Corporate Security and Integrity Threat Assessment

CLUE

Content

Foreword

Matt Horne, Director of Intelligence and Investigations, Clue Software

Corporate security and integrity today are shaped by converged, people-centred risk. Adversaries, criminals and activists blend digital and physical tactics: identity compromise, supplier breaches and online mobilisation sit alongside on-site disruption, organised crime activity, pressure on executives, and attempts to seed insiders. A single trigger can escalate quickly into operational, legal and reputational impact.

This report summarises nine threat areas we assess as most significant for large corporates, drawing on ongoing research, open-source and official reporting, and our team's domain experience. Our aim is practical: to help boards and senior leaders frame decisions, align functions and build proportionate resilience without unnecessary complexity or cost.

Corporates are not expected to fix societal problems or perform law enforcement functions. But serious threats to collective safety, security and integrity require clarity and coordination across security, cyber, HR, legal and supply-chain teams - and an intelligence-led response that protects people, operations and trust.

This assessment addresses the integrity of people, processes and partners as much as physical and cyber security, reflecting the needs of organisations across sectors. And it provides actionable advice on how to create intelligence-led resilience for organisations navigating an increasingly complex threat landscape.

Introduction

Large corporates operate in a converged threat environment where identity, suppliers, people, systems, and premises are all viable attack surfaces - some with potentially existential implications if mishandled. The most consequential patterns we see include:

- Serious and organised crime (SOC) converting corporate scale into criminal scale through theft, counterfeiting, piracy, laundering illicit finance and exploitation of logistics and professional enablers.
- Fraud accelerated by AI-driven impersonation and deepfake techniques.
- Terrorism and extremism where the most likely threat is lone-actor, low-sophistication harm requiring stress-proof response routines.
- Cyber crime and information security dominated by identity-led intrusions, ransomware/data-extortion, and low-noise persistence on edge devices.
- Insider threat amplified by hybrid work, contractors and credential misuse, often negligent or compromised rather than malicious.
- Corporate espionage and hostile state activity exploiting human-centred entry points such as CVs, expert briefs and research channels.
- Sanctions risk and geopolitical exposure with tighter UK enforcement and rising expectations for event-driven due diligence and evidential decision-making.
- Protest, activism and physical security where campaigns move rapidly between online narratives and on-site action.
- Safeguarding and exploitation risks where modern-slavery and labour exploitation risks persist beyond direct suppliers, and stakeholders expect remedy, not just policy.

About this threat assessment

Scope and basis.
These threat areas represent the issues we judge most significant now, based on continuous monitoring of credible public reporting, regulatory updates and law-enforcement intelligence, combined with our domain expertise in corporate security and integrity. They are not exhaustive but reflect common patterns across sectors.

What this report does.
Each threat area is presented in two parts: a current snapshot (how the threat is evolving) and implications for corporates (principle-led considerations). Short case studies illustrate real-world impact. The final section sets out practical steps for an intelligence-led approach to resilience and decision-making. Where proportionate, collaboration with peers, regulators, law enforcement and government is encouraged - including sharing relevant intelligence to protect people and reduce harm.

'So what' for leadership.
The through-line across all nine areas is convergence. Issues rarely stay in one lane. Organisations that fare best think and act cross-functionally, bringing intelligence, risk, and incident data into a single view to act early, disrupt threats at source and recover fast. They treat identity and suppliers as part of a single perimeter, design for the first five minutes of any incident, and judge resilience by how they protect people and sustain trust, not just by uptime or loss figures.

Across all areas, threat understanding and intelligence need to be translated into risk assessment - evaluating likelihood, impact and exposure in your specific context - so responses and investigations are proportionate, defensible and effective.

In practice, this means strengthening protect, prevent and prepare* capabilities as everyday habits.

The 4P approach*
The 4Ps - Prevent, Pursue, Protect, and Prepare - form the strategic framework used by UK law enforcement to counter terrorism and serious organised crime. This model focuses on stopping individuals from engaging in criminal activity, disrupting offenders, securing vulnerable targets, and reducing the impact of incidents. These concepts can help to frame thinking around how to deter, detect, and disrupt security and integrity threats in the private sector.

