4TH GEN

Red Flags Reimagined

A CIA Operations Officer on Today's Insider Risk Challenge

by Val LeTellier

https://4thgen.com

The Challenge

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 off boarding processes and fueled the 'Great Exfiltration' of intellectual property. COVID and political divisions increased employee stress, distraction, and disenfranchisement.

Nation states and criminal groups have become bolder at recruiting vulnerable employees to steal and ransom data. Then there were the mass tech layoffs and a 21-year old Air National Guardsman named Jack Teixeira. To borrow from the cybersecurity 'CIA Triad', the *Confidentiality, Integrity and Availability* of our people, processes, and property are at risk.

And 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'. And 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. And you need to balance employee privacy, welfare, morale, organizational culture, and possibly even trusted workforce and zero trust strategies. And 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.

The Insider Threat Kill Chain

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 determined they would do anything to better their situation, including betraying their country. Meaning, they were predisposed toward recruitment and 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 have the right pitch.

Knowing that, I started looking beyond standard motivations and vulnerabilities and focused on the telltale signs of **predisposition** while waiting for **critical events** that would move my target forward. I would then exploit their resulting internal **conflict**, channel their **determination**, and **prepare** them for action – as aligned with the below-noted insider threat 'kill chain'.

Using insider threat terminology, I was **looking for early indicators early on the critical path**, and then exploiting the resultant internal conflict.

Early Warning

Leveraging this offensive tradecraft to develop our defensive posture, it's easy to see the overwhelming importance of predisposition and critical events to **early warning**. While arguably the most critical element of insider risk mitigation, early warning is 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 different forms: theft, sabotage, violence, etc. These statistically consistent root causes provide the opportunity to identify and intercept a budding insider early along the critical path, well before an incident occurs.

But we often don't maximize that opportunity, failing to see what's right in front of us. The reasons are well-known: the lack of critical resources and the cultures, biases, and assumptions of organizations. Then, there's an overreliance on traditional insider threat indicators that are less and less meaningful in today's world -- like debt, wealth, working hours, foreign contacts/travel, and personal device usage.

To complicate matters further, the move to remote work is particularly detrimental: behavioral observation is a leading way that malicious insiders are discovered. But with many workers now only observed through the limited aperture of a computer screen, this countermeasure is largely lost.

Early Warning con't.

But enough of 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? Well, quite simply it would be the automated identification of a limited number of at-risk employees that require a closer look, saving them hours and removing subjectivity that won't stand up in a boardroom or courtroom. But how to do we accomplish this?

Well, 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 connects 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 government and corporate security officials; new mechanisms and methodologies are available to identify and mitigate risk.

And 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 analysis of thousands of employees in a few minutes. Simply put, **we can make insider risk mitigation smarter, faster, and more proactive.**

Decision Advantage

And most importantly - we can create 'decision advantage' for analysts and program managers by judiciously highlighting employees requiring analyst review. In the intelligence world, we call that 'tipping and cuing'.

But how do we create this decision advantage? By conducting ***holistic insider risk identification*** using a whole person and whole threat perspective across human, technical, and physical domains. By executing ***continuous risk assessment*** using data analytics that detect at-risk employees or contractors before they act, are manipulated by outsiders, or allow their security negligence to harm an organization. And by employing ***operational excellence*** achieved through governance, transparency, auditability, security, privacy, quality assurance and trackable metrics.

To structure these processes, let me propose five connected concepts. The first two create the **right environment**, and the last three create the **right process.**

The Right Environment

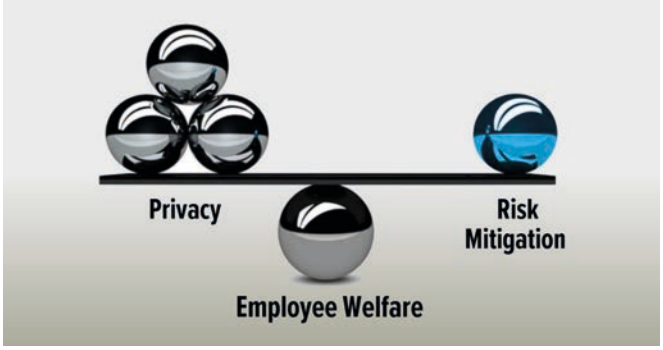
A positive security culture is critical to the creation of the right environment. Your program should provide early warning of employees who may need assistance and then actually deliver that assistance. In doing so, the program will start being viewed as positive rather than punitive, with increased buy-in at all levels.

#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 the data they've voluntarily publicized.

