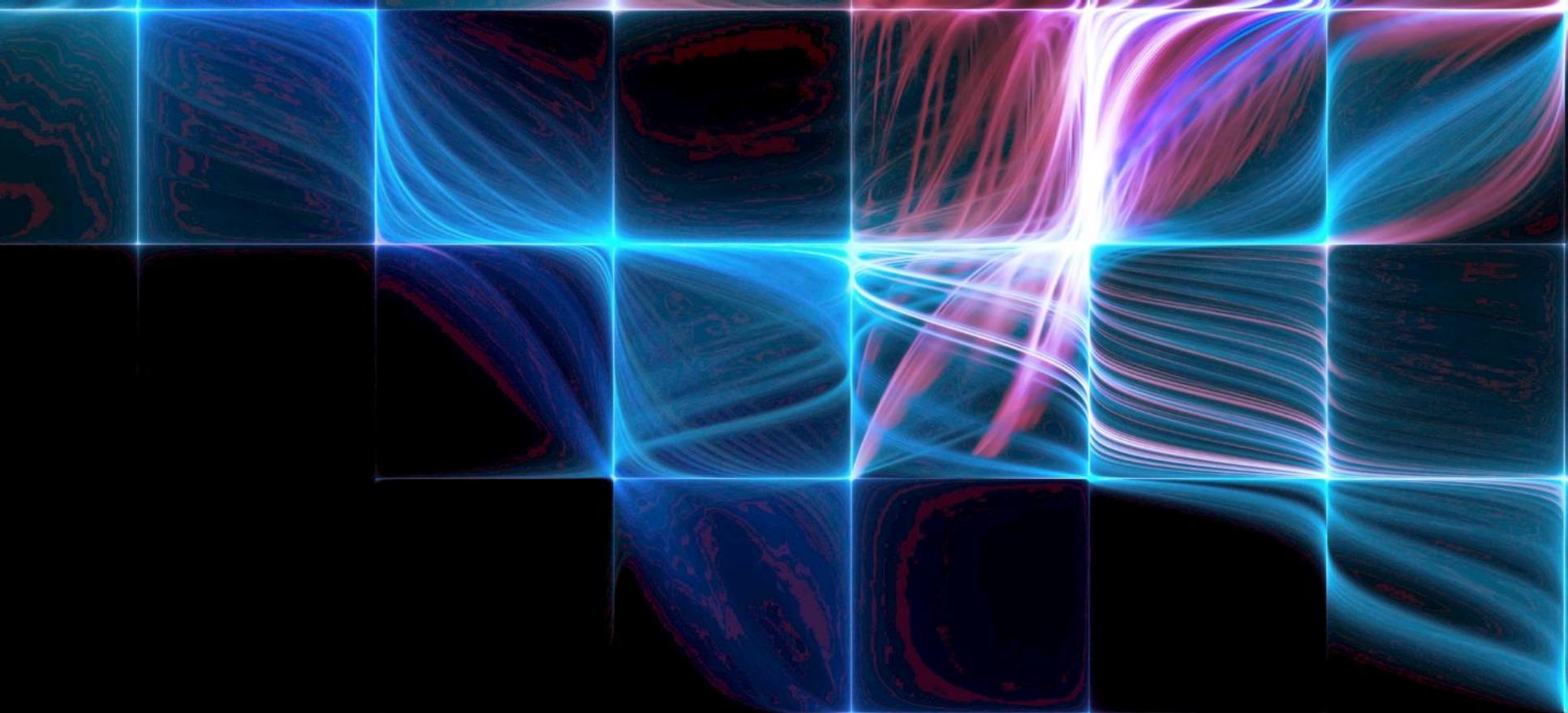
# Poster/demo Plug

**Come to our poster session and demo to see:**

- Dynamic meta-network analysis of espionage incidents
- Machine learning of Enron "insiders" showing false/true positive detection rates
- Simulation model of an emerging *physics* of job engagement and espionage

**Software Engineering Institute** | **Carnegie Mellon University**

# Contact Information

Bill Claycomb

Telephone:  412.268.8931

Email:  claycomb@cert.org

Andrew Moore

Telephone:  412.268.

Email:  apm@cert.org

**Software Engineering Institute** | Carnegie Mellon University

# CERT Insider Threat Mitigation to Date

**Create**

**Apply**

**Amplify**

**2001**
First empirical studies of insider crime

**2007**
Interactive training simulation and workshop developed

**2009-current**
Insider Threat Vulnerability Assessment applied

**2012**
The CERT Guide to Insider Threats published (Theft, Fraud, Sabotage)

**2014-current**
Insider threat mitigation patterns applied in industry (OSIT group)

**2014-current**
Assist all DoD military branches to develop ITPs

**2015**
ITPM, ITVA, ITPE certificates offered

**2006-13**
Espionage model developed for DoD

**2009-current**
Insider Threat Workshop offering

**2011-current**
Line-funding: Insider threat mitigation patterns developed and tested in DoD, DoE, DHS

**2014**
LENS-funding: Develop linguistic clues of insider risk

**2014-current**
Line-funding: Insider socio-technical network modeling and analysis

**2015-current**
Transition tools to DoD/IC customers

To date, 33 workshops presented to over 550 students

*ITPM = Insider Threat Program Manager; ITVA = Insider Threat Vulnerability Assessor; ITPE = Insider Threat Program Evaluator*
*OSIT = Open Source Insider Threat Information Sharing Working Group*

**Software Engineering Institute** | **Carnegie Mellon University**