IAM

M

Latest developments in trade secrets strategy and enforcement

The hidden crisis: why insider threat statistics fail to capture trade secret theft reality

Tim Schnurr

18 June 2025

Shutterstock/Michal Balada

For intellectual property attorneys and strategists, understanding the true scope of trade secret theft is critical to assessing risk and protecting clients' most valuable assets. Yet the statistics we rely on paint an incomplete – and often misleading – picture of insider threat incidents.

The disconnect between reported incidents and actual occurrences creates a dangerous blind spot in IP protection strategies.

The gap between reported statistics and actual incidents stems from multiple structural, regulatory, and economic factors that collectively render traditional cybersecurity metrics nearly useless for understanding the true insider threat landscape.

The regulatory blind spot: customer data v crown jewels

The fundamental flaw in current insider threat reporting begins with regulatory focus. Virtually every major cybersecurity regulation – from GDPR and CCPA to HIPAA and PCI DSS – centres on protecting customer data, personal information, payment details, and health records. These frameworks mandate breach notification requirements, impose penalties for non-compliance, and create detailed reporting obligations that drive the statistics we see in annual cybersecurity reports.

However, insider threats typically target what security professionals call the "crown jewels" – proprietary algorithms, manufacturing processes, strategic plans, research data, customer lists, and other trade secrets that form the core competitive advantages of modern businesses.

These assets fall outside the scope of customer data protection regulations. When an engineer downloads proprietary manufacturing specifications before joining a competitor, or when a sales executive copies the company's customer database for personal use, these incidents often trigger no regulatory reporting requirements whatsoever.

This regulatory gap means that the most damaging forms of insider theft – those targeting intellectual property and trade secrets – remain invisible in official breach statistics.

The reputational damage dilemma

Unlike external cyberattacks, which can generate sympathy and understanding from stakeholders, insider threat incidents carry a unique reputational burden. When an organisation suffers a ransomware attack or external breach, it can position itself as a victim of sophisticated criminals. However, insider threat incidents suggest failures in hiring, vetting, monitoring, and corporate culture – areas where leadership bears direct responsibility.

The reputational calculus is stark: reporting an insider threat incident signals to competitors, investors, customers, and partners that the organisation cannot protect its most sensitive assets or effectively manage its own personnel.

For publicly traded companies, such disclosures can trigger stock price volatility, analyst downgrades, and customer defections. For private companies seeking investment or partnerships, insider threat incidents can derail negotiations and damage competitive positioning.

This creates a powerful disincentive for voluntary disclosure. Since most trade secret theft falls outside mandatory reporting requirements, organisations routinely choose silence over transparency, further skewing the available data on insider threat prevalence.

Insurance coverage gaps and incident response failures

Traditional cybersecurity insurance policies were designed around external threat models and typically provide limited coverage for insider threat incidents. Many policies explicitly exclude or significantly limit coverage for employee theft, privilege abuse, or other insider activities. This coverage gap means that organisations often absorb the full financial impact of insider threat incidents without insurance support.

The lack of insurance coverage creates a secondary reporting problem: insurance claims typically drive much of the incident data that feeds into industry reports and statistics. When insider threat incidents do not trigger insurance claims, they are absent from these crucial data sources, further contributing to underreporting.

Moreover, many organisations lack comprehensive incident response plans specifically designed for insider threats. While companies may have detailed protocols for responding to external attacks, insider threat response often falls into a gray area between cybersecurity, human resources, and legal departments. This fragmented response means that incidents may be handled internally without triggering the documentation and reporting processes that would normally capture security incidents in organisational metrics.

The employment law alternative: litigation as cover

A significant portion of insider threat incidents are reframed as employment law matters rather than cybersecurity incidents. When employees misappropriate trade secrets or proprietary information, organisations often pursue resolution through employment litigation, non-compete enforcement, or breach of contract claims rather than through cybersecurity incident response channels.

This legal strategy serves multiple organisational interests: it moves the matter into confidential litigation proceedings, positions the incident as a contractual dispute rather than a security failure, and often results in settlement agreements that include non-disclosure provisions. These sealed settlements effectively remove incidents from public view and ensure they never appear in cybersecurity statistics or breach reports.

Pre-litigation interventions are even more common and invisible. Human resources departments, leadership teams, and legal counsel often intervene quickly when insider threat indicators emerge, using settlement agreements, enhanced NDAs, and other legal tools to resolve matters quietly. These early interventions may prevent incidents from escalating but also ensure they remain completely untracked in security metrics.

Statistical misclassification and aggregation problems

Even when insider threat incidents are reported in cybersecurity contexts, they are often misclassified in ways that obscure their true nature and impact. **The Verizon Data Breach Investigations Report** (DBIR), widely considered the gold standard for cybersecurity

statistics, frequently categorises insider activities under "privilege misuse" or other generic categories that do not distinguish between different types of insider behavior, intent or motivations.

This classification problem is compounded by the tendency to aggregate negligent insider incidents with malicious ones. When security reports combine statistics for employees who accidentally expose data with those who deliberately steal trade secrets, the resulting numbers provide little insight into the specific threat profile that most concerns IP attorneys and corporate strategists.

Implications for IP strategy and risk assessment

For intellectual property attorneys and corporate strategists, the systematic underreporting of insider threat incidents creates several critical challenges. Risk assessments based on published cybersecurity statistics likely dramatically underestimate the actual threat to proprietary information. Budget allocations for insider threat protection may be insufficient given the true scope of the problem. And benchmarking exercises comparing organisational security postures to industry standards become meaningless when the baseline data excludes the majority of relevant incidents.

The solution requires a fundamental shift in how organisations and the broader IP community approach insider threat measurement and reporting. This includes developing industry-specific reporting frameworks that capture trade secret theft incidents, creating safe harbour protections that encourage voluntary reporting without triggering unnecessary liability, and establishing metrics that distinguish between different types of insider activities and their respective impacts on intellectual property assets.

Until these changes occur, IP professionals must operate under the assumption that insider threat statistics significantly understate the actual risk to their organisations' most valuable assets, and develop protection strategies accordingly.

Tim Schnurr

CISM, CRISC, PSM, CFA, Managing Partner
LeastTrust
tim@leasttrust.com