

# The **MIROR** JOURNAL

Managing Insider Risk and Organizational Resilience

## IN THIS ISSUE

### Breaking the Early Risk Assessment Ceiling

#### **Early Risk Assessment: Pushing “Left of Flash”**

The Art and Science of  
Early Risk Assessment

#### **Advancing Organizational Health for Protection:**

Maximally preventing and  
managing insider risk

Volume 1 | Number 1 | Summer 2023



WEST POINT  
PRESS

# The Department of Defense Insider Threat Program



The Department of Defense (DoD) Insider Threat Program leads DoD efforts to prevent, deter, detect, and mitigate insider threats to the DoD enterprise.

Located within the Office of the Under Secretary of Defense for Intelligence and Security, Counterintelligence, Law Enforcement, and Security (OUSD(I&S), (CLS), the program provides governance and advocacy for insider threat programs across the DoD Components and Services supporting nearly 15 million personnel.

The program is dedicated to the pursuit of advanced capabilities integrated within DoD security reform and vetting efforts, and to the development of a well-equipped, trained, and vigilant workforce to protect DoD resources, personnel, installations, and other equities from insider threats.

The DoD Insider Threat Program provides strategic oversight, issues policy and implementation guidance, and advocates for resources for the DoD Insider Threat community.

The office has played a critical role in advancing the mission through targeted investments in training and workforce professionalization and in advanced social and behavioral science research. The program also facilitates information sharing, collaboration, and continuous improvement of the insider threat discipline for stakeholders across the U.S. government and key partners in critical infrastructure.

For more information contact the  
OUSD(I&S) InT team's organizational box

[osd.pentagon.ousd-intel-sec.mbx.dodcounterinsidethreat@mail.mil](mailto:osd.pentagon.ousd-intel-sec.mbx.dodcounterinsidethreat@mail.mil)



**THE U.S. ARMY INSIDER THREAT OPERATIONS HUB IS THE OPERATIONAL ELEMENT OF THE COUNTER-INSIDER THREAT PROGRAM. IT IS DESIGNED TO DETECT CONCERNING BEHAVIORS FROM ARMY PERSONNEL AND TO DETER, PREVENT, AND MITIGATE THREATS TO ARMY PERSONNEL, RESOURCES, AND INFORMATION.**



**The Hub utilizes Artificial Intelligence, Machine Learning, and other computer aided tools to identify behavioral patterns that may indicate an individual poses a risk to the Army.**

Analysts compile information and consult with subject matter experts to assess risk and develop mitigation strategies.

The Hub further coordinates with "spoke" elements, including law enforcement, counter-intelligence, and security to ensure synchronized detection and response. We are proud to be the Army's first-line in detecting threats from within.

**FOR QUESTIONS OR MORE INFORMATION ABOUT THE HUB, OR TO REPORT CONCERNING BEHAVIOR, PLEASE CONTACT:**

**[usarmy.pentagon.hqda-dcs.mbx.g-34-int-hub-reports-cell@army.mil](mailto:usarmy.pentagon.hqda-dcs.mbx.g-34-int-hub-reports-cell@army.mil)**

# The **MIROR** JOURNAL

Managing Insider Risk and Organizational Resilience

The Managing Insider Risk and Organizational Resilience (MIROR) Journal

Produced and edited by the West Point Insider Threat Program  
Published by West Point Press

## EDITORS

### Program Manager

Jonathan W. Roginski, PhD  
Email: jonathan.roginski@westpoint.edu

### Editor-in-Chief

Jan Kallberg, PhD  
Email: jan.kallberg@westpoint.edu

### MIROR Journal

D/MATH USMA  
646 Swift Rd, West Point, NY 10996, USA

### Connect with The Journal

email: insiderthreat@westpoint.edu  
twitter: twitter.com/InTWestPoint  
web: insiderthreat.westpoint.edu

The Insider Threat Program is a part of the United States Military Academy, Department of Mathematical Sciences.

## WEST POINT PRESS

### Director

COL Jordon Swain, PhD

### Deputy Director

Corvin Connolly, PhD

## DESIGN/CREATIVE DIRECTORS

Sergio Analco  
Gina Lauria

## FUNDING FOR THE MIROR JOURNAL

Provided by the Office of the Undersecretary of Defense Intelligence and Security OUSD(I&S)

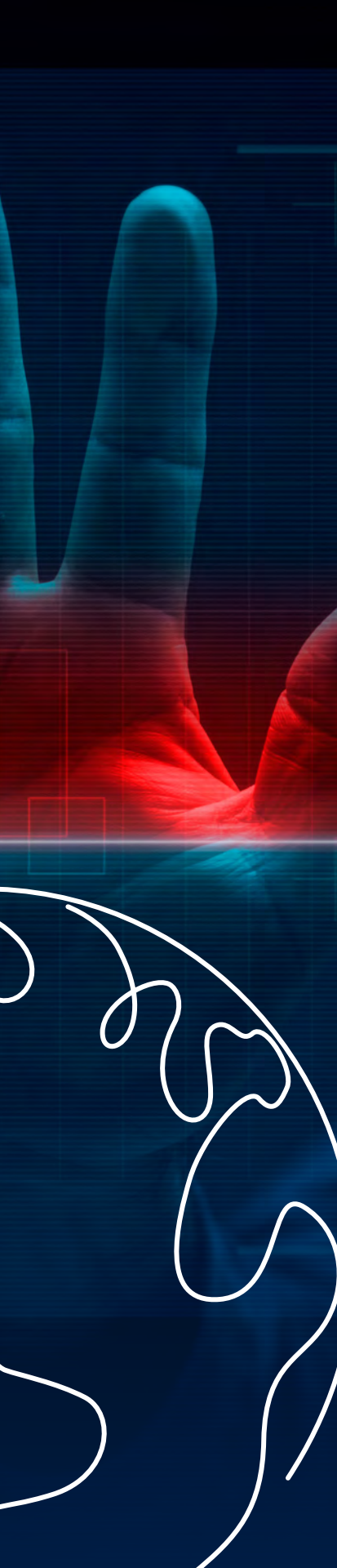
.....



The West Point Press is the publishing arm of the US Military Academy, producing scholarly content for students, scholars, and leaders.

Our scholarly books, digital textbooks, journals, and other content reflect a commitment to the highest standards of scholarship.





## ABOUT

*The Managing Insider Risk & Organizational Resilience (MIROR) Journal* (Online ISSN 2832-5427 Print ISSN 2832-5419) is a scholarly Open Access journal published by the West Point Press, the publishing arm of the United States Military Academy, and produced by the Insider Threat Research Program at the Department of Mathematical Sciences at the United States Military Academy. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute an endorsement by the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

## COPYRIGHT

© U.S. copyright protection is not available for works of the United States Government or works written by United States Government personnel (military or civilian) as part of their official duties. However, the authors of specific content published in *The MIROR Journal* retain copyright to their individual works and grant a Creative Commons CC-BY-NC 4.0 license to ensure Open Access.

## OPEN ACCESS STATEMENT

*Managing Insider Risk & Organizational Resilience (MIROR) Journal* is an Open Access Journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles, or use them for any other lawful purpose, without asking prior permission from the publisher or the author. This is in accordance with the Budapest Open Access Initiative (BOAI) definition of open access.

*The Managing Insider Risk & Organizational Resilience (MIROR) Journal* does not charge authors for submission, processing, and publication.

## REPOSITORY POLICY

*Managing Insider Risk & Organizational Resilience (MIROR) Journal* is an Open Access journal and supports the author's self-archiving their manuscripts/articles on their personal or institutional website, university, specialized repositories such as ArXiv.org, and research sharing websites such as ResearchGate. Authors are allowed to deposit their works after it has been published in the *Managing Insider Risk & Organizational Resilience (MIROR) Journal*, either online or in print, with no embargo. Authors can publish submitted, accepted, published manuscript/article, or publisher's PDFs.

## ARCHIVING POLICY

*Managing Insider Risk & Organizational Resilience (MIROR) Journal* allows anyone to archive the content. The *MIROR Journal* will ensure long-term open access to the content by uploading the content to the Department of Defense digital repository DTIC (Defense Technical Information Center) DoDTechpedia public collections, Internet Archive (Archive.org), and deliver the printed journal to the Library of Congress.

.....

■ WELCOME

Jonathan W. Roginski

Is there a nobler pursuit than of protecting our people and the organizations they serve and that serve their employees?

Page 09

■ SENIOR LEADER PERSPECTIVES

Lewis R. Call

Bystander Engagement

Page 15

Savannah Grace Clemente, Nik Seetharaman

Adapt or Die: Building Internal Intelligence Networks to Combat Modern Insider Threats

Page 19

Chris Hagner

Complexity: Leveraging Data While Being Human Centric

Page 25

■ PROFESSIONAL COMMENTARY

Val LeTellier

Red Flags Reimagined - A former CIA Operations Officer on Today's Insider Risk Challenge

Page 31

The staff, faculty and cadets of West Point Insider Threat Program would like to thank the hosts of the 2023 Insider Threat Internship Team:

- Army Analytics Group Research Facilitation Lab
- Logistics Management Institute
- Army Insider Threat Hub
- TRADOC Network Engagement Team



**Bottom row:** CDTs Kayla Teuscher, Claire Tsay, Angelina Pfister, Elena Teague  
**Second:** CPT Anna Tucker, CDTs Magnolia Flamhaft, Max Felter, Blake Coston, Jamison Uptgraft, Saleem Ali  
**Third:** CDTs Cooper Shafer, Michael Lenart, Samin Kim, Joshua Blackmon, Ethan Collins  
**Back:** Dr. Jon Roginski, COL Joe Lindquist, LTC Patrick Mugg, CPT James Sherrell

■ **RESEARCH ARTICLES**

**Tin L. Nguyen, Matthew T. Allen, Kat Parsons**

Advancing an Organizational Health Perspective for Insider Threat Prevention and Management **Page 43**

**Robert Graves**

Pushing Left of Flash – The Art and Science of Early Risk Assessment **Page 61**

**Jonathan Shedler, Luisa E. Marin-Avellan, Olga G. Shechter,**

**Peter Fonagy, Michael Karson, Eric L. Lang**

Breaking the Ceiling on Risk Assessment **Page 77**

.....

■ **LESSONS LEARNED AND CASE STUDIES**

**Christopher Babie**

The Difference is Human – Building Preventative Insider Threat Programs **Page 105**

.....

■ **SUBMISSIONS AND CALL FOR PAPERS**

**Page 115**

.....







**WELCOME**





# Is there a nobler pursuit than of protecting our people and the organizations they serve and that serve their employees?

---

**Jonathan W. Roginski**



**T**hank you for spending a measure of your precious time diving into the content offered by the *Managing Insider Risk and Organizational Resilience (MIROR) Journal*. At every age before and since antiquity, people have been the world's greatest resource. Even with the advent of great technology, people remain paramount. Is there a nobler pursuit than of protecting our people and the organizations they serve and that serve their employees? Many in this community would say no. So, thank you for helping us advance the conversation about risk, threat, and resilience. Let's have the conversation at every level of the organization, from entry to C-Suite.



Dr. Jon Roginski is an Assistant Professor in the United States Military Academy's Department of Mathematical Sciences (West Point) and Program Manager for the Army's Insider Threat research program located at West Point. A West Point alumnus ('96—For Freedom We Risk!), Jon served the Army as a military policeman (Army Provost Marshal in Okinawa, Japan), Operations Research Analyst (Chief of Operational Assessments at Fort Drum and Afghanistan), and Network Scientist (Director of West Point's Network Science Center).

.....

The West Point Insider Threat Program was activated in 2020 when leaders in the United States Department of Defense's Undersecretary of Intelligence and Security and U.S. Army Protection Directorate recognized a gap in our enterprise's theoretical and research understanding of insider threat. Insider activity that maliciously or accidentally reduces organizational efficacy has been a threat since the dawn of human organizations. This is not news. Over time, it was recognized that DoD organizations have been so busy operating that we did not have a resident capability to understand the problem in the abstract and connect theory to practice.

That the study of insider threat—and insider risk—are interdisciplinary is also not news. This community understands that if one field believes it has the answers, those practitioners do not understand the problem. West Point (and specifically, the United States Military Academy) provides a unique set of capabilities that address the gap identified in an interdisciplinary manner. Resident at USMA are approximately 50 academic departments, research centers, and programs that span every domain from STEM to humanities, quantitative to qualitative, operational to theoretical, pragmatic to ethical, and more. It is a natural fit for an organic capability that enhances the discussion of an important topic.

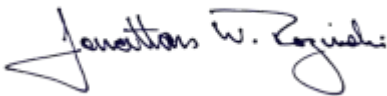
So, how can we make all of this happen? The words interdisciplinary, multidisciplinary, complication, complexity, and chaos (in the mathematical sense) all fit the ideas behind insider risk, insider threat, and organizational resilience. As a decades-long rugby player,

coach, and mentor, I see striking parallels between our operational, academic, and research endeavors with the game of rugby...which is often referred to as “organized chaos.” There is an underlying structure to rugby (albeit not always apparent), just as there is to corporate and military operations. The rugby team is comprised of 15 players that all look different and have different roles on the pitch. Those different players must come together and rely on each other to do their job. The adversary is always looking for a gap or seam exploit and gain territory or burst through the line to cause your team to retreat and attempt to re-organize while the adversary continues to leverage their advantage.

In the best rugby teams, you find a cohesive group of men or women with a common understanding of the mission at any place on the pitch. They count on the player to the left and right to do their job. There is smooth execution resulting from connection and vision that extends through each of the players, across the pitch. So, it is with organizational culture as well as the research and practice of insider-oriented research and practice. To be most impactful, we must synchronize the different disciplines across our enterprises toward a shared vision to protect and foster resilience in our people and institutions.

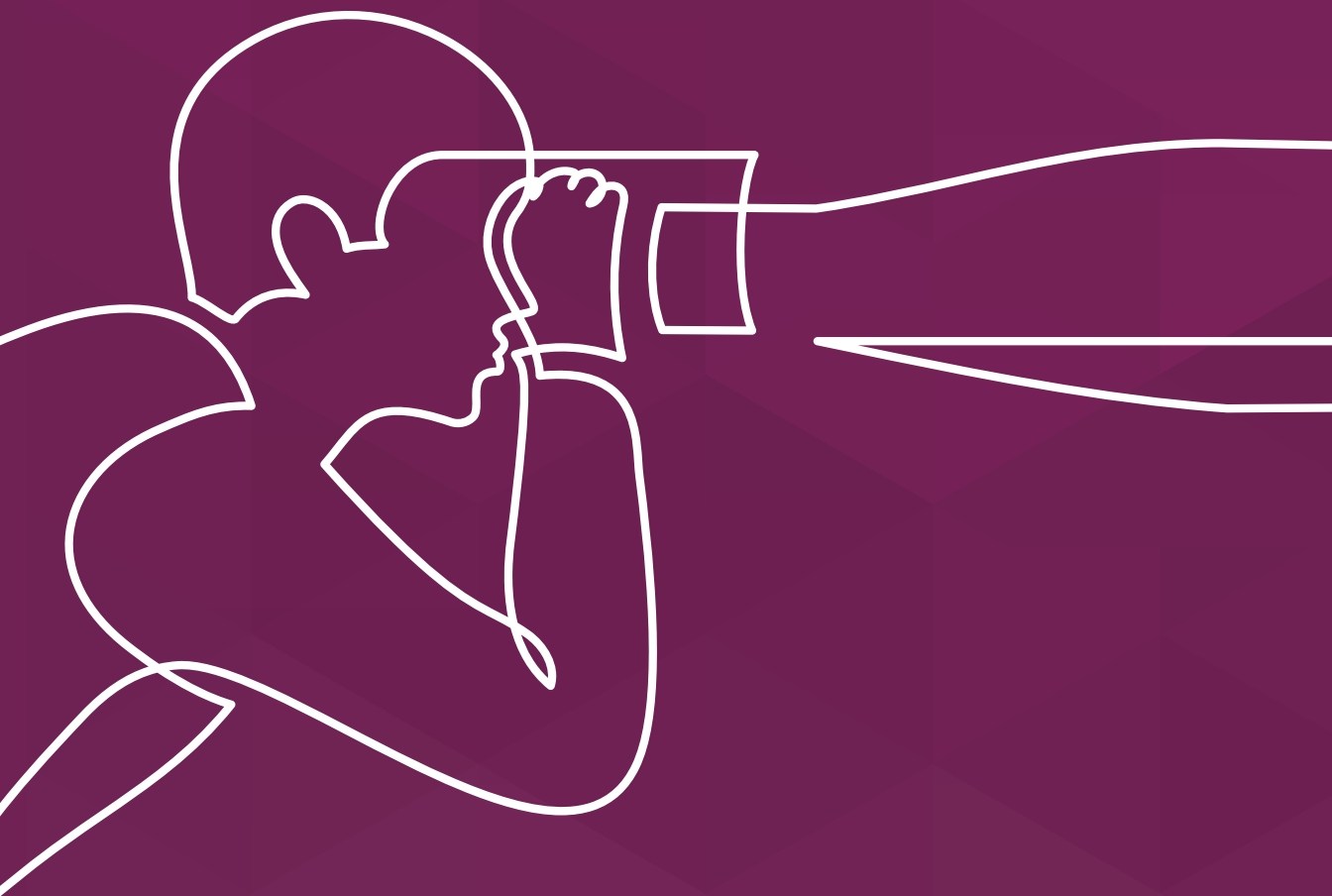
It was to this end that we conceived and launched *The MIRROR Journal* to bring together a variety of viewpoints from as diverse an audience as we could manage to advance the discussion of insider risk and organizational resilience.

In our first issue, you will find senior leader perspectives from the DoD and industry. We have research articles from the DoD, academia and law enforcement, and case studies and professional commentary from industry and law enforcement. We hope you find this topic and writing worth reading...and may want to contribute your thoughts to the journal or our blog. Thank you once again for your time and interest—enjoy!✓



**LTC (ret) Jonathan W. Roginski, Ph.D.**

Program Manager, Insider Threat  
jonathan.roginski@westpoint.edu



**SENIOR  
LEADER  
PERSPECTIVES**







# Bystander Engagement

---

**Lewis R. Call**

**T**he power of the Department of Defense’s (DoD) Insider Threat Program resides in every individual in the DoD and their willingness to take action to help a friend, co-worker, supervisor, or family member in need. This requires us all to be aware, know whom to communicate with, understand which avenues for assistance are available, and take action.

How many times have we seen a change in the behavior of someone close to us over the course of a day, a week, or a month? What if that person was suddenly no longer at their desk or, worse, in trouble? What a terrible feeling. What could have been done to help?

The first preventative measure is to be aware of changes of behavior in your environment. Is that person next to you acting differently than usual? Is this behavior recent or lingering? Are you aware of any changes in their life? Don’t keep this information to yourself. We often don’t tell anyone when we notice a change in behavior because we feel we are telling on a friend. However, people often struggle in silence and only those closest to them can detect the behavior changes and act. If you don’t know whom to talk to, ask a co-worker, a supervisor, or a chaplain for support, but don’t keep it to yourself.



**This requires us all to be aware, know whom to communicate with, understand which avenues for assistance are available, and take action.**





**LEWIS R. CALL**

Mr. Call served in various Air Force intelligence roles for 25 years, including Operations Superintendent, deployment in support of Operation Iraqi Freedom (OIF), and SRA International as a Senior Systems Analyst. Since transitioning to civilian government employment in 2009, Mr. Call has served as Deputy Director, ISR and Special Communications; Deputy Director, SIGINT ISR Programs; Integration Branch Chief, and Deputy Director, DoD Insider Threat Program, where he has been since 2015. Mr. Call holds a Bachelor of Science in Business and Technical Management from the University of Maryland, a Master's Degree in Human Resource and Personnel Management from Central Michigan University, and a Master of Science Degree in Strategic Intelligence from the National Intelligence University. Mr. Call is a 2021 Harvard Kennedy School National Security Fellow. He completed the George Washington University Elliot School of International Affairs, National Security Studies Program, Senior Manager Course. Mr. Call was awarded DAWIA level III Certification in Program Management and completed the Federal Executive Institute, Leadership for a Democratic Society.

.....

Second, learn about the Employee Assistance Programs (EAP) that are available, not only for those around you but for yourself and your family. EAP services provide counseling and referrals for many services to employees with personal and/or work-related concerns, such as stress, financial and legal issues, family problems, office conflicts, and alcohol and substance use disorders. Know them, use them. They are there for you.

Finally, stay up to date with resources. New programs are being developed to assist in supporting you and your coworkers. In the near future, Prevention, Assistance, and Response Coordinators will be at every installation providing training and guidance on how to deal with uncomfortable situations. A hotline is also being established that will allow for anonymous communication about behaviors of concern. Each September, National Insider Threat Awareness Month brings new resources to support your engagement and raise your awareness of these issues.

Don't just be a bystander; be an informed and engaged upstander. Be the person who intervenes because they understand a personal situation can sometimes be harmful or dangerous to everyone. ✓





“

Don't just be a bystander; be an informed and engaged upstander. Be the person who intervenes because they understand a personal situation can sometimes be harmful or dangerous to everyone.

.....

