WHY INSIDER THREATS REMAIN AN UNRESOLVED CYBERSECURITY CHALLENGE

INDUSTRY INSIGHT

In Collaboration with:
The National Insider Threat Special Interest Group
& The Insider Threat Defense Group

IntroSecurity
ASEAN Cyber Growth Partners

NITSIG

Executive Summary

In an era defined by digital fortresses and sophisticated cyber defences, the most dangerous threat is not always external. Insider threats, originating from an organisation's own employees, contractors, or trusted partners, continue to bypass even the most advanced security systems. Despite billions spent on protecting networks from outside intrusion, internal actors still manage to exploit trust, avoid detection, and cause significant harm. The persistence of this problem raises a critical question: why does the insider threat remain one of cybersecurity's most enduring and unresolved challenges?

A May 2025 Insider Threat Incidents Report by the National Insider Threat Special Interest Group (NITSIG) and Insider Threat Defense Group (ITDG) underscores the gravity of the problem. It documents how malicious, negligent, or opportunistic insiders can be just as costly and damaging as outside attackers. In fact, insiders often operate in the shadows of external cyber threats, receiving far less organizational attention than external attacks despite evidence that the insider threat problem is massive and growing. The NITSIG/ITDG report draws on over 6,300 documented insider incidents spanning 15+ years, providing *indisputable evidence* that no sector or organization size is immune. From government agencies to private businesses, critical infrastructure to academia, all types of organizations have suffered insider incidents.

Yet despite increased awareness, insider threats remain an unresolved challenge. This paper investigates why, examining the technical, organizational, behavioural, and legal factors that make insider risk so persistent. We ground our analysis in the May 2025 NITSIG/ITDG report as a primary source of real-world incident data and trends, supplemented by public case studies, industry surveys, and scholarly insights. The evidence reveals that insider threats are multifaceted human-centric problems that defy purely technical fixes. Insiders often have legitimate access and intimate knowledge of defences, enabling them to evade traditional security controls. Organizations, for their part, have historically underestimated the insider risk- a tendency rooted in human trust and skewed priorities. Meanwhile, the motivations and behaviours driving insider attacks are diverse and complex, complicating detection and prevention efforts. Constraining legal and privacy considerations further inhibit robust monitoring of employees, leaving gaps that insiders can exploit.

After critically reviewing these contributing factors, the paper provides detailed recommendations for mitigating insider risk. We outline strategies for strengthening insider risk management (IRM) programs and cross-departmental governance, adopting advanced detection techniques, and fostering employee engagement and a security-aware culture. The goal is to chart a path forward whereby organizations can better deter, detect, and respond to insider threats, transforming this "weakest link" in cybersecurity from an unresolved liability into a manageable risk.

The depth and tone of analysis are intended to meet academic and professional standards, offering insights suitable for both scholarly understanding and practical implementation in enterprise security programs.

The Persistent Threat from Within: Scope and Impact

Insider threats encompass a broad range of malicious and inadvertent actions by individuals with authorized access. Unlike external hackers who must breach network perimeters, insiders already hold the keys to the kingdom, making their betrayals particularly damaging. The NITSIG/ITDG May 2025 report highlights that **insider incidents can take many forms**, far beyond the classic notion of a disgruntled spy stealing trade secrets. Through extensive research, NITSIG has identified types of insider threats including unintentional but damaging errors by careless staff, disgruntled employees sabotaging systems, theft or misuse of sensitive data, **financial fraud and embezzlement**, abuse of access for personal gain, collusion with external criminals, workplace violence, and more. In essence, *any abuse of trust or failure of duty by insiders falls under this umbrella*. Table 1 (from the NITSIG report) lists many insider threat categories discovered through research:

- **Non-malicious but negligent insiders** - e.g. untrained or careless employees whose mistakes cause data leaks or security breaches.
- **Malicious insiders driven by grievance**- disgruntled staff who deliberately steal or destroy assets as revenge.
- **Insider fraudsters**, employees engaged in financial fraud, embezzlement, bribery, or creation of fake invoices/shell companies to steal money.
- **Data thieves and spies-** insiders who exfiltrate confidential information (customer data, intellectual property, trade secrets, classified info) for personal gain or on behalf of competitors/foreign governments.
- **Saboteurs -** insiders who sabotage IT systems, damage equipment, or otherwise disrupt operations (sometimes linked to IT administrators planting logic bombs or users misusing access).
- **Collusion and external influence**- cases where employees work in concert with other insiders or external actors (organized crime, nation-states) to undermine the organization.
- **Policy violations and abuse of position**- e.g. employees holding two jobs in conflict with company policy or using work systems for illicit activities like distributing contraband.
- **Insider-extremism or espionage**- insiders driven by ideology or divided loyalties (e.g. terrorism support, allegiance to a foreign nation).
- **Workplace violence**- extreme cases where insider grievance escalates to physical violence or threats on premises.

This wide scope means *every organization function and industry is at risk*. Indeed, NITSIG's data shows no sector is immune. Insider incidents have struck government agencies (federal, state, local), defence contractors, critical infrastructure providers (energy, transportation, healthcare, finance, etc.), private businesses of all sizes, schools and universities, non-profits, and more. A trusted insider can be a low-level clerk or a C-suite executive. For example, high-profile cases in recent years include a banking executive opening millions of fraudulent accounts to meet sales targets (Wells Fargo, 2002–2016), a senior portfolio manager at an investment firm misleading clients and falsifying records in a $3 billion fraud (Allianz Global Investors, 2014–2020), and even a Managing Director at a major bank (Goldman Sachs) conspiring to launder money and pay massive bribes in the 1MDB corruption scandal.

At the other end of the hierarchy, front-line employees have committed equally damaging acts: e.g. a Tesla employee caught attempting sabotage and data theft in 2020 (a breach fortunately averted by prompt detection), or a longtime U.S. government employee abusing her privileged access to enable a $36 million food assistance fraud scheme.

These cases illustrate how *insider threat manifests at all levels*, from corporate fraud by leaders to opportunistic crimes by staff.

The impacts of insider incidents are correspondingly severe and multi-dimensional. The NITSIG report delineates the damage categories, which span financial losses, operational disruption, reputational damage, and cultural harm. Financially, organizations can suffer direct monetary theft (embezzlement, fraud) and indirect costs like lost revenue from stolen intellectual property or competitive advantage. Insider incidents often force costly remediation efforts and increase overhead (investigations, legal fees, compliance fines).

Operationally, malicious insiders have caused IT outages, data destruction, and productivity loss. In extreme cases even forcing businesses to shut down or undergo mass layoffs. Reputation damage is another painful consequence: publicized insider breaches erode customer trust, tarnish brand image, and can devalue a company's market position. Internally, the discovery of an insider betrayal often breeds distrust and low morale among remaining employees, and in tragic instances like workplace violence, can even result in injury or loss of life. In short, the cost of insider threats is enormous, often reaching millions or even billions in damages when all factors are tallied.