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. And importantly, we need to evolve our internal program marketing alongside our methodology and make insider risk mitigation **less about threat reduction and more about employee welfare.**



#2: Organization Buy-in

Leadership and employee buy-in is not only necessary to the end goal, but also to the means required to accomplish that goal. So, take a moment and examine your program 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 your program provides early warning of employees who may need assistance. And then, you need to 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.**

The Right Process

#1: Holistic Approach

A holistic approach incorporates the individual and their mental, emotional, financial, physical, virtual, and chronological state – utilizing a 'whole person' and 'whole threat' perspective.

To me, 'whole person' is contextual and psychosocial, and uses personality, environment, and precipitating events to identify risk. And 'whole threat' addresses the common root causes that result in different forms of attacks (data theft, fraud, sabotage, violence) – and in 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 that highlight the need for closer inspection.

#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.

#3: Advanced Risk Modeling

By applying a holistic approach with the right data, you can conduct advanced risk modeling. This is where the science 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, how they would plan and act.

And 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 determine the insider profiles most relevant and threatening to our organizations. And we need to understand the personality characteristics and critical events that are known to drive them to action. And then, we must develop and automate a watchlist of the most relevant trip wires.

Conclusion

To summarize, it's always been a high-stakes game – even before China's 'Thousand Talents' program, the rise of ransomware, and mass layoffs. More so than ever, we need to conduct modern insider risk tradecraft. To do so, we must harness advanced 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.

There are new and innovative insider risk solutions available that harness the internal data already collected by most organizations and the external public data that is widely and affordably available.

The key is using the right software to continuously examine the workforce for indicators of insider behavior, both malicious and benign.

This is how a company protects itself at scale from insider harm.

And if done correctly, this will not only significantly reduce insider risk, but will promote a positive security culture, increase organizational morale, and reduce employee attrition.

As they say, a 'win-win' for everyone.

Val LeTellier ran security, intelligence, and counterintelligence operations as a State Department Diplomatic Security Special Agent and CIA Operations Officer. Twenty years penetrating foreign intelligence targets and recruiting sources provided 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 a 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).

Addendum

Putting Theory into Practice

Consider how holistic insider risk mitigation can be applied against the major insider threat actors:

The Negligent

Personality characteristics: flighty, unfocused, disorganized, scatter- brained, stressed, strained.
Precipitating events: new personal or professional distractions.
Potential indicators: personal cell phone/computer overuse at work, unwitting provision of sensitive information to outsiders, inappropriate discussion of sensitive matters, sensitive documents or devices left accessible to others, failure to meet deadlines.
Relevant external data: law enforcement issues, legal cases, social media conflicts, online posting of sensitive corporate details.

The Intellectual Property/Sensitive Data Thief

Personality characteristics: entitlement, narcissism, anti-social, controlling.
Precipitating events: failed promotions, poor performance review, unmet career aspirations, resignations/terminations.
Potential indicators: "borrowing" office items for home use, attempted privilege escalation, questionable downloads, cyber security policy violations, anomalous data transfers and/or printing, use of unauthorized recording equipment.
Relevant external data: negative personal financial events, costly legal issues, and arrests (particularly for computer fraud).

The Violent or Self-Harmer

Personality characteristics: aggression, emotional detachment; confrontational, control-seeking, disengaged and unremorseful behavior; strained thoughts and actions.
Precipitating events: negative personal, family or relationship events.
Potential indicators: emotional outbursts, failure to communicate, failure to work in groups or specific individuals, bullying, difficulty taking criticism, violating boundaries, threatening violence, physical altercations.
Relevant external data: reflections of extremist beliefs, membership in extremist groups.

The Saboteur

Personality characteristics: angry, vengeful, vindictive, disengaged, or destructive.
Precipitating events: confrontation with management, poor performance reviews, failed promotions, demotion, workplace embarrassment, termination.
Potential indicators: testing of security procedures, defacing company website pages, accidentally" breaking a component in a critical machine, altering software, misconfiguring products to cause failure, unmerited complaints, and computer hacking.
Relevant external data: arrests and legal cases related to property destruction, vandalism, defacement, assault, road rage, etc.

The Fraudster

Personality characteristics: egoism, entitlement, privilege, self-importance.
Precipitating events: significant additional expenses, negative personal financial events, unmet career aspirations.
Potential indicators: violating enterprise policy, influencing a supplier for personal gain, reporting minor fraudulent expenses, insider trading, excessive control over financial duties, shrewd or unscrupulous behavior.
Relevant external data: bankruptcy, debt collection, legal issues, close association with vendors, and arrests for financial issues.

4TH GEN

Val LeTellier
4thgen.com
info@4thgen.com
800-876-2293