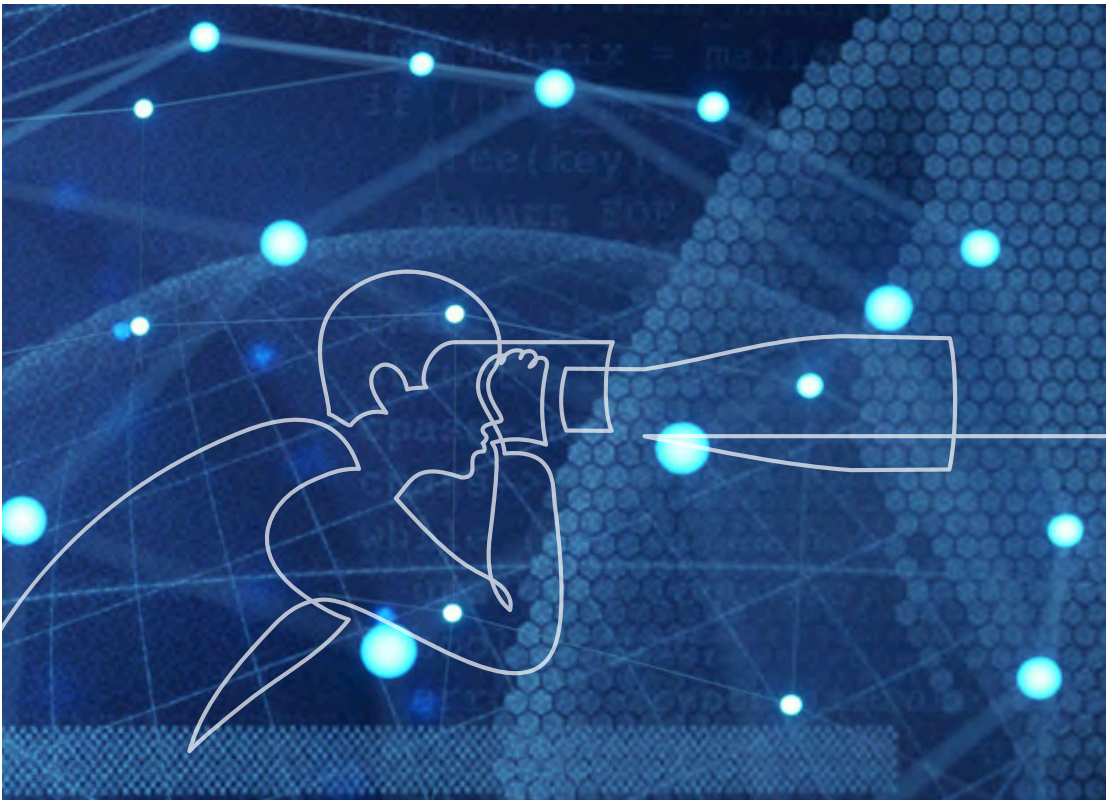


# Adapt or Die: Building Internal Intelligence Networks to Combat Modern Insider Threats

---

**Savannah Grace Clemente**

**Nik Seetharaman**



**I**nsider threat professionals across Western governments, industry, and academia face a reckoning. As near-peer adversaries continue to target wide swathes of American innovation, industry, and government, a generation of tech-savvy millennials have joined the workforce with the



**GRACE CLEMENTE**

Grace Clemente is Senior Director of Insider Threat and Counterintelligence at Anduril Industries, a multinational defense technology startup that provides advanced weapons systems for the United States and its Allies. Since joining Anduril in January 2021, she has built and expanded Anduril's insider threat and CI programs stateside and globally. Previously, Grace worked at Space Exploration Technologies (SpaceX) for 6 years, where she architected the Insider Threat & Counterintelligence Programs in preparation for crewed launches of SpaceX's Dragon capsule and other advanced space vehicles.



ability to exfiltrate unprecedented amounts of data with a few swipes of the finger. This generation no longer solely betray a company or country for a political cause or because they were indoctrinated with foreign ideology. Oftentimes, motives are as frivolous as ego-boosting Internet upvotes, a contributing factor in the recent Teixeira leaks. Consider that for many of us; an insider threat incident could mean loss of human life, businesses destroyed, or ultimately, in the case of Western democracies, forfeiture of technological or military dominance to autocratic adversaries. These are existential-scale problems, and they require innovative solutions from bold practitioners.

Insider threat programs must not only contend with all of these emerging risks, but they must do so while staying abreast of rapidly changing tactics, techniques, and procedures. Dead drops in parks outside of Washington DC have been supplanted by covert digital exfiltration methods, Discord, Reddit, and dark web forums where foreign intelligence agents patiently lie in wait to elicit secrets.

Combating these threats requires architecting 360-degree views of an enterprise, its personnel, and the ways in which nefarious external entities may seek to manipulate them. No longer is it enough to deploy point solutions like data loss prevention tools or point-in-time background checks. Detecting an employee printing a sensitive document or transferring files to removable media, without necessary context, yields a small preview into what may be at play. Perhaps that same individual was in recent email contact with a sponsor from a foreign talents



NIK SEETHARAMAN

Nik Seetharaman is CIO at Anduril Industries, where he stood up the cybersecurity and product security programs as the company's first security engineer. Nik previously built the cybersecurity operations function at SpaceX and served as the Cybersecurity Lead for APAC and EMEA for Palantir Technologies. Prior to working in the private sector, Nik spent 11 years in the United States Air Force where he served as a Special Operations Aviator and Special Reconnaissance team lead attached to Naval Special Warfare Development Group.



program or recently informed HR that they were planning to start a competing company overseas or are in contact with a disgruntled former employee who requested copies of sensitive files. Context reigns supreme, and context requires data that is unified and synthesized.

“  
Context reigns supreme, and context requires data that is unified and synthesized.  
.....”

Insider threat leaders must build partnerships and break down data silos across their parent organizations to construct “internal intelligence networks” that produce holistic, dynamic pictures of behavior and risk across vast spans of time. Human resources files regarding performance concerns, travel system itineraries, badge records, external intelligence feeds, engineering database logs, and endpoint telemetry from cybersecurity tools must all be fused together to form a synthesized view of behavioral anomalies. We can leverage existing cybersecurity tooling, such as Security Information and Event Management (SIEM) platforms to bring these disparate data points together and alert near-instantaneously on concerning activity. These anomaly detections must be tuned and adapted continuously over time, complimented by open-source intelligence and counterintelligence indicators from law enforcement and other government partners. Such data sharing models are critical to staying ahead of the adversary, regardless of one's operating environment.

## ADAPT OR DIE: BUILDING INTERNAL INTELLIGENCE NETWORKS

---

Building these programs is difficult work, but it can be done. It requires time, patience, navigating politics, and stepping outside traditional comfort zones. It takes leaders who can subordinate their ego, welcomes the necessary data sharing partnerships across departments, and deploy scrappy solutions where needed. Our collective failure to rapidly adapt to the modern nature of insider threats invites catastrophic consequences: erosion of the United States and Allied technological and military dominance, loss of human life, and, ultimately, the ceding of global power to authoritarian regimes. How will we, as leaders, rise to the occasion? ✓





“

Building these programs is difficult work, but it can be done. It requires time, patience, navigating politics, and stepping outside traditional comfort zones.

.....





# Complexity: Leveraging Data While Being Human Centric

---

**Chris Hagner**

**I**t is crucial to identify and mitigate insider risks within our organizations; however, there are two persistent challenges:

1. Leveraging ever more complex and disparate data sources for the mission.
2. Balancing this information system-driven approach with the human elements of our organization.

A holistic information system that can identify insider threat risks based on known data about our people and their actions addresses the first challenge. This is crucial because the technologies that make our people more productive and effective can also be used to damage an organization at a significant cost. Like most complex operational environments, there are not enough analysts to stay on top of the myriad of emerging threats. An information system capable of supporting analysis and the decision-making process is one option that can competently scale and keep pace with evolving risks.

Our industry must push beyond the ‘low-hanging fruit’ of cyber data to effectively counter insider threats. These data streams are (relatively) clean

and structured. Thus, they can be straightforward to exploit for the mission. However, they often lack the real context needed to address the bigger picture, which is required for our monitoring and investigations. That context likely



**Despite our massive technological advances, the need for human centered design is not to be overlooked.**

---



**CHRIS HAGNER**

Chris Hagner is a CTO at LMI focused on their Intel practice. He has served the national security community for over two decades. With expertise in big data, high-performance computing, cloud architectures, and cybersecurity, he brings a practical and mission-oriented approach to his customers' challenges. Before LMI, Chris was a managing director at Accenture Federal Services through its acquisition of Novetta in 2021. As a member of Novetta's executive team, his roles ranged from running a division of hundreds of employees to leading a diverse portfolio of software products.



comes from bringing in data from other domains, and this is the hard work ahead of us. Non-cyber domains (e.g., social media, email, and other behavioral sources) are inordinately messy yet rich with signals and context. Tackling these challenges and utilizing other data sources for our insider risk mission is the smart way forward—not because it's straight-forward or that we're sure to succeed quickly, but because determining how to exploit these messy domains is the best preparation for the next generation of data sources, which will likely be even more complicated and offer greater value.

I'm deeply optimistic that our organizations are up for the first challenge, even if the journey is opaque and ongoing. However, we still must keep our eye on the second challenge: implementing an information system-driven approach while centering the human elements of our organization. As technology changes so quickly, it's easy to overlook the human side of the organization. This integration is one of the most critical design elements in any system.

Central to our thinking must be the question, "How do we ensure that the human stays at the center of our design?" For example, while OpenAI's ChatGPT is the definition of a 'black box,' when Microsoft released Bing Chat, powered by OpenAI's GPT-4, it offered the advantage of providing web links to documents used in its responses, which ChatGPT lacked. This is a perfect example of a relatively small feature fundamentally shifting how value and trust in a system are experienced by human users. Despite our massive technological advances, the need for human centered design is not to be overlooked.



“  
An information system capable of supporting analysis and the decision-making process is one option that can competently scale and keep pace with evolving risks.  
.....

Furthermore, organizations have been countering insider risk well before we had abundant computing resources at our disposal. There's real potential that our obsession with ever-evolving information systems will downplay the assets and strengths foundational to a healthy organization. These assets are the people in the organization. Thus, the use of new technologies needs to be deployed with an eye for how they impact our foundation. In the most extreme case, our reliance on technical wizardry can overshadow the need for a strong, healthy, and mission-focused culture. If that happens, our organizations will be fundamentally weakened and less effective.

We need to do the hard work and push for integrating domain data that is far beyond our typical 'low-hanging fruit.' Let's push these boundaries for the context they bring to our investigations and for the possibility of even more exciting data streams in the future. As we do this work, let's keep the human in the center of our designs. As we roll out new technical capabilities, let's be mindful of and alert to how they impact our culture and the people within our organizations. ✓



# PROFESSIONAL COMMENTARY







# Red Flags Reimagined: A Former CIA Operations Officer on Today's Insider Risk Challenge

---

Val LeTellier



**T**he last few years have been particularly challenging for insider risk professionals. Remote work creates new attack vectors and makes employee assessment harder. The 'Great Resignation' overburdened offboarding processes and fueled the 'Great Exfiltration' of intellectual



Val LeTellier ran security, intelligence, and counterintelligence operations as a State Department Diplomatic Security Special Agent and CIA operations officer. Twenty years of penetrating foreign intelligence targets and recruiting sources gave him an intimate understanding of the psychology of insiders. Following government service, he co-founded a cyber security firm that combined CIA HUMINT and NSA technical expertise for insider risk vulnerability assessment and countermeasure design. He has designed, implemented, and overseen insider threat programs for leading private and public sector organizations. He holds an MS in Systems Management from the University of Southern California, an MBA from the Thunderbird School of Global Management, and is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Project Management Professional (PMP), Red Team Thinker (RTT) and CERT Insider Threat Vulnerability Assessor (ITVA).

.....

property. COVID and political divisions are increasing employee stress, distraction, and disenfranchisement. Nation states and criminal groups are getting bolder at recruiting vulnerable employees to steal and ransom data. To borrow from the cybersecurity 'CIA Triad', the *Confidentiality, Integrity, and Availability* of our people, processes, and property are at risk.

As reflected in the increasing number and costs of insider events, traditional countermeasures simply aren't up to the task. Observable indicators are diminished by remote employees being 'out of sight, out of mind'. Unfortunately, network monitoring solutions only go so far, are complicated by remote work, are cyber and log centric, are singularly focused on network anomalies and are generally reactive.

To illustrate our challenge, mentally put yourself in the chair of the insider risk analyst at a large organization; each day begins fresh with the need to somehow identify a few potential bad actors from thousands of employees. But it gets better: you also need to identify potential negligent or accidental insider risk. Further, you also need to balance employee privacy, welfare, morale, organizational culture, and possibly even a trusted workforce and zero trust strategies. The stakes are high: the consequences of a single malicious insider act can ruin your day, your year, and your organization. It's a high-wire act. And none of these challenges are going away.

But let me share something I learned after recruiting a dozen or so insiders (sources) overseas. I realized that many of my targets had either consciously or subconsciously



The stakes are high: the consequences of a single malicious insider act can ruin your day, your year, and your organization. It's a high-wire act. And none of these challenges are going away.



determined they would do anything to better their situation. Doing anything included giving me sensitive information and betraying their country. Meaning, they were predisposed toward recruitment. They had already decided what they would do if presented with the right scenario. I only needed to be

at the right place, at the right time, and with the right pitch. Knowing that, I started looking beyond standard motivations and vulnerabilities and focused on the telltale signs of predisposition, waiting for critical events that would move my target to action. Using insider threat terminology, I was looking for key indicators early on the critical path.

## Early Warning

Let's leverage this offensive tradecraft to inform our defense and examine early warning, arguably the most critical element of insider risk mitigation, but often also the most neglected. Why? Because it's hard and complex.

To quote Marty Byrde from the television series *Ozark*,



*As individuals, people are completely unpredictable. One person making one bet, I couldn't possibly tell you what they're going to do. But the law of large numbers tells me that a million people making a million bets - that is completely predictable -completely ordered.*

So, apply that to our challenge. Insiders are individuals, but hundreds of them tell a story. The same 'root causes' of personality predisposition and critical events tend to result in harmful action (albeit in different forms: theft, sabotage, violence, etc.), providing the opportunity to intercept a budding insider along the critical path before an incident occurs.

But we don't maximize that opportunity, failing to see what's right in front of us. The reasons are the lack of critical resources as well as the cultures, biases, and assumptions of organizations. To complicate matters further, moving to remote work is particularly detrimental: behavioral observation is

a leading way to discover malicious insiders. With many workers now only observed through the limited aperture of a computer screen, this countermeasure is largely lost.

## **Enough admiring the problem. What can we do about it?**

Remember the analyst looking at thousands of employees, trying to help create a trusted workforce? What would help them? Quite simply, the automated identification of a limited number of at-risk employees that require a closer look. But how do we accomplish this?

One way is by leveraging the advances of technology. Klaus Schwab of the World Economic Forum predicted that the Fourth Industrial Revolution would bring the “fusion of our physical, digital, and biological identities.” This is happening, and we see it every day in our lives and in the news. Data analytics connect dots that once took weeks to link if they could be linked at all. This fusion enables multiple surfaces to track, assess, and even predict behavior in real-time. The implication is significant for the government and corporate security officials; new mechanisms and methodologies are available to identify and mitigate risk.

For insider risk professionals, this algorithmic-fueled fusion can quickly highlight individuals and areas of concern.

- We can run behavioral, network, access, public data, and other feeds through link analysis and machine learning.
- We can identify and sort indicators into risk models that enable holistic continuous evaluation and zero-trust governance.
- We can create tailored, advanced predictive analyses of thousands of employees in a few minutes. Simply put, we can make insider risk mitigation smarter, faster, and more proactive.

And, most importantly:

- We can create a ‘decision advantage’ for analysts and program managers.
- We can highlight employees requiring analyst review.

In the intelligence world, we call that ‘tipping and cueing.’ But how do we create this decision advantage?

Let me propose five connected concepts. The first two create the right environment, and the last three create the right process.



“  
We need to be transparent in the program methods, processes, and goals. We need to show how we use anonymization, masking, generalization, and encryption to protect privacy.  
.....”

### Right environment #1: Balance

To create the right environment, you need balance. Your program must run that fine line between the risk mitigation you need, the employee welfare you seek, and the employee privacy you must protect.

But as important as ‘decision advantage’ is to a program, it can’t be at the expense of trust. And privacy and trust are symbiotic. So, while we’ve all surrendered varying degrees of our digital privacy to ‘surveillance capitalism’, we need to be understanding when employees aren’t welcoming of our use of that volunteered public data.

We need to be transparent in the program methods, processes, and goals. We need to show how we use anonymization, masking, generalization, and encryption to protect privacy. Importantly, we need to evolve our marketing alongside our methodology and make insider risk mitigation less about threat reduction and more about employee welfare.

### Right environment #2: Organization Buy-in

Leadership and employee buy-in not just to the *end goal*—but also to the *necessary means* to accomplish that goal. So, take a moment and examine your program—or one you know—through the eyes of employees. How does it look? If this makes you uncomfortable, you have work to do.

As stated, the goal is to create a positive security culture. You should show that the program provides early warning of employees who may need assistance. And then, actually, deliver that assistance. In doing so, the program will start being viewed as positive rather than punitive, with increased buy-in at all levels.

### **Right process #1: Holistic approach**

A holistic approach is critical. It should take into consideration the individual *and* their mental, emotional, financial, physical, virtual, and chronological state. Specifically, a “whole person” and ‘whole threat’ approach.

To me, ‘whole person’ is contextual and psychosocial, using personality, environment, and precipitating events to identify risk. ‘Whole threat’ addresses the common root causes that result in different forms of attacks (data theft, fraud, sabotage, violence) across all domains (cyber, human, and physical),

Combined, the whole person and threat approach focuses an organization’s limited resources on its most sensitive holdings: the insider personalities meriting greatest concern, the precipitating events that can turn those personalities into harmful actors, and the corresponding indicators highlighting the need for closer inspection.

### **Right process #2: Right data**

To quote former Hewlett Packard CEO Carly Fiorina, “The goal is to turn data into information and information into insight.’ But first, you need the data. And the better the data, the better the analysis, and the more accurate the risk scoring.

To get the best data, we need refined research and an understanding of which indicators are statistically proven against the progression of different insider types along the critical path. We need behavioral psychologists, insider risk analysts, and data scientists to help us find the right combinations of data capable of highlighting the disparate indicators taken from thousands of cases.

### **Right process #3: Advanced risk modeling**

By applying a holistic approach with the right data, you can conduct advanced risk modeling.

This is where the ‘magic’ happens; this is where a ‘digital twin’ is created. This is where we get into the head of the insider and understand what sets them off, and how they would plan and act.

This is where advanced analytics and fusion technologies eliminate the spaces between data points. By using a tailored suite of algorithms and

machine-learned analysis that churns through internal and public records and live sensor feeds, we can continuously develop employee risk scores that allow ‘risk triage’ of large employee populations and a manageable number of cases for analyst attention.

But to do this efficiently and effectively, we need to understand the insider profiles most relevant to our organizations. We need to understand their personality characteristics and develop and automate a watchlist of the most relevant tripwires.

## Conclusion

To summarize, this has always been a high-stakes game—even before China’s ‘Thousand Talents’ program and the rise of ransomware. More so now than ever, we need strong and modern insider risk tradecraft. We need to harness modern technology to create proactive continuous evaluation that enables early engagement of at-risk employees, remediation of toxic situations, and preemption of costly and life-threatening incidents. If done correctly, this can also promote a positive security culture, reduce employee attrition, and increase organizational morale. ✓

“

We need to harness modern technology to create proactive continuous evaluation that enables early engagement of at-risk employees, remediation of toxic situations, and preemption of costly and life-threatening incidents.

.....

## Putting Theory into Practice

To illustrate how this would work, we can examine each major insider threat actor



### The Negligent

Common personality characteristics include flighty, unfocused, disorganized, scatter-brained, stressed, and strained. So, we need to watch internal and external data for indications of common precipitating events such as new personal or professional distractions.

We may see this manifested in internal data (HR, security, IT) that shows personal cell phone/computer overuse, an unwitting provision of sensitive information to outsiders, discussion of sensitive matters with uncleared personnel, sensitive documents or devices left accessible to others, consistent failure to meet deadlines, etc.

Public data may highlight the distraction: law enforcement or legal cases, social media conflict, or posting of confidential organizational details to social media sites.



### The Intellectual Property/ Sensitive Data Thief

Common personality characteristics include entitlement, narcissism, anti-social tendencies, and controlling behavior. Therefore, we look at internal data for common precipitating events: failed promotion attempt, poor performance review, unmet career aspirations, resignations/terminations, etc. We look at internal data for common tripwires: "borrowing" office items for home use, attempted privilege escalation, questionable downloads, cyber security policy violations, anomalous data transfers and/or printing, or use of unauthorized recording equipment. We also looked at public data for indicators: negative personal financial events, costly legal issues, and arrests (particularly for computer fraud).



### The Violent or Self-Harmer

Common personality characteristics include aggression, emotional detachment, behavior that is confrontational, control-seeking, disengaged, or unremorseful, and strained thoughts and actions. Common precipitating events include negative personal, family, or relationship events. We watch for internal data highlighting: emotional outbursts, failure to communicate, failure to work in groups or with specific individuals, bullying, difficulty taking criticism, violating boundaries, threatening violence, or physical altercations; we can also watch for public data on reflections of extremist beliefs, membership in extremist groups, and so forth..







### The Saboteur

Common personality characteristics include anger, vengefulness, vindictiveness, disengagement, or destruction. So, we're looking at internal data that highlight relevant precipitating events like confrontation with management, a poor performance review, failed attempts to win promotion, demotion, workplace embarrassment, or termination. Internal data that highlights tripwires include testing security procedures, defacing company website pages, "accidentally" breaking a component in a critical machine, altering enterprise software, misconfiguring products to cause failure, unmerited complaints to supervisors, and computer hacking. We examine external data highlighting law enforcement and/or legal cases related to property destruction, vandalism, defacement, assault, road rage, etc., and public-facing social media postings promoting the destruction of property.



### The Fraudster

Common personality characteristics include egoism, entitlement, privilege, and self-importance. We look for common precipitating events: significant additional expenses, an adverse personal financial event, and unmet career aspirations. Internal data that may highlight potential indicators include violating enterprise policy, using an enterprise server inappropriately, influencing a supplier for personal gain, reporting minor fraudulent expenses, insider trading, demonstrating excessive control over financial duties, or exhibiting shrewd or unscrupulous behavior. Public data may also reveal bankruptcy, debt collection, legal issues, unusually close association with a vendor, and arrests for financial issues..





# RESEARCH ARTICLES

---



# Advancing an Organizational Health Perspective for Insider Threat Prevention and Management

---

**Tin L. Nguyen**

**Matthew T. Allen**

**Kat Parsons**



**M**alicious insiders pose a serious risk to valued organizational assets, including proprietary information, institutional processes, personnel, finances, reputation, and firm connections. Research-based solutions for predicting, detecting, and mitigating insider threats



DR. TIN NGUYEN

Dr. Tin Nguyen is a Senior Research Associate at the National Counterterrorism Innovation, Technology, and Education Center (NCITE) and the collaboration instructor for USSTRATCOM's Strategic Leadership Fellows Program. His research focuses on innovation management and novel threats. His work has been supported by the Department of Homeland Security, and he has eight years of experience consulting for teams and organizations across the United States.



have focused heavily on individual, organizational, and cyber risk factors (Kont et al. 2015; Greitzer et al. 2018). To that end, scholars have increasingly recognized that people's personalities, motivations, grievances, and work stressors raise the risk of insider threat events, and the corresponding intervention-al strategies involve cybersecurity and work design practices to safeguard the organization against human error and deviance (Homoliak et al. 2019; Greitzer et al. 2013; Maasberg, Warren, and Beebe 2015). Yet, despite evidence that insider threat events are perpetrated by people situated within a social and organizational context, discussions of insider threat have only started to recognize the importance of socio-organizational protective factors for reducing the occurrence of insider threats (Moore, Gardner, and Rousseau 2022; Whitty 2021). We argue that a healthy organization—an organization whose people, practices, and policies effectively sustain its survival and performance—may be key to preventing and managing insider threats.