A 2023 global study by the Ponemon Institute found the average annual cost for organizations to deal with insider incidents had risen to $16.2 million, and by 2025 it climbed further to $17.4 million. Individual incidents can be extremely expensive: malicious insider breaches averaged over $700,000 per incident in that study, not counting the hardest-to-quantify losses like intellectual property theft or reputational fallout.

Despite these staggering impacts, insider threats persist and have even increased in recent years. Multiple data points illustrate this troubling trend. According to Ponemon's 2023 survey, 71% of companies reported experiencing 21 or more insider incidents per year - up from 67% just a year before. Industry reports estimate that insiders are responsible for anywhere from one-third to well over half of all data breaches, depending on definition. For instance, one 2024 analysis attributed about 60% of data breaches to insider threats (including errors and negligence) and noted insider incident frequency had risen nearly 50% since 2018.

The time to detect and contain insider breaches also remains disconcertingly long. On average it takes organizations on the order of 2–3 months to contain an insider incident (81–86 days), giving rogue insiders ample time to inflict damage before they are stopped. In one study only 13% of incidents were caught and contained within a month. This lag exacerbates losses- incidents that took more than 90 days to contain cost nearly $18 million on average, versus $10.6 million for those contained within a month. In summary, by every measure (frequency, cost, and impact), insider threats remain a pressing and unresolved challenge.

Why do insider threats continue to plague organizations despite increased attention? The next sections critically examine the contributing factors through multiple lenses. We find that the persistence of insider risk stems from a *convergence of technical, organizational, human, and legal challenges*. Understanding these root causes is essential to formulating effective countermeasures.

Technical Challenges in Insider Threat Detection and Prevention

From a technical standpoint, insiders are notoriously difficult to detect using traditional cybersecurity tools. Unlike external attackers who generate abnormal network traffic or exploit known signatures, insiders operate *within normal authorization boundaries*. They often misuse legitimate credentials and authorized access, which means their malicious actions do not always trigger obvious alarms on firewalls or intrusion detection systems. As one CISO notes, "insider threats are complex threats that cannot be detected with traditional correlation rules… as insiders have legitimate or privileged access, their position within the organization makes them a significant threat". A savvy malicious insider familiar with the organization's security monitoring can intentionally evade detection. For example, by using access they know is logged less rigorously, or by slowly exfiltrating data to avoid triggering volume-based alerts. Insiders may also exploit their knowledge of *security blind spots* (e.g. data stored in less-monitored systems, or abusing administrative tools under the guise of normal work). This insider advantage was infamously demonstrated by Edward Snowden in 2013; as an NSA contractor, Snowden leveraged inadequate internal controls and overly broad access to smuggle out thousands of classified documents without immediate detection. The Snowden case highlighted how legacy system weaknesses such as lack of granular access controls, insufficient user activity monitoring, and failure to enforce least privilege, can be exploited from within. Many organizations today still struggle with outdated systems and logging gaps that make it difficult to trace what insiders are doing with sensitive data in real time.

Another technical challenge is the sheer variety of systems and channels insiders can use to leak or sabotage data. Modern enterprises have sprawling IT environments: on-premises databases, cloud applications, personal devices, IoT devices, shared network drives, email, etc. Insiders have many avenues to carry out an attack or leak. A 2023 survey indicated insider-driven data loss most often occurred via cloud platforms and IoT devices (59% and 56% of incidents, respectively), more so than through corporate laptops or BYOD endpoints. Traditional security tools focused on the network perimeter or corporate PCs might miss exfiltration via a cloud storage account or an IoT sensor being repurposed to siphon data.

The lack of unified visibility across all these data channels is a persistent issue. Without integrated monitoring, unusual data transfers or access patterns can slip through unnoticed. For example, misconfigurations in cloud file storage or Network Attached Storage (NAS) systems could lead to large troves of data being accessible without triggering alerts. Insiders can take advantage of such misconfigurations (whether intentionally or via negligence) to steal information. The complexity of IT ecosystems thus broadens the attack surface insiders can abuse, while fragmenting the audit trail that security teams must piece together.

Moreover, detecting an *insider's intent* is intrinsically hard for automated tools. User activity monitoring solutions and Data Loss Prevention (DLP) systems can generate mountains of alerts for policy violations (e.g. an employee emailing an attachment to a personal address or downloading a client list). But distinguishing a benign action (like an employee working late from home and emailing themselves a file) from malicious exfiltration can be tricky. Advances in User and Entity Behaviour Analytics (UEBA) use machine learning to profile normal behaviour and flag anomalies, which helps, but is not foolproof. Malicious insiders often *mimic normal behaviour* or act within expected ranges to avoid anomaly detection. On the other hand, many alerts turn out to be false positives (an employee with a legitimate new job responsibility might suddenly access a lot of files, appearing anomalous but for innocent reasons). High false-positive rates can overwhelm analysts and lead to "alert fatigue", causing genuine insider warning signs to be missed among the noise. The Ponemon report notes that large organizations deal with an average of 7,300+ insider incidents in their data, and scaling monitoring to that level is hard- especially managing false positives as data volume grows.

Compounding the detection challenge is the blend of cyber and physical actions insiders might take. An insider could directly cause harm in ways that bypass digital monitoring, e.g., physically stealing backup drives, or intentionally damaging hardware. Traditional cybersecurity tools focus on digital events and might not correlate them with physical security logs (such as door entry records or camera footage). The convergence of IT security with physical security is still maturing in many organizations, creating gaps a determined insider could exploit.

In summary, purely technical defences struggle against insiders because insiders *operate from a position of trust inside the perimeter*. They can hide in plain sight by leveraging legitimate tools and permissions. Many organizations rely on detection mechanisms that are reactive, triggering after data is moved or a policy is violated, rather than proactive detection of precursor behaviours.

As the NITSIG report emphasizes, insider threat is not just a technical problem; focusing only on network security tools without addressing human factors will give a false sense of security. Indeed, organizations often invest heavily in sophisticated cybersecurity infrastructure, yet find it did not prevent an employee from abusing authorized access. Technical solutions are necessary but not sufficient. The limitations of technology in isolation mean that insider risk requires equal attention to organizational and human dimensions, which we examine next.

Organizational Factors and Blind Spots

Insider threats persist not only because of technical difficulties, but also due to organizational culture and management shortcomings. Many organizations have historically underestimated or mis-prioritized insider risk, devoting the bulk of security resources to external threats. There is a natural human tendency to fear "the unknown outsider" more than the familiar insider, we lock our doors against strangers but rarely suspect our friends. In corporate terms, this translates to executives obsessing over the latest external hacker group or malware outbreak,

while overlooking the dangers posed by their own employees. As an ISACA analysis observes, organizations are "more likely to be on guard against unknown stranger hackers than against our own internal people," even though statistically insiders are very often the source of breaches.

This inherent trust in employees makes it difficult for leadership to acknowledge insider risks or invest in measures that imply mistrust of staff. After all, companies hire people *because* they believe in them. Handing someone the keys to sensitive data requires trust, and managers may feel that focusing on insider threat undermines that trust or company morale. Thus, a cultural reluctance to suspect one's own team can create a blind spot, warning signs get dismissed ("Oh, Bob would never do that!") until it's too late.

