PROFESSIONAL COMMENTARY

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

Val LeTellier

The 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

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.

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

CCommon 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..