The Insider

THE THREAT LAB NEWSLETTER

the ThreatLab

Volume 1 • Issue 1

The Threat Lab: A Brief History

The Defense Personnel and Security Research Center (PERSEREC) founded The Threat Lab in 2018 to realize the DoD Insider Threat Program Director's vision to incorporate the social and behavioral sciences into the counter-insider threat mission space. Our team is headquartered in Seaside, California, and includes psychologists, sociologists, policy analysts, computer scientists, and other subject matter experts in research design and analysis. Our business model is simple: We work with stakeholders to transform operational challenges into actionable research questions. We then design and execute research projects that result in accessible, concise findings and recommendations that we integrate into training and awareness materials that organizations can use or customize for their own purposes.

FROM THE EDITOR

In 2017, Dr. Millick pointed at me and told me to build a social and behavioral science research program to help counter the insider threat. This was the first time I had met Dr. Millick, so I turned around to make sure he was pointing at me. All I saw was an empty wall behind me, so I told him I was on board. Two years later, I am very proud to present the inaugural issue of The Threat Lab's newsletter, **The Insider**. **The Insider** is intended to connect researchers with operators across academic, government, and industrial sectors, and in this issue, we highlight the insider threat research that is going on at six of our Federally Funded Research and Development Centers (FFRDC) and University Affiliated Research Centers (UARC). Special thanks to CERT, JHU/APL, MIT Lincoln Laboratory, MITRE, The RAND Corporation, and ARLIS for sharing their research. I hope **The Insider** inspires future collaborations across the mission space.

Onward & Upward,

Stephanie Jaros

FROM THE DOD INSIDER THREAT PROGRAM DIRECTOR

As I review the evolution and direction of the Counter Insider Threat mission, I know that The Threat Lab is vital to attaining our goals. The threat is a human risk problem, and social and behavioral science research will impact many areas. More than the research, I am particularly excited by the diverse group involved with The Threat Lab's activities. Countering the insider threat is a mission that includes many threat vectors, crosses diverse research areas, involves numerous layered capabilities, and is being undertaken across the full spectrum of society. In other words, diverse expertise and organizational representation in the social and behavioral science arena is needed for success in this mission area. I appreciate and support your efforts, and I look forward to any and all recommendations generated by The Threat Lab. The Counter Insider Threat mission is challenging, but with your help, we will continue to protect personnel, resources, information, and operations.

Best Regards,

Brad Millick

CERT National Insider Threat Center

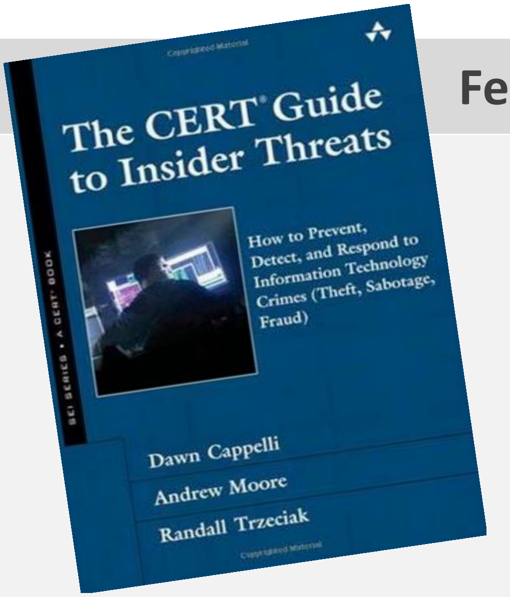
National Insider Threat Center

OUR MISSION

As a part of Carnegie Mellon University's Software Engineering Institute, we strive to enable effective insider threat mitigation by researching and developing capabilities for preventing, detecting, and responding to evolving cyber and physical threats. We do this through empirical research, modeling, analysis, and outreach to develop and transition socio-technical solutions to combat insider threats.