Another factor is the miscalculation of risk and ROI. It can *appear* that most breaches are caused by external adversaries, highly publicized incidents often involve hacker groups or nation-state cyberattacks. This skews perception. In reality, insiders contribute heavily to breaches (as noted, around half or more by some counts), and they can be even more damaging on a per-incident basis. Yet, security budgets often allocate minimal resources to insider threat programs.

A survey by Cybersecurity Insiders found 74% of organizations considered themselves moderately to extremely vulnerable to insider threats, but many still lacked dedicated insider threat solutions or personnel. Budget constraints and competing priorities lead security teams to focus on "bigger" external threats first, leaving insider risk mitigation under-funded. In some cases, organizations establish an insider threat program in name but fail to sufficiently staff or empower it, resulting in reactive post-incident response rather than proactive prevention.

Organizational silos and lack of cross-departmental coordination further impede insider risk management. Effective insider threat mitigation spans multiple domains- HR, IT security, legal, compliance, and management all have roles to play. However, many companies treat it as solely an IT security issue, or conversely as just an HR issue if it involves employee misconduct. The result is fragmented information: for example, HR might know that an employee has been disgruntled due to a demotion, but IT security is unaware and doesn't treat that user's anomalous file downloads with extra suspicion. Siloed handling of insider issues means critical context is missed. Best practices recommend a multidisciplinary insider risk team or steering committee that integrates these perspectives.

In U.S. federal agencies and defence contractors, for instance, insider threat programs are explicitly required to be cross-functional, combining inputs from counterintelligence, HR, security, and legal, to "deter, detect, and mitigate insider threats" holistically. In many commercial organizations, this integration is still lacking or immature. Departments might be protective of data (e.g. privacy concerns limit HR-to-security info sharing) or simply not used to collaborating regularly. This allows insiders to slip through cracks, e.g., an employee with performance issues (known to HR) might also be triggering minor IT policy violations (seen by IT), but no one connects the dots to intervene before a major incident occurs.

Organizational culture and internal pressures can also inadvertently fuel insider threats. An extremely competitive or pressure-cooker environment may drive employees to rationalize unethical behaviour. The Wells Fargo fake-accounts scandal is a case in point: thousands of employees engaged in fraud (opening unauthorized customer accounts) because intense sales goals and fear of losing jobs created a toxic incentive structure. In that case, insider misconduct was not due to one rogue actor but rather a culture where cheating became normalized as "gaming" the system. This shows how poor organizational governance, and ethics can lead to systemic insider threats. Similarly, lack of recognition or unfair treatment can turn loyal employees into malicious insiders.

NITSIG's report notes common grievance triggers like being passed over for promotion, receiving no bonus, or other perceived slights that cause resentment. If management does not have channels for employees to air grievances or if a culture of disengagement prevails, the risk rises that frustrated staff will either maliciously act out or become apathetic about following security policies (leading to negligent breaches). Low employee engagement correlates with higher insider risk. Engaged employees with positive morale are less likely to "go rogue" or be careless, whereas disengaged workers may feel little loyalty.

Finally, many organizations lack a clear strategy or policy around insider threats until after a serious incident has occurred. Unlike areas such as phishing or malware (for which companies often have training and incident playbooks), insider threat plans are sometimes ad-hoc. There may be confusion internally about who is responsible for insider risk management, leading to slow or clumsy responses when an incident is suspected. In the absence of strong leadership messaging, employees might also be unclear on their role in preventing insider incidents, e.g., are they encouraged to report suspicious coworker behaviour?

The NITSIG 2025 report suggests using real incident examples to educate employees on the importance of reporting colleagues who may pose risks. When organizations have not fostered that reporting culture, employees often stay silent ("not my business") or fear retaliation, allowing concerning behaviour s to escalate unchecked.

In summary, organizational factors, from misplaced trust and insufficient budgeting, to siloed information and negative workplace culture, significantly contribute to why insider threats remain inadequately addressed. These are not problems that technology alone can solve; they require changes in mindset, policies, and inter-departmental cooperation at the management level.

Human Behaviour and Psychological Drivers

At its core, the insider threat problem is a human behaviour problem. Every insider incident originates from a person's decisions, whether malicious or unintentional. Understanding the motivations and psychology behind these behaviour s is crucial to grasp why insider threats persist. Unlike external attackers who usually have clear motives (e.g. financial gain, political agenda), insiders have a spectrum of possible motivations that can be deeply personal and varied. This makes it challenging to predict or profile who might become a threat.

Common malicious motives for insiders include anger, revenge, greed, ideology, and coercion. The NITSIG report outlines that many incidents start with *dissatisfaction or grievances*: an employee feels wronged, perhaps due to a negative performance review, lack of promotion, demotion, or other perceived injustices, and eventually retaliates against the employer. Emotional drivers like revenge or a sense of being undervalued can cloud judgment and lead a previously good employee to justify sabotage or data theft as "teaching the company a lesson." On the other hand, some insiders are driven by financial stress or greed rather than emotion. They might think "the company owes me," especially if they feel underpaid, and decide to enrich themselves through fraud or theft. Personal hardships (debt, gambling addiction, medical bills) have also pushed employees into insider crimes for money.

The *fraud triangle* concept from criminology is relevant here: pressure (financial need or desire), opportunity (access to resources), and rationalization ("I deserve this" or "no one will notice") combine to enable occupational fraud. For instance, a payroll manager facing financial trouble might rationalize embezzling funds if internal controls are weak (opportunity) and they feel underappreciated (rationalization).

Another category is ideological insiders- those motivated by beliefs or allegiance. This could range from corporate espionage (selling secrets to a competitor or foreign government due to ideological alignment or patriotism) to acts of workplace violence driven by personal convictions. Though less common than financial or grievance-based cases, ideology-driven insiders (like spies or saboteurs) tend to be highly damaging, as seen in espionage cases such as the Cold War spies or more recently, insiders leaking information to foreign adversaries. Additionally, coercion and social engineering can turn otherwise loyal employees into insider threats.

Organized criminals or hostile entities might bribe, blackmail, or trick an insider into cooperating. For example, there have been cases of employees who were extorted into stealing data under threat or offered money to plug in a malware-laden USB stick. With the rise of ransomware, some cybercriminal gangs explicitly recruit insiders (e.g. via the dark web or even LinkedIn) to help plant malware in exchange for a cut of the ransom, essentially outsider-insider collusion.

Crucially, not all insider incidents are malicious. Unintentional human error and negligence are a huge part of the problem. Numerous breaches occur because an employee was careless: clicking a phishing link that lets in an attacker, misconfiguring a server, losing a laptop, or emailing sensitive data to the wrong address. The Ponemon study found that a negligent insider was the root cause in 55% of incidents, making it by far the most common insider threat cause. Such incidents may stem from lack of awareness, oversight, or simple mistakes, but they persist because *to err is human*. Employees juggling many tasks sometimes prioritize convenience over security (like using weak passwords or circumventing cumbersome security protocols), inadvertently creating vulnerabilities.