Corporate risk.
Some threats described here can become existential if mishandled - for example, catastrophic disruption of services and supply chains, sanctions breaches or irreversible trust loss. Others may still materially affect profitability, valuation or reputation if not detected, escalated and investigated properly. We raise this once, for context, while keeping the report practical and proportionate. This assessment will help organisations attain the goal of intelligence-led resilience

Note on Critical National Infrastructure (CNI).
CNI operators face heightened threat and regulatory expectations. While the principles in this assessment apply broadly, CNI organisations should calibrate controls and investigation capabilities to sector-specific regulations and dependencies (e.g., safety-of-life, upstream/downstream reliance and regional impact) and maintain tighter operational liaison with competent authorities and law enforcement. The bar for threat intelligence assessment, evidentially sound casework, auditable decision-making and tested continuity plans is correspondingly higher.

Emerging threat themes

Convergence. Threats rarely stay in one lane - digital, physical, criminal, national security, legal and reputational impacts blend quickly.

Identity as the perimeter. Attackers increasingly log in through social engineering rather than break in, exploiting weak controls or stolen credentials.

Third-party exposure. Suppliers and partners act as extensions of your perimeter - and your attack surface.

Emerging threat themes

People and process over perimeters. Fraud or theft through diversion often relies on manipulating people, sometimes boosted by AI-driven impersonation.

The insider is often unintentional. Much insider harm stems from error, compromise or coercion, not malice. But bad actors inside your perimeter are a reality.

Low-noise infiltration. Hostile actors prefer quiet routes - collaboration channels, expert calls, HR entry points.

Emerging threat themes

Shifting compliance ground. Sanctions regimes and expectations change rapidly; seemingly routine payments or business services can have extraordinary consequences.

Narrative risk and public pressure. Online mobilisation, deepfakes, data leaks, and activism mean reputation can move faster than response.

CORE THREAT AREAS

1. Serious and organised crime

The current snapshot

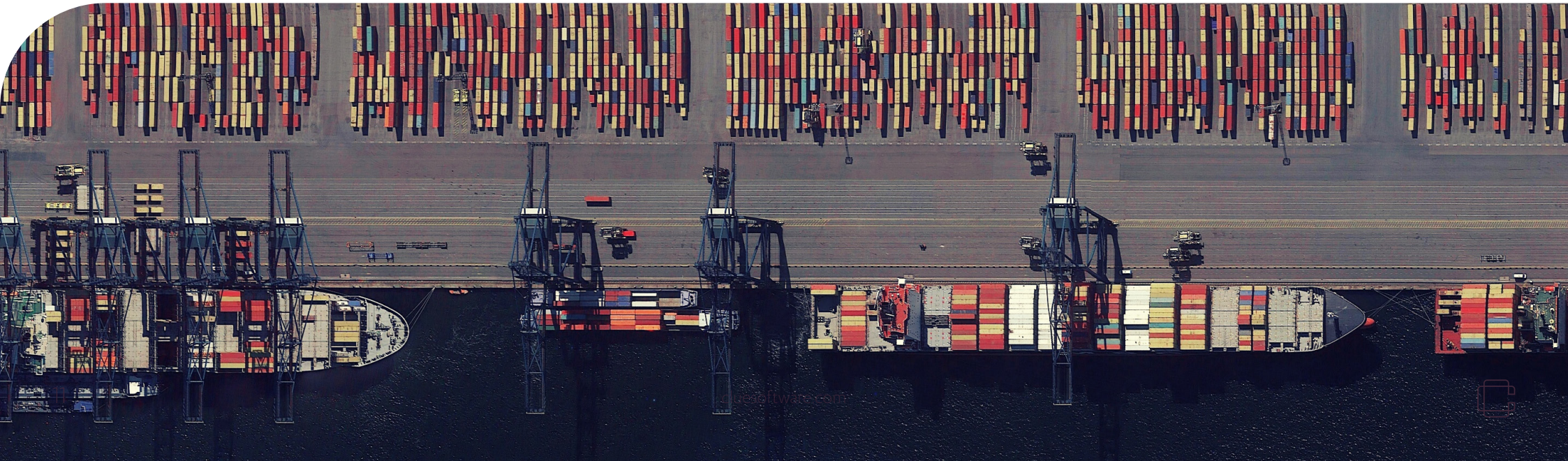
SOC increasingly operates across digital and physical channels, combining global supply networks for illegal commodities with logistics, front companies, and complex money-laundering infrastructure to exploit corporate scale. Acquisitive crime is increasingly organised, with sophisticated groups targeting corporate assets, sites, stock and supply chains for financial gain. UK assessments for 2025 highlight continued diversification and greater reliance on professional enablers, cryptoassets and opaque corporate vehicles to obscure ownership and financial flows.[1]