**A healthy organization—an organization whose people, practices, and policies effectively sustain its survival and performance—may be key to preventing and managing insider threats.**





DR. MATTHEW T. ALLEN

Dr. Matt Allen is an Assistant Professor of Management in the College of Business Administration and on NCITE's executive team at the University of Nebraska Omaha (UNO). He has over 15 years of experience as an industrial and organizational (I/O) psychology consultant, professor, and manager specializing in applied research and implementation of evidence-based solutions.

.....

The inner workings of an organization contain a blend of formalized elements such as policies, practices, values statements, and job roles, along with informal social norms established by organization members (McEvily, Soda, and Tortoriello 2014). Often, people's work behaviors are shaped by the way they view and react to these organizational attributes. For example, when people receive fair treatment, meaningful duties, and social belonging at work (i.e., drivers of organizational health), they are more inclined to internalize organizational values, align their efforts with organizational goals, and hold each other accountable in that process (Littman-Ovadia and Lavy 2016; Holtz and Harold 2013; Chiaburu and Harrison 2008). In contrast, deprivation of meaning, equitable treatment, and belongingness can push people to undermine organizational interests (Mackey et al. 2021; Priesemuth, Arnaud, and Schminke 2013; Kelloway et al. 2010), in minor (Lim, Cortina, and Magley 2008) or extreme ways (Elamroussi 2022; White 2021). Organizational practices and social work environments that support employee interests therefore serve a protective role against deviant insider activity by laying the foundation for organizations to adaptively address and mitigate identified threats. Applying lessons from organizational psychology and political violence research, we discuss how a layered (i.e., multilevel) approach to organizational health can reduce the risk of insider threats. We then conclude with implications and recommendations for insider threat response and risk management.



DR. KAT PARSON

Dr. Kat Parsons is a Research Specialist at NCITE. She handles a range of research and project management duties for NCITE's threat assessment and targeted violence prevention efforts. Her research examines the variable link between support for political extremism, violence, and engagement in violence, with a particular focus on the impact of violent rhetoric in the U.S. and beyond.

.....

## Organizational Health as an Insider Threat Deterrence Strategy

Organizational health refers to an organization's state of functioning that supports the work and well-being of its members. Much in the way that physical and mental health equips people with the vitality to fulfill their interests and goals, organizational health reflects the formal and informal work conditions that support employees' satisfaction, motivation, and sustained performance (Miller, Griffin, and Hart 1999). Accordingly, our organizational health perspective contends that people will choose citizenship over deviance when they believe that their work structures and social climates enhance, rather than diminish, their ability and willingness to work (Moore, Gardner, and Rousseau 2022; Fox, Spector, and Miles 2001). The extent that people feel that they have valued membership and support in the organization corresponds with their motivation to threaten organizational assets (Mackey et al. 2021). To that end, we summarize two pathways to keeping organization members content, committed, and engaged in their work lives. Namely, organizations should first (a) grant entry to the right people and then (b) ensure that those people feel supported by the policies, practices, and peers in their workplace. For these two pathways to organizational health, we share organization, job, and social factors that deter insiders from causing intentional harm to an organization and its people.



## Hiring the Right People

Sound employee hiring practices are an essential component of a healthy, well-functioning organization. Recruiting and selecting for people who share in the organization's values, have skills to meet job demands, and get along with current employees has been shown to benefit work-related outcomes such as retention, performance, and reduced counterproductive activity. Simply put, finding the right people for the organization, its jobs, and its people reduce the likelihood of insider threat events.

**Person-organization fit.** When seeking employment, people look to a variety of sources (e.g., personal and professional networks, employer websites, employment review websites) to understand the culture, practices, and broader identity of a future employer, with the intention of assessing whether they would belong and be satisfied in the workplace. Often, prospective job candidates hope to pinpoint an organization's "personality," seeking to uncover information about its warmth (i.e., values, trustworthiness, likability) and competence (i.e., prestige, performance excellence) (Zhu et al. 2021). This information search process enables people to identify whether they fit with an organization's values, mission, capabilities, and performance objectives. Assessing person-organization fit is mutually beneficial to the job candidate and the employer, as well-matched interests and goals help employees identify with the organization and aim to contribute to its pursuits. In turn, this reduces the likelihood that employees will detach from organizational objectives and attempt to sow internal disruption. (Harold et al. 2016) Crafting recruitment messaging to clearly showcase organizational values and missions will provide higher-fidelity information to attract better-fitting job candidates. Further, recruitment efforts targeted at qualified populations whose values align with the organization (e.g., LinkedIn, college campus recruiting, professional recommendations) can limit the chances of hiring newcomers that may cause harm to the organization or its constituents (Breagh 2013).

**Person-job fit.** Job seekers also want to find job roles to fit their skillsets, provide meaningful work, and have the opportunity for growth. Thus, employers must strike a fine balance in setting high, yet reasonable job expectations

“

Simply put,  
finding the right  
people for the  
organization,  
its jobs, and its  
people reduce the  
likelihood of insider  
threat events.

.....

for potential hires. During the job search process, organizations should write job descriptions that clearly and accurately list job demands, required skill-sets, work resources, and promotion opportunities. Outlining a realistic job preview for job seekers makes it simpler and more efficient for potential candidates and future employers to evaluate a person's fit for a job role (Breugh 2013). Without accurately representing job roles, resources, and future opportunities, the organization will run the risk of hiring someone who may be under- or over-qualified for a job. In such cases, newcomers to the organization can eventually lose job satisfaction and commitment, withdraw from their work duties, and deliberately undermine organizational interests either in protest to excessive job demands or boredom from a lack of work challenges (Harold et al. 2016; Podsakoff, LePine, and LePine 2007). Person-job fit can thus lessen the occurrence of insider threats from disgruntled employees.

**Person-group fit.** In addition to fit with the organization and job duties, fitting in socially with current employees also serves as a protective factor against insider threat. Prospective job candidates often gravitate to workplaces where they share similarities with current employees (Devendorf and Highhouse 2008). Moreover, fit with potential work group members has been linked to lower instances of counterproductive work behaviors (Harold et al. 2016), suggesting that hiring people who would get along with other employees would deter deviance given the lower chance of social exclusion.

## Providing Worker Support and Ethical Guidance

Once employees have gained entry into the organization, it is vital that they feel a continued sense of support by the organization and its members. Supportive workplace practices and personnel are essential to employee well-being and performance (Caesens et al. 2017; Meyers et al. 2019), and as such, are core drivers of organizational health. Furthermore, treating employees fairly, equipping them with resources to do good work, and building camaraderie among workers can minimize frustration and harmful insider behaviors (Mackey et al. 2021). These factors are important for deterring minor forms of deviance and aggression, but evidence from political violence suggests that these protective factors may also decrease the risk of radical and violent behavior (Wolfowicz et al. 2020). That is, supporting workers' efforts and well-being prevents organizational and social grievances from forming, and as a result safeguards organizations against potentially devastating acts by insiders.

**Organizational support.** Organizational support for workers is reflected in the policies, practices, and resources that enable employees to perform their



work while supporting their mental and physical health, and has been shown to increase work performance and citizenship (i.e., above-and-beyond) behaviors, as well as lower counterproductive work behaviors (Kurtessis et al. 2017). Employee perceptions of organizational support tend to come from equitable organizational policies and practices (Moorman, Blakely, and Niehoff 1998), meaning that prioritizing fairness makes employees feel appreciated and cared for. Just treatment at work broadly entails receiving the necessary training and tools to meet the demands of one's job, experiencing dignified treatment from management, and an awareness that organizational policies are applied consistently over time and across employees (Greenberg 1987; Colquitt 2001).

A few examples of fair policies and practices include transparent reward structures that reasonably correspond with employees' work contributions, equitable access to professional development opportunities for all personnel, and justly distributing material resources across work units to support job-related tasks. In response to fairness in the organization's formal structures, people tend to feel that they hold valued membership in an organization, feel more satisfied in their roles, are more mentally well, and are consequently less likely to impose harm on the organization itself (Spell and Arnold 2007; Kurtessis et al. 2017; Priesemuth, Arnaud, and Schminke 2013). Hence, organizational policies and practices that are seen as supportive and just can improve worker performance and well-being while curtailing motives to transgress against the organization (Fox, Spector, and Miles 2001).

**Job design.** Work design poses a continual challenge to organizations. Whereas expecting too much of employees can result in job stress, dissatisfaction, burnout, and retaliation (Meier and Spector 2013; Fox, Spector, and Miles 2001), demanding too little can also result in frustration and misbehavior in high performers who feel unchallenged (Harold et al. 2016). As such, work stressors should challenge people in their roles without hindering their well-being and performance (Podsakoff, LePine, and LePine 2007). Creating manageable workloads or supplying essential work resources may reduce the stress on workers who experience excessive strain from their jobs. On the other end of the work design problem, to combat counterproductive activity from unfulfilled workers, designing jobs with a variety of tasks can enrich people's work experiences (Morf, Feierabend, and Staffelbach 2017; Grant 2007). Another way to increase work enrichment involves giving workers the autonomy to craft their roles to their strengths and preferences, which can make their work feel more personally meaningful, increase perceived fit with their job roles, and motivate prosocial rather than antisocial behaviors (Grant 2007; Tims, Derks, and Bakker 2016). Taken together, possible remedies to job-related disgruntlement and insider threat may lie in designing jobs with reasonable workloads and resources, assigning a variety of stimulating tasks, and giving workers more ownership over how work is done.

**Leadership and social work environment.** Organizational leaders play an outsized role in shaping healthy organizational cultures (i.e., workplace values, attitudes, norms, artifacts). The formal authority granted to leaders within organizational contexts enables them to influence the behaviors of others through the reward structures they implement and the behaviors they showcase (Klein, Wallis, and Cooke 2013; Sims 2000). Accordingly, research on ethical leadership indicates that leaders can mold followers' ethical behavior through their own ethical conduct (i.e., being honest, trustworthy, and showing concern for others), along with their communication and enforcement of ethical standards to other members of the organization (Brown and Treviño 2006; Mayer et al. 2009). Through observing and imitating leaders' ethical behaviors and reciprocating such treatment to others, ethical norms slowly emerge among workers, which creates a sense of shared ethical accountability that deters employee misconduct and insider threat events (Den Hartog 2015; Mayer, Kuenzi, and Greenbaum 2010). As such, leaders have great responsibility and capability to role model and enforce ethical conduct, as doing so can prevent internal harm to their organization.

Beyond ethical leadership and norms, work and social support from leaders and coworkers can also act as a strong deterrent to destructive insider

behaviors. Leaders who provide clear mission guidance, demonstrate ethical behaviors, and deliver helpful feedback are more likely to motivate their followers to expend high effort toward organizational goals (Chiaburu and Harrison 2008; Shanock and Eisenberger 2006). Peers can also lessen the risk of deviance. Adequate socialization and encouragement from work peers yields higher trust and accountability, consistent knowledge sharing, and increased citizenship behaviors (Adil et al. 2021; Chen and Klimoski 2003). The resource networks and friendships formed at work help people adjust to organizational life by aiding work efforts, building shared identities, and promoting camaraderie among colleagues (Jones 1986). Additionally, positive social connections at work can help people regulate their emotions (Mathieu, Eschleman, and Cheng 2019) and avoid aggressive outbursts (Yan et al. 2014; Mao et al. 2018)—a resource that may be especially valuable if they lack social support outside of work. Considering that social exclusion and ostracism can generate anger, stoke radical intentions (Pfundmair 2019), and culminate in violent behavior (Wolfowicz et al. 2020), organizations would do well to build work cultures and climates that encourage leader and peer empathy, care, and mutual support. Although the creation of a positive social environment begins at the hiring stage, the social milieu must be actively maintained and championed by current members of the organization.

## **Implications and Recommendations for Threat and Risk Management**

Thus far, we have argued that organization, job, and social factors must be considered when seeking to lower insider threat risk through hiring or delivering organizational support to existing employees. Beyond threat deterrence, these organizational health practices also build the foundational capacity to mitigate threats swiftly and effectively. One mechanism by which the organizational health perspective helps to prevent and manage insider threat risk is by enhancing individual and team adaptability. Adaptability refers to the ability to recognize changing circumstances and take action that results in a positive outcome, and is facilitated by well-designed organizational policies and procedures, clearly defined work roles, and social cohesion. More adaptive individuals and teams are more likely to be proactively prepared for potential threat events, and better able to respond when a threat event occurs. Different jobs have different adaptability requirements that vary along dimensions such as (a) emergency or crisis situations, (b) work stress, (c) creative problem solving, and (d) cultural adaptability (Pulakos et al. 2000). Understanding the adaptability requirements of a partic-

ular job, paired with selecting individuals who are a good fit to that job, will help to increase individual adaptability (Dorsey et al. 2017). For example, occupations that require a high degree of cultural adaptability would likely want to hire individuals with a high degree of cultural awareness, flexibility, self-regulation, and interpersonal skills as they are more likely to fit those situations (Abbe, Gulick, and Herman 2007). Following effective organizational health practices have also been found to increase team-level adaptability. For example, supportive work climates that foster feedback and encourage continuous learning have been shown to increase team adaptability (Han and Williams 2008; Burke et al. 2006). Enhanced team adaptability is likely to also enhance team decision-making and performance (Maynard, Kennedy, and Sommer 2015), creating the relationship and trust networks needed to reduce insider threat risk.

Adding to this discussion, our organizational health view of insider threat prevention and management can also benefit from lessons in the targeted violence and terrorism space. In particular, interventions designed for individuals and communities at risk for radicalization can inform efforts to diffuse potential insider threats. Years of deradicalization and countering violent



extremism (CVE) programming iterations have produced knowledge about what constitutes a successful intervention, which can be extended into the organizational context.

- **First.** Interventions that work to build collective engagement are especially effective tools for developing organizational resilience against insider threats. Organization-level engagement can effectively empower organization members to successfully identify warning signs of extreme intentions and build social support networks that reinforce a sense of belonging (Savoia et al. 2020; Williams, Horgan, and Evans 2016). That is not to say that individual-level interventions are ineffective, but rather highlights the robustness of collective measures.
- **Second.** How organizations engage their members to prevent insider threats is also important. For example, informational campaigns designed to challenge violence and educate individuals are most effective when driven by members within the group (Richardson 2014).
- **Third.** Programming designed to bolster individual resilience to extreme ideas and ideologies through self-esteem and empathy-building have also been shown to be effective in reducing attitudes toward violence (Feddes, Mann, and Doosje 2015). This points to the value of mental health services such as employee assistance programs for those who may be inclined to hurt the organization or its people (Baweja, Dunning, and Noonan 2022).
- **Fourth.** A one-to-one messaging campaign on Facebook targeted at individuals who had openly expressed extremist views found that sharing personal stories or offering assistance can counter extremist views more effectively than warning people of personal consequences to such actions (Frenett and Dow 2015). Together, findings from these CVE programs can help inform insider threat and risk management efforts by offering guidelines for collective (i.e., organization-wide) and individual interventions. Thus, organizational health can be further achieved with collective engagement and strategic messaging to at-risk individuals.

## Conclusion

As described previously, insider threat research generally focuses on risk factors, proximal indicators, and threat mitigation strategies. We believe an organizational health perspective will help to better articulate organizational procedures and practices that enhance protective factors in mitigating insider threat risk. This perspective addresses several calls by counter-insider threat researchers and practitioners. For example, the Intelligence and National Se-

curity Alliance's (INSA) Insider Threat Subcommittee recently wrote a report calling for better integration of organizational human resources (HR) functions into counter-insider threat programs ("Human Resources and Insider Threat Mitigation: A Powerful Pairing" 2020). An organizational health perspective provides a shared language for security professionals to discuss objectives and desired outcomes for counter-insider threat programs in concrete terms. Moore, Gardner, and Rousseau (Moore, Gardner, and Rousseau 2022) argue that "positive deterrence" strategies—practices that align employee and company interests—should be considered by insider risk management programs as a complement to traditional "command-and-control" approaches. Practices that increase perceived organizational support and organizational commitment, the authors argue, are particularly effective at mitigating insider threat risk. The organizational health perspective provides a coherent framework to systematically increase outcomes associated with positive deterrence.

This work also complements and extends the recent work of insider threat researchers emphasizing the importance of organizational factors in reducing insider threat risk. Whitty (2021), based on organizational case studies, developed a model of threat prevention and detection. A key part of the model is "closing down opportunities," which includes items such as "improve pre-screening methods," "improve workplace culture," and "improve reporting procedures." The organizational health approach builds upon this work by providing an underlying theoretical framework for describing insider threat prevention programming. Bedford and van der Laan (2021) developed and validated a tool for determining organizational vulnerability to intentional insider threat (OVIT) risk. OVIT is composed of three dimensions—individual, organizational, and technical—with the organizational dimension including factors such as "organizational leadership and culture" and "organizational complacency." The organizational health perspective and associated recommendations provide a framework for increasing scores on a subset of these organizational factors, reducing the risk of intentional insider threat.

In this piece, we have argued that organizational health bolsters insider threat prevention and management efforts. Well-designed organizational infrastructures are fundamental to the well-being and performance of workers, and by extension, are central to an organization's health (i.e., longevity and effectiveness). By hiring those who reasonably fit the values, work, and social environment of the organization, and implementing fair policies and practices that support those personnel upon entry into the organization, employees will stay more intrinsically motivated to act in accordance with organizational



interests rather than against them. Moreover, work-related assistance and social encouragement from leaders and coworkers (often a product of quality hiring and leader role modeling) can promote a sense of social belonging and ethical reciprocity that is essential to deterring deviance. For those reasons, we believe that taking concerted efforts to maintain an organization's health, as is the case with human health, builds immunity and resilience against threats from within. Ensuring the health and performance of an organization and its workers, in other words, can reduce insider threat risks and enhance the organization's adaptive responses to threat events. ✓



“

Practices that increase perceived organizational support and organizational commitment, the authors argue, are particularly effective at mitigating insider threat risk. The organizational health perspective provides a coherent framework to systematically increase outcomes associated with positive deterrence.

.....

REFERENCES

Abbe, Allison, Lisa M. V. Gulick, and Jeff L. Herman. 2007. "Cross-Cultural Competence in Army Leaders: A Conceptual and Empirical Foundation."

Adil, Adnan, Saima Kausar, Sadaf Ameer, Saba Ghayas, and Sultan Shujja. 2021. "Impact of Organizational Socialization on Organizational Citizenship Behavior: Mediating Role of Knowledge Sharing and Role Clarity." *Current Psychology*, May. <https://doi.org/10.1007/s12144-021-01899-x>.

Baweja, Jessica, Madelyn P. Dunning, and Christine Noonan. 2022. "Domestic Extremism: How to Counter Threats Posed to Critical Assets." *Counter-Insider Threat Research and Practice* 1 (1). <https://citrap.scholasticahq.com/article/36185-domestic-extremism-how-to-counter-threats-posed-to-critical-assets>.

Bedford, Justine, and Luke van der Laan. 2021. "Operationalising a Framework for Organisational Vulnerability to Intentional Insider Threat: The OVI as a Valid and Reliable Diagnostic Tool." *Journal of Risk Research* 24 (9): 1180–1203. <https://doi.org/10.1080/13669877.2020.1806910>.

Breaugh, James A. 2013. "Employee Recruitment." *Annual Review of Psychology* 64 (1): 389–416. <https://doi.org/10.1146/annurev-psych-113011-143757>.

Brown, Michael E., and Linda K. Treviño. 2006. "Ethical Leadership: A Review and Future Directions." *The Leadership Quarterly* 17 (6): 595–616. <https://doi.org/10.1016/j.leaqua.2006.10.004>.

Burke, C. Shawn, Kevin C. Stagl, Eduardo Salas, Linda Pierce, and Dana Kendall. 2006. "Understanding Team Adaptation: A Conceptual Analysis and Model." *Journal of Applied Psychology* 91: 1189–1207. <https://doi.org/10.1037/0021-9010.91.6.1189>.

Caesens, Gaëtane, Florence Stinglhamber, Stéphanie Demoulin, and Matthias De Wilde. 2017. "Perceived Organizational Support and Employees' Well-Being: The Mediating Role of Organizational Dehumanization." *European Journal of Work and Organizational Psychology* 26 (4): 527–40. <https://doi.org/10.1080/1359432X.2017.1319817>.

Chen, Gilad, and Richard J. Klimoski. 2003. "The Impact Of Expectations On Newcomer Performance In Teams As Mediated By Work Characteristics, Social Exchanges, And Empowerment." *Academy of Management Journal* 46 (5): 591–607. <https://doi.org/10.5465/30040651>.

Chiaburu, Dan S., and David A. Harrison. 2008. "Do Peers Make the Place? Conceptual Synthesis and Meta-Analysis of Coworker Effects on Perceptions, Attitudes, OCBs, and Performance." *Journal of Applied Psychology* 93: 1082–1103. <https://doi.org/10.1037/0021-9010.93.5.1082>.

Colquitt, Jason A. 2001. "On the Dimensionality of Organizational Justice: A Construct Validation of a Measure." *Journal of Applied Psychology* 86 (3): 386–400.

Den Hartog, Deanne N. 2015. "Ethical Leadership." *Annual Review of Organizational Psychology and Organizational Behavior* 2 (1): 409–34. <https://doi.org/10.1146/annurev-orgpsych-032414-111237>.

Devendorf, Shelba A., and Scott Highhouse. 2008. "Applicant–Employee Similarity and Attraction to an Employer." *Journal of Occupational and Organizational Psychology* 81 (4): 607–17. <https://doi.org/10.1348/096317907X248842>.

Dorsey, David W., Jose M. Cortina, Matthew T. Allen, Shonna D. Waters, Jennifer P. Green, and Joseph Luchman. 2017. "Adaptive and Citizenship-Related Behaviors at Work." In *Handbook of Employee Selection*, 2nd ed. Routledge.

Elamroussi, Aya. 2022. "Survivors and Investigators Are Spending Thanksgiving Questioning the Motive behind a Mass Shooting in a Virginia Walmart That Left 6 Workers Dead." CNN. November 24, 2022. <https://www.cnn.com/2022/11/24/us/chesapeake-virginia-walmart-shooting-thursday/index.html>.

Feddes, Allard R., Liesbeth Mann, and Bertjan Doosje. 2015. "Increasing Self-Esteem and Empathy to Prevent Violent Radicalization: A Longitudinal Quantitative Evaluation of a Resilience Training Focused on Adolescents with a Dual Identity." *Journal of Applied Social Psychology* 45 (7): 400–411. <https://doi.org/10.1111/jasp.12307>.

Fox, S., P. E. Spector, and D. Miles. 2001. "Counterproductive Work Behavior (CWB) in Response to Job Stressors and Organizational Justice: Some Mediator and Moderator Tests for Autonomy and Emotions." *Journal of Vocational Behavior* 59: 291–309.

Frenett, Ross, and Moli Dow. 2015. "One to One Online Interventions – A Pilot CVE Methodology." Institute for Strategic Dialogue.

Grant, Adam M. 2007. "Relational Job Design and the Motivation to Make a Prosocial Difference." *The Academy of Management Review* 32 (2): 393–417.