In other cases, they might not even know that a certain action (like uploading a file to a personal cloud drive to work from home) violates policy and puts data at risk. This human fallibility means insider risks can never be entirely eliminated, and organizations must assume that some level of mistakes will happen and design controls to catch or mitigate them before they escalate.

Detecting problematic human behaviour s before they result in incidents is another ongoing challenge. There are often warning signs that an employee might be a risk, for instance, a normally reliable worker becoming disengaged and cynical (potentially disgruntled), or someone working unusual hours and accessing atypical data (possible malicious intent). Behavioural sciences research has tried to identify red flags, such as personality changes, rule-breaking, or conflicts with colleagues, that correlate with insider threat risk. Indeed, “early warning indicators” of risky behaviour are a focus of modern insider risk programs. But human behaviour is complex and false alarms are common. Not every employee who complains about management will steal data; distinguishing idle venting from true malintent is difficult. Furthermore, privacy and ethical concerns limit how deeply companies can probe into personal behaviour s (discussed more in the next section). Even with monitoring tools, an insider’s state of mind is not directly observable. For example, two employees may both download a large database backup: one is maliciously preparing to leak it, another is doing a legitimate analysis. Their technical action is identical, but the intent differs. Security teams often lack context into that intent until after a breach occurs.

Human factors also include the social dynamics of reporting and intervention. Coworkers might notice concerning behaviour (e.g., someone asking for access they don’t need, or expressing extreme resentment), but they may hesitate to report a peer. People worry about falsely accusing someone or damaging a colleague’s career, especially if the signs are subtle. This hesitation allows many insider issues to fester. Creating a culture where employees are empowered to speak up, and managers are trained to spot and address behaviour al red flags (like sudden performance declines or policy violations) is tough, but necessary. Unfortunately, if an organization has an overriding culture of “mind your own business” or weak managerial oversight, these human early warnings go unheeded.

In summary, the persistence of insider threats is deeply rooted in human nature, be it the range of personal motives that drive malicious acts or the propensity for human error.

Insiders can rationalize their misdeeds in ways outsiders cannot (feeling justified due to perceived slights or need), and every individual has unique psychological factors that might lead them down a bad path. Because one cannot reprogram human nature as easily as a firewall, this aspect of insider threat is inherently challenging. The best an organization can do is *understand and account for human factors* through careful hiring and vetting, employee support programs (to address grievances or financial stress ethically), training to reduce errors, and vigilant attention to behaviour al cues. The next section will discuss how legal and regulatory constraints intersect with these efforts, further explaining why insider threat management is a nuanced endeavour.

Legal and Regulatory Constraints

Organizations must navigate a delicate balance between security and privacy when addressing insider threats. Legal and regulatory frameworks (such as data protection laws, employee privacy rights, and labour regulations) can inadvertently make insider threat monitoring and response more difficult. These constraints are another reason the challenge remains unresolved, even when companies have the will to crack down on insider risks, they must do so without violating laws or ethical norms.

One major consideration is employee privacy law. In jurisdictions like the European Union, the General Data Protection Regulation (GDPR) and national employment laws place strict limits on how employers can monitor and process employee data. Real-time surveillance of user activities, reading personal communications, or collecting extensive personal background data may be deemed disproportionate and illegal in many cases. For example, GDPR expects that any monitoring of employees must be necessary and proportionate, with respect for their privacy and dignity. An overly aggressive insider threat program (e.g. recording all employee keystrokes or webcam monitoring) could trigger legal penalties or lawsuits if it infringes on privacy rights. As a privacy professional publication notes, *"Real-time monitoring or recording of user activities may constitute a serious breach of privacy,"* and organizations must carefully define where such monitoring is truly justified. This means insider threat teams often have to operate with caution, focusing on specific high-risk roles or actions and ensuring employees are informed about any monitoring. Employers typically are advised to obtain consent or at least provide clear notice in acceptable use policies about what kinds of monitoring may occur. Even then, they might need to avoid capturing content of personal communications and stick to metadata or work-related actions. These legal boundaries can constrain the use of some advanced tools like full packet inspection, keylogging, or continuous video surveillance on employee machines.

Another aspect is data access and labour regulations that vary across countries. For instance, conducting thorough background checks on new hires is a recommended practice to screen out individuals with red flags (like past fraud convictions), but some jurisdictions limit how far an employer can delve into an applicant's history. Broad background investigations might run afoul of anti-discrimination laws or privacy rules, especially in the EU. Even within one country, state laws might differ on what monitoring is permissible. In the U.S., there's a patchwork of state laws about consent to monitor phone calls or computer use. Most states allow it with employer-owned devices (with notice), but a few require explicit consent. International companies face the challenge of implementing a uniform insider threat program across jurisdictions with different legal requirements. What is allowed in one country (e.g. monitoring emails without user consent) might be illegal in another. This complicates insider threat management, often forcing companies to tailor their approach region by region, which can leave inconsistent protections.

Legal constraints also affect how organizations respond to insider incidents once detected. For example, if an employee is suspected of an insider crime, the company must handle evidence collection carefully to ensure it is admissible in court and that it doesn't violate the employee's rights. Engaging legal counsel early is important to navigate laws on employee dismissal, law enforcement notification, and breach disclosure obligations. Under laws like GDPR, if an insider causes a personal data breach, the company might be required to report it to authorities within 72 hours. This adds pressure to quickly investigate and ascertain the facts, all while respecting due process for the employee. Labor laws may require that an employee be given an opportunity to respond to allegations, and wrongful termination suits are a risk if the organization acts without solid evidence. Thus, companies sometimes proceed cautiously or slowly in insider investigations, which can allow damage to continue if the insider senses something and accelerates their activities.

Additionally, when insiders are caught, there can be legal liability and reputation concerns that discourage public disclosure or prosecution. Some organizations prefer to quietly handle an incident (e.g. terminate the employee and hush it up) rather than prosecuting, to avoid public embarrassment or regulatory scrutiny. This lack of transparency means lessons from incidents aren't widely shared across industries, and perpetrators might even go on to offend elsewhere. The NITSIG report points out that *how insider threats are defined and reported is not standardized*, leading to underreporting of the true scope of the problem. For instance, if a company experiences a minor insider fraud and

settles it internally, that incident may never appear in any statistics or serve as a warning to others. This underreporting can perpetuate a false sense of security industry-wide.

Finally, compliance requirements in some sectors can both help and hinder. Industries like finance and healthcare have strict regulations around data handling (GLBA, HIPAA, etc.) that mandate controls which indirectly mitigate insider misuse (e.g. need-to-know access, audit trails). However, those same regulations impose privacy safeguards that require careful anonymization and role-based access to audit data, sometimes making it harder for insider threat teams to get all the information they need quickly. In government settings, the insider threat programs themselves are mandated (after the 2011 U.S. executive order, all federal agencies and cleared contractors must have insider threat programs), but they also must adhere to Privacy Act provisions and employee rights, which requires an intricate framework of oversight.

