Dealing with Insider Threats

By James Careless

Insider threats are one of the most insidious dangers to face the transportation industry. This is because of the element of betrayal and surprise associated with them. The reason: "Insider threats are risks that originate from trusted individuals, namely employees, contractors, or third parties who have legitimate access to an organization's systems, data, and infrastructure," said Ryan LaSalle, CEO of Nisos (nisos.com, which helps organizations detect, prevent, and respond to insider threats before they escalate). "Historically, the term referred mostly to negligent mistakes, such as misconfigurations or mishandling sensitive information. Today, the definition is far broader. Insider threats now encompass deliberate acts of sabotage, theft, fraud, and policy violations, as well as negligent or accidental behaviors that expose the organization to risk. In transportation companies, this can result in financial leakage, smuggling or industrial espionage."

"While some organizations may have a robust security posture, all that it takes is just one employee to conduct their own security controls assessment to identify weaknesses in an attempt to evade detection," added Jim Henderson. He is CEO of the Insider Threat Defense Group

Ryan LaSalle, Nisos

(ITDG, www.insiderthreatdefensegroup.com). It has assisted more than 700 organizations in developing, implementing, managing and optimizing their insider risk management programs. "The damages inflicted by these insiders have caused billions of dollars of damage. Some affected companies have suffered large layoffs or gone out of business as a result."

Three Types of Insider Threats

Although there are many kinds of insider threats, the experts interviewed for this article generally agreed that they can be classified into three main categories:

- **The Malicious Insider:** This is an employee who intentionally damages systems, steals data, or sabotages operations.
- **The Negligent Insider:** This is an employee who unintentionally causes harm through mistakes like clicking phishing links, mishandling credentials, or ignoring procedures.
- **Third-Party Insider:** These are an organization's vendors or partners who have access to the organization's systems and misuse this privilege, sometimes for profit, other times through carelessness.

Dealing with negligent insiders is a matter of detection, education, and — if they then refuse to improve — possible termination. It is the malicious and third-party insiders that constitute the real risks.

So why do they do it? Their motivations vary as widely as the crimes they commit. But there are some common threads. "Malicious insiders are often driven by motivations such as personal gain, revenge, ideology, or coercion, but these motives rarely appear in isolation," said Ashleigh Diserio, president of Diserio Consulting (https://www.diserioconsulting.com), which specializes in behavioral consulting, insider risk detection, and risk management. "They can be influenced by factors in a person's professional or personal life, such as job dissatisfaction, financial hardship, burnout, feeling undervalued, or unresolved conflicts with management or coworkers. For example, a frustrated employee who feels overlooked for promotion or mistreated by leadership might rationalize leaking sensitive data to a competitor or sabotaging logistics systems as a form of payback or self-justified justice."

Third-party insiders, such as contractors, vendors, or technology partners, can be motivated by similar pressures. "Financial strain, loyalty to another organization, or even social manipulation can lead them to share or misuse access," Diserio told TSI. "In some cases, their weak security habits or personal vulnerabilities make them easy targets for coercion or exploitation by external actors.

Detecting Insider Threats

Detecting insider threats is a daunting task, especially for transportation companies that cover great distances and often have multiple locations to monitor. But it is a task that can be done — and must be.

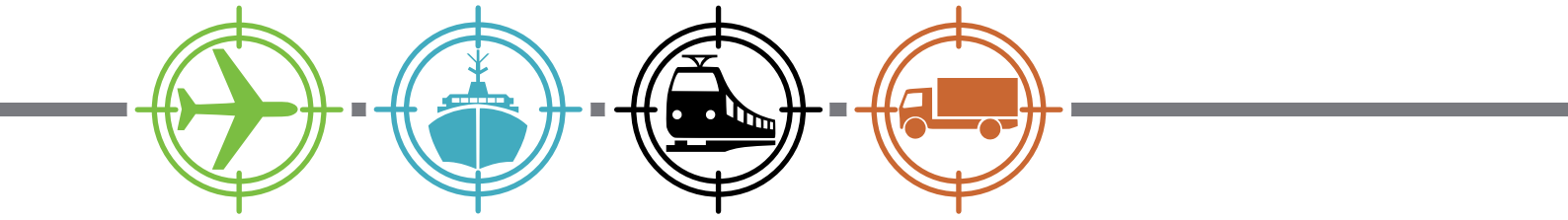
"Transportation companies operate with large, distributed workforces and high access environments, from logistics centers to maintenance shops and drivers in the field," said Col (Ret) Brian "Patton" Searcy, president and founder of The Paratus Group (www.paratus.group), which trains people to recognize and respond to threats. "This makes insider threat awareness essential."