Counterfeiting and piracy is a core SOC revenue stream impacting multiple sectors - including consumer goods, creative media, and pharmaceuticals - with OCGs infiltrating supply chains, online marketplaces and distribution. UK and international reporting evidences billions in counterfeit trade linked to organised networks, with UK enforcement led by IPO, PIPCU and MHRA targeting unsafe and illicit products.[2]

For corporates, SOC activity often sits within ordinary operations. Routine ordering, warehousing and distribution processes are targeted at volume; goods are legitimately purchased and diverted in transit; vehicles are targeted at depots or roadside; high-volume theft occurs across retail and logistics sites; and criminally controlled front companies deliver genuine services while facilitating theft or laundering. Insider involvement can further mask activity, making losses appear as shrinkage, damage or administrative error. Estimates suggest more than £12bn is generated annually by SOC in the UK, with around £100bn laundered through or via UK structures.[3]

Implications for corporates

- Treat serious and organised crime as an enterprise risk. It affects operations, commercial relationships, supply chains, and trust - not just losses.
- Assume criminals will target your busiest processes. High-volume, routine workflows are attractive precisely because abnormalities blend in.
- Make joined-up decisions the norm. Finance, security, legal and procurement surface risk fastest when they share signals and act together.
- Treat counterfeits and piracy as a supply chain security risk. Align brand protection, content protection, quality assurance and physical security with intellectual-property and specialist policing intelligence to disrupt organised counterfeit activity, particularly in high-risk sectors
- Escalate from response to investigation when patterns persist. Use joined-up intelligence and casework to identify front companies, insider enablement and laundering routes, and share relevant intelligence with UK intellectual-property authorities, specialist police teams, local enforcement bodies and industry groups where appropriate.



“**When I was running** national investigations, the organised crime we cracked wasn’t just hidden in dark corners; it was also sitting inside everyday business processes. Criminal groups rely on speed, volume and familiarity. If it feels routine, they assume no one will look closely.”

Matt Horne, Director of Intelligence and Investigations, Clue Software

Case study - Organised retail crime

UK retail sector, **2024**

In 2024, a specialist national policing unit within OPAL (the national intelligence unit focused on serious organised acquisitive crime) disrupted 28 organised crime groups behind coordinated shop theft across major UK retailers. The groups operated across regions to evade detection, targeting high-value goods for resale through secondary markets. Within seven months, 93 offenders were arrested, linked to over £4m in confirmed losses, illustrating how apparently low-level shoplifting can mask industrial-scale theft enabled by coordination, mobility and resale infrastructure.

Shoplifting Object Detection Model Dataset - Roboflow Universe

Footnotes
[1] NCA, National Strategic Assessment 2025 (SOC trends).
[2] IPO Counterfeit goods research (Wave 4)
[3] Summaries of NCA findings on illicit finance/laundering scale.