In summary, legal and regulatory factors mean that organizations cannot simply monitor and crack down on insiders with impunity. They must design insider risk measures that respect privacy and comply with the law, which often means a more limited or focused approach than a purely technical solution might permit.

While necessary for ethical and legal reasons, these constraints can slow down detection or leave certain avenues (like personal device monitoring) off-limits, thereby contributing to why completely resolving the insider threat challenge remains elusive.

Mitigating Insider Risk: Strategies and Recommendations

Confronting the persistent insider threat problem requires a comprehensive, multi-layered approach. No single tool or policy will suffice; instead, organizations should develop an integrated Insider Risk Management strategy that combines technical controls, organizational policies, human-centric measures, and legal/ethical best practices.

Based on the challenges analysed above, this section provides evidence-based recommendations in key areas: enhancing insider risk management programs, establishing cross-departmental governance, improving detection techniques, engaging employees through training and support, and fostering a security-conscious culture. Together, these measures can significantly reduce insider risk and enable earlier intervention before small issues become major incidents.

Strengthen the Insider Risk Management (IRM) Program

First and foremost, organizations should establish or strengthen a formal Insider Risk Management (IRM) program. This program should be a dedicated function (or team) with the mandate to proactively deter, detect, and respond to insider threats across the enterprise. An effective IRM program begins with leadership recognition of insider risk as a serious enterprise threat (on par with external cyber threats).

The NITSIG/ITDG report highlights that educating CEOs and C-suite stakeholders with real incident examples can help garner the necessary support and funding for an IRM program. When executives see concrete cases from industry, e.g., how an insider embezzled millions or how an IP theft nearly sank a competitor, they are more likely to invest in prevention. In fact, the NITSIG report itself is used by many Insider Risk Program Managers as *justification for ROI* and to secure budgets for insider threat initiatives.

A robust IRM program should include clear policies and procedures for insider threat detection and incident handling. This means defining what constitutes an insider incident, how employees can report concerns, how investigations will be conducted (with HR and legal oversight), and what disciplinary actions or support interventions are available. It's advisable to perform a risk assessment and gap analysis as a starting point to identify where the organization's current controls might fail to catch insider activity. For example, NITSIG suggests IRM managers analyse whether their

existing security tools are capable of detecting fraud and non-IT misconduct, which are on the rise. If not, that gap needs to be addressed either through process changes or new tools.

Importantly, an insider risk program must not focus solely on malicious insiders but also address negligence. This involves implementing training (discussed later) and other safeguards to reduce accidental breaches. Metrics should be established to track the program's effectiveness (e.g. number of incidents detected internally before causing damage, time to contain incidents, reduction in policy violations, etc.). The Ponemon 2025 report provides encouraging data: organizations that invested in insider risk management saw improvements such as reduced incident containment time (down to ~81 days from 86) and were more often able to *pre-empt breaches* by early detection of risky behaviour. In fact, 65% of organizations with an IRM program reported that it enabled them to detect and stop insider threats before a breach occurred. This underscores that a well-resourced program can shift security from reactive to proactive.

To succeed, the IRM program should be properly resourced with skilled staff and tools. Many organizations under-invest here and Ponemon notes companies still spend much more on cleaning up insider incidents than on monitoring to prevent them (e.g. spending $211k on containment for every incident but only ~$37k on monitoring). This imbalance needs correction: more budget toward continuous monitoring, analytics, and prevention will reduce the costly fallout.

Tools that an IRM program might deploy include insider threat detection software (for user activity monitoring, UEBA, DLP), case management systems for investigations, and data integration platforms to compile logs from various sources. However, equally important is investing in people- dedicated analysts who understand both technical signals and human behaviour al indicators, and who can work closely with other departments. The IRM team should ideally include or have access to specialists in cybersecurity, HR (for employee relations insight), legal (for compliance), and psychology/behaviour al science (for understanding concerning behaviours). Training insider threat analysts to recognize patterns (e.g. combining digital footprints with HR context) is a worthwhile investment.

Implement Cross-Departmental Governance and Collaboration

An IRM program cannot operate in a vacuum; it should be supported by a cross-departmental governance structure. This typically takes the form of an *Insider Threat Working Group* or committee that brings together stakeholders from different parts of the organization. Key departments to include are: IT/Security, Human Resources, Legal/Compliance, Physical Security, and Senior Management. Each plays a distinct role. For instance, HR manages employee relations and can provide context on terminations or disciplinary actions; Legal ensures monitoring and responses align with laws; physical security can report incidents like badge access anomalies or theft of equipment. Integrating these disciplines is critical because, as discussed, insider risk signals often manifest across domains. A collaborative approach enables the organization to "connect the dots."

The U.S. Department of Defense's guidance on insider threat programs explicitly states the goal to *integrate multiple disciplines to deter, detect, and mitigate insider threats*. In practice, this might mean a periodic meeting where, say, HR can flag a trend of increased grievances or resignations in a team (potentially elevating insider risk), while the IT team shares any technical anomalies observed, and together they assess if intervention is needed.

To formalize this, organizations should develop escalation workflows that span departments. For example, if a security monitoring tool flags that an employee is downloading unusually large amounts of data, the insider threat analyst might first consult HR to see if that employee has given two weeks' notice (signalling a potential data theft before departure scenario). If so, Legal might advise on a targeted scan of the employee's emails for any signs of sending confidential data outside. By working as a team, they can act swiftly and appropriately. Without such integration, each department may have only a piece of the puzzle.

Cross-department governance also helps in creating a unified policy framework. Policies around acceptable use of company resources, data handling, and reporting suspicious behaviour should be crafted with input from all stakeholders to ensure they are effective yet fair. For instance, a monitoring policy might need legal vetting (to comply with privacy laws) and HR input (to ensure it's communicated in a way that employees accept). Once in place, consistent enforcement of policies across departments is important. IT can't make exceptions for "star employees" if they violate data policies, and HR can't quietly handle a serious security violation without involving the security team.

Another benefit of cross-functional governance is it provides support for difficult decisions. Dealing with an insider threat can be fraught; having consensus from HR, legal, and management gives confidence in actions like searching an employee's workstation or placing someone on leave pending investigation. It spreads responsibility and ensures due process, which protects the organization from legal blowback and the employee from unfair treatment.

Many organizations find value in conducting regular insider threat briefings or training exercises with the multidisciplinary team. For example, tabletop exercises where a simulated insider incident is walked through can reveal gaps in communication or procedure between departments. It's far better to discover and fix those in a drill than during a real incident.

In short, tearing down silos and fostering collaboration is a vital recommendation. An isolated approach almost guarantees blind spots in insider risk management. By contrast, a coordinated governance structure can leverage each department's strengths- technical detection from IT, behaviour al red flags from HR, legal guidance on limits, etc., to create a more complete protective shield. This ties directly into the next recommendation, as one of the collaborative outcomes is implementing better detection and prevention mechanisms.