So how can an organization generate insider threat awareness internally? "Train employees to look for changes in behavior, unusual stress, sudden wealth, rule-bending, isolation, and who to report it to," Searcy replied.

"Detection begins with visibility," added Diserio. "Transportation companies must understand who is accessing what, when, and why. Given the scale and complexity of logistics operations, insider risk detection cannot rely on guesswork. It requires structured policies, layered monitoring, and a clear framework for accountability."

Being aware of what is happening in the organization at all times is paramount. "The key is to monitor all three potential dimensions of insider threat: behavioral, technical, and organizational," LaSalle noted. "Behavioral signals might include sudden changes in work hours, unexplained conflicts with colleagues, or controversial activity on social media. Technical signals could be large, unauthorized data transfers, use of personal devices on the network, or attempts to disable security controls. Organizational signals include declining performance reviews, disciplinary actions, or notice of resignation."

"Detecting insider threats involves more than just monitoring the network," said Henderson. "Comprehensive insider risk management involves many key stakeholders: the Insider Threat Program manager, the Insider Threat investigator-analyst, the FSO, CSO, CISO, human resources, CIO – IT, network security, counterintelligence investigators, mental health/behavioral science professionals, and the legal department. These stakeholders must work together sharing employee risk and threat information, as no one individual within an organization is positioned to see every single employee risk factor or behavioral indicator. Collaboration among key



stakeholders is a critical element for detecting and mitigating insider threats."

To maximize the value of these actions, transportation companies should have monitoring policies that integrate their internal detection results with external intelligence. "For example, detecting unusual financial behavior, side employment, or suspicious online affiliations outside the company can provide early warning before an insider escalates to harmful actions," LaSalle said. "Once risks have been identified, companies need clear escalation paths — often through a collaboration between HR, security, and legal teams — to investigate quickly, attribute activity accurately, and take proportionate action."

How the Experts Do It

Transportation companies exist to move people and goods. Dealing with insider threats is not their core business, which is why hiring an outside expert to do this for them can often make sense. We asked the experts we interviewed how their companies do this.

"At Diserio Consulting, we take a full-lifecycle approach to insider threat management, from prevention and early detection to investigation, response, and long-term resilience," said Ashleigh Diserio. "We understand that insider risks are not just a technology problem but a human one. That's why our services combine behavioral science, analytics, and organizational strategy to address risk from every angle."

This is how Diserio Consulting helps transportation and logistics companies protect their people, assets, and operations from insider threats.

The process begins by compiling insider threat risk assessments at the client company. To do this, "we conduct comprehensive assessments that evaluate vulnerabilities across an organization's systems, workforce, and vendor ecosystem," Diserio told TSI. "Our process involves structured interviews, behavioral risk mapping, and analysis of access controls and workflows. For transportation companies, this often includes reviewing logistics management systems, driver access points, cargo tracking data, badging data, and maintenance records to uncover where insider risks are most likely to emerge."

Having done this, Diserio Consulting starts monitoring and assessing employee activities on an ongoing basis. "Our behavioral analytics platforms go beyond standard cybersecurity monitoring," said Diserio. "By establishing individual and team baselines for everyday activity, we can identify deviations that indicate emerging risks, such as increased data downloads, sudden changes in work patterns, or behavioral red flags like frustration or disengagement. Our team integrates these tools with existing IT and HR systems, ensuring seamless insight across both digital and human data points."

Of course, the transportation sector depends heavily on vendors, contractors, and logistics partners, all of whom can introduce third-party insider risks into a client's business environment. To mitigate these risks, Diserio Consulting assists organizations in establishing a structured third-party risk management framework. "We conduct vendor security assessments, review access controls, and develop standardized onboarding and offboarding protocols to minimize exposure to external partners and ensure a secure environment," Diserio explained.

Whenever an insider incident does occur, Diserio Consulting's response team is ready to investigate and contain it. "We use digital forensics and behavioral analysis to identify root causes, preserve evidence, and recommend remediation steps," said Diserio. "For transportation clients, this may involve tracing unauthorized access to routing systems, shipment databases, or employee credentials, while maintaining operational continuity."