Greenberg, Jerald. 1987. "A Taxonomy of Organizational Justice Theories." *Academy of Management Review* 12: 9–22.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Christopher R. Brown, and Thomas Ferryman. 2013. "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis." *E-Service Journal* 9 (1): 106–38. <https://doi.org/10.2979/eservicej.9.1.106>.

Greitzer, Frank L., Justin Purl, Yung Mei Leong, and D.E. Sunny Becker. 2018. "SOFIT: Sociotechnical and Organizational Factors for Insider Threat." In *2018 IEEE Security and Privacy Workshops (SPW)*, 197–206. San Francisco, CA: IEEE. <https://doi.org/10.1109/SPW.2018.00035>.

.....

## REFERENCES

- Han, Tae Young, and Kevin J. Williams. 2008. "Multilevel Investigation of Adaptive Performance: Individual- and Team-Level Relationships." *Group & Organization Management* 33 (6): 657–84. <https://doi.org/10.1177/1059601108326799>.
- Harold, Crystal M., In-Sue Oh, Brian C. Holtz, Soojung Han, and Robert A. Giacalone. 2016. "Fit and Frustration as Drivers of Targeted Counterproductive Work Behaviors: A Multifoci Perspective." *Journal of Applied Psychology* 101: 1513–35. <https://doi.org/10.1037/apl0000150>.
- Holtz, Brian C., and Crystal M. Harold. 2013. "Effects of Leadership Consideration and Structure on Employee Perceptions of Justice and Counterproductive Work Behavior." *Journal of Organizational Behavior* 34 (4): 492–519. <https://doi.org/10.1002/job.1825>.
- Homoliak, Ivan, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa. 2019. "Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures." *ACM Computing Surveys* 52 (2): 30:1–30:40. <https://doi.org/10.1145/3303771>.
- "Human Resources and Insider Threat Mitigation: A Powerful Pairing." 2020. Intelligence and National Security Alliance. [https://www.insonline.org/docs/default-source/uploadedfiles/2020/01/insa-int-sept252020.pdf?sfvrsn=38fab99\\_2](https://www.insonline.org/docs/default-source/uploadedfiles/2020/01/insa-int-sept252020.pdf?sfvrsn=38fab99_2).
- Jones, Gareth R. 1986. "Socialization Tactics, Self-Efficacy, and Newcomers' Adjustments to Organizations." *The Academy of Management Journal* 29 (2): 262–79. <https://doi.org/10.2307/256188>.
- Kelloway, E. Kevin, Lori Francis, Matthew Prosser, and James E. Cameron. 2010. "Counterproductive Work Behavior as Protest." *Human Resource Management Review* 20 (1): 18–25. <https://doi.org/10.1016/j.hrmr.2009.03.014>.
- Klein, Andrew S, Joseph Wallis, and Robert A. Cooke. 2013. "The Impact of Leadership Styles on Organizational Culture and Firm Effectiveness: An Empirical Study." *Journal of Management & Organization* 19 (3): 241–54. <https://doi.org/10.1017/jmo.2013.34>.
- Kont, Markus, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, and Anna-Maria Osula. 2015. "Insider Threat Detection Study." *NATO CCD COE, Tallinn*.
- Kurtessis, James N., Robert Eisenberger, Michael T. Ford, Louis C. Buffardi, Kathleen A. Stewart, and Cory S. Adis. 2017. "Perceived Organizational Support: A Meta-Analytic Evaluation of Organizational Support Theory." *Journal of Management* 43 (6): 1854–84. <https://doi.org/10.1177/0149206315575554>.
- Lim, Sandy, Lilia M. Cortina, and Vicki J. Magley. 2008. "Personal and Workgroup Incivility: Impact on Work and Health Outcomes." *Journal of Applied Psychology* 93: 95–107. <https://doi.org/10.1037/0021-9010.93.1.95>.
- Littman-Ovadia, Hadassah, and Shiri Lavy. 2016. "Going the Extra Mile: Perseverance as a Key Character Strength at Work." *Journal of Career Assessment* 24 (2): 240–52. <https://doi.org/10.1177/1069072715580322>.
- Maasberg, Michele, John Warren, and Nicole L. Beebe. 2015. "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits." In *2015 48th Hawaii International Conference on System Sciences*, 3518–26. <https://doi.org/10.1109/HICSS.2015.423>.
- Mackey, Jeremy D., Charn P. McAllister, B. Parker Ellen, and Jack E. Carson. 2021. "A Meta-Analysis of Interpersonal and Organizational Workplace Deviance Research." *Journal of Management* 47 (3): 597–622. <https://doi.org/10.1177/0149206319862612>.
- Mao, Yina, Yan Liu, Chunyan Jiang, and Iris D. Zhang. 2018. "Why Am I Ostracized and How Would I React? – A Review of Workplace Ostracism Research." *Asia Pacific Journal of Management* 35 (3): 745–67. <https://doi.org/10.1007/s10490-017-9538-8>.
- Mathieu, Michael, Kevin J. Eschleman, and Danqiao Cheng. 2019. "Meta-Analytic and Multiwave Comparison of Emotional Support and Instrumental Support in the Workplace." *Journal of Occupational Health Psychology* 24: 387–409. <https://doi.org/10.1037/ocp0000135>.
- Mayer, David M., Maribeth Kuenzi, Rebecca Greenbaum, Mary Bardes, and Rommel (Bombie) Salvador. 2009. "How Low Does Ethical Leadership Flow? Test of a Trickle-down Model." *Organizational Behavior and Human Decision Processes* 108 (1): 1–13. <https://doi.org/10.1016/j.obhdp.2008.04.002>.
- Mayer, David M., Maribeth Kuenzi, and Rebecca L. Greenbaum. 2010. "Examining the Link Between Ethical Leadership and Employee Misconduct: The Mediating Role of Ethical Climate." *Journal of Business Ethics* 95 (1): 7–16. <https://doi.org/10.1007/s10551-011-0794-0>.
- Maynard, M. Travis, Deanna M. Kennedy, and S. Amy Sommer. 2015. "Team Adaptation: A Fifteen-Year Synthesis (1998–2013) and Framework for How This Literature Needs to 'Adapt' Going Forward." *European Journal of Work and Organizational Psychology* 24 (5): 652–77. <https://doi.org/10.1080/1359432X.2014.1001376>.
- McEvily, Bill, Giuseppe Soda, and Marco Tortoriello. 2014. "More Formally: Rediscovering the Missing Link between Formal Organization and Informal Social Structure." *Academy of Management Annals* 8 (1): 299–345. <https://doi.org/10.5465/19416520.2014.885252>.

REFERENCES

- Meier, Laurenz L., and Paul E. Spector. 2013. "Reciprocal Effects of Work Stressors and Counterproductive Work Behavior: A Five-Wave Longitudinal Study." *Journal of Applied Psychology* 98 (3): 529–39. <https://doi.org/10.1037/a0031732>.
- Meyers, Maria Christina, Byron G. Adams, Lusanda Sekaja, Carmen Buzea, Ana-Maria Cazan, Mihaela Gotea, Delia Stefanel, and Marianne van Woerkom. 2019. "Perceived Organizational Support for the Use of Employees' Strengths and Employee Well-Being: A Cross-Country Comparison." *Journal of Happiness Studies* 20 (6): 1825–41. <https://doi.org/10.1007/s10902-018-0026-8>.
- Miller, Renee L., Mark A. Griffin, and Peterm. Hart. 1999. "Personality and Organizational Health: The Role of Conscientiousness." *Work & Stress* 13 (1): 7–19. <https://doi.org/10.1080/026783799296156>.
- Moore, Andrew P., Carrie Gardner, and Denise M. Rousseau. 2022. "Reducing Insider Risk Through Positive Deterrence." *Counter-Insider Threat Research and Practice* 1 (1). <https://citrap.scholasticahq.com/article/34612-reducing-insider-risk-through-positive-deterrence>.
- Moorman, Robert H., Gerald L. Blakely, and Brian P. Niehoff. 1998. "Does Perceived Organizational Support Mediate the Relationship between Procedural Justice and Organizational Citizenship Behavior?" *Academy of Management Journal* 41 (3): 351–57. <https://doi.org/10.5465/256913>.
- Morf, Manuela, Anja Feierabend, and Bruno Staffelbach. 2017. "Task Variety and Counterproductive Work Behavior." *Journal of Managerial Psychology* 32 (8): 581–92. <https://doi.org/10.1108/JMP-02-2017-0048>.
- Pfundmair, Michaela. 2019. "Ostracism Promotes a Terroristic Mindset." *Behavioral Sciences of Terrorism and Political Aggression* 11 (2): 134–48. <https://doi.org/10.1080/19434472.2018.1443965>.
- Podsakoff, Nathan P., Jeffery A. LePine, and Marcie A. LePine. 2007. "Differential Challenge Stressor-Hindrance Stressor Relationships with Job Attitudes, Turnover Intentions, Turnover, and Withdrawal Behavior: A Meta-Analysis." *Journal of Applied Psychology* 92 (2): 438–54. <https://doi.org/10.1037/0021-9010.92.2.438>.
- Priesemuth, Manuela, Anke Arnaud, and Marshall Schminke. 2013. "Bad Behavior in Groups: The Impact of Overall Justice Climate and Functional Dependence on Counterproductive Work Behavior in Work Units." *Group & Organization Management* 38 (2): 230–57. <https://doi.org/10.1177/1059601113479399>.
- Pulakos, Elaine D., Sharon Arad, Michelle A. Donovan, and Kevin E. Plamondon. 2000. "Adaptability in the Workplace: Development of a Taxonomy of Adaptive Performance." *Journal of Applied Psychology* 85: 612–24. <https://doi.org/10.1037/0021-9010.85.4.612>.
- Richardson, Roslyn. 2014. "Fighting Fire with Fire: Target Audience Responses to Online Anti-Violence Campaigns." Australian Strategic Policy Institute. <https://apo.org.au/node/40145>.
- Savoia, Elena, Megan McBride, Jessica Stern, Max Su, Nigel Harriman, Ajmal Aziz, and Richard Legault. 2020. "Assessing the Impact of the Boston CVE Pilot Program: A Developmental Evaluation Approach." *Homeland Security Affairs* 16 (August).
- Shanock, Linda Rhoades, and Robert Eisenberger. 2006. "When Supervisors Feel Supported: Relationships with Subordinates' Perceived Supervisor Support, Perceived Organizational Support, and Performance." *Journal of Applied Psychology* 91 (3): 689–95. <https://doi.org/10.1037/0021-9010.91.3.689>.
- Sims, Ronald R. 2000. "Changing an Organization's Culture Under New Leadership."
- Spell, Chester S., and Todd J. Arnold. 2007. "A Multi-Level Analysis of Organizational Justice Climate, Structure, and Employee Mental Health." *Journal of Management* 33 (5): 724–51. <https://doi.org/10.1177/0149206307305560>.
- Tims, Maria, Daantje Derks, and Arnold B. Bakker. 2016. "Job Crafting and Its Relationships with Person–Job Fit and Meaningfulness: A Three-Wave Study." *Journal of Vocational Behavior* 92 (February): 44–53. <https://doi.org/10.1016/j.jvb.2015.11.007>.
- White, Stephen G. 2021. "Workplace Targeted Violence: Assessment and Management in Dynamic Contexts." In *International Handbook of Threat Assessment, 2nd Ed*, 107–35. New York, NY, US: Oxford University Press. <https://doi.org/10.1093/med-psych/9780190940164.003.0006>.
- Whitty, Monica T. 2021. "Developing a Conceptual Model for Insider Threat." *Journal of Management & Organization* 27 (5): 911–29. <https://doi.org/10.1017/jmo.2018.57>.
- Williams, Michael, John Horgan, and William Evans. 2016. *Evaluation of a Multi-Faceted, U.S. Community-Based, Muslim-Led CVE Program*.
- Wolfowicz, Michael, Yael Litmanovitz, David Weisburd, and Badi Hasisi. 2020. "A Field-Wide Systematic Review and Meta-Analysis of Putative Risk and Protective Factors for Radicalization Outcomes." *Journal of Quantitative Criminology* 36 (3): 407–47. <https://doi.org/10.1007/s10940-019-09439-4>.
- Yan, Yanling, Erhua Zhou, Lirong Long, and Yang Ji. 2014. "The Influence of Workplace Ostracism on Counterproductive Work Behavior: The Mediating Effect of State Self-Control." *Social Behavior & Personality* 42 (6): 881–90. <https://doi.org/10.2224/sbp.2014.42.6.881>.
- Zhu, X. Susan, Dev K. Dalal, Kevin P. Nolan, and Janet L. Barnes-Farrell. 2021. "Understanding the Role of Organizational Personality and Social Identity Concerns on Initial Recruitment Outcomes." *Journal of Vocational Behavior* 124 (February): 103518. <https://doi.org/10.1016/j.jvb.2020.103518>.





# Pushing Left of Flash – The Art and Science of Early Risk Assessment

---

**Robert Graves**

“*How can we anticipate and mitigate crimes, attacks, or betrayals by bad actors?*” This is the perennial question faced by security professionals. The contributions of the discipline of behavioral threat assessment have been invaluable in enabling the disruption and diversion of those preparing to commit acts of targeted violence. Behavioral threat assessment has been most effective in interrupting the “flash-to-bang” cycle – that is, the time between the first overt action or broadcast of intent, and the commission of the bad act itself. Keeping people safe means doing even better. Combining operational art with behavioral science, it is possible to begin risk assessment even earlier in the operational cycle, to get “left of flash.”

With an understanding of the origins of grievance and how betrayal, corruption, or violence may grow from them, or be exploited by others, security professionals have an opportunity to anticipate and mitigate those bad acts. If we detect risks and threats early enough, we can employ administrative, clinical, or criminal justice means to disrupt them.

Rarely is someone “born bad”— the stereotypical clinical psychopath is largely an artifact of popular fiction. Occasionally, a person is born into a culture of villainy, such as a family-based criminal enterprise. In most cases, a person’s turn down the road of violence, corruption, or betrayal of trust is the result of a confluence of events and influences in their lives. That turn



Robert Graves is a 22-year veteran of the Federal Bureau of Investigation where, as a Supervisory Special Agent, he specialized in National Security investigations, behavioral analysis, human intelligence, and undercover operations. Prior to joining the FBI, Graves served as a US Army Military Intelligence officer. In 2019, Graves joined the Secure Community Network (SCN), a 501(c)(3) nonprofit, the official safety and security organization of the Jewish community in North America. Graves currently serves as SCN's Deputy Director for Strategic Operational Development, overseeing program development/evaluation and innovation.



begins where grievance and ideation intersect with a key facet of a person's identity. Progress down that road comes as a person is then pushed or pulled by an agent of influence, and ultimately presented with a choice: to exercise their human agency and respond morally and ethically to challenges they face, or to choose villainy.

## **At the Crossroads**

Most of us travel our whole lives on the road of accepted social norms and behaviors. Some among us, however, will find themselves at a crossroads with the path to villainy. That path, in turn, may lead to radicalization and violence, corruption and crime, or an "insider threat" and betrayal of trust. Like the well-recognized pathway observed in targeted violence, it begins with a grievance—a real or perceived insult to some fundamental human need. Whether you subscribe to Maslow's Hierarchy of Needs or another model, we all recognize there are needs common to all people, ranging from the physical (food, water, shelter) to the emotional (companionship, respect, love) to the spiritual (faith, sense of identity). The pain point—that is, the need that is perceived as being under threat—is specific to each individual. It may be something as existential as the threat of loss of an income or a home. It might be something more emotional, yet still existential, such as the loss of a pair-bond partner. Proceeding along the spectrum of needs, the pain point may be a sense of isolation or alienation from the person's group or tribe.

A particularly perilous grievance can be the perception of loss or denial of status as relates



to membership within a community that represents a key dimension of the person's identity. An insult or injustice, real or perceived, against such a community can also be a powerful pain point for an individual—for example, the sense that one's ethnic, religious, or gender group is being discriminated against or displaced.

Moreover, part of our human tendency to organize into bands, groups, and tribes is the need to establish ourselves within the hierarchy of the communities with which we identify. The position an individual holds in a given hierarchy reflects the value the group places on that person and can determine the person's ability, real or perceived, to meet other needs, from finding food and shelter to successfully competing for a pair-bond partner. There are prestige economies within all communities, from criminal "families" to academia to bowling leagues. As people strive for success and position within their communities, failure to attain greater success or loss of status can engender a sense of disrespect and humiliation. This is a particularly powerful pain point and can be a substantial source of grievance.

Whatever the insult or pain point, the natural human response is to look for remedy, which can lead to that next step on the path to villainy: grievance-focused ideation. Everyone ideates on their grievances, looking for an explanation, a solution, and in many cases, someone to blame. For most of us, this ideation is part of our process for finding a healthy resolution to the grievance. The person most vulnerable to becoming a threat to others, in contrast, may seize on an external focus for the grievance. They may blame a person or group as having either deliberately or negligently caused the harm. Here we may see the earliest signs of emotional leakage or broadcasting, indicating that a grievance has begun to turn malignant. This can also be our best (and sometimes only) opportunity to divert or re-direct that sense of grievance into something more constructive. Failing that, our potential villain may begin to rationalize that some affirmative act on their part is, in fact, not only justified but necessary for redress of the grievance. That rationalization can lead to the belief that action against the person or entity blamed is the best or only logical recourse.

“  
**To move someone off those norms requires a radicalizing or corrupting influence—an idea, movement, or person—to leverage some portion of that person's identity to justify and accept, if not demand, action, violent or otherwise.**  
.....

That action may come in the form of theft, fraud, or an effort to impose reputational harm. It may also be in the form of acting out in a kinetic, even violent, manner.

Most of us are socialized to believe that it is wrong to cause harm to or use violence against another person except in the most extraordinary, and largely defensive, circumstances. This belief is usually built into the moral foundations of our identity by religious, legal, and social norms. To move someone off those norms requires a radicalizing or corrupting influence—an idea, movement, or person—to leverage some portion of that person’s identity to justify and accept, if not demand, action, violent or otherwise.

## **The Challenge of Balancing Identities and Loyalties**

Human identity is multi-faceted. If you make a list of nouns to describe yourself (“I am a \_\_\_\_\_”), consistently at the front and center of your sense of self will be a set of identifiers. These are in constant competition for primacy, depending largely on situational factors. Some social psychologists argue that we possess a number of “selves,” each manifesting itself depending on context (Markus & Nurius, 1986). At work, we may be defined by our profession or tasks. At home, we may define ourselves first and foremost as a partner or parent. With friends, we may be defined by our common experiences. Within a religious community, we may define ourselves by our piety. When different aspects of our identity come into conflict with each other, the tension can be stressful. When satisfying one of those dimensions of self requires subordination or denial of another, loyalties can become divided, and some people may find villainy beckoning.

The tipping point to action comes when a person engaged in grievance-focused ideation is presented with a solution that both validates a core aspect of their identity while relieving the internal conflict between identities. Invariably, that solution is identification with, and membership in, a new affinity group that endorses the grievance. Whether this person will continue down the path and graduate to acts of violence or other harm will depend on where this new self-identification comes out in the competition for primacy in the person’s sense of self. If this new tribe conflicts with another—and stronger—aspect of the person’s identity, then the aggrieved person may choose a moral or ethical path and may never become more than a sympathizer to the cause. If, on the other hand, the new ideology or identity, and its associated embrace of a particular course of action, are compatible with, or stronger than, other core aspects of the person’s identity, that person

may choose the road to radicalization, corruption, or betrayal. If the new ideology or identity aligns with and validates other core facets of the individual's identity, then the person may not merely be vulnerable to calls to action, but may enthusiastically wade into the fray, viewing such action as required for the realization of their true identity.

How well a person can frame-switch between competing or conflicting facets of their identity is a good indicator of their ability to resist the more extreme demands of any facet, including demands that are in conflict with another facet of their identity. Those who are not able to frame-switch with fluency may find themselves forced to make a choice as to which aspect of their identity they will serve, making them vulnerable to radicalization, corruption, or betraying trust.

For insight into the mechanics of balancing competing identities and potentially divided loyalties, and as a means of better understanding who might be more vulnerable to those challenges, it is illuminating to look at studies of bicultural integration. People who move between cultures may find their ability to successfully operate in one or both of those cultures stressed in much the same way that an aggrieved person may find themselves stressed when attempting to balance the various elements of their identity.

Work on bicultural integration has shown that the Five Factor Model for measuring personality traits can provide useful indicators of a person's ability to frame-switch between divided and divergent identity needs (Benet-Martinez, 2005). A low degree of openness, correlating to rigidity of thought and being closed to new experiences, may be characteristic of individuals who are more likely to compartmentalize the conflicting aspects of their identities rather than balance them. A high degree of neuroticism, correlating to feelings of

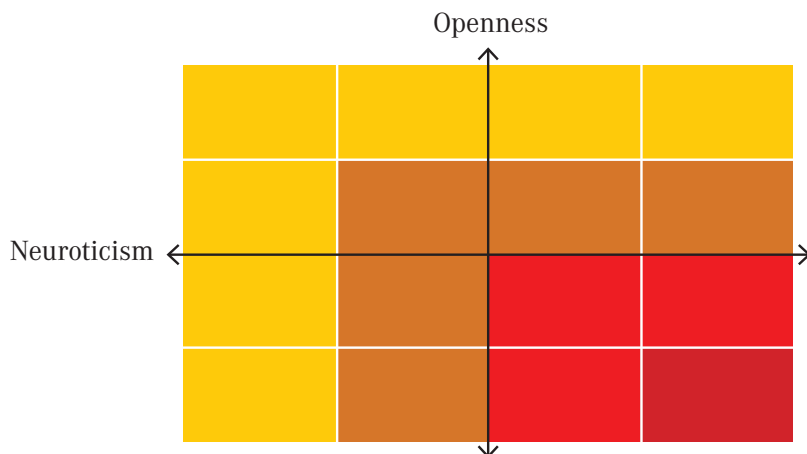
**Patriot commits espionage on behalf of perennial adversary**

Carsten Linke, a German Army veteran, arrested in December 2022, was accused of espionage on behalf of Russia. Linke, who at the time was director of technical reconnaissance for Germany's Federal Intelligence Service, had confided to colleagues his concerns that Germany was deteriorating and was openly disdainful of its center-left government. Outside of work, he was in contact with a member of the far-right populist political party "Alternative for Germany," (AfD) and appeared to have subscribed to a YouTube channel suspected to be linked to the far-right "Reichsbürger" scene, which was the source of a coup plot disrupted in 2022. The German populist far-right has been openly enamored of Russia and its leader, Vladimir Putin (Solomon, et al, 2023).