CORE THREAT AREAS

2. Fraud

The current snapshot

Fraud is shifting from breaking in to talking its way in. AI-enabled impersonation and synthetic media now allow criminals to convincingly present as executives, suppliers or customers during routine calls, video meetings and verification steps, turning ordinary workflows into attack paths. These techniques exploit trust, time pressure and familiarity rather than technical weaknesses, and they nest unobtrusively inside contact centre, finance and supplier interactions where "business as usual" is the camouflage.

Incident reporting shows rapid growth in business-targeted deepfakes and synthetic voice abuse, with high-quality fakes increasingly difficult to spot unaided. Insiders committing fraud directly against employers or facilitating external attacks are a persistent challenge. The result is a faster path from a single conversation to payment diversion, data disclosure, contractual commitments or wider reputational harm. [1, 2]

The most exposed points remain where people make quick decisions under perceived urgency - payment authorisation, supplier onboarding, credit or refund handling - and where controls rely on who someone appears to be rather than what is being asked and whether it fits context and process. [3, 4]

Implications for corporates

- Treat unusual requests as signals, not annoyances. Payment changes, supplier updates or urgent approvals are often where social engineering shows up first.
- Slow the moment down. Pausing to verify context is usually more effective than relying on recognition of voices, faces or titles.
- Escalate when patterns repeat. One odd request may be noise; multiple similar attempts point to an organised approach and justify deeper investigation.
- Rebuild the story afterwards. Understanding who contacted whom, through which channel, and why it worked is what prevents the next loss.

Case study - Arup duped of £20M in deepfake videocall

UK engineering sector, **2024**

British engineering firm Arup was defrauded of £20m after a Hong Kong employee was deceived into transferring funds during an AI-generated deepfake video call impersonating senior executives. The case highlights the rapidly escalating sophistication of cyber-enabled fraud, where realistic voice and video cloning can bypass traditional corporate controls without compromising internal systems. It underscores growing risks to global businesses from AI-driven social engineering and the need for stronger verification safeguards.

Arup Building, Dublin Docklands

Footnotes
[1] Resemble AI, Q3-2025 Deepfake Incident Report.
[2] Deepfake growth/detection round-ups (Keepnet; Deepstrike).
[3] Contact-centre/voice-fraud growth metrics (Keepnet roundup).
[4] Case coverage - deepfake video conference payments.

CORE THREAT AREAS

3. Terrorism and extremism

The current snapshot

The UK national threat level remains Substantial*, meaning an attack is considered likely. While organised, high-impact attacks remain a realistic possibility, the most credible risk continues to come from lone actors using low-tech methods such as knives, vehicles or arson, often radicalised online and sometimes without a fixed ideological label.[1]

In 2024-25, Prevent referrals reached record levels, with a growing proportion involving young people and cases framed as fascination with extreme violence rather than formal extremist affiliation.[2] Across Western countries, the overwhelming majority of fatal attacks in recent years have been carried out by lone actors, reinforcing a pattern of low-frequency but high-impact risk, particularly for publicly accessible and crowded places. UK guidance increasingly emphasises preparedness over prediction.

Protect Duty proposals under Martyn's Law place clearer expectations on organisations responsible for public venues, while National Protective Security Authority (NPSA) principles, reflected in ProtectUK and Security Industry Authority (SIA) guidance, stress proportionate physical security, staff awareness, clear procedures and effective coordination with emergency services.[3]

Sabotage, espionage, and influence by hostile states are also increasingly converged with organised criminal threats. For example, the recruitment and tasking of criminals to commit arson or similar disruptive attacks facilitated through platforms such as Telegram. Organisations with sites or assets of potential interest should recognise this shift in tradecraft.

*Current at publication; threat levels may change - always check MI5/JTAC updates.