OUR HISTORY

We have been researching insider threats since 2001 in partnership with the DoD, DHS, Secret Service, numerous additional federal agencies, the intelligence community, private industry, academia, and the vendor community. We use our database of over 2,800 insider incidents to characterize the nature of the evolving insider threat problem, develop indicators of insider risk, and prototype and transition technical and administrative controls for insider threat mitigation. In our insider threat lab, we measure the effectiveness of new tools, indicators, and analytic techniques. We've developed assessments to help organizations identify their vulnerabilities to insider threats, and several training courses on establishing and operating an insider threat program.


The CERT® Guide to Insider Threats
How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)
Dawn Cappelli
Andrew Moore
Randall Trzeciak
SEI SERIES • A CERT® BOOK

Featured Research

The Common Sense Guide to Mitigating Insider Threats, Sixth Edition – A collection of 21 best practices for insider threat mitigation, complete with case studies and statistics

Balancing Organizational Incentives to Counter Insider Threat – A study on how positive incentives can complement traditional security practices to provide a better balance for organizations' insider threat programs

Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program – An exploration of the types of tools that organizations can use to prevent, detect, and respond to multiple types of insider threats

Insider Threats Across Industry Sectors – A multi-part blog series that contains the most up-to-date statistics from our database on sector-specific insider threats

COMING SOON

Stay up-to-date with us by visiting our **blog**, where we will soon be posting links to our recent work in establishing evaluative criteria for insider threat tools, and a reference architecture for establishing an insider threat tool testing capability.

Contact Us: insider-threat-feedback@cert.org

ADDITIONAL REPORTS

- Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls
- Analytic Approaches to Detect Insider Threats
- Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments
- Workplace Violence & IT Sabotage: Two Sides of the Same Coin?
- An Insider Threat Indicator Ontology

Johns Hopkins Applied Physics Laboratory (JHU/APL)

OUR MISSION

JHU/APL—the nation's largest university affiliated research center—solves complex research, engineering, and analytical problems to support U.S. government agencies and national priorities.

OUR HISTORY

Founded on March 10, 1942—just three months after the United States entered World War II—JHU/APL was created as part of a federal government effort to mobilize scientific resources to address wartime challenges. APL continues to relentlessly pursue the mission it has followed since its first day: to make critical contributions to critical challenges for our nation. Learn more at: https://www.jhuapl.edu/

OUR ROLE ON IARPA'S SCITE PROGRAM

JHU/APL serves as the Thrust 1 Test & Evaluation team on the Intelligence Advanced Research Projects Activity (IARPA) Scientific advances to Continuous Insider Threat Evaluation (SCITE) program. Thrust 1 focuses on research to develop a new class of indicators, active indicators, and associated detection tools. JHU/APL independently tested and evaluated variations of performer-developed active indicators. Send questions to SCITE@jhuapl.edu

Active Indicator Research

Active Indicators (AIs) are stimuli designed to evoke indicative responses from potential insider threats engaged in espionage.

JHU/APL conducted an experiment to test how well four classes of AI stimuli differentiate benign employees from potential insider threats, based on behavioral response.

AI 1: Time-specific security events. Emails announced security software update and scheduled security scan. File access and exfiltration behaviors were measured.

AI 2: Insider-relevant information. Emailed newsletter links offered both security- and insider threat-related information as well as general purpose information. Click rates were measured.

AI 3: Increased access. Emails advertised two available positions with extra information access (no prior experience & minimal responsibilities). Application rates were measured.

AI 4: Effortful opt-out. Emails announced optional forms could be completed to opt-out of security monitoring (network activity & file activity). Forms required justification & delivery of signed paper copy to a remote location. Form submission rates were measured.

METHODOLOGY

Experiment's contextual setting was an "Alternate Reality Game" centered on a fictional project.

56 JHU/APL staff members completed a 4-week study, spending 1-2 hours per week on project tasks.

A within-subjects design randomly assigned participants to one of two conditions: insider-first (performing insider-like activities) or control-first (acting as regular employee performing data loss prevention work) for Weeks 1 and 2. For Weeks 3 and 4, participants switched conditions.