Enhance Detection Techniques and Monitoring Capabilities

Improving the detection of insider threats is paramount to reducing the time to respond and contain incidents. Given the technical challenges discussed, organizations should deploy a combination of advanced tooling and strategic controls to catch insiders in the act or, better yet, in the precursory stages of risky behaviour. Modern insider threat detection revolves around understanding baseline behaviour and identifying anomalies.

User and Entity Behaviour Analytics (UEBA) solutions are highly recommended. These tools use machine learning on logs from endpoints, servers, and networks to identify when a user's activity deviates from their norm or from peers. For example, if an employee who typically accesses at most 10 files per day suddenly accesses 500 files and uses a script to copy them, UEBA would flag that anomaly. Similarly, if an accountant starts logging in at odd hours or a database admin begins querying tables outside their usual scope, those patterns can be caught. UEBA has the advantage of being able to detect unknown threat patterns (not just matching pre-defined rules), which is crucial for insiders who often don't trigger signature-based alerts.

Alongside UEBA, organizations should utilize Data Loss Prevention (DLP) solutions. DLP can inspect data flows (emails, file transfers, USB copying, etc.) for sensitive content and enforce rules (like blocking or alerting on large file transfers or emails to personal addresses containing confidential keywords). While DLP alone may produce false positives, when combined with context from UEBA and HR (such as noticing a person is about to resign), it becomes a powerful tool to thwart exfiltration. Endpoint monitoring agents can also play a role, especially for detecting technical sabotage (e.g. an IT admin running deletion scripts, or someone plugging in unauthorized storage devices). Some endpoint monitoring tools even record user sessions (screen recording) for later forensic analysis, though these must be used judiciously considering privacy.

It's also important to monitor for policy violations and precursors. Not every policy violation is a breach, but smaller infractions can be warnings. For instance, an employee circumventing security (like installing unapproved software, or using someone else's credentials) may indicate disregard for rules, a potential precursor to bigger issues. Catching and correcting these early is part of an effective detection strategy.

Technical controls like enforcing least privilege and segregation of duties (as recommended in the IAPP best practices) help limit how much damage an insider can do undetected. If no single individual has all the keys, and certain actions require dual approval (two-person rule), it becomes harder for an insider to act alone maliciously. For example, requiring two authorized employees to jointly approve large fund transfers might have prevented some of the rogue trading and fraud incidents in banks.

Another recommended strategy is adopting a "zero trust" security model as it applies to internal systems. Zero trust means no user is inherently trusted, and every access is continuously verified with principles of least privilege. In practice, this could involve re-authenticating users for sensitive actions, using adaptive access control (if a user's behaviour is suspicious, temporarily restrict their access until verified), and micro-segmentation of networks so that even an insider can only reach what they absolutely need. Zero trust architectures can significantly contain the blast radius of an insider incident, even if credentials are stolen or an insider attempts lateral movement, strong identity and access management combined with monitoring will hinder them.

One must also integrate diverse data sources for detection. Insider anomalies might show up in digital logs (file access, login times) *and* in physical realm (badge access at odd hours, printing large volumes of documents). Forward-leaning organizations integrate physical security logs with IT logs to catch patterns (e.g. an employee entering a data centre at night and shortly after there's a spike in server data copies). Likewise, email or chat communications, where legally permissible to monitor, can provide clues (such as an employee expressing intent to harm or discussing new job plans which might correlate with data downloads).

The goal is an aggregated view of activity. Some companies are investing in Security Information and Event Management (SIEM) systems or specialized insider risk platforms that pull together these feeds and apply correlation rules. Ponemon's research indicates that such technology deployments can reduce costs. For instance, use of SIEM and user training significantly lowered incident costs in their study.

However, technology must be configured and tuned correctly. Too strict monitoring can generate a firehose of alerts that overwhelm security teams, so tuning and automation are key. Use machine learning to filter out normal behaviour and highlight the truly anomalous. Leverage automation to respond to certain triggers in real-time: for example, if a user starts downloading an unusually large amount of data, an automated response could temporarily lock their account or require step-up verification before continuing. This kind of just-in-time control can stop an insider in their tracks and signal security to investigate immediately.

Detection is only half the battle. It should be paired with robust incident response plans for insiders. This includes playbooks for steps to take when an insider incident is suspected: who to involve (HR, legal, etc.), how to preserve evidence (device seizure, log archival), when to engage law enforcement, and how to communicate to staff or the public if needed. Having this ready ensures a swift, coordinated reaction, minimizing the harm.

In conclusion, improving detection and monitoring involves both adopting state-of-the-art security tools and implementing smart policies (like zero trust and least privilege). Early detection has enormous benefits: containing incidents faster (thus cutting average costs drastically, as data showed from ~$18M down to ~$10M when contained quickly). As one report succinctly put it, "breach prevention begins with early risk detection, if detection focuses solely on exfiltration, the chance to be proactive is already lost". Organizations should take that to heart and emphasize catching risky patterns *before* they fully manifest as data loss or damage.

Engage and Educate Employees

Employees are often described as the weakest link in security, but they can also be the first line of defence if properly engaged. A crucial recommendation is to invest in *employee training, awareness, and engagement programs* focused on insider risk. This serves two purposes: reducing unintentional incidents (by educating staff on security best

practices and how to avoid common errors) and creating a vigilant workforce that can help spot and deter malicious activity.

Firstly, security awareness training should cover insider threat scenarios, not just external phishing and malware. Many employees do not realize how their everyday actions could lead to breaches. Regular training can remind them of policies like data classification (what data can be shared, what must be encrypted), safe use of corporate resources, and the importance of following procedures (for example, not bypassing access controls or sharing passwords).

Training should also highlight the damage insider incidents can cause, perhaps referencing real-world examples (e.g., "an employee at X company accidentally leaked customer data by doing Y"). When people see concrete examples, it dispels the notion that "it wouldn't happen here." The NITSIG report suggests using case studies in awareness sessions to show employees the severe impacts insiders have had on organizations. This not only educates but also helps build a culture where employees understand why certain rules are in place.

Training should be ongoing and role-specific. Ponemon's research found that user training and awareness programs can save organizations an average of $5.4 million by preventing incidents- a testament to the ROI of education. New hires should get onboarding training that emphasizes data protection responsibilities. High-risk roles (like system administrators, finance personnel) might need specialized training that covers relevant threats (e.g., admins being aware of the signs of account compromise, or finance staff learning about fraud schemes). Also, periodic refreshers (at least annually) with updated threat information keep security top-of-mind. Interactive trainings, such as workshops or even gamified exercises, can improve retention compared to dry lectures.

Secondly, beyond formal training, companies should strive to engage employees as part of the solution. Encourage them to take ownership of security in their day-to-day jobs. One approach is implementing an *insider threat awareness campaign* internally. This could involve newsletters or intranet posts that share anonymized lessons learned from past incidents, tips for safeguarding information, and how to report suspicious behaviour.