Beyond the above, Diserio Consulting develops tailored training programs that educate employees, supervisors, and contractors on how to identify and report potential insider risks. They also conduct behavioral workshops that teach leadership teams how to spot early warning signs of stress, burnout, or dissatisfaction, factors that can precede malicious or negligent actions. "In addition to training, we help companies build supportive, transparent workplace cultures that reduce the motivations behind insider threats," Diserio said. "Our consultants work with HR and management to develop employee engagement strategies, confidential reporting channels, and intervention processes that address personal or professional issues before they escalate into security incidents. By combining behavioral insights with advanced analytics, we help transportation organizations shift from a reactive stance to a proactive one, predicting and preventing insider risks before they impact operations."

The Insider Threat Defense Group (ITDG) offers similar services to its clients. "A first step for any organization, to include transportation companies, is to have a baseline and much deeper understanding of what insider threats are, and what is involved in insider risk management (IRM) — including extensive training," said Henderson. "Key stakeholders must have a comprehensive understanding of the collaboration components and responsibilities required by them, and the many underlying and interconnected components that are essential for a comprehensive IRM program. Key stakeholders must be universally aligned from an enterprise/holistic perspective to detect and mitigate employee risks/threats. As well, an IRM program must be built on a solid framework of non-technical and technical security controls for the program to be comprehensive and effective."

Worth noting: In addition to its IRM services, ITDG publishes a fascinating free monthly newsletter that details the latest happenings in insider-related crime. Available at www.insiderthreatdefense.us/insider-threat-incidents-reports-news, this newsletter provides insights into insider threat activities (much of it sourced from

U.S. Department of Justice news releases), including the following: "Operations Manager Charged For Role In Embezzling $500,000 From Trucking Company." In this report, ITDG explained how an operations manager at a large trucking business filed fraudulent truck driver reimbursement requests. This insider activity happened for over three years before the fraud was detected and stopped.

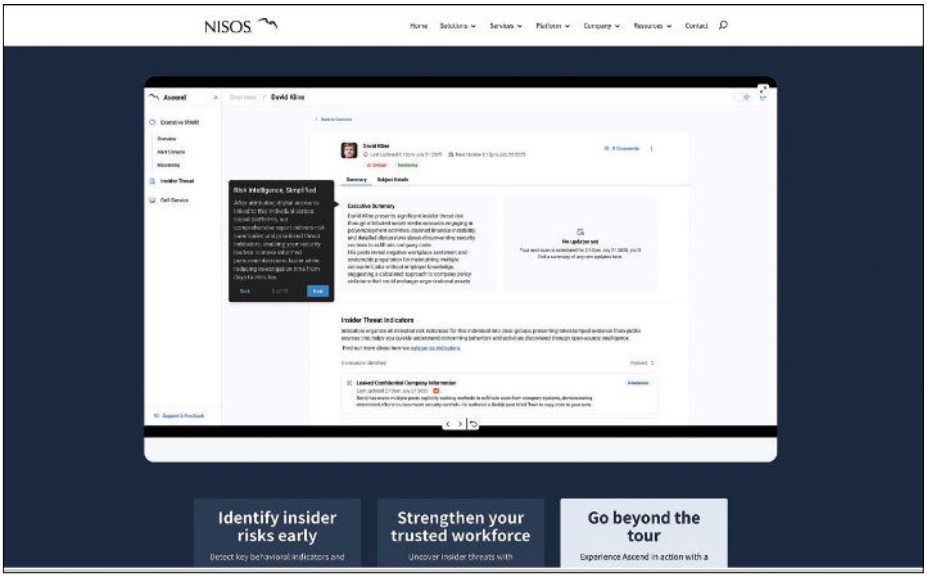
As for Nisos? "Our Insider Threat solutions combine technology with white-glove analyst services to provide holistic coverage," said LaSalle. "By integrating external intelligence, continuous monitoring, and AI-driven attribution, Nisos helps organizations detect, investigate, and prevent insider threats before they manifest internally."

Nisos' Insider Threat services include:

- **Early Risk Identification:** Detecting potential indicators of insider threat – from concerning financial behavior, to social media, to undisclosed side employment — before they can escalate.
- **Accurate Attribution:** Connecting digital accounts and external signals to real-world individuals with AI-powered attribution and confidence scoring, to reduce false positives.
- **Actionable Investigation Insights:** Transforming risk signals into investigation-ready insights, to enable informed decision-making and speed up threat responses
- **Continuous Monitoring:** Maintaining real-time awareness of emerging insider threats with dynamic, always-on coverage that complements internal telemetry and reduces blind spots.