AIs were counterbalanced to minimize the effect of AI timing.

RESULTS SUMMARY

AI 3 Increased access was most effective. Insider threat role-players were more likely to try to gain increased access.

AI 2 Insider-relevant information was moderately effective. Insider threat role-players were more likely to click on insider-relevant information.

AI 1 Time-specific security events was moderately effective. Insider role-players were more likely to access non-required and restricted files during the security software update. There was no differential behavior between insiders and benign staff before the security scan.

AI 4 Effortful opt-out was not effective as implemented. The false positive rate was higher than the true positive rate indicating no diagnostic value in explaining behavioral differences.

A logistic regression model of combined AIs predicted probability of being an insider role-player with an 87.5% true positive rate.

MIT Lincoln Laboratory

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

OUR MISSION

We develop advanced technology in support of national security. As a Department of Defense federally funded R&D center, we create technology aimed at both long-term DoD focuses and critical short-term needs. What sets us apart from many national R&D laboratories is our emphasis on building operational prototypes of the unique systems we design.

OUR HISTORY

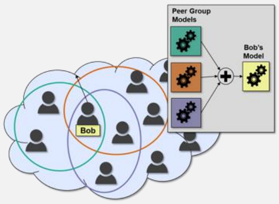
MIT Lincoln Laboratory was established in 1951 to develop an air defense system for the United States, due to MIT's seminal work on radar at its Radiation Laboratory during World War II. The air defense system, known as 'SAGE', connected hundreds of radar sites to centers that coordinated information on activity in the U.S. air space and, if needed, would direct the response to an air attack.

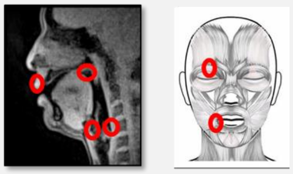
Our experience in sensors, computing, decision support technology, and electronics has led to a diverse portfolio of work that still includes air and missile defense, and communications, but has expanded to areas like cybersecurity, autonomous systems, bioengineering, and space systems.

Our work in bioengineering seeks to improve human health and performance, prevent injury and disease, and enhance rehabilitation and recovery with advanced bioengineering technology, and covers four broad technical areas: biomedical research, engineered and synthetic biology, bioinformatics, and forensic biology.

POC: Dr. William Streilein, Principal Staff, Homeland Protection and Air Traffic Control Division, email: wws@ll.mit.edu

Featured Research





Insider threat detection: We characterize an individual's peer-group behavior through the application of Long-Short Term Memory (LSTM) network models to user activity monitoring (UAM) data [1]. The resultant method requires fewer computational resources to train and produces more accurate predictions of insider threat activity when compared to a per-user modeling approach.

Remote detection of anomalous mental states: To support rapid assessment and early intervention, we leverage recent advances in off-body physiological sensing and AI, to fuse neuro-motor coordination-based vocal and facial biomarkers to detect anomalous mental states, such as depression and cognitive fatigue [2].

Detection system modeling: In support of optimal deployment of insider threat systems, we modeled user behavior and developed baseline system enterprise models in order to leverage them to predict the impact of sensor and data additions [3] .

COMING SOON

We will continue to leverage UAM data for modeling individual behavior, augmenting prediction capabilities by accessing expanded relevant datasets. Additionally, future non-intrusive sensing work will combine biomarker sensing with physiologic measures, such as heart rate, skin conductance, and body movement measures, to develop a capability for improved emotional state discrimination.

ADDITIONAL REPORTS

1. Matterer, J., et al., "Peer Group Metadata-Informed LSTM Ensembles for Insider Threat Detection." The Thirty-First International Flairs Conference. 2018.
2. Quatieri, TF, et al., Multi-modal biomarkers to discriminate cognitive state, Book Chapter in The Role of Technology in Clinical Neuropsychology, Oxford Press, 2017.3
3. 3. Roberts, C., et al. "A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems." 2016 IEEE Security and Privacy Workshops (SPW). IEEE, 2016

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the Under Secretary of Defense for Research and Engineering under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Under Secretary of Defense for Research and Engineering.