By normalizing the conversation about insider threats, it removes stigma. Employees should not feel that reporting a concern is an accusation of a colleague, but rather a responsible action akin to reporting a safety hazard. NITSIG's monthly incident reports are actually used by some firms to educate staff on the importance of reporting risky behaviour among peers. Consider establishing clear, confidential reporting channels, e.g., a hotline or an email alias for insider risk concerns, possibly even allowing anonymous tips. Ensure that employees know about these channels and trust that reports will be taken seriously and handled discreetly.

Recognize employees who do the right thing (without naming specifics publicly) to reinforce positive behaviour. For instance, if an employee reports a security weakness or a suspicious incident that leads to prevention of a breach, management can commend that proactive behaviour in general terms. This creates positive reinforcement for engagement.

Employee engagement also means addressing the human needs of employees, so they are less likely to become threats. Employee assistance programs (EAPs) offering counselling, financial advice, or stress management can indirectly mitigate insider risk by helping staff cope with pressures that might otherwise push them toward malfeasance. For example, if an employee is struggling with debts or addiction (common precursors for fraud motivation), an effective assistance program might help them find help rather than resort to desperate measures. Making sure employees are aware of such resources and encouraging their use can be a preventive measure.

Furthermore, involve employees in developing practical security solutions. Often the people on the ground know where security measures hinder productivity, leading to workarounds. By getting feedback, security teams can adjust policies to be more user-friendly (without compromising safety), thus increasing adherence. If employees feel their input is valued, they are more likely to buy into the security culture rather than view it as an external imposition to circumvent.

In summary, an engaged, educated workforce reduces both the likelihood of accidental insider incidents and the success of malicious ones. When employees understand the *why* behind security measures and feel responsible for protecting the organization, they act as force multipliers for the security team. This human layer of defence, eyes and ears on the ground, can notice and prevent things technology might miss. As the adage goes, "security is everyone's responsibility," and nowhere is that more true than with insider threat mitigation.

Foster a Security-Conscious and Trustworthy Culture

Culture is perhaps the hardest element to change, but it is also one of the most impactful in mitigating insider threats long-term. A security-conscious culture is one where good security behaviour is ingrained in the organizational DNA, and employees at all levels prioritize protecting information as part of their job. Achieving this while maintaining a positive work environment (not one of paranoia) is the ultimate balancing act. The following cultural shifts are recommended:

- **Promote Ethical Behaviour and Fair Treatment:** Leadership should set the tone that ethical conduct is paramount and that any fraudulent, dishonest, or harmful actions will not be tolerated. Equally, they should ensure employees are treated fairly and grievances are heard. Studies of insider incidents often find the perpetrator felt wronged or unappreciated. By proactively addressing legitimate employee concerns, through open-door policies, fair compensation, recognition of good work, and transparent HR processes, organizations can reduce the pool of disgruntled employees who might seek retaliation. A culture of respect and fairness can defuse the emotional drivers of insider attacks. The Wells Fargo example, where unrealistic goals led to widespread misconduct, is a cautionary tale: a culture that pressures employees to cut corners will breed insider risk. Instead, aligning performance incentives with ethics (e.g., rewarding compliance and reporting of issues, not just raw results) is vital.

- **Encourage "Trust but Verify":** Organizations should communicate that while they trust their employees, verification is a standard practice. This is akin to the zero-trust mindset applied culturally. For example, implement peer code reviews, dual approval for critical actions, or rotation of duties not because any one person is suspected, but because it's healthy to have checks and balances. Framing it as protecting employees as much as the company can help, e.g., "Having two people involved in this process protects you from any false blame and ensures accuracy." When done transparently, these measures become accepted norms.

  It's important that monitoring and audits are not secret; let employees know generally that monitoring is in place (within privacy limits) to deter wrongdoing. If everyone knows that "someone is watching" in a general sense, an insider is less likely to attempt something, and others feel safer reporting since they know it's taken seriously.

- **Balance Security and Privacy to Maintain Trust:** Overly intrusive monitoring or a draconian atmosphere can backfire by eroding trust and morale. Employees might then actively try to evade monitoring out of resentment. To avoid this, implement privacy-conscious monitoring. For instance, monitor only work-related activities and avoid prying into personal content. Clearly communicate what is monitored and why. Emphasize that the purpose is to protect the company *and* employees' livelihoods (since a major breach could endanger the business).

  By being upfront and showing respect for privacy (no surveillance beyond what's necessary), organizations can maintain a healthier relationship with staff. As noted earlier, focusing monitoring on critical assets and behaviour s rather than blanket surveillance helps maintain this balance. Periodic privacy reviews of the insider threat program by legal or external auditors can ensure it stays within agreed bounds.

- **Develop a Speak-Up Culture:** Encourage employees to report not just security issues but also any unethical practices or policy violations (akin to a whistleblower-friendly culture). Ensure that those who raise concerns are protected from retaliation and that their reports are acted upon. When employees see that the company addresses problems rather than shooting the messenger, they are more likely to come forward with information that could stop an insider threat early. For example, if someone notices a colleague printing large volumes of

client records, in a speak-up culture they'd feel comfortable alerting a manager. Internal campaigns can reinforce that *reporting is a responsibility*, not disloyalty. Some organizations integrate this into their core values or code of conduct training.

- Leadership Involvement and Modelling: Leaders should actively participate in security initiatives, not exempt themselves. If executives bypass security protocols (e.g., using personal email for work or not following data handling rules), it sends a message that security is not important. Leaders need to model the desired behaviour. For instance, a CEO could mention in a town hall how they themselves underwent the phishing training or how they abide by access restrictions just like everyone else. Visible endorsement of the insider risk program by top management also reinforces its importance. In one case, a major corporation's CEO sent a company-wide memo about an incident of insider IP theft that was caught, praising the teams that detected it and reaffirming commitment to trust with verification. Actions like this demonstrate that management is serious about the issue.

Building such a culture does not happen overnight. It requires consistency and reinforcement. Recognition programs can be used to highlight teams with good security practices. Incorporating security and ethical behaviour into performance reviews or at least into employee feedback cycles can also institutionalize it. Some firms include a section in annual reviews for managers to confirm the employee follows security policies diligently, making it part of performance metrics sends a signal that it matters.

In a strong security culture, insider threats will still exist (one cannot eliminate all malintent or mistakes), but they are more likely to be prevented or caught early. The organization essentially creates an environment where it's hard for an insider to justify a malicious act (due to loyalty and satisfaction) and hard to execute it without someone noticing. And if an incident does occur, the response will be faster and more unified, because everyone understands the importance and their role. The ultimate goal is that *security becomes as ingrained and unquestioned as workplace safety*, just as employees would stop someone from doing something physically dangerous on a factory floor, they should instinctively flag something that endangers information security. That is the cultural ideal to strive for.

Final Thoughts

Insider threats remain an unresolved cybersecurity challenge because they stem from the fundamental complexity of human behaviour intersecting with organizational systems. The May 2025 NITSIG/ITDG report and numerous other sources make clear that insiders, whether malicious employees, negligent staff, or exploited partners, can cause devastating harm that rivals or exceeds external attacks.