Finally, the Paratus Group provides a full range of threat detection services, staff training programs, and surveillance technology solutions to help their clients detect and defeat insider threats. Brian Searcy contextualizes these offerings in terms of the practical steps that transportation organizations can take to protect themselves:

- **Behavioral Observation and Communication:** Train employees to look for changes in behavior, unusual stress, sudden wealth, rule-bending, isolation, and know who to report it to.
- **Micro-Learning and Scenario Training:** Short, consistent awareness sessions



Nisos says their Insider Threat solutions combine technology with white-glove analyst services to provide holistic coverage. The group says by integrating external intelligence, continuous monitoring, and AI-driven attribution, they can help organizations detect, investigate and prevent insider threats before they manifest internally. Nisos image.

are far more effective than one-time lectures. The Paratus Group uses five-minute daily and weekly drills that fit seamlessly into operations.

- **Integrated Monitoring:** Combine human awareness with technical monitoring. Systems can detect unusual logins; people can recognize unusual attitudes or motives.
- **End-of-Shift "Hot Wash" Reviews:** Encourage teams to share observations before they forget, because small concerns often connect to larger patterns.
- **Faith and Purpose Mindset:** When employees understand the higher purpose of their work, that they're protecting people, not just property, it strengthens both ethics and performance. This approach transforms employees from passive observers into active protectors of the mission.

An important point: "All of this requires buy-in at the highest levels," said Searcy. "If they continue to conduct 'check the box information events', then nothing will change."

Success Stories

Deploying a comprehensive insider threat defense program takes time, effort, and money. So, is it worth it? To answer this question, Ashleigh Diserio offered the following two success stories.

Case 1: Airline Industry

An airline approached Diserio Consulting after noticing inconsistencies in maintenance scheduling and access logs. "Our behavioral analytics platform flagged an employee who was repeatedly accessing sensitive aircraft maintenance data outside regular working hours and from an unusual geographic location outside the United States," Diserio said. "This employee was not authorized to take their work computer outside the United States."

After some digging, Diserio Consulting detected a pattern suggesting both insider knowledge and external coordination. "Our investigation revealed that the employee had been approached by a third party offering financial incentives to share internal system access credentials," said Diserio. "By combining data analytics with behavioral profiling, which identified sudden changes in the employee's work habits, communication tone, and stress indicators, we were able to alert the airline's security and HR teams before any data was leaked. The individual was removed from their role, and the incident was contained without operational disruption or public exposure. The airline was later able to utilize our findings to enhance employee wellness programs and improve communication between maintenance and management teams, thereby addressing the root causes of insider risk.

Case 2: Bus Transportation

A bus transportation company faced a potential insider threat when Diserio Consulting's continuous monitoring system detected irregular data activity from an operations supervisor's account. The account had begun accessing passenger manifests and route scheduling data at irregular intervals, an activity that didn't align with the employee's role or prior work behavior.

"Our response team immediately launched a forensic review, uncovering that the employee's access credentials were being used to gather and sell data related to competitor routes and operational schedules," Diserio told TSI. "Motivated by personal financial stress, the insider had been approached through social media by an external buyer. Due to early behavioral flagging, which included signs of disengagement, attendance issues, and changes in communication tone, our system alerted leadership before any significant data was shared."

Working closely with HR and law enforcement, the company managed to contain the incident. "Notably, our consultants helped management implement new employee support channels and financial wellness initiatives to mitigate similar motivational risks across the workforce," she said.

The Paratus Group has its own success story to offer. "In one transportation maintenance operation, a team we had trained noticed a pattern that didn't sit right: an employee was repeatedly accessing restricted maintenance records and working after hours without authorization," said Brian Searcy. "Instead of ignoring it or assuming it was harmless, they used the Paratus Process: Identify, Assess, Predict, Decide, Act. They verified the pattern, documented what they saw, and escalated appropriately. The investigation revealed a contractor

attempting to exfiltrate operational data. The issue was stopped before any damage was done. That's what true awareness looks like; not paranoia, but informed observation and confident action."