Linke's grievance was a perceived threat to his tribe, the Germany he had served as a soldier and intelligence officer. He found endorsement for his grievance in AfD and the populist far-right of German politics, to which he appears to have affiliated covertly. His involvement with a new tribe, one with pro-Russian sympathies, put Linke in a position to betray the trust of his colleagues and transfer his loyalty to an adversary, Russia.

vulnerability and anxiety, may be found in individuals having difficulty facing competing demands for their loyalty. A combination of the two (low openness and high neuroticism) may be characteristic of an individual who is unable to frame-switch, instead feeling an imperative to go all-in with one facet of their identity, rather than balancing competing forces. (Figure 1)

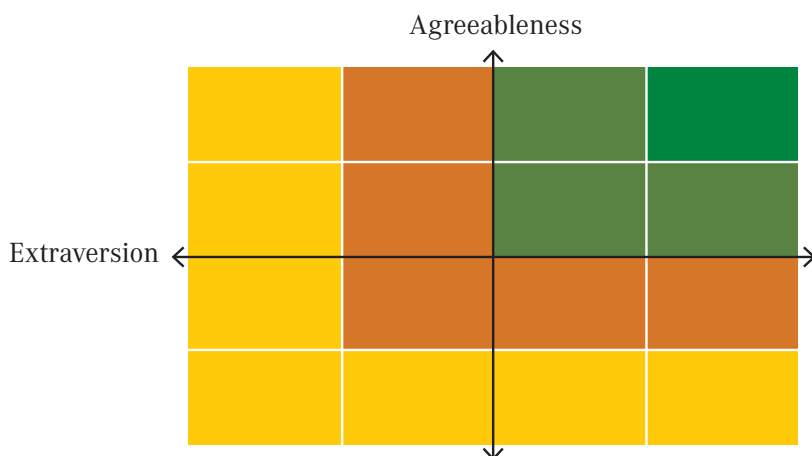
**FIGURE 1. Openness and neuroticism**



Conversely, other Five Factor Model personality traits play an offsetting role. People with high degrees of agreeableness and extraversion appear more fluent in frame-switching. Those who are more agreeable are generally less likely to experience conflict. The extraverted generally have greater interpersonal resources and are likely more adaptable to their circumstances. (Figure 2)

It is noteworthy that the fifth factor, conscientiousness (the predictor of success in so many domains) does not appear to have bearing on a person's ability to frame-switch and balance competing demands of identity or loyalty (Benet-Martinez, 2005). Low conscientiousness, manifesting as low self-control, however, comes into play as it correlates to an increased risk of criminality (Tharsini et al., 2021).

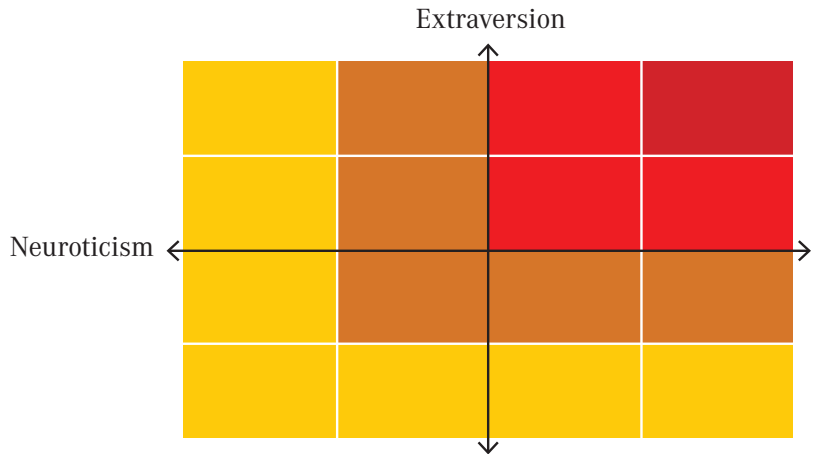
**FIGURE 2. Agreeableness and extraversion**



Other research suggests that the

confluence of high extraversion and high neuroticism may make a person susceptible to inducements to otherwise unacceptable behavior. Studies of persons in high-risk work exhibiting this combination of traits showed they were particularly susceptible to criminally risk-taking behavior (Girodo, 1991). In combination with traits suggesting difficulty in balancing competing loyalties or identities, a tendency towards societally unacceptable risk-taking can be an exacerbating risk factor for radicalization, corruption, or betrayal of trust. (Figure 3)

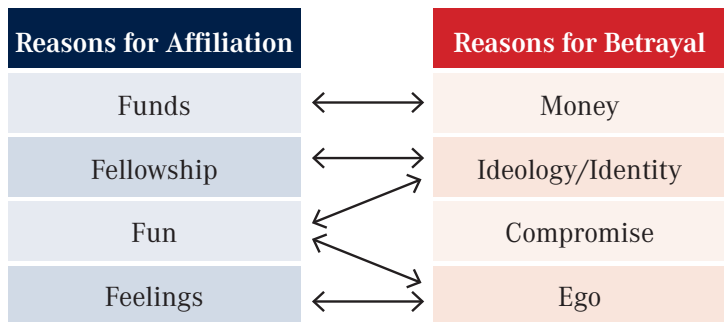
**FIGURE 3. Extraversion and neuroticism**



## The Allure of a Group

A validation of the grievance and framework for blame, by itself, is likely insufficient to entice a person to villainy, violent or otherwise. Affiliating with a group and its purpose requires something more. The four principal reasons people affiliate with any type of group are funds, fellowship, fun, and feelings (Reed, 2015). For a person to join an extremist organization, a criminal enterprise, or other clandestine relationship, however structured or unstructured it might be, some combination of these must be present. The reasons an individual may affiliate with a group generally align with the classic paradigm of the reasons the person might betray: “MICE,” or Money, Ideology, Compromise, or Ego (Figure 4).

**FIGURE 4. Reasons for affiliation and betrayal**



**Funds.** It is doubtful anyone joins an affinity group simply to get rich. However, a person amenable to the group's message may see the group or its message as a means for obtaining or protecting critical resources to meet those existential human needs discussed earlier, or to otherwise ensure safety for themselves or others to whom they may feel a sense of responsibility or obligation. This can be a powerful incentive or rationalization for a change in allegiance. This aligns directly with "Money" under the MICE paradigm.

**Fellowship.** Friends and allies can be powerful influencers toward a person adopting or aligning with the *raison d'être* of a new affinity group. There is a maxim among those who recruit and handle spies that no one betrays the trust of others out of friendship with their handler, but friendship makes it easier. Similarly, a sense of camaraderie with like-minded persons goes a long way in ushering an individual down the path of radicalization, corruption, or betrayal. The sense of belonging to a group, especially a group built around a similar outlook, is an elemental human need. Two key messages of predators, corruptors, recruiters, and radicalizers alike are, "I like you," and "I am like you" (more on this later). Finding fellowship with the like-minded helps to meet the need to belong to a group, especially among those whose grievances include a sense of alienation or exclusion. This aligns with the "Ideology," or more broadly "Identity," component of MICE.

**Fun.** For some people, the activities of an extremist group, criminal enterprise, or other clandestine relationship may be particularly exciting. The emotional intensity an individual associates with a given person, group, or activity can be intoxicating and addictive. When we are part of something so special that it must be kept secret, the emotional connection becomes more intense, elevating the sense of adventure. When physically demanding activity is added to the mix, along with an element of danger, the adventure, and the resulting sense of fun, increases. The clandestine nature of the contacts and any "crash-bang" of training for actions, the association with a new tribe, especially a clandestine one, can have a powerful effect, not unlike falling in love or using mood-altering drugs. The drive to obtain and maintain that heightened emotional state contributes to the allure and escalation of the affiliation. "Fun," may align with either "Ideology," or "Ego," or both.

**Feelings.** Potentially the most powerful of the four reasons for affiliating with any group, the sense that one is part of something larger than oneself is often its own reward. When the affiliation not only addresses the individual's sense of personal grievance, but also gives them a perceived sense of purpose or empowerment to address the grievance on behalf of

their tribe, the sense of self-righteousness and greater mission can combine into missionary zeal. Add this to the individual's belief that their zealotry earns them respect and status in this new peer group, and the probability of radicalization, corruption, or betrayal, and action, increases substantially. This directly aligns with MICE's "Ego," component.

## The Push-Pull of Influence

Once a vulnerable person finds themselves at the point where villainy beckons, external influence is sometimes needed to either push or pull the person across the line. In the past, this push-pull often came in the form of in-person introduction and recruitment into a movement or group, relationship building, and a "pitch." In the modern era, the pervasiveness of digital platforms allows recruiters to expand their reach, using mass communications to reach and cultivate many more potential recruits to their cause. Many times, the recruiter may never have direct, much less in-person, contact with the recruit. In fact, the recruiter may never know the recruit. Nevertheless, the principles of the recruitment remain the same.

Modern technology makes it far easier for the recruiter to reach potential recruits than in the past. In the 1990s, we first saw widespread radicalization efforts through mass media tools. Unmarked tape cassettes of sermons by radical imams were passed hand-to-hand (like drug deals) in souks around the Islamic world. In the US, shortwave radio broadcasts and cassette tapes drove recruitment for militias and other domestic extremist groups. In the 21st century, we have seen radical Islamist groups publish slick on-line magazines to propagate their messages and tactical instruction, while we see domestic extremists building their reach via the proliferation of dark-web chatrooms, grievance and ideology-focused messaging, and social media apps. Anyone with a grievance, looking to assign blame, and wanting redress, can find a digital platform with an ideological framework to suit their needs.

A psychopath manipulates their target using four key lines of messaging (Babiak and Hare, 2005). A recruiter, radicalizer, or corruptor, like other predators, uses similar messaging. Whether in-person or through on-line contacts, those messages are:

**"I like you."** We all want to be appreciated within our group. The desire to be appreciated is exploited with two distinct messages. The first message is that the group is special, and membership in it is desirable and only open to those who bring value to the group. This usually requires building a sense of value for the group that competes with existing affiliations and loyalties.

If membership in the group is hard to achieve, then it becomes more valuable to the potential recruit. If interaction with the recruiter is rare, then any engagement becomes of higher value. The second message is the hook – telling the recruit that they are liked. With exclusivity of membership and scarcity of interaction, the message of “I (or we) like you,” helps to develop affinity for the recruiter or group.

**“I am like you.”** The message of “you, me, same, same,” is foundational to rapport building in personal relationships. It applies as well in radicalization and recruitment into extremist movements or other anti-social enterprises. Again, the human drive towards grouping with like-minded persons, those with whom we share common interests, or with whom we can make common cause, builds affinity for the new group in a potential recruit. This strengthens the bonds with the extremist movement or group and better enables it to compete with any countervailing affinity group for the recruit’s loyalty.

**“I am your perfect partner.”** Effectively convincing a potential recruit that

### Recruitment to White Supremacy and Redemption

Christian Picciolini, the son of Italian immigrants to the US, had been bullied as a child and often felt abandoned by his parents, who worked 14-hour days, seven days a week, as small business owners. Picciolini was 14 years old, standing in an alley smoking marijuana, when he was first approached by the leader of a neo-Nazi group. In a single conversation, that extremist recruited Picciolini:

“

*He knew that I was searching for three very important things: a sense of identity, a community, and a purpose.*

By the age of 16, Picciolini had become the leader of the group after a series of arrests and criminal charges sent the group’s leadership to prison or into hiding. By the age of 19, Picciolini acquired a new sense of identity, that of husband, and at 21, father, both of which conflicted with his role as leader of a neo-Nazi gang. By 22, his marriage had fallen apart and Picciolini questioned his hatred of immigrants, Jews, and LGBTQ persons. As a result, he began distancing himself from the group and spent the next 25 years working to regain a normal life and helping others leave extremist groups behind (Lipman, 2020).

Picciolini’s sense of grievance was abstract yet existential. He felt abused by the world and abandoned by those he would expect to protect him. Recognizing Picciolini’s alienation, the neo-Nazi leader and recruiter offered him the sense of identity and community he needed (“Friends”), as well as a sense of purpose (“Feelings”). Over time, Picciolini acquired a competing sense of identity as a husband and father. When those came into conflict with his affiliation with the group, “husband” and “father” proved to have the greater importance for him. When his marriage failed, he withdrew from the neo-Nazi gang to reintegrate into society and help others.



the recruiter, movement, or group perfectly fills the gap in the recruit's life is the tipping point in building the relationship. Once this has been achieved, the potential recruit fully accepts and identifies with the extremist group, giving their loyalty to that group primacy over other competing identity affinities.

**“You can trust me.”** At the core of all human relationships is trust. At the point where the recruit has been effectively radicalized or otherwise corrupted, they have come to believe that the recruiter, leadership, and movement are who they say they are and are invested in the recruit's well-being and success. The recruiter builds this trust by demonstrating consistency of ideology and purpose, by modeling sincerity and integrity in interactions with the recruit, and by demonstrating concern for the recruit's safety. This latter concern is most directly demonstrated through measures to ensure the clandestine nature of the relationship to keep it hidden from law enforcement or others who would seek to disrupt it.

## Recognizing the Early Steps on the Path to Villainy

Viktor Cherkashin, the Soviet-era KGB officer who famously handled two high-level spies within the US government, summed up the role of the recruiter as being to find those who want to be recruited, then to listen (Cherkashin, 2005). Whatever our role in addressing radicalization, corruption, or betrayal of trust, it is key that we also listen. We should listen with the ear of the recruiter, firstly to recognize when an individual is vulnerable to or looking to be recruited and, secondly, to recognize when an individual may be hearing what they need to assign blame and to shift loyalties to groups or ideologies that may lead to kinetic or other adverse outcomes.

It may be possible to identify those most vulnerable to radicalization or inducements to betray trust, or to recognize when those are in progress. Whether we are talking about so-called self-radicalization via social media and on-line platforms or “in real life” recruitment via in-person interactions, the indicators are the same.

The earliest observable indicator of risk would be a mix of observable personality traits— including low openness to experience, neuroticism, and extraversion—that can be leveraged to create stress and competition with counterbalancing facets of the person's identity and to induce risk-taking. The appearance of low “Openness,” potentially manifesting as an aversion to change or a lack of curiosity about new things, in combination with high “Neuroticism,” which may appear as anxiousness, irritability, or vulnerability to stress, would suggest the individual may not be able to effectively balance competing demands

on their sense of self and may be more susceptible to a push or pull towards radicalization or betrayal. This may be offset somewhat if the individual manifests high “Agreeableness,” often displayed as trust, straightforwardness, or compliance, along with high “Extraversion,” such as sociability and positive engagement with others. Persons with these traits would be less likely to experience personal conflict and would have better social resources to manage any conflicts that arise. The appearance of high “Extraversion,” in the form of excitement-seeking, interacting with high “Neuroticism,” may indicate a propensity for socially unacceptable, even criminal, risk-taking behavior. The presence of low “Conscientiousness,” in the form of low self-control, would increase the risk associated with other negative traits.

The next risk factor likely to be observable would be a perceptible sense of grievance that has alienated the person from their traditional group or tribe. Statements suggesting alienation, disaffection, or a sense of betrayal may creep into casual conversation or, as is increasingly common, appear in postings on the individual’s social media accounts. Another sign of alienation would be the individual’s withdrawal from their customary level of participation in work and social activities. This may also be accompanied signs of self-medication, such as changes in the use of alcohol (from teetotaler or social-drinker to binge-drinker), off-label use of mood-altering medications, or use of illegal drugs. This risk would be particularly high if the alienation is accompanied by a sense of status loss, humiliation, or disrespect.

“  
As the grievance deepens, an at-risk person would next likely demonstrate a need to assign blame for the grievance to someone other than themselves.”

As the grievance deepens, an at-risk person would next likely demonstrate a need to assign blame for the grievance to someone other than themselves. When this is accompanied by a sense that a kinetic, potentially violent, or otherwise illegal act is the best or only redress for the insult, the individual has embarked upon the well-known pathway to violence. Overt public or social media statements assigning that blame may develop slowly over time or appear along with the statements of grievance. These may grow in intensity over time, from, “...someone needs to do something...,” to “...I need to do something...”

The shift from the third-party imperative to first person ideation would likely also be accompanied by emotional “leakage” suggesting that a key facet of

the person's identity may be increasingly aligned with an ideological or philosophical framework that supports violent action or other socially unacceptable means of addressing the grievance. These would likely appear as statements or posts on social media that are empathetic to this new ideology. Over time the degree of visible empathy or intensity of identification with a new affiliation would likely increase; the sudden disappearance of such statements from conversation or posts could indicate the person's affiliation with the ideology or group had entered a covert phase.

These indicators should not be taken as guarantees of radicalization, corruption, or vulnerability. They can be used, however, to elevate an individual in the risk assessment process. They should be used in the broader inquiry and assessment effort to identify people at risk of traveling the path to villainy, and to divert them if possible. Whether the means of diversion is administrative, clinical, or judicial, when grievance, identity, and influence intersect and there is vulnerability to radicalization, corruption, or betrayal, there is a potential to off-ramp the person from a destructive path that can lead to violence and more.

## A Way Forward

Combining operational art with behavioral science, we can better meet our responsibilities for keeping people safe. To push the risk assessment process "left of flash," security professionals should partner with behavioral science experts, especially clinical psychologists with forensic or operational specializations. Forensic and operational psychologists bring an array of tools to this effort, from psychometrics for gauging personality and temperament, such as the NEO-PI-R for Five Factor Model assessments, to more specialized structured professional judgement tools to evaluate risk of violence and radicalization. Security professionals bring their operational experience as investigators of a broad variety of crimes and threats. Many will also bring additional perspective as recruiters themselves, having experience inducing people to betray the trust of the criminal enterprises and extremist groups to which they belong.

“  
...an understanding  
of the path to villainy  
can help to identify  
when a person may  
be at the crossroads  
of grievance,  
identity, and  
influence and may  
be confronting the  
choice between right  
and wrong, good and  
evil, loyalty and be-  
trayal, or law  
and criminality.

The combination of those unique capabilities, working in partnership, may be used as part of an organizational personnel reliability or suitability program, or a trusted workforce program. In this way, these tools may be integrated into hiring processes as part of pre-employment suitability screenings. In most instances, a review of available personal history either provided by the applicant or through formal background investigations may be sufficient to identify candidates requiring more detailed or formal screening before a hiring decision is made. Similar processes may be applied if an employee is referred for review or intervention through the organizational workplace violence prevention or counter-insider threat programs. Organizations with staff in high-risk and high-trust positions may require a more structured program of formal psychometric testing and interviews, both before hiring and at periodic intervals, in order to meet their responsibilities to stakeholders.

No amount of foreknowledge can eradicate all risk or pre-empt all crime. At the same time, an understanding of the path to villainy can help to identify when a person may be at the crossroads of grievance, identity, and influence and may be confronting the choice between right and wrong, good and evil, loyalty and betrayal, or law and criminality. We can recognize when someone is at risk of turning down that path, creating the potential to divert that person to an off-ramp from the path to villainy—even, perhaps, an off-ramp that leads our potential bad actor to a productive path. ✓

.....

## REFERENCES

Babiak, P. & Hare, R.D. (2007). *Snakes in Suits: When Psychopaths Go to Work*. Harper Collins.

Benet-Martinez, V. & Haritatos, J. (2005). Bicultural Identity Integration (BII): Components and Psychosocial Antecedents. *Journal of Personality*, 73:4, 1015-1049.

Cherkashin, V. & Feifer, G. (2005). *Spy Handler: Memoir of a KGB Officer: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames*, Basic Books.

Girodo, M. (1991), Drug Corruption in Undercover Agents: Measuring the Risk. *Behavioral Sciences and the Law*, 9(3), 361 - 370.

Lipman, N., "Christian Picciolini: The neo-Nazi who became an anti-Nazi," BBC World Service, 5 December 2020 (<https://www.bbc.com/news/stories-54526345>).

Markus, H., & Nurius, P. (1986). Possible Selves. *American Psychologist*, 41(9), 954-969.

Reed, G.E. & Norton, R.J. (2016). Tarnished: Toxic Leadership in the U.S. Military. *Naval War College Review: Vol. 6: No.*, Article 19.

Solomon, E., Schuetze, C.F., and Barnes, J.E., "A Russian Mole in Germany Sows Suspicions at Home, and Beyond," *New York Times*, 17 Feb 2023. (<https://www.nytimes.com/2023/02/17/world/europe/germany-russia-spies.html>).

Tharshini, N.K, Ibrahim, F, Kamaluddin, M.R., Rathakrishnan, B, and Nasir, N.C.M., (2021), *The Link between Individual Personality Traits and Criminality: A Systematic Review*, *Int J Environ Res Public Health*, Aug 2021

.....

## DISCLAIMER

*The views and content of this article are wholly the opinion of the author. They do not represent the views, positions, or policies of the author's current or former employers.*



# Breaking the Ceiling on Risk Assessment: Dispositional Indicators of Risk Exposure (DIRE) Scale

---

**Jonathan Shedler**

**Peter Fonagy**

**Luisa E. Marin-Avellan**

**Michael Karson**

**Olga G. Shechter**

**Eric L. Lang**

## Abstract

*Current risk-assessment methods may be approaching a ceiling on accuracy. The domain of personality represents a source of untapped information for enhancing prediction not only of criminality but also of broadly defined misconduct, including breaches of trust and other forms of non-criminal insider threat in organizations. We describe the Shedler-Westen Assessment Procedure (SWAP), a comprehensive method of personality assessment, and the Dispositional Indicators of Risk Exposure (DIRE) scale, a psychometric scale designed to harness implicit and explicit expert knowledge concerning personality and risk. Study 1 examined the convergent validity of the DIRE scale in a national clinical sample of  $N = 1,201$  patients. DIRE correlated significantly with a range of risk-related criterion measures, including global maladaptive functioning ( $r = .64$ ), employment trouble ( $r = .49$ ), mental instability ( $r = .34$ ), criminality and violence ( $r = .46$ ), and child/adolescent antisociality ( $r = .53$ ). Study 2 examined the prospective prediction of criminal recidivism in a sample of violent offenders. DIRE was a significant prospective predictor of criminal recidivism over a 1-year period ( $r = .37$ ). We discuss implications for risk assessment in both general and criminal populations.*

### Authors' note

We express our appreciation to the late Professor Gill McGauley for her contributions to this paper. As a dedicated psychiatrist in forensic services in the UK, she pioneered forensic psychotherapy through clinical work, service creation, postgraduate teaching, and research.

---



**DR. JONATHAN SHEDLER**

Jonathan Shedler, PhD is a Clinical Professor in the Department of Psychiatry and Behavioral Sciences at the University of California, San Francisco (UCSF). He is among the leading experts on personality styles and disorders and their treatment. He is co-author of the Psychodynamic Diagnostic Manual (PDM-2) and co-author of the Shedler-Westen Assessment Procedure (SWAP). He lectures internationally and consults to mental health professionals, organizations, and government agencies.



