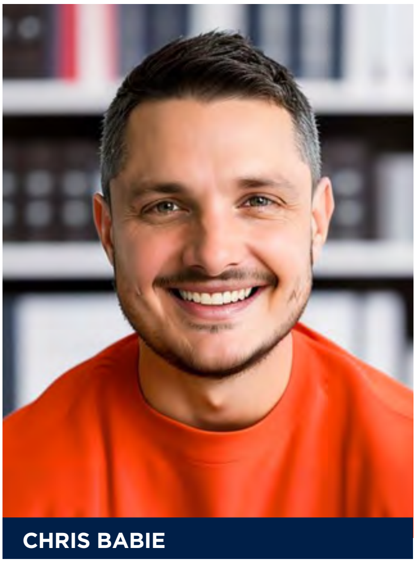
The Difference is Human – Building Preventative Insider Threat Programs

Chris Babie

Recent U.S. events have highlighted insider risk, the lack of preventive 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. Organizations 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.