[1] Global Terrorism Index—lone-actor prevalence in the West (2025).
[2] Pool Re/HSToday on Prevent referrals and patterns (Dec-2025/Jan-2026).
[3] ProtectUK guidance on Self-Initiated Terrorists (Jan-2025).
[4] Case reporting—Manchester (Oct-2025)

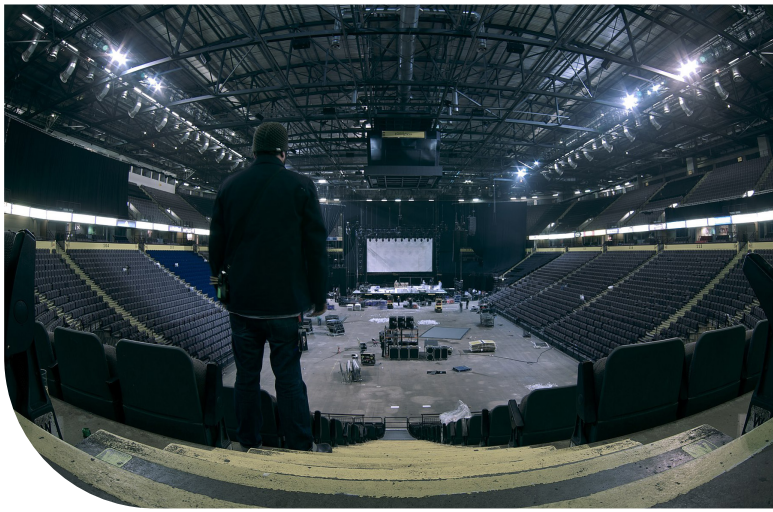
Implications for corporates

- Expect weak signals before clear threats. Early indicators often come from staff observations, site behaviour or changes in local context, not formal warnings.
- Make early actions muscle memory. Clear first-five-minutes routines matter more than detailed plans when stress is high.
- Use the support that exists. National protective security guidance and counter-terrorism advisers are there to help organisations calibrate proportionate responses.
- Understand Martyn's Law. The Terrorism (Protection of Premises) Act 2025 requires duty-holders for publicly accessible premises and events to prepare for and, where appropriate, protect against terrorist attacks.

Case study - Manchester Arena and the Protect Duty

UK hospitality sector, **2017**

The 2017 Manchester Arena bombing killed 22 people and injured more than 1,000 others at a publicly accessible venue. The attack exposed vulnerabilities in perimeter security, information sharing and emergency response. The subsequent public inquiries informed Martyn's Law, reinforcing expectations that organisations responsible for public venues take proportionate steps to assess terrorism risk, train staff, plan responses and coordinate with partners.[4]



Manchester Arena - Rob Sinclair, Flickr

CORE THREAT AREAS

4. Cyber crime and information security

The current snapshot

Cyber risk remains operationally front-rank and increasingly identity-led. 2025 closed with record ransomware and data-extortion activity, including a marked shift toward data-only extortion, smaller affiliate crews and compressed timelines from intrusion to demand - shortening the window for detection, decision-making and customer communication.[1]

Attackers are leaning hard on identity weaknesses, social engineering, identifying and paying insiders for access, and third-party paths.Often starting on edge devices - routers, VPNs and gateways - that sit outside typical endpoint and identity controls and provide quiet, durable footholds.[2] Once inside, they pivot quickly to exfiltration, leverage brand-impact tactics to pressure payment, and exploit supply-chain dependencies to magnify disruption.[3]

In this environment, resilience depends less on preventing every intrusion and more on how you grant, monitor and remove access; how quickly you can pause, notify and coordinate with suppliers and customers; and how reliably you can prove fixes by investigating initial access, identity drift and partner routes rather than assuming a patch equals resolution.[4]

Implications for corporates

- Assume access will be abused. Most serious incidents now begin with legitimate credentials, not broken defences.
- Look where visibility is weakest. Edge devices, supplier connections and service accounts often provide quiet footholds.
- Decisions matter as much as alerts. Knowing when to pause systems, notify partners or isolate access shapes outcomes more than detection speed alone.
- Prove the fix before moving on. Investigations should explain how access was gained and closed, not just confirm that systems are back online.

“After an incident, pressure mounts to look busy. Patching is visible; proving is harder. But unless you prove how access was gained and closed, you’re just resetting the stopwatch.”