**R**isk assessment, broadly defined as the prediction of undesirable outcomes (cf. Kraemer et al., 1997), appears to be approaching a ceiling on accuracy (Skeem & Monahan, 2011, p. 41). Contemporary risk-assessment scales comprise items developed to distinguish criminal recidivists from non-recidivists in correctional populations, with the result that the various scales commonly used for risk assessment are largely interchangeable (Kroner, Mills & Morgan, 2005; Yang, Wong & Coid, 2010). Prior research has highlighted four factors related to criminal violence: criminal history, persistent antisocial lifestyle, psychopathic personality (McWilliams & Shedler, 2017; Meloy, 1988), and substance abuse and/or mental health issues (Kroner, Mills, & Morgan, 2005).

The domain of personality, beyond psychopathy, represents a relatively untapped source of information for risk assessment that could enhance prediction not only concerning criminality, violence, and insider threat (Harms, et. al., 2022) but also with respect



**The domain of personality, beyond psychopathy, represents a relatively untapped source of information for risk assessment that could enhance prediction not only concerning criminality, violence, and insider threat (Harms, et. al., 2022) but also with respect to misconduct and more broadly defined undesirable outcomes.**







**DR. LUISA E. MARIN-AVELLAN**

Luisa E. Marin-Avellan, PhD is a psychologist, psychotherapist, and psychoanalyst with a deep-rooted interest in personality. Her 10-year research experience in England's forensic psychiatric services explored the link between personality factors and the risk of violent recidivism. Dr. Marin-Avellan now focuses on her private clinical practice in Geneva, Switzerland.



to misconduct and more broadly defined undesirable outcomes. Such undesirable outcomes may include, for example, insider threats in organizations such as compromise of information systems, failure to protect sensitive information, security breaches, misuse of resources, and breaches of trust, whether or not they involve illegal activity.

Many aspects of personality that are conceptually linked to risk are not represented or represented only minimally in risk assessment item pools. The domain of personality has been partially tapped in risk-assessment instruments described as structured professional judgment (SPJ), such as the Historical-Clinical-Risk Management-20 (HCR-20; Webster, et al., 1997), where a clinician considers an array of historical, clinical, and risk factors to render an overall judgment of risk. However, the personality variables included in the HCR-20 address relatively overt (easily observable) aspects of personality functioning such as personality disorder, impulsivity, negative attitudes, and lack of insight. These concepts stay close to the four factors noted above and do not significantly expand the potential item pool for risk assessment. With respect to personality dynamics, these variables can be said to represent relatively surface-level phenomena.

Conceptually, many personality pathways could lead to risky behavior (Buss, 1961; Daf-fern & Howells, 2002). For example, transgression by individuals with psychopathic personalities may be motivated by a desire for power or personal gain, and transgression by individuals with paranoid personalities may be motivated by a misdirected sense of justice and a desire to turn the ta-



DR. OLGA SHECHTER

Olga Shechter, PhD is a project director at the Defense Personnel and Security Research Center (PERSEREC), which is a division of the Defense Personnel Assessment Center (DPAC). She completed her doctoral education in social and personality psychology from University of Wisconsin, Madison. At PERSEREC, Dr. Shechter manages research projects in the areas of military suicide prevention and postvention.



bles on perceived persecutors (e.g., avenger violence), and transgression by individuals with borderline personality pathology may represent the externalization or “exportation” of internal chaos. Analyzing personality dynamics associated with misconduct not only increases the potential for accurate prediction, but also enhances the ability to take effective countermeasures (Heilbrun, 1997; Nicoletti, Spencer-Thomas, & Bollinger, 1999) based on an accurate understanding of motivation and likely precipitating circumstances.

This article describes the *Shedler-Westen Assessment Procedure* (SWAP), an approach to personality assessment that relies on informed clinical observation and judgment, and a risk-assessment scale derived from it, the *Dispositional Indicators of Risk Exposure* (DIRE) scale. Study 1 examines convergent validity of the DIRE scale with respect to a range of risk-related criterion measures in a large national clinical sample, and Study 2 examines the prospective prediction of criminal recidivism in a psychiatrically disturbed correctional population.

### Overview of the Shedler-Westen Assessment Procedure (SWAP-200)

The SWAP is a personality-assessment instrument completed by an expert clinical assessor after developing a thorough knowledge of a patient or assessment subject in a professional evaluative context (the instrument is available online at [swapassessment.org](http://swapassessment.org)). The SWAP provides assessors with a “standard vocabulary” for describing and quantifying clinical observation and inference about personality. The vocab-



**DR. PETER FONAGY**

Peter Fonagy, OBE is Professor of Contemporary Psychoanalysis and Developmental Science, Head of Division for Psychology and Language Sciences, University College London (UCL); Chief Executive of the Anna Freud National Centre for Children and Families and Executive Clinical Director, UCL Partners Mental Health and Wellbeing Programme. Dr. Fonagy’s clinical and research interests lie in early attachment relationships, social cognition, borderline personality disorder and violence. A central focus has been a research-based psychodynamic therapeutic approach, mentalization-based treatment.



ulary comprises 200 personality-descriptive statements or items, each of which may describe a given person very well, somewhat, or not at all. An assessor describes a person by ranking the SWAP items into eight categories, from most descriptive of the person (scored 7) to not descriptive or irrelevant (scored 0). Thus, the instrument yields a score from 0 to 7 for 200 personality-descriptive variables. The major editions of the SWAP instrument are the SWAP-200 and revised SWAP-II (Shedler, 2022; Shedler, 2015; Shedler & Westen, 2004a, 2004b, 2007; Westen & Shedler, 1999a, 1999b; Westen, Shedler, Bradley, & DeFife, 2012).

The “standard vocabulary” of the SWAP allows an assessor to provide a comprehensive, in-depth psychological description of a patient or assessment subject in a systematic form. SWAP items stay close to the clinical data (e.g., “Tends to get into power struggles,” or “Is capable of sustaining meaningful relationships characterized by genuine intimacy and caring”) and items that require inference or deduction are written in a clear, jargon-free language (e.g., “Tends to express anger in passive and indirect ways [e.g., may make mistakes, procrastinate, forget, become sulky, etc.]” or “Tends to see own unacceptable feelings or impulses in other people instead of in him/herself”). Writing items in jargon-free language minimizes unreliable interpretive leaps by assessors and makes the item set useful to clinicians of all theoretical orientations.

The initial SWAP item pool was drawn from a wide range of sources including the clinical literature on personality pathology written over the past 50 years (e.g., Kernberg, 1975, 1984; Kohut, 1971; Linehan, 1993; McWilliams,



**DR. MICHAEL KARSON**

Michael Karson, PhD, J.D., A.B.P.P. (Clinical) was on the faculty at the University of Denver for 20 years before returning to clinical practice and consultation. He is the sole or senior author of six books, including *Principles of Forensic Report Writing* and *What Every Therapist Needs to Know*. He has consulted on safe termination practices and personnel selection for numerous organizations.



1994; Shapiro, 1965); DSM Axis II diagnostic criteria included in DSM-III through DSM-IV; selected DSM Axis I criteria that could reflect enduring dispositions (e.g., depression and anxiety); research on coping, defense, and affect regulation (e.g., Perry & Cooper, 1987; Shedler, Mayman, & Manis, 1993; Vaillant, 1992; Westen, Muderrisoglu, Fowler, Shedler, & Koren, 1997); research on interpersonal functioning in patients with personality disorders (Westen, 1991; Westen, Lohr, Silk, Gold, & Kerber, 1990); research on personality traits in non-clinical populations (e.g., Block, 1971; John, 1990; McCrae & Costa, 1990); research on personality pathology conducted since the development of DSM Axis II (see, e.g., Livesley, 1995); pilot studies in which observers watched videotaped interviews of patients with personality disorders and described them using draft versions of the SWAP item set; and the clinical experience of the SWAP authors.

Most important, the SWAP item pool was revised and refined through a 12-year iterative revision process that incorporated the feedback of over 2,000 clinician-consultants of all theoretical orientations who used earlier versions of the SWAP instrument to describe their patients. The instrument developers asked each clinician-consultant one crucial question: “Were you able to describe the things you consider psychologically important about your patient?” They added, rewrote, and revised items based on this feedback, then asked new clinician-consultants to describe new patients, repeating this process over many iterations until most clinicians could answer “yes” most of the time. In a sample of 1,201 psychologists and psy-



DR. ERIC LANG

Eric Lang, PhD is the Director of the Department of Defense Personnel and Security Research Center (PERSEREC). Dr. Lang has over 30 years' experience leading social science research to improve the effectiveness, efficiency and fairness of personnel security, insider threat and suitability policies and operations to help DoD, other Federal agencies, and partners in industry, academe, and over a dozen allied countries.



chiatrists who used the SWAP-II to describe a current patient, 84% “agreed” or “strongly agreed” with the statement “The SWAP-II allowed me to express the things I consider important about my patient’s personality” (fewer than 5% disagreed). The ratings were unrelated to clinicians’ theoretical orientation (Shedler & Westen, 2007).

The SWAP is based on the Q-Sort method, which requires assessors to assign each score a specified number of times (there is a “fixed” score distribution). The fixed score distribution is asymmetric, with 100 items receiving scores of 0 or “not descriptive” and progressively fewer items receiving higher scores (the shape of the fixed distribution mirrors the naturally occurring distribution in the population; for a discussion of this and other psychometric issues, see Westen & Shedler, 2007). Use of a fixed distribution has psychometric advantages and reduces measurement error or “noise” inherent in standard rating scales.<sup>1</sup> The psychometric rationale for the Q-Sort method has been described in detail by Block (1978).

When the SWAP is used in the context of psychotherapy, an experienced clinician can

“  
**When the SWAP is used in the context of psychotherapy, an experienced clinician can score the instrument after a minimum of 6 clinical contact hours with a patient.**  
 ”

score the instrument after a minimum of 6 clinical contact hours with a patient. When used in a pure assessment context, as in personnel or forensic evaluation, the SWAP can be scored on the basis of the Clinical Diagnostic Interview (CDI), which systematizes and compresses into an approximately 2.5-hour time frame the kind of interviewing skilled clinicians engage in during the initial hours of patient contact to assess personality (Westen, 2004; Westen & Muderrisoglu, 2006; Westen & Weinberger, 2004). The interview does not rely on self-report questions about personality; rather, it elicits narrative accounts of past and present relationship experiences, which provide a psychologically rich data source from which clinically expert assessors can draw reliable and valid inferences about personality. The SWAP can also be scored reliably and validly from other comparably psychologically rich interview sources (e.g., Marin-Avellan, McGauley, Campbell, & Fonagy, 2005).

Software-based scoring algorithms combine and weight item scores to derive diagnostic scale scores. SWAP-2 00 generates 37 diagnostic scales organized into three score profiles (Shedler, 2009). The three score profiles provide (1) dimensional scores for DSM-5 personality disorder diagnoses, (2) dimensional scores for an alternative set of personality syndromes identified empirically through SWAP research, and (3) dimensional trait scores derived via factor analysis of the SWAP item set. SWAP also generates a global Psychological Health Index, which measures personality strengths or adaptive resources and capacities (e.g., ego strengths). To facilitate score interpretation, all diagnostic scores are reported as T-scores ( $M = 50$ ,  $SD = 10$ ).<sup>2</sup>

```
particles = [p for p in psys.particles] if pset.type == 'ALIVE']
filenames = []
if pset.render_type == "OBJECT":
    dupli_ob = pset.dupli_object
    if dupli_ob is not None and draw_dat.instances_write_dupli:
        filepath = [bpath.abspath(draw_dat.path), dupli_ob.name]
        if os.path.exists(bpath.abspath(draw_dat.instance_export_path)):
            filepath = [bpath.abspath(draw_dat.instance_export_path), dupli_ob.name]
        filepath = "".join(filepath)
        dupli_world = dupli_ob.matrix_world.copy()
        transl_inv = Matrix.Translation(-dupli_world.translation)
        dupli_ob.matrix_world = transl_inv * dupli_ob.matrix_world
        filenames.extend(writeDupliObjects(scene, [dupli_ob], filepath, temp))
        dupli_ob.matrix_world = dupli_world
        obj.matrix_world = Matrix.Identity(4) * (unsigned long **) lookup->data;
        writeObject(context, instance_filepath, [obj]);
```

1 One way it does so is by ensuring that raters are “calibrated” with one another. Consider the situation with rating scales, where raters can use any value as often as they wish. Inevitably, certain raters will gravitate toward extreme values (e.g., values of 0 and 7 on a 0–7 scale) and others toward middle values (e.g., values of 4 and 5). Thus, the scores reflect not only the personality characteristics of the subjects but also the calibration of the raters. The Q-Sort method, with its fixed distribution, eliminates this kind of measurement error, because all clinicians must assign each score the same number of times. If the use of a standard item set gives clinicians a common vocabulary, use of a fixed distribution can be said to give them a “common grammar” (Block, 1978).

Median inter-rater reliability of SWAP diagnostic scales is above .80 in all studies to date and is often above .90 (Marin-Avellan, McGauley, Campbell, & Fonagy, 2014; Westen & Muderrisoglu, 2003; Westen & Shedler, 2007). Median test-retest reliability of SWAP-II personality disorder diagnostic scales, over a four-to-six-month interval, is .90 (Blagov, Bi, Shedler, & Westen, 2012). With respect to validity, SWAP diagnostic scales show predicted relations with a wide range of criterion measures, including genetic history variables (e.g., psychotic disorders in first- and second-degree biological), developmental history variables (e.g., childhood physical or sexual abuse), adult life events (e.g., arrests, psychiatric hospitalizations, suicide attempts), employment trouble (e.g., job loss due to interpersonal problems in the workplace), social functioning, global adaptive functioning, response to mental health treatment, and numerous other variables (for reviews, see Blagov et al., 2012; Shedler, 2015; Westen & Shedler, 2007).

## Overview of the Dispositional Indicators of Risk Exposure (DIRE) Scale

A SWAP scale for risk assessment was constructed using the same method used to construct SWAP-200 scales for DSM personality disorders (Westen & Shedler, 1999a, 1999b). The method involved tapping the explicit and implicit knowledge of expert clinicians by asking them to use the SWAP-200 to describe a hypothetical, prototypical patient representing a specific personality disorder in its “ideal” or pure form (e.g., a prototypical patient with paranoid personality disorder). The resulting SWAP-200 item scores were then averaged across the clinicians to create a *diagnostic prototype* for each personality disorder—a quantified personality description representing experts’ consensus understanding of the disorder. SWAP-200 diagnostic scale scores measure the resemblance or “match” between an assessment subject and the personality disorder diagnostic prototypes, with higher scores indicating greater resemblance to a diagnostic prototype and more severe personality pathology.

We applied this method to develop a risk-assessment scale, called the *Dispositional Indicators of Risk Exposure (DIRE)* scale. We tapped the explicit and implicit knowledge of experts about personality attributes associated with risk by asking them to use the SWAP-200 to describe a hypothetical, prototypical person who poses maximal risk. In this case, the experts were 20 adjudicators from four U.S. government intelligence agencies. Adjudicators make determinations with respect to granting or revoking security



clearances for sensitive positions such as those requiring access to classified information. The 20 adjudicators were asked to describe a hypothetical, prototypical high-risk individual “capable of endangering the safety of others, compromising important systems, or otherwise undermining national security.” We relied on adjudicators rather than clinical psychologists and psychiatrists because of their extensive experience with security risk. Clinicians are experts in diagnosis, but generally have less direct experience addressing impaired judgment, reliability, or trustworthiness in settings where security breach can be catastrophic. All adjudicators were highly experienced and had expertise in personnel security and counterintelligence.

The 20 adjudicators showed high inter-rater reliability in their SWAP-200 descriptions (Cronbach’s alpha = .92, based on intercorrelations among their SWAP-200 descriptions), indicating shared understanding (implicit or explicit) with respect to personality attributes associated with risk. The SWAP-200 descriptions were averaged across the adjudicators to create the DIRE diagnostic prototype representing maximal risk. The DIRE scale measures the degree of resemblance or match between an assessment subject and the DIRE diagnostic prototype, with higher scores indicating greater resemblance and higher risk. DIRE scores are reported as T-scores. As a general interpretive guideline, we have treated DIRE scores of  $T > 60$  as indicative of unacceptable risk and scores of  $T > 55$  as danger signs warranting close scrutiny (the cut-points mirror those for personality disorder diagnosis, where  $T > 60$  warrants a categorical DSM personality disorder diagnosis and  $T > 55$  warrants a diagnosis of traits or features of a personality disorder). The development and characteristics of the DIRE scale have been described in greater detail elsewhere (Shechter & Lang, 2011).

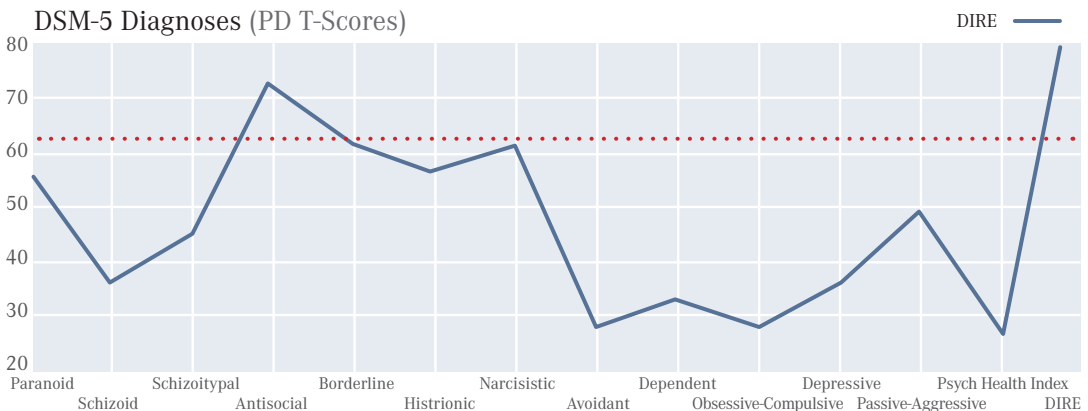


Examination of the SWAP items weighted heavily in the DIRE diagnostic prototype highlighted three personality syndromes associated with risk (Shechter & Lang, 2011). One syndrome is psychopathy, characterized by lack of an internalized value system, readiness to use and exploit others, deceitfulness, power seeking for its own sake, lack of remorse, sadism, impulsivity, thrill seeking, and externalization of blame (note that these descriptors refer to personality dynamics, not criminality or antisocial behavior). The second syndrome is what has been termed *malignant narcissism* in the clinical literature—a variant of narcissistic personality in which grandiosity, entitlement, and self-importance are suffused with aggression and shade into exploitation (e.g., Kernberg, 1975, 1984). Malignant narcissism is one of three subtypes of narcissistic personality identified empirically in prior research conducted with the SWAP (Russ, Shedler, Bradley, & Westen, 2008). The third syndrome is *borderline personality organization* (Clarkin, Yeomans, & Kernberg, 2006; Kernberg, 1975, 1984; McWilliams, 1994), characterized by affect dysregulation, unstable attachments, and unstable identity.

Clinical theory and experience suggest that these syndromes represent different pathways to risk. Individuals with psychopathic personality styles may transgress for personal gain or for the thrill of manipulating others and getting away with it. Individuals with malignantly narcissistic personality styles may transgress because they do not believe that rules created for lesser beings apply to them, or out of rage and desire for revenge when they feel slighted or devalued. Individuals with borderline personality are unstable and unpredictable (e.g., their attitudes, values, and loyalties are subject to unexpected change). Consequently, the person you are dealing with today may not be the person you are dealing with tomorrow. Additionally, individuals with borderline personality are prone to recreate internal emotional chaos in the external interpersonal world, fueling animosity, discord, and dysfunction in organizational settings (e.g., Clarkin, Yeomans, & Kernberg, 2006; Linehan, 1993).

It is also possible to look at the DIRE prototype through the lens of DSM-IV/DSM-5 personality disorder diagnoses. Recall that the DIRE diagnostic prototype is a SWAP description of a hypothetical person representing maximal risk. Figure 1 shows the SWAP-200 DSM-IV/DSM-5 personality disorder score profile for this hypothetical high-risk person. The score profile indicates how the person would be diagnosed with respect to DSM-IV/DSM-5 personality disorders by a consensus of expert clinicians (who do not limit themselves to DSM diagnostic criteria when making DSM personality disorder diagnoses; see Shedler & Westen, 2004b).

FIGURE 1. DSM-IV/DSM-5 Personality Disorder Score Profile



The recommended cut-point for making a categorical DSM diagnosis is a SWAP-200 scale score of  $T > 60$  (Shedler & Westen, 2007).<sup>3</sup> Figure 1 shows three DSM personality disorder scales with score elevations above this threshold (indicated by the red horizontal line). In DSM terms, the hypothetical, maximally high-risk individual would therefore be diagnosed with antisocial personality disorder, narcissistic personality disorder, and borderline personality disorder. Also noteworthy is the low score of  $T=27$  on the Psychological Health Index, which is nearly 2.5 standard deviations below the normative sample mean. Thus, severe personality pathology and deficits in adaptive psychological resources represent risk in their own right, independent of specific personality disorder(s).

The SWAP-200 and DIRE scale underwent initial field testing at U.S. government facilities where clinical psychologists perform psychological evaluations of personnel who require high-level security clearances for positions involving access to sensitive information. The SWAP-200 was added to a rigorous psychological assessment protocol (comprising interviews and a battery of tests including the Minnesota Multiphasic Personality Inventory [MMPI-2-RF; Ben-Porath & Tellegen, 2008] and Personality Assessment Inventory (PAI; Morey, 2009)) to evaluate clinical utility under real-world conditions. Utility was evaluated via structured surveys and debriefing interviews at the conclusion of the field trial. Participating clinicians reported that the SWAP-200 and DIRE scale was more effective than existing tools for assessing personality and for making legally defensible recommendations with respect to risk (Shechter & Lang, 2011).

<sup>3</sup> For SWAP-200, a T-score of 50 indicates average functioning in a reference sample of patients with DSM personality disorder diagnoses. A T score of 60 represents an elevation of one standard deviation relative to a reference sample of patients with DSM personality disorder diagnoses.

## Study 1: Convergent Validity of DIRE Scale

### Overview

This study examines the convergent validity of the DIRE scale by examining correlations between the scale and a range of risk-related criterion measures recorded by participating psychologists and psychiatrists in a large national clinical sample.

### Method

We contacted a random national sample of psychiatrists and psychologists with at least 5 years' experience post-training, selected from the membership rosters of the American Psychological Association and American Psychiatric Association, and asked them to use the SWAP-II to describe "an adult patient you are currently treating or evaluating who has enduring patterns of thoughts, feeling, motivation or behavior—that is, personality patterns—that cause distress or dysfunction." To obtain a sample with a broad spectrum of personality functioning, we emphasized that patients need not have a DSM personality disorder diagnosis but did need to meet the following inclusion criteria: > 18 years of age, not currently psychotic, and known well by the clinician (using the guideline of > 6 clinical contact hours but < 2 years). To obtain a random selection of patients from clinicians' practices, we instructed clinicians to consult their calendars to select the last patient they had seen during the previous week who met the study criteria. Each clinician provided informed consent, contributed data describing one patient, and received \$200 in compensation. The sample and data-collection methods have been described in prior publications (Russ et al., 2008; Westen & Shedler, 2007; Westen, Shedler, & Bradley, 2006; Westen et al., 2012).