MITRE

Human Behavior and Cybersecurity Capability

Insider Threat Focus Area

OUR MISSION

We leverage the behavioral sciences to improve insider threat prevention, detection, and mitigation.

OUR APPROACH

Insider threat is not solely a technological issue but has an inherently human component. We use quality data and rigorous scientific methodologies to generate and evaluate approaches to effectively counter insider threats.

Our subject matter expertise spans a spectrum of harmful cyber and non-cyber (behavioral) insider threats that our sponsors face daily from malicious or non-malicious (e.g., negligent, outsmarted) employees.

As recognized national and international subject-matter-experts in the field of insider risk and threat, MITRE's work is widely sought out from government, industry, and academia for research, consultations, presentations, and partnerships. Request a brief of our data-driven *MITRE Insider Threat Behavioral Framework.*

Our Research

Program Design: Reviewed best practices and lessons learned from 20 industry insider threat programs, developing a benchmark for government programs.

Indicator Design: Developed a methodology to identify novel cyber indicators that differentiate malicious from non-malicious employee-generated computer activity.

Psychosocial Characteristics: Identified a large set of psychosocial characteristics of known malicious spies and operationalized these into data-driven proactive indicators.

Tool Evaluation: Developed a methodology to evaluate and compare the effectiveness of data analytics tools (e.g., sentiment analysis in email, User Activity Monitoring).

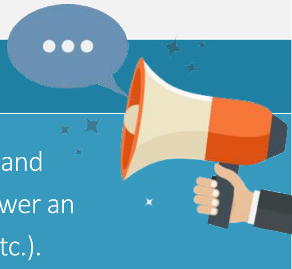
Supervisor & HR Reporting: Created low-burden tools to increase the quantity and quality of insider risk reporting by supervisors and HR.

New Data Sources: Developed a methodology to generate data for insider threat programs based on insights directly from benign frontline employees.

Post-attack: Developed an interview protocol that can be used to interview malicious insiders post-incident to generate new insider characteristics.

Critical Assets Risk Assessments: Developed a methodology to identify and prioritize the highest value insider threat human, cyber, and physical assets in organizations.

COMING SOON



MITRE is a thought leader in insider threat, generating ideas to make the world a safer place. Recently, we have been exploring:

- **Remote Work:** An early assessment of insider risk in remote work environments, including behavioral and cyber gaps in detection and prevention.
- **Insider Threat-Based Framework:** Identifying and analyzing the most frequent risk characteristics from real government and industry insider cases (over 6,000 cases).
- **Protective Factors:** Identifying, evaluating, and operationalizing positive factors that can lower an employee risk score (e.g., signs of coping, etc.).
- **Financial Strain:** Identifying, testing, evaluating, and operationalizing indicators of high financial strain, rather than debt which fails to consider level of concern for debt.
- **Screening and Vetting:** Identifying the most effective investigative characteristics that are used by adjudicators in clearance revocation decisions.

Point of Contact: Dr. Deanna D. Caputo, Chief Scientist for Behavioral Sciences & Cyber Security
The MITRE Corporation (FFRDC), Phone: 703-983-3846 Email: dcaputo@mitre.org

The RAND Corporation

OUR MISSION

The RAND Corporation is a nonprofit institution that helps improve policy and decision-making through research and analysis. As a nonpartisan organization, RAND is widely respected for operating independent of political and commercial pressures. Quality and objectivity are our two core values.

OUR HISTORY

On May 14, 1948, Project RAND became an independent, nonprofit organization. Adopting its name from a contraction of the term research and development, the newly formed entity was dedicated to furthering and promoting scientific, educational, and charitable purposes for the public welfare and security of the United States.

Assessing Continuous Evaluation Approaches for Insider Threats

How Can the Security Posture of the U.S. Departments and Agencies Be Improved?