We have seen that the persistence of this threat is not due to a single failure, but a convergence of issues: technical limitations in detecting authorized users' bad acts, organizational blind spots and resource gaps, behaviour al and psychological factors that drive insiders, and legal constraints that require balance and finesse in monitoring. These factors together explain why insider risk is so difficult to eradicate and why high-impact incidents continue to surface regularly across all industries.

However, "difficult" does not mean impossible to mitigate. Through a holistic and proactive approach, organizations can significantly reduce their insider threat exposure. This paper outlined a multi-faceted strategy: building robust Insider Risk Management programs backed by leadership, fostering cross-department collaboration so no red flag goes unseen, leveraging advanced analytics and zero-trust principles to detect issues early, deeply engaging employees in security efforts, and nurturing a corporate culture that values ethics and vigilance. Implementing these recommendations requires effort and investment, but the evidence shows the payoff, shorter incident response times, lower financial losses, and perhaps most importantly, prevented breaches that never become tomorrow's headlines.

Going forward, organizations should treat insider risk as an ongoing program of improvement. Threat patterns will evolve (for instance, insiders may abuse emerging technologies or new remote work paradigms), so continuous

adaptation is key. Regularly revisiting the contributing factors, e.g., assessing if technical tools need upgrading, if policies cover new scenarios, if employees are reporting issues, will keep the defences aligned with the threat. Sharing information within industry groups (as NITSIG does with its reports) and learning from others' incidents can also help collectively raise the bar against insider threats.

In conclusion, while we may never completely eliminate the risk of someone betraying trust, we can manage and contain insider threats through knowledge, preparedness, and a united organizational front. As one expert insightfully noted, cybersecurity at its core is a human challenge requiring a human-centric approach. By remembering that and embedding it in our security strategies, we stand a far better chance of detecting the insider in the shadows and preventing the next big insider incident. The challenge is formidable, but not insurmountable, with diligence and the right approach, organizations can turn the unresolved insider threat into a risk that is understood and mitigated as part of normal business, rather than a lurking crisis.

Karl DiMascio, *IntroSecurity ASEAN*

Sources:

- NITSIG & ITDG, *Insider Threat Incidents Report, May 2025*
- Ponemon Institute, *2023–2025 Cost of Insider Threats Global Reports*
- ShieldCRS Blog, "The Growing Menace of Insider Threats" (Dec 2024)
- ISACA Blog, "Why So Many Organizations Underestimate Insider Threats" (Jul 2024)
- IAPP Article, "How to manage insider threats without violating privacy laws" (2020)
- U.S. DoD CDSE, *Developing a Multidisciplinary Insider Threat Capability* (Mar 2024)
- NITSIG, *Insider Threat Motivations Overview* (2025 report)
- NITSIG, *Severe Impacts from Insider Threat Incidents* (2025 report)
- Case Study references: Wells Fargo scandal; Allianz fraud case; Goldman Sachs/1MDB case; Tesla 2020 sabotage attempt; USDA SNAP fraud case; Desjardins 2019 breach; Snowden NSA leak.

About IntroSecurity ASEAN

IntroSecurity ASEAN is a specialist growth and execution firm dedicated to supporting cybersecurity vendors seeking to establish or expand their footprint across Southeast Asia. With its strategic base in the region and operational reach into markets including Thailand, Vietnam, Malaysia, Indonesia, and Singapore, IntroSecurity delivers a fully integrated solution to market entry and commercial acceleration.

Founded by cybersecurity leaders Karl DiMascio and Mike Loginov, the firm brings decades of senior-level industry experience, both in executive roles and in leading regional go-to-market efforts for some of the world's most recognised cyber brands. What sets IntroSecurity ASEAN apart is its execution-first model. The firm does not operate as a reseller, distributor, or passive advisor. Instead, it embeds itself directly into the vendor's growth journey, acting as a strategic extension of the client's leadership team. This includes developing localised go-to-market strategies, building and enabling high-performance partner ecosystems, identifying and engaging talent, and generating early-stage pipeline through direct field engagement.

IntroSecurity's value lies in its ability to operate where many global vendors struggle: inside the nuance of ASEAN's diverse regulatory environments, language barriers, fragmented partner landscapes, and relationship-driven sales cycles. By offering real-time local presence combined with global commercial thinking, the firm bridges the gap between strategic intent and in-market delivery. This enables clients to build brand credibility, achieve faster traction, and avoid costly misalignment or delays.

Clients benefit from a hands-on, results-oriented approach that focuses on measurable impact. From initial market scoping through to signed enterprise deals, IntroSecurity ASEAN ensures every step is rooted in deep regional knowledge, operational discipline, and long-term strategic alignment.

For cybersecurity companies serious about Southeast Asia, IntroSecurity ASEAN provides the clarity, access, and execution required to turn ambition into reality.

For more information, visit www.introsecurity.com or contact karl.dimascio@introsecurity.com

---

About The National Insider Threat Special Interest Group (ITDG)

The NITSIG was created in the United States (U.S.) in 2014 to function as a National Insider Threat Information Sharing & Analysis Center (ISAC), as no such ISAC existed. The NITSIG has been successful in bringing together Insider Risk Management (IRM) and other security professionals within the U.S and globally to enhance the collaboration and sharing of information, best practices and resources related to IRM. The NITSIG stands at the forefront of helping organizations safeguard their assets (Facilities, Employees, Financial Assets, Data, Computer Systems - Networks) from one of today's most damaging threats, the Insider Threat.
https://www.nationalinsiderthreatsig.org

The NITSIG in conjunction with the Insider Threat Defense Group (ITDG) has conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over 6,300+ Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all types and sizes. This research is posted in the NITSIG monthly reports and specialized reports that can be found on www.insiderthreatincidents.com

The NITSIG Membership is FREE.

Link To NITSIG Membership Application
https://www.nationalinsiderthreatsig.org/pdfs/National%20Insider%20Threat%20Special%20Interest%20Group%20Membership%20Application.pdf

About The Insider Threat Defense Group (ITDG)

Since 2009, the Insider Threat Defense Group (ITDG) has been a leading authority in Insider Risk Management (IRM) Programs, providing both consulting services and the most extensive selection of specialized classroom instructor led and web-based training courses in the field.

The ITDG has provided training and consulting services to over 1000+ individuals and 700+ organizations. Their instructors are experts in providing real-world experience and empowering organizations with the core / advanced knowledge and resources to develop, implement, manage, evaluate and optimize a comprehensive IRM Program. Their client listing is quite impressive.
https://www.insiderthreatdefense.us/wp-content/uploads/2024/05/insider-threat-defense-group-client-listing.pdf

Combing ITDG training / consulting services, with NITSIG meetings, symposium events, the ITDG + NITSIG have provided IRM training and guidance to over 3000+ individuals.

More information on their training courses and consulting services is available at:
www.insiderthreatdefensegroup.com