### Dependent Measures

In addition to completing the SWAP-II, each participating clinician completed the Clinical Data Form (CDF), a clinician-report form that gathers extensive data on demographic, diagnostic, etiological, and adaptive functioning variables. CDF life event and developmental history variables show strong agreement (cross-method validity) with independent data collected via patient self-report (DeFife, Drill, Nakash, & Westen, 2010), and adaptive functioning variables assessed via the CDF (e.g., Global Assessment of Functioning [GAF]) show high validity with respect to ratings by independent observers (DeFife et al., 2010; Dutra, Campbell, & Westen, 2004; Westen et al., 1997).

Thirty CDF variables were chosen a priori by experts in personnel security as outcome or criterion variables, because they directly addressed specific undesirable events and outcomes (e.g., violence, criminality, domestic abuse, employment termination due to interpersonal problems, psychiatric hospitalization) or because of their conceptual and empirical link to risk (e.g., childhood and/or adolescent antisociality).

The criterion variables covered a wide spectrum of specific undesirable life events and behaviors as well as indicators of severe mental instability. Multiple measures of adaptive functioning provided a broad-based assessment of psychiatric stability/instability. They included the DSM-IV Global Assessment of Functioning (GAF) scale as well as clinician ratings of chronic level of personality functioning (high-functioning to severe pathology). Other items addressed quality and stability of social relationships and occupational functioning. The CDF variables also included items addressing historical life events of potential relevance to risk assessment (rated dichotomously as “no/unsure” or “yes”). These items addressed psychiatric history (i.e., suicide attempts, self-mutilation, psychiatric hospitalization), criminality and violence (e.g., arrest within the past 5 years, violence in the past 5 years, being a perpetrator in an abusive domestic relationship), or severe interpersonal or occupational problems (e.g., job loss within the past 5 years due to interpersonal conflict in the workplace). Other items addressed childhood and adolescent behaviors and events that are empirically and conceptually linked to psychopathy or antisociality (e.g., fire setting, animal torture, physical fights, stealing, violent/armed crime, running away from home, substance abuse, school trouble, sexual promiscuity).

## Results

### Sample Characteristics

The sample was  $N = 1,201$  patients, 53.2% female, 73.1% seen in private practice settings (with the remainder seen in a range of settings from outpatient clinics to forensic units), 82.7% White (with the remainder Black and/or Hispanic), with a mean age of 42.3 ( $SD = 12.3$ ) years. Patients spanned all social classes. GAF scores spanned a broad range of functioning, ranging from 10 to 93 ( $M = 57.9$ ,  $SD = 10.8$ ). One third of the sample had had at least one psychiatric hospitalization, one fourth had a history of suicide attempt(s), and one in ten had been arrested during the previous 5 years. Clinician respondents were highly experienced ( $M = 19.8$  years' practice experience,  $SD = 9.2$  years) and diverse in theoretical orientation.

## Construction of Composite Outcome Indices

To create reliable criterion measures and facilitate data interpretation, we constructed five composite scales or indices from the CDF variables. Item selection for the composite scales was guided by a principal components analysis of the 30 CDF variables, which yielded five conceptually coherent factors (technically, components), described below. We created a composite index for each factor by averaging the CDF variables with the highest loadings on each factor, after first standard scoring the CDF variables (i.e., transforming them to create score distributions with  $M = 0$ ,  $SD = 1$ ). This procedure ensures equal weighting of the items comprising a composite index. We reversed the direction of scoring of variables as needed so that higher scores always indicated maladaptive behavior or impairment.

- 1. Adult Maladaptive Functioning** provides a global measure of impaired functioning across multiple life domains. The scale comprises Global Assessment of Functioning (GAF) scores, ratings of overall personality functioning, ratings of social and occupational functioning, history of self-mutilation, history of psychiatric hospitalization, being arrested during the previous 5 years, committing a violent crime during the previous 5 years, losing a job during the past 5 years due to interpersonal problems in the workplace, and being the perpetrator in an abusive domestic relationship. Scale reliability (Cronbach's alpha) is  $\alpha = .76$ .
- 2. Employment Trouble** measures maladaptive functioning in employment settings. The scale comprises two variables—rating of occupational functioning and job loss in the past 5 years due to interpersonal problems in the workplace. Scale reliability is  $\alpha = .54$ .
- 3. Mental Instability** measures severe mental health problems. The scale comprises history of suicide attempts and history of psychiatric hospitalization. Scale reliability is  $\alpha = .71$ .
- 4. Forensic Risk/Violence** measures criminality and violence. The scale comprises arrest in the past 5 years, committing a violent crime in the past 5 years, and being the perpetrator in an abusive domestic relationship. Scale reliability is  $\alpha = .50$ .
- 5. Childhood/Adolescent Psychopathy** measures childhood/adolescent behaviors conceptually and empirically related to the constructs of psychopathy and/or antisociality. The scale comprises childhood/adolescent fire setting, animal torture, running away from home, substance abuse, physical fights, school conduct problems, school performance, lying, stealing, violence, arrests, and age at first intercourse (reverse scored). Scale reliability is  $\alpha = .74$ .

### Convergent Validity

Table 1 lists the correlations between the DIRE scale and the five CDF composite indices. All correlations involving DIRE were in the predicted direction, statistically significant ( $p < .001$  for all variables), and moderate to large in magnitude. The highest observed correlation was between DIRE and Adult Maladaptive Functioning,  $r = .64$ ,  $p < .001$ .

For more fine-grained detail, Table 2 lists the correlations between the DIRE scale and the individual CDF variables that constitute the composite indices. Within the five content domains, CDF variables are listed in descending order by magnitude of correlation. The DIRE scale showed statistically significant relations ( $p < .001$  for all variables), in the expected direction, with all 30 criterion variables.

**TABLE 1. Correlations of DIRE scale with Clinical Data Form composite indices (N = 1,201)**

Composite Scale	DIRE
Adult Maladaptive Functioning	.64*
Employment Trouble	.49*
Mental Instability	.34*
Forensic Risk/Violence	.46*
Childhood/Adolescent Psychopathy	.53*

\* $p < .001$ , two-tailed

**TABLE 2. Correlations of DIRE scale with individual Clinical Data Form items (N = 1,201)**

CDF Item	DIRE	CDF Item	DIRE
<b>Adult Maladaptive Functioning</b>		<b>Employment Trouble</b>	
Overall personality functioning	-.47*	Employment functioning	-.46*
Employment functioning	-.46*	Lost job due to interpersonal problems in past 5 years	.39*
Quality of friendships	-.44*	<b>Childhood/Adolescent Psychopathy</b>	
Lost job due to interpersonal problems in past 5 years	.39*	School trouble	.42*
Arrested in past 5 years	.36*	School performance	-.40*
Violent crime in past 5 years	.35*	Physical fights	.37*
The perpetrator in an adult abusive relationship	.34*	Chronic lying	.37*
Prior psychiatric hospitalization	.32*	Substance abuse	.35*
GAF	-.31*	Stealing	.35*
Suicide history	.28*	Age at first intercourse	-.32*
Self-mutilation	.20*	Arrest	.31*
<b>Mental Instability</b>		Running away frequency	.29*
Past suicide attempt	.28*	Promiscuity	.26*
Prior psychiatric hospitalization	.32*	Violent crime	.26*
<b>Forensic Risk/Violence</b>		Animal torture	.21*
Arrested in past 5 years	.36*	Fire setting	.17*
Violent crime in past 5 years	.35*		

\* $p < .001$ , two-tailed

## Discussion of Study 1

The SWAP harnesses reliable clinical observations and inference with respect to personality processes, which are largely lacking from risk-assessment measures beyond global psychiatric disturbance and relatively overt markers of psychopathy. The DIRE scale, derived from the SWAP instrument, shows strong correlations with a wide range of past and current risky behaviors and undesirable outcomes, suggesting that the personality features encompassed by the DIRE scale are valid predictors of undesirable outcomes and risk, including, but not limited to, criminality.

A limitation of the study is that the same clinicians who completed the SWAP completed the CDF and knew the subjects' history. Although SWAP items address dynamic psychological and personality variables rather than risky events and outcomes, knowledge of an assessment subject's history may have influenced the scoring of SWAP items, or alternatively, knowledge of current personality functioning may have influenced the scoring of CDF items.

A number of considerations mitigate these concerns. With respect to the CDF, research shows high convergent validity of clinician-rated CDF variables with independent data sources; many of the variables code objective events which leave little room for interpretation; and where clinician- and self-report data occasionally diverged with respect to historical events (e.g., childhood sexual abuse), clinicians were appropriately conservative in their ratings and followed instructions to code "no/unsure" when uncertain (Westen et al., 1997; DeFife et al., 2010; Dutra et al., 2004). With respect to SWAP scores, research consistently shows high inter-rater reliability between treating clinicians and independent research interviewers who score the SWAP on the basis of the CDI or other personality-oriented research interviews that do not address life history (Marin-Avellan, McGauley, Campbell, & Fonagy, 2005; Westen & Muderrisoglu, 2003; Westen & Shedler, 2007; Westen et al., 2012). It therefore appears that SWAP diagnostic scores reflect, as intended, reliable clinical observations and inferences drawn from the here-and-now interaction between clinician and subject. Had the SWAP-II been scored by research interviewers with little or no knowledge of the subjects' history, the SWAP-II diagnostic scale scores would have been largely unchanged (for further discussion, see Westen & Shedler, 2007).

The magnitude of the correlations between DIRE and the composite and individual criterion variables suggests that the DIRE functions as intended, as a measure of personality-related risk. An additional advantage of SWAP

over a history review for risk assessment is that it provides a comprehensive, in-depth assessment of personality that can inform intervention and risk management strategies in ways that a generic tabulation or sum of risky past behaviors cannot.

## Study 2: Predictive Validity of DIRE

### Overview

This study examined the prospective relation between the DIRE scale and criminal recidivism in a sample of psychiatrically disturbed criminal offenders during a 1-year period of living in the community. Predictive validity of DIRE is compared with that of two standard risk-assessment measures for prediction of criminality and violence with mentally disordered offenders, the HCR-20 and the Hare Psychopathy Check List: Screening Version (PCL-SV; Hart, Cox & Hare, 1995).

### Method

All offenders were assessed with the SWAP-200 at baseline. All had been convicted of violent crimes and were either living in the community or about to be discharged into the community. They were followed for a 1-year period. The outcome measure was criminal recidivism, defined as criminal offense(s) during the 1-year follow-up period.

### Sample

The initial sample consisted of  $N = 35$  psychiatrically disturbed male criminal offenders in England who had been convicted of at least one violent offense and were currently living in the community or about to be discharged from a secure psychiatric facility into the community, having been detained under the 1983 Mental Health Act for England and Wales (Department of Health, 1983). As part of their sentence, they were required to be under the supervision of a forensic psychiatrist, and many were also in treatment with a forensic clinical psychologist. Exclusion criteria were a diagnosis of schizophrenia or impaired intelligence. Outcome data are reported for  $N = 31$  offenders for whom follow-up data were available.

All offenders had previously been diagnosed with one or more DSM-IV personality disorders (mean = 1.4), the most prevalent being antisocial personality disorder, as well as a variety of other lifetime or current mental health conditions, the most common of which were lifetime alcohol and/or drug abuse (69%) and current mood or anxiety disorder (17%).



The offenders had an average of 21 criminal convictions, the most common being minor violence (75%) (e.g., assault, affray, actual bodily harm, child cruelty) and crimes against the person (68%) (e.g., harassment, menacing). The offenders had served an average of 3.2 years in prison ( $SD = 4.5$ ). Ninety percent of the sample started to offend between the ages of 10 and 24, and 60% started to engage in violent criminal behavior between the ages of 14 and 24. Mean age was 38 ( $SD = 9$ ). The sample characteristics have been described in greater detail elsewhere (Marin de Avellan, 2010).

### Assessment

The SWAP-200 was completed by the offender's treating psychiatrist or psychologist at the start of the study. Clinicians who contributed SWAP-200 data had a minimum of 2 years' experience working with forensic psychiatric patients. A clinical researcher (not involved with offenders' treatment) separately scored the HCR-20 and PCL-SV based on chart review as well as brief conversations with treating clinicians when necessary to clarify or verify information. The HCR-20 (Webster et al., 1997) contains 20 items designed to structure and systematize professional judgments about risk with mentally disordered offenders. The HCR-20 items were combined to create a scale score for research use. The PCL-SV (Hart et al., 1995) is a 12-item version of the Hare Psychopathy Checklist—Revised (Hare, 2003), a standard risk-assessment instrument in forensic and correctional populations, originally developed to assess offenders convicted of violent crimes. The PCL-SV correlates sufficiently highly with the parent test ( $r = .95$ ; Guy & Douglas, 2006) to be considered empirically interchangeable.



**Outcome**

The outcome measure was criminal recidivism, defined as criminal arrests(s) during a 1- year period living in the community (0 = no reported offense, 1 = one or more arrests).

**Results**

Ten (32.3%) of the 31 offenders for whom follow-up data were available re-  
cidivated during the follow-up period, with eight arrested for violent offenses.

As expected, the mean DIRE score was significantly elevated in the offender sample, with a sample mean of  $T = 59.2$  ( $SD = 7.1$ , range = 47.1 to 72.2), or approximately one standard deviation above the mean of the clinical reference sample. DIRE prospectively and significantly predicted criminal recidivism,  $r = .37$  ( $p < .05$ , two-tailed). To facilitate communication to individuals who may lack a statistical background, the relation between DIRE and recidivism can also be expressed in percentage terms: The probability of criminal recidivism increases by 12.5 percentage points for each 5-point (half a standard deviation) increase in the DIRE score. Receiver operating characteristic (ROC) analysis showed that the DIRE scale discriminated offenders who did and did not recidivate, with an area under the ROC curve of .72. A DIRE cut-score of  $T = 59$  correctly identified 80% of offenders who recidivated (sensitivity) and 60% of those who did not recidivate (specificity).

DIRE was a somewhat better predictor of criminal recidivism than the HCR-20 ( $M = 22.8$ ,  $SD = 6.7$ ), which yielded an area under the ROC curve of .65 and a positive but nonsignificant correlation with recidivism,  $r = .27$ , ns. DIRE was approximately equivalent in prediction to the PCL-SV ( $M = 12.3$ ,  $SD = 5.4$ ), which yielded an area under the ROC curve of .74 and a correlation with recidivism of  $r = .42$  ( $p < .05$ , two-tailed). Findings for the three risk-assessment measures are summarized in Table 3.

<b>TABLE 3. Predictive validity of three measures of risk</b>			
<b>Scale</b>	<b>Mean (SD)</b>	<b>Area under ROC curve</b>	<b>Correlation with Recidivism</b>
DIRE	59.2 (7.1)	.72	.37*
HCR-20	22.8 (6.7)	.65	.27
PCL-SV Total	12.3 (5.4)	.74	.42*

*\*p < .05, two-tailed*

**Discussion of Study 2**

This study puts the DIRE scale to a stringent test, due to the use of a psychiatrically disturbed offender sample in which all subjects had DSM personality disorder diagnoses. The study inclusion criteria imposed considerable range restriction on the prediction side of the prediction equation, since all subjects had severe personality pathology and clinically diagnosed personality disorders. Such range restriction

necessarily has the statistical effect of attenuating the relation between the DIRE scale and any outcome measure. Use of a correctional population also places the DIRE scale at a disadvantage relative to the two comparison risk-assessment instruments, both of which were developed to discriminate *within* offender samples. The study sets a far more difficult task for DIRE than assessment and prediction in a general (non-correctional) population, such as in personnel screening, where the majority of subjects do not have criminal histories or diagnosed personality disorders. However, even within this truncated group of criminal offenders with personality disorder diagnoses, DIRE was roughly equivalent to the PCL-SV as a predictor of recidivism and a slightly better predictor than the HCR-20.



## General Discussion

One way to break through the current “ceiling” (Skeem & Monahan, 2011, p. 41) on the accuracy of risk prediction is to increase the breadth and depth of dynamic personality constructs (vs. static historical events) addressed by assessment and prediction methods. One advantage of the SWAP and DIRE scale over the Psychopathy Checklist is that the SWAP, for roughly the same expenditure of assessor time and effort, provides a comprehensive assessment of personality and a broad array of psychological information which can inform intervention and risk management strategies.

In non-forensic populations—for example, among individuals who pass background checks for government and private sector positions—there is every reason to believe that DIRE will outperform current risk-assessment procedures that were developed in correctional populations and designed for use specifically when there is a known prior offense. The vast majority of members of the general population do not have criminal backgrounds or show overt signs of antisociality. Where risk-assessment instruments that assume a prior offense may give a “free pass,” DIRE has the potential to identify personality styles and syndromes that could pose risk, including both criminal and non-criminal insider threats in organizations that conduct background checks to screen for criminality and other static variables (past events and behavior) indicative of risk. Even in a truncated, range-restricted sample of psychiatrically disturbed criminal offenders with DSM personality disorder diagnoses, DIRE performed as well as or slightly better than standard, widely used risk-assessment methods. ✓

“

Where risk-assessment instruments that assume a prior offense may give a “free pass,” DIRE has the potential to identify personality styles and syndromes that could pose risk.

.....

.....

## REFERENCES

- Ben-Porath, Y. S. & Tellegen A. (2008). *MMPI-2-RF (Minnesota Multiphasic Personality Inventory-2-Restructured Form) manual for administration, scoring, and interpretation*. Minneapolis, MN: University of Minnesota Press.
- Blagov, P., Bi, W., Shedler, J. & Westen, D. (2012). The Shedler-Westen Assessment Procedure (SWAP): Evaluating psychometric questions about its reliability, validity, and impact of its fixed score distribution. *Assessment*, 19, 370–382.
- Block, J. (1971). *Lives through time*. Berkeley, CA: Bancroft.
- Block, J. (1978). *The Q-Sort method in personality assessment and psychiatric research*. Palo Alto, CA: Consulting Psychologists Press.
- Buss, A. H. (1961). *The psychology of aggression*. New York, NY: Wiley.
- Clarkin, J. F., Yeomans, F. E., & Kernberg, O. F. (2006). *Psychotherapy for borderline personality: Focusing on object relations*. Washington, DC: American Psychiatric Publishing.
- Daffern, M., & Howells, K. (2002). Psychiatric inpatient aggression: A review of structural and functional assessment approaches. *Aggression and Violent Behavior*, 7, 477–497.
- DeFife, J. A., Drill, R., Nakash, O., & Westen, D. (2010). Agreement between clinician and patient ratings of adaptive functioning and developmental history. *American Journal of Psychiatry*, 167, 1472–1478. doi: 10.1176/appi.ajp.2010.09101489
- Department of Health (1983). *Mental Health Act*. London, HMSO
- Dutra, L., Campbell, L., & Westen, D. (2004). Quantifying clinical judgment in the assessment of adolescent psychopathology: Reliability, validity, and factor structure of the Child Behavior Checklist for Clinician-Report. *Journal of Clinical Psychology*, 60, 65–85.
- Guy, L. S. & Douglas, K. S. (2006). Examining the utility of the PCL:SV as a screening measure using competing factor models of psychopathy. *Psychological Assessment*, 18, 225–230.
- Hare, R. D. (2003). *Manual for the Revised Psychopathy Checklist (2nd ed.)*. Toronto, ON, Canada: Multi-Health Systems
- Harms, P. D., Marbut, A., Johnston, A. C., Lester, P. & Fezzey, T. (2022). Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats. *Journal of Information Security and Applications*. 71. 103378. 10.1016/j.jisa.2022.103378. <https://doi.org/10.1016/j.jisa.2022.103378>
- Hart, S. D., Cox, D. N., & Hare, R. D. (1995). *Manual for the Psychopathy Checklist: Screening Version (PCL: SV)*. Toronto, Canada: Multi-Health Systems.
- Heilbrun, K. (1997). Prediction versus management models relevant to risk assessment: The importance of legal decision-making context. *Law and Human Behavior*, 21, 347–359.
- John, O. (1990). The big five factor taxonomy: Dimensions of personality in the natural language and in questionnaires. In L. Pervin (Ed.), *Handbook of personality: Theory and research* (pp. 66–100). New York, NY: Guilford Press.
- Kernberg, O. (1975). *Borderline conditions and pathological narcissism*. Northvale, NJ: Jason Aronson.
- Kernberg, O. (1984). *Severe personality disorders*. New Haven, CT: Yale University Press.
- Kohut, H. (1971). *The analysis of the self: A systematic approach to the treatment of narcissistic personality disorders*. New York, NY: International Universities Press.
- Kraemer, H., Kazdin, A., Offord, D., Kessler, R., Jensen, P., & Kupfer, D. (1997). Coming to terms with the terms of risk. *Archives of General Psychiatry*, 54, 337–343.
- Kroner, D., Mills, J., & Morgan, B. (2005). A coffee can, factor analysis, and prediction of antisocial behavior: The structure of criminal risk. *International Journal of Law & Psychiatry*, 28, 360–374.
- Linehan, M.M. (1993). *Cognitive-behavioral treatment of borderline personality disorder*. New York, NY: Guilford Press.
- Livesley, W.J. (1995). *The DSM-IV personality disorders*. New York, NY: Guilford Press.
- Marin de Avellan, L. E. (2010). *Systematizing clinician judgment of personality and risk: Validation of the SWAP-200 with forensic patients*. Unpublished manuscript. University College London, London, UK.
- Marin-Avellan, L., McGauley, G., Campbell, C., & Fonagy, P. (2014). The validity and clinical utility of structured diagnoses of antisocial personality disorder with forensic patients. *Journal of Personality Disorders*, 28, 500–517.
- Marin-Avellan, L., McGauley, G., Campbell, C., & Fonagy, P. (2005). Using the SWAP-200 in a personality-disordered forensic population: Is it valid, reliable and useful? *Criminal Behaviour and Mental Health*, 15, 28–45.
- McCrae, R., & Costa, P. (1990). *Personality in adulthood*. New York, NY: Guilford Press.
- McWilliams, N. (1994). *Psychoanalytic diagnosis: Understanding personality structure in the clinical process*. New York, NY: Guilford Press.
- McWilliams, N. & Shedler, J. (2017). *Psychodynamic Diagnostic Manual-2 (PDM-2): Personality Syndromes*. NY: Guilford Press.
- Meloy, J. R. (1988). *The psychopathic mind: Origins, dynamics, and treatment*. Northvale, NJ: Jason Aronson.
- Morey, L. (1991). *Personality Assessment Inventory: Professional manual*. Odessa, FL: Psychological Assessment Resources.