David Luckey, David Stebbins, Rebeca Orrie, Erin Rebhan, Sunny D. Bhatt, Sina Beaghley

Featured Research

Continuous Evaluation approaches can mitigate insider threats against the U.S. Government says David Luckey, the lead author in a new RAND report.

The report states that the threat from insiders is very real, and this insider threat puts the United States and U.S. government employees at grave risk. The report recommends that the U.S. government should employ the most thorough form of vetting available to mitigate the threat to the extent possible, and a process that can continuously evaluate those who could do us harm from the inside. Neglecting to do so is potentially irresponsible and dangerous, as demonstrated by the many cases of harm caused by insiders.

The report examines Continuous Evaluation (CE) approaches to detect insider threats available to the U.S. government and assesses the relevance of these approaches to the challenges posed by such insider threats.

The virtues of CE are compelling, with the potential superiority in effect and cost over the current method of granting security clearances to personnel based on periodic reinvestigation and re-adjudication. CE, however, has yet to be widely adopted and the current security clearance system is decades old. Technology has advanced significantly; an updated, improved system and process should capitalize on these advancements.

To schedule an interview about, “Assessing Continuous Evaluation Approaches for Insider Threat: Can the Security Posture of the U.S. Departments and Agencies Be Improved?” contact Khorshied Samad in the RAND Office of Media Relations at (703) 413-1100 ext. 5317 or ksamad@rand.org.

ADDITIONAL REPORTS

Bruce, J., et al. Secrecy in US National Security: *Why a Paradigm Shift is Needed*.

University of Maryland Applied Research Laboratory for Intelligence and Security (ARLIS)

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

OUR MISSION

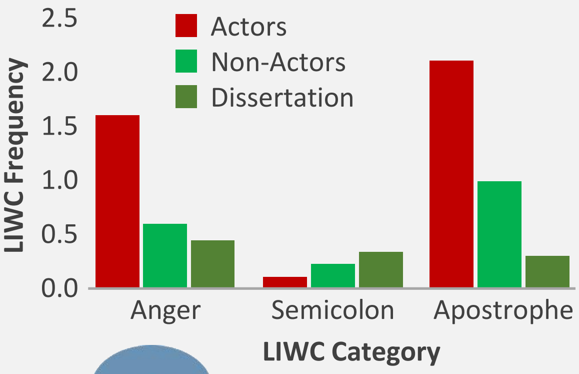
At ARLIS, we conduct innovative, academically rigorous, and mission-centric research on human behavior and risk, artificial intelligence, information engineering, conflict and security, and advanced computing. We provide cutting-edge training solutions and offer unbiased guidance to policymakers. Our research is interdisciplinary and collaborative, bringing together people from the government, academia, and the private sector.

OUR HISTORY

The University of Maryland's University Affiliated Research Center (UARC) was founded in 2003 as an organization dedicated to the research, training, and policy challenges of the Department of Defense (DoD) and the Intelligence Community (IC). In 2018, the UARC, now under the sponsorship of the Office of the Under Secretary of Defense for Intelligence (OUSD-I), was renamed ARLIS and revectored to meet the evolving needs of the DoD and IC.

Featured Research

Researchers collected publicly posted manifestos or other texts from individuals who were actors who had used insider information or access to damage their organization. The linguistic characteristics of these texts were compared to texts from non-actors who posted ideological statements, and dissertation writers who wrote about topics that overlap with topics in actors' and non-actors' texts. Latent Semantic Analysis (LSA) was carried out using Linguistic Inquiry Word Count (LIWC) which works by comparing words in a text with predefined dictionary words that have been coded for the relevance to a variety of emotions and emotional states (Pennebaker, Boyd, Jordan, & Blackburn, 2015).



Analyses showed that linguistic attributes of the writing could be used to differentiate actors from non-actors and dissertation writers. Actors had a higher number of negations, negative emotions, and anger words compared to non-actors and dissertation writers. Actors also used more words related to perceptual feeling and to certainty. Non-actors and dissertation writers were more likely than actors to use semicolons, and less likely to use apostrophes.