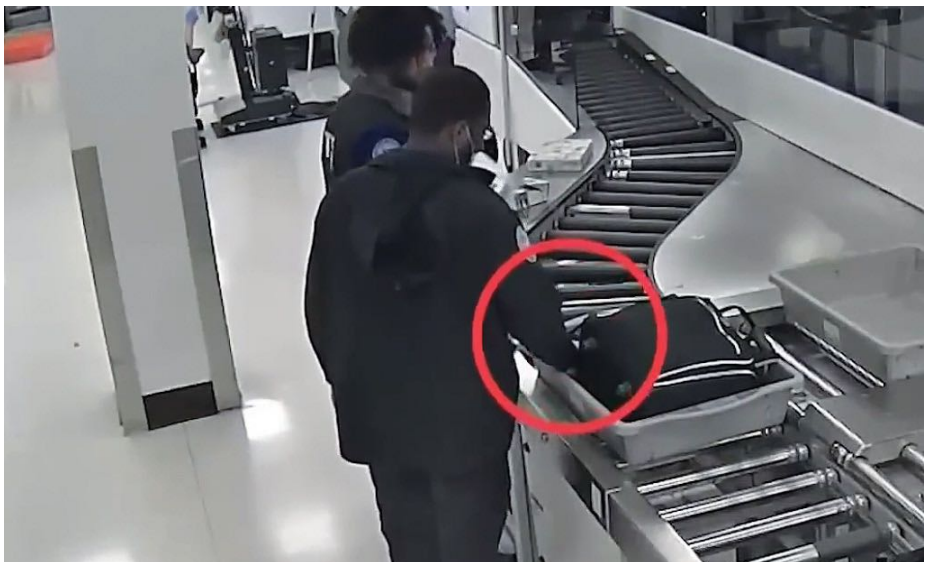
Actionable Expert Advice

Based on the experts' insights, it is possible for transportation companies to successfully detect and defend against a wide variety of insider threats. To conclude this story, TSI magazine asked the experts for actionable advice that transportation companies could implement on their own. Here is what they told us.

"The best defense against insider threats starts with building a trusted workforce," LaSalle said. "That means looking beyond traditional background checks to adopt proactive vetting strategies — verifying identities, validating credentials, and using modern tools to uncover hidden risks or fraudulent employment attempts. Equally important is adopting a lifecycle approach, monitoring for risk ethically and proportionally from pre-hire to exit. Transportation companies should also expand their visibility beyond the firewall. Internal telemetry alone won't reveal hidden affiliations, online behavior, or financial stressors that often precede insider threat activity. By combining inside-the-network monitoring with external intelligence, organizations can connect the dots earlier, investigate with greater clarity, and take swift action."

"You need to start with education for all key stakeholders involved in managing and supporting the Insider Threat Program," said Henderson. "The success of a program is largely dependent on key stakeholders collaborating with the Insider Risk Program manager, and sharing employee risk and threat information of concern. This proactive approach is critical to ensure that everyone is universally aligned from an enterprise/holistic perspective for identifying, responding to, preventing and mitigating insider risks and threats."

"Start with a clear framework: define what 'insider risk' means for your organization, including the scope of employees, contractors, and vendors," Diserio said. "Insider threats often intersect with behavioral or workplace issues. So, HR, legal, finance, civil liberties, and security teams must work hand in hand. Leverage automation but keep the human element. Technology should assist, not replace judgment, so combine AI-based monitoring with human oversight. You should also create a culture of security awareness because employees are your first line of defense while regular training builds vigilance and trust. Finally, insider risk programs should grow with the company and adapt to new technologies, regulations, and threat landscapes."



TSA agents, Jose Gonzalez and Labarius Williams, were caught on camera stealing from passengers' luggage at a security checkpoint at the Miami International Airport. Both agents were charged with grand theft in the third degree.

The question of whether the June 12, 2025, Air India Flight 171 crash was an example of an insider threat (an intentional act) is a central focus of the ongoing investigation and has not been definitively confirmed or ruled out. The cause of the crash remains under investigation by India's Aircraft Accident Investigation Bureau (AAIB).

Brian Searcy delivered his advice in the following list:

- Start with Culture, Not Technology. Technology is an enabler, but awareness is the foundation.
- Empower Every Employee. Make security everyone's responsibility, not just IT's.
- Train Continuously. Replace long, once-a-year training with short, real-world refreshers that build muscle memory.
- Lead with Values. Whether that's faith-based or organizational values, grounding people in purpose creates accountability.
- Review and Adapt Regularly. After incidents or near misses, conduct "hot washes" to capture lessons learned and reinforce awareness.

"At the end of the day, insider threat prevention isn't about surveillance, it's about stewardship," said Searcy. "It's about empowering your people to protect what matters most." That's a thought worth remembering for anyone tasked with protecting their organization against insider threats. TSI