REFERENCES

- Nicoletti, J., Spencer-Thomas, S., & Bollinger, C. (1999). *Violence goes to college*. Springfield, IL: Charles C. Thomas.
- Perry, J. C., & Cooper, S. H. (1987). Empirical studies of psychological defense mechanisms. In R. Michels & J. O. J. Caenar (Eds.), *Psychiatry*. Philadelphia, PA: J. B. Lippincott.
- Russ, E., Shedler, J., Bradley, R., & Westen, D. (2008). Refining the construct of narcissistic personality disorder: Diagnostic criteria and subtypes. *American Journal of Psychiatry*, 165, 1473-1481.
- Shapiro, D. (1965). *Neurotic Styles*. New York, NY: Basic Books.
- Shechter, O. G. & Lang, E. L. (2011). Identifying personality disorders that are security risks: Field Test results. *Defense Personnel Security Research Center*, Technical Report 11-05.
- Shedler, J. (2022). The personality syndromes. In R. Feinstein (Ed.), *Personality Disorders*. Oxford: Oxford University Press.
- Shedler, J. (2015). Integrating clinical and empirical perspectives on personality: the Shedler-Westen Assessment Procedure (SWAP). In S. Huprich (Ed.), *Personality disorders: Toward Theoretical and Empirical Integration in Diagnosis and Assessment*. Washington, DC: American Psychological Association.
- Shedler, J. (2009). *Guide to SWAP-200 Interpretation*. Denver, CO: SWAPassessment LLC.
- Shedler, J., Mayman, M., & Manis, M. (1993). The illusion of mental health. *American Psychology*, 48, 1117-1131.
- Shedler, J., & Westen, D. (2004a). Dimensions of personality pathology: An alternative to the Five Factor Model. *American Journal of Psychiatry*, 161, 1743-1754.
- Shedler, J., & Westen, D. (2004b). Refining personality disorder diagnoses: Integrating science and practice. *American Journal of Psychiatry*, 161, 1350-1365.
- Shedler, J., & Westen, D. (2007). The Shedler-Westen Assessment Procedure (SWAP): Making personality diagnosis clinically meaningful. *Journal of Personality Assessment*, 89, 41-55.
- Skeem, J. L. & Monahan, J. (2011). Current directions in violence risk assessment. *Current Directions in Psychological Science*, 20, 38-42. doi: 10.1177/0963721410397271.
- Vaillant, G. (Ed.). (1992). *Ego mechanisms of defense: A guide for clinicians and researchers*. Washington, DC: American Psychiatric Association Press.
- Webster, C., Douglas, K., Eaves, D., & Hart, S. (1997). *HCR-20: Assessing risk for violence (Version 2)*. Vancouver, Canada: Simon Fraser University.
- Westen, D. (1991). Social cognition and object relations. *Psychological Bulletin*, 109, 429-455.
- Westen, D. (2004). *Clinical Diagnostic Interview: Unpublished Manual*. Emory University, Atlanta, GA. Retrieved from www.psychsystems.net.
- Westen, D., Lohr, N., Silk, K.R., Gold, L., & Kerber, K. (1990). Object relations and social cognition in borderlines, major depressives, and normals: A Thematic Apperception Test analysis. *Psychological Assessment: A Journal of Consulting and Clinical Psychology*, 2, 355-364.
- Westen, D., & Muderrisoglu, S. (2003). Reliability and validity of personality disorder assessment using a systematic clinical interview: Evaluating an alternative to structured interviews. *Journal of Personality Disorders*, 17, 350-368.
- Westen, D., & Muderrisoglu, S. (2006). Clinical assessment of pathological personality traits. *American Journal of Psychiatry*, 163, 1285-1287.
- Westen, D., Muderrisoglu, S., Fowler, C., Shedler, J., & Koren, D. (1997). Affect regulation and affective experience: Individual differences, group differences, and measurement using a Q-sort procedure. *Journal of Consulting & Clinical Psychology*, 65, 429-439.
- Westen, D., & Shedler, J. (1999a). Revising and assessing Axis II, Part 1: Developing a clinically and empirically valid assessment method. *American Journal of Psychiatry*, 156, 258-272.
- Westen, D., & Shedler, J. (1999b). Revising and assessing Axis II, Part 2: Toward an empirically based and clinically useful classification of personality disorders. *American Journal of Psychiatry*, 156, 273-285.
- Westen, D., & Shedler, J. (2007). Personality diagnosis with the Shedler-Westen Assessment Procedure (SWAP): Integrating clinical and statistical measurement and prediction. *Journal of Abnormal Psychology*, 116(4), 810-822.
- Westen, D., Shedler, J., & Bradley, R. (2006). A prototype approach to personality diagnosis. *American Journal of Psychiatry*, 163, 846-856.
- Westen, D., Shedler, J., Bradley, B., DeFife, J. (2012). An empirically derived taxonomy for personality diagnosis: Bridging science and practice in conceptualizing personality. *American Journal of Psychiatry*, 169, 273-284.
- Westen, D., Waller, N. G., Shedler, J., & Blagov, P. S. (2014). Dimensions of Personality and Personality Pathology: Factor Structure of the Shedler-Westen Assessment Procedure-II (SWAP-II). *Journal of Personality Disorders*. 28. 281-318. 10.1521/pedi\_2012\_26\_059.
- Westen, D., & Weinberger, J. (2004). When clinical description becomes statistical prediction. *American Psychologist*, 59, 595-613.
- Yang, M., Wong, S. C. P., & Coid, J. (2010). The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychological Bulletin*, 136, 740-767.







# **LESSONS LEARNED AND CASE STUDIES**

---



# The Difference is Human – Building Preventative Insider Threat Programs

---

**Chris Babie**



**R**ecent U.S. events have highlighted insider risk, the lack of preventative postures, and addressing insider threat as a human behavioral risk. A Swedish example highlights the problem. The two Kia brothers operated almost in plain sight. Still, nobody reacted or was ready



**CHRIS BABIE**

Chris Babie is a motivated cyber professional with 10+ years of experience across several cyber disciplines. Chris graduated from Rensselaer Polytechnic Institute in 2011 and was selected to join GE’s Digital Technology Leadership Program (DTLP) where he led large-scale technical projects across a broad range of technologies & functions. Chris currently leads the Insider Threat team @ GE Gas Power where he & the team are protecting the GE Gas Power’s intellectual property by building a proactive, human-centric program.



to challenge, and this tells a story of a failed insider threat program, even if the behavioral indicators were obvious.

Peyman Kia conducted intelligence operations on Swedish soil for the Russian military intelligence service (GRU) between 2007-2015, giving the Russian military countless classified documents from the Swedish Security Service (SÄPO) as well as the Swedish Military Intelligence Service (MUST)—. Kia and his brother were in January 2023 found guilty of aggravated espionage and will now serve a life sentence and a nine and half-year sentence.

The fascinating element of this case is the overwhelming human risk factors displayed by Peyman Kia for years, allowing him to funnel Swedish classified information to the Russian intelligence agencies. Some of the anomalous/outlier behavior included:

- 1.** Frequently visited the office late at night and during off-hours and accessed highly sensitive material, which would eventually be found on his personal device.
- 2.** Repeatedly displaying counter-productive work behaviors/personal risk factors (e.g., disgruntlement, aggression)
- 3.** Spending considerable time coordinating meetings with Russian agencies, transferring documents and devices at “drop” locations - time investment in non-work/role-related activities.
- 4.** Attaching as many as 15 different external devices to his work computer to transfer classified information.

This case highlights that insight into human risk factors and behaviors, above all else, are critical in detecting future insider risk. Orga-

nizations spend an extraordinary amount of time, effort, and money in implementing transactional detection systems. These teams then route an incredible amount of information to them—but this “tech first” strategy is flawed. This approach inundates teams with alerts, lacks context that would allow for effective prioritization of high-risk events, and leads to a large volume of false-positive events. Organizations who put their attention on transactional intelligence are immediately operating in a “reactive” state.

“  
Organizations who  
put their attention  
on transactional  
intelligence are  
immediately  
operating in a  
“reactive” state.  
.....

The case above, and many other instances of malicious Insider cases, highlights how a non-technical, human-based approach puts an organization in a far better position—a preventative posture against Insider risk.

Suppose SÄPO’s intelligence teams had insight into the above “human” markers and an organizational culture comfortable reporting outlier human behavior. In that case, it’s possible that the unauthorized sharing of information that “could be detrimental to Sweden’s security” could have been prevented.

These behaviors and human markers are not unique to Peyman Kia; they are a common observation across documented malicious Insider cases over time. This factor was highlighted in Lenzenweger & Shaw’s article Critical Pathway to Insider Risk Model published in CITRAP (Counter-Insider Threat Research and Practice) last year, stating:

“  
*What is particularly noteworthy in these initial pilot studies is a pattern of a steady accumulation of stressors, concerning behaviors, contextual risks as one would expect. But, we have also seen predisposing factors (e.g., personality traits such as hostility or anger) begin to reveal themselves in more amplified or accentuated observable behaviors over time.*

It is essential to understand that these observations provide little value if an organization doesn’t have a culture where non-compliance / outlier behavior is reported. Whether you are operating a mature insider program, or just starting to build one, you need to ensure that the entire matrix of your business has a consistent threshold and openness for reporting workplace



“  
Whether you are operating a mature insider program, or just starting to build one, you need to ensure that the entire matrix of your business has a consistent threshold and openness for reporting workplace concerns.  
.....”

concerns—this must be a critical path item for any effective program as it is the primary pipeline of human intelligence. Here are a few ways to understand any culture gaps within your organization:

- 1. Surveys:** Issue a cross-functional study and ask a straightforward question - “Do you feel comfortable reporting outlier behavior / non-compliance?” Areas, where the workforce feels less comfortable would be great candidates for insider training, education, and awareness. This indicator is also an opportunity to partner with functional leadership to understand the root cause of underreporting.
- 2. Training:** Often, reporting channels are too complex, or people aren’t aware of the reporting channels available to them. It’s important that there is a constant stream of awareness around reporting channels and how to escalate concerns available to your users. This can be done via training, newsletters, educational videos, etc.

With a company culture now in place that is comfortable with reporting suspicious behavior / non-compliance, organizations need to tap into this concern data meaningfully. Teams can consume this data from the reporting system directly and/or create tight partnerships with people-facing functions (e.g., Human Resources, Compliance) to ensure that concerns that could morph into insider risk are conveyed to the insider teams at some frequency (e.g., weekly, monthly, etc.)

This data is valuable because these concerns alone may warrant an insider review or investigation. This intelligence becomes even more powerful when used in conjunction with transactional intelligence as it provides richer context to the events and analyst teams—this now enables a priority-based alert model where the team can analyze events originating from users demonstrating counter-productive work behaviors and where there may be intended to cause harm to an organization.

Creating a company culture where reporting suspicious behavior is encouraged is one element of a human-first insider program; the other is helping create a positive working environment for your user base. Insider teams likely have not considered this work in-scope for their program. Still, data suggests that overall employee sentiment and company culture will directly impact the insider team through increased cases of negligence and possible intentional insider events:

“*With respect to insider threat, research has shown that burned-out employees are substantially less likely to adhere to security requirements (59% for burned-out employees vs. 80% for others). Similarly, burned-out employees are much more likely to download and use software without their organizations' permission (48% vs. 30%), according to the study “The Burnout Breach: How employee burnout is emerging as the next frontier in cybersecurity” as stated in a study conducted by the security firm 1Password in 2021.*

As Ponemon Institute points out in their 2022 Insider report, “3,807 attacks, or 56%, were caused by employee or contractor negligence.”

Since the insider team's mission is to protect the organization from potentially harmful events through negligence or intent, the team must actively influence positive organizational culture. This is where partnerships must be

built with people-facing functions (Human Resources, Compliance) to ensure both the right organizational culture is being driven and that there is an action plan in place to address gaps in that culture across the enterprise.

It also helps to adjust the tone of your overall insider / security teams. You need to ensure your brand is not that of “Big Brother.” This may drive negative sentiment within the workforce because users feel as though they are constantly being judged, watched, and there is inherently a lack of trust in the user base. The operations team needs to make it crystal clear that everyone has an active role to play in protecting the organization from insider events.



“

The operations team needs to make it crystal clear that everyone has an active role to play in protecting the organization from insider events.

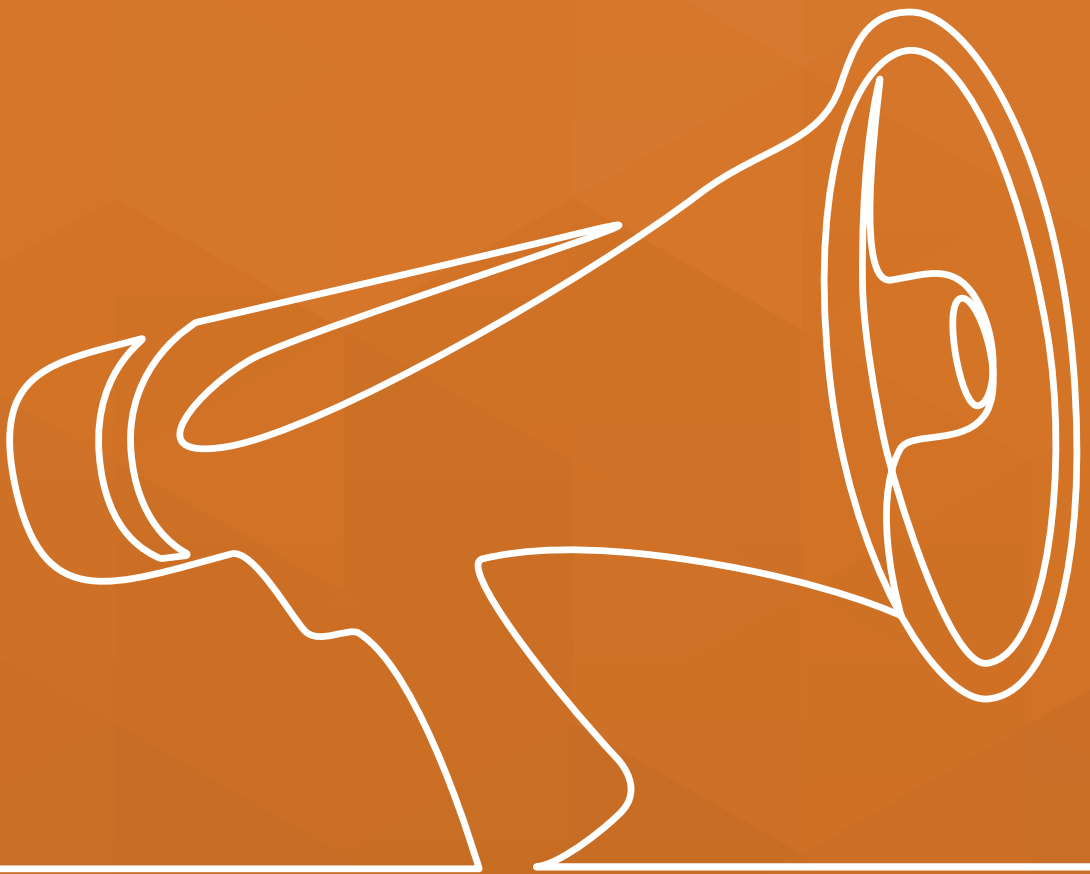
.....



The most vital asset for an insider team is, and always will be, humans. They are also the most significant risk as insider risk, at its core, is a human problem to solve. There needs to be a fundamental shift in how we collectively attack the insider problem. The workforce is the closest to those who may display toxic work and/or outlier behavior and may be your only line of sight to outlier behavior. Also, the workforce who feels supported sees opportunities for professional growth and has an investment in the organizational mission will work more compliantly, yielding a decrease in insider events.

Through this human-first approach and overall investment, we will shift insider programs from reactionary to preventative. ✓





**SUBMISSIONS  
AND CALL  
FOR PAPERS**

# Submissions and Call for papers

---



## EDITORIAL

Jonathan W. Roginski, Ph.D.  
Jan Kallberg, Ph.D., J.D./LL.M.  
James Bluman, Ph.D., P.E.

## CONTACT

jonathan.roginski@westpoint.edu  
insiderthreat@westpoint.edu

## MANUSCRIPT SUBMISSIONS

<https://www.editorialmanager.com/mirrorjournal/default2.aspx>

**Managing Insider Risk and Organizational Resilience (MIROR) Journal** is an editorial-reviewed online and print publication. MIROR will share research, best operational practices, leadership perspectives, and reviews of relevant work that further both the proactive practices of insider risk management and promotion of holistic wellness and resilience in organizations.

The editors will review content across those areas that move discussion forward concerning insider risk and organizational resilience, including but not limited to the following:

- **Recruitment and pre-employment screening.** How do we recruit and hire the right "fit" for our organization, setting the stage for longer term and higher quality retention?
- **Development and/or implementation of policies and practices.** How does an agency build policies and practices to accomplish its mission while maximally protecting against risks presented to mission accomplishment from the inside?
- **Training and education.** How do we effectively train the workforce on policies and practices (prepare for the known) and educate toward continuous improvement (prep for the unknown)?
- **Continuous evaluation.** How do we foster trust across the enterprise by thoughtfully and respectfully verifying the alignment of values between individual and organization extant at hiring continues to result in mutually supportive behaviors?

## SUBMISSIONS AND CALL FOR PAPERS

- **Risk modeling and reporting.** How do we leverage the tremendous suite of quantitative and qualitative mathematical, statistical, and mental models that exist (or will exist) against the challenge of keeping people and organizations happy, healthy, and safe? How are the results of those models communicated to leaders to facilitate decision making and change?
- **Data science applications.** Data science is arguably the most “in-demand” contemporary analytical field—how may we benefit from the groundbreaking knowledge and techniques in the insider risk and threat management field?
- **Creation and maintenance of positive organizational culture.** Employees that are connected to and invested in their organization are protective and constructive toward themselves, their peers, and the company. How do we make, keep, and foster such an environment?
- **Employee intervention.** How do we identify people and practices that increase risk of negative insider activity and align appropriate resources to protect people and the enterprise?

### ARTICLE TYPES AND SUBMISSION

#### Submissions in the following categories are welcome:

**Professional Commentary** (800+ words) Professional commentaries seek to bring forward insight from leaders in the field and highlight recent developments, concerns, and bridge gaps between industry, government, and academia. A Professional Commentary includes references as embedded discussions in the text and no endnotes.

**Original Research** (1500 – 5000 words)

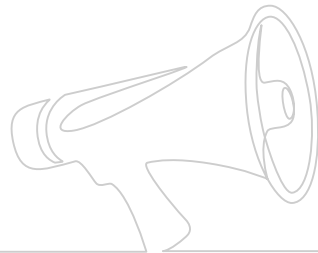
**Traditional Research Article** (up to 5,000 words) with findings and results

**Research Notes are short articles** (1500 – 2500 words) with preliminary findings, early results, or responses to current developments. Endnotes must be hyperlinked with the text referenced. Discursive endnotes are strongly discouraged; cite only direct quotations and paraphrases. No need for a bibliography. The journal’s formatting style is the Chicago Manual of Style (CMS), 17th edition, endnotes.

**Lessons Learned, Case Studies, Vignettes** (500 – 1500 words) Experiences from practitioners and professionals close to the developments in the field. The article type is a feedback loop from the field back to the community. A Lessons Learned, Case Studies, Vignettes article has needed references as embedded discussions in the text and no endnotes.

**Book Review** (1000 words) Traditional academic book review with no endnote references.

.....





**THE HQDA G-3/5/7, DAMO-ODP, ARMY COUNTER-INSIDER THREAT PROGRAM IS AN INTEGRATED EFFORT ACROSS THE TOTAL ARMY ESTABLISHED TO PROTECT INSTALLATIONS, NETWORKS, FACILITIES, PERSONNEL, AND MISSIONS FROM THE RISK INSIDERS POSE TO NATIONAL SECURITY.**



**U.S. ARMY**

**COUNTER-INSIDER THREAT PROGRAM**

**HQDA | DCS | G-3/5/7 | DAMO-ODP/DAMO-ODH**

**From the offsite contractor logically accessing Army networks to the senior Army leader stationed on the Pentagon Reserve, and Soldiers, staff, and personnel everywhere in between, the Army Counter-Insider Threat Program develops policies and procedures to improve the Army's reaction and preemptive responses to combat risks posed by existing and evolving threats.**

**The Army Counter-Insider Threat Program Management Team** consists of highly trained individuals focused on policy development training and awareness, reporting procedures, and data processing to continually enable all Army Commands, Army Service Component Commands, and Direct Reporting Units to prevent, deter, detect, and mitigate insider threats

**OR QUESTIONS OR FOR MORE INFORMATION ABOUT THE ARMY COUNTER-INSIDER THREAT PROGRAM PLEASE CONTACT THE ORGANIZATIONAL INBOX:**

**[usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.damo-odp-counter-int@army.mil](mailto:usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.damo-odp-counter-int@army.mil)**



The insider threat is a human problem resulting from a complex interaction among individuals and environmental factors.

Social and behavioral sciences are well-suited to address this complicated and persistent human problem.

The Defense Personnel and Security Research Center founded the Threat Lab in 2018 to incorporate the social and behavioral sciences into the counter-insider threat mission space. Our vision is to be a global leader in creating and sharing social and behavioral sciences knowledge to counter the insider threat.

- We work with stakeholders to transform operational challenges into actionable research questions.
- We design and execute research projects that result in accessible, concise findings and recommendations
- We integrate into training and awareness materials that organizations can use or customize for their own purposes.



Access Threat Lab tools and products available for public distribution:  
<https://www.dhra.mil/perserec/threat-lab-toolkit/>



**The West Point Insider Threat Program connects Department of Defense and Department of the Army's Insider Threat efforts with an interdisciplinary team to counter insider threat by fostering a positive leadership climate that reduces threat likelihood and impact.**



When the Office of the Under Secretary of Defense (I&S) and the Department of Army recognized a need; the US Military Academy and Department of Mathematical Science answered the call. The result is the Insider Threat Program which builds an ecosystem of trust, development, and caring to create an environment incompatible with Insider or Inside Threat.

#### **Change the conversation about Insider Threat**

- Why does Insider Threat happen?
- How do we prevent?
- How do we detect?
- How do we mitigate effects?

#### **Support to DoD and Army**

- Oath to Constitution
- Army Prioritized Protection List
- Network Engagement Team

#### **Deploy Artifacts**

- Undergraduate internships, presentations, theses
- MIROR Journal

**For inquiries and information about West Point Insider Threat Program**

**email: [insidertthreat@westpoint.edu](mailto:insidertthreat@westpoint.edu)**

**web: [insidertthreat.westpoint.edu](http://insidertthreat.westpoint.edu)**