Alexis Turner, Temple University
Petra Bradley, University of Maryland

COMING SOON

Current research on insider threat detection focuses on identifying factors and indicators that predict ethical behavior, risky behavior, and individual investment in the organization. Future research might expand to include genres of writing that are not publicly available (e.g., email and work-related reports) to determine whether content available to the employer might also hold relevant clues about which employees might be more likely to pose a threat to the organization.

REFERENCED REPORTS

Pennebaker, J.W., Boyd, R.L., Jordan, K., & Blackburn, K. (2015). The development and psychometric properties of LIWC2015. Austin, TX: University of Texas at Austin.

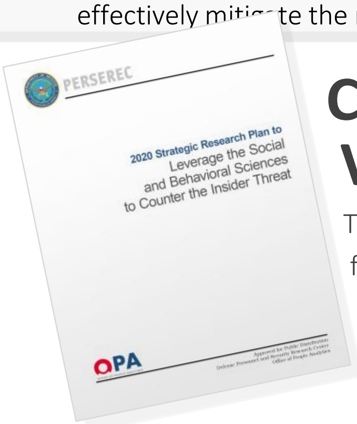
The Threat Lab: To be Published in Autumn 2019

AN EVALUATION OF THE UTILITY OF EXPANDING PSYCHOLOGICAL SCREENING TO PREVENT INSIDER ATTACKS

The Critical Pathway Model (CPM) has emerged as the leading framework to conceptualize the transformation of a trusted insider into a malicious attacker. CPM, however, is a descriptive framework rather than a predictive model, which complicates its implications for policymakers. This report assesses the unclassified empirical evidence that underlies one portion of the CPM—individual predispositions—in order to determine whether or not DoD should expand its psychological screening program to include more applicants as a way to fairly, efficiently, and effectively mitigate the risk of future insider attacks.

AN EXPLORATORY ANALYSIS OF THE RELATIONSHIP BETWEEN WORKPLACE HARM AND INDIVIDUAL ADVERSE OUTCOMES

This project quantifies the occurrence of workplace-related adverse outcomes (i.e., stressors) and workplace-related violence, and leverages data science techniques to explore the relationship between the two in the DoD workforce. The authors summarize characteristics of individuals with documented workplace stressors and workplace violence, and then focus specifically on cases in which a stressor preceded a violent event. Finally, the authors qualitatively explore repeated incidents of workplace harm.



PERSEREC

2020 Strategic Research Plan to Leverage the Social and Behavioral Sciences to Counter the Insider Threat

OPA

Call for Volunteers

The Threat Lab is updating its foundational document and needs your help. **Contact us to be included as a subject matter expert** in the forthcoming *2020 Strategic Research Plan to Leverage the Social and Behavioral Sciences to Counter the Insider Threat.*

SBS Summit 2020

The Threat Lab announces **SBS Summit 2020**, the first annual social and behavioral science insider threat research conference open to government, industry, and academia. We are targeting a northern California location in Summer 2020 for the Summit. **Stay tuned for more information!**

FY20 Initiatives

October 2019 marks the start of the new fiscal year, and The Threat Lab has an ambitious agenda. Here are just a few of our FY20 initiatives:

- **2 Toolkits for Managers**, one to help build and maintain resiliency on their teams and the other to help managers respond to concerning behavior
- **1 Toolkit for the STEM Workforce** to help integrate the counter-insider threat program into the research and development mission
- **A Report on The Future of Insider Threat** to identify relevant factors, practices, and scenarios that have the potential to disrupt the forces that motivate DoD personnel to act with integrity, maintain well-being, and align their values with those of the organization.
- **A Research Note on Best Practices** to prevent unauthorized disclosures

To learn more and stay connected, join The Threat Lab's community! **Email us at dodhra.threat-lab@mail.mil.**