Matt Horne, Director of Intelligence and Investigations, Clue Software

Case study – Jaguar Land Rover cyber disruption

UK and overseas automotive sector, **2025**

A cyber incident in August 2025 forced Jaguar Land Rover (JLR) to shut down IT and halt production for five weeks, disrupting UK and overseas plants and dealer systems. JLR later disclosed £196m in incident-related costs and a £485m loss for the quarter. Affecting the supply chain and 5,000 businesses, wider estimates put the UK-economy impact near £1.9bn, making it the most financially damaging cyber incident in UK history.

The event showed how identity abuse, supplier dependencies and edge-device footholds can turn a single intrusion into sustained operational and reputational harm, reinforcing the need to prove fixes, not just patch, before resuming full operations.

Jaguar Land Rover at the 2015 Dubai Motor Show - Jaguar MENA, Flickr

[1] Ransomware Attack 2025 Recap – From Critical Data Extortion to Operational Disruption; The State of Ransomware
[2] Ransomware Trends 2025: Tactics, Data, and Key Threat Insights
[3] Ransomware Surges, Extortion Escalates: ThreatLabz 2025 Ransomware Report; Extortion and Ransomware Trends January–March 2025
[4] Ransomware Trends 2025: Tactics, Data, and Key Threat Insights

CORE THREAT AREAS

5. Insider threat

The current snapshot

Insider risk spans malicious, negligent and compromised users - including contractors - operating across home networks and personal devices. Alongside data leakage and IP theft, this includes unauthorised exploitation of internal or competitor information, internal fraud, and employees or contractors stealing from their employer, sometimes incrementally and sometimes at scale. Surveys and incident data indicate most organisations report an insider incident in the past year, with average containment times of 81 days and programme costs estimated at around £13m annually per organisation.[1, 2]

Hybrid work expands token theft and data-egress paths, while financial pressure, role changes and access churn can increase misuse risk. In parallel, state-linked actors increasingly seek to manufacture insiders via fake CVs, contract roles and expert consultations, using HR and recruitment processes as collection channels for sensitive information and IP.[3]

Beyond technical misuse, insider threat also includes abuse of trust or position, where authority, influence and access combine with reduced scrutiny. This can range from conflicts of interest and misuse of authority through to harassment, corruption and criminal conduct, often developing gradually where hierarchy, trust and siloed oversight delay challenge or intervention.

Implications for corporates

- See insider risk as a people-and-context issue first. Use risk assessment to distinguish between lowlevel concerns, emerging patterns and issues requiring formal investigation.
- Mind the edges of your workforce. Contractors, temporary staff and joiners/leavers often sit where oversight, loyalty and controls are weakest.
- Support speaking up with capability. Confidential reporting must be backed by joined-up intelligence handling and credible investigative capacity, so concerns are connected, assessed and acted on before harm escalates.
- Make recruitment part of security. Proportionate hiring and onboarding hygiene reduces fraud, insider misuse and IP risk without turning HR into a policing function.

“**Most insider harm** didn’t start as crime. It started as pressure, confusion or entitlement. You won’t fix that with slogans - only with early reporting routes and credible investigations.”

Matt Horne, Director of Intelligence and Investigations, Clue Software

Case study - Rippling vs Deel

US technology sector, **2025**

HR tech firm Rippling filed a major lawsuit alleging that competitor Deel had cultivated an insider within Rippling. The insider reportedly accessed and exfiltrated sensitive sales intelligence, internal Slack messages and competitive data, and attempted to delete evidence when confronted - showing how contractors and trusted staff can be exploited to steal IP, and how insider threats can be manufactured by external actors.

[1] Fortinet Insider Risk Report 2025.
[2] DeepStrike/Ponemon-based summaries (costs, containment).
[3] DCSA, Targeting U.S. Technologies 2025 (résumés/consultations).

6. Corporate espionage and hostile state activity

The current snapshot

Corporate espionage is typically quiet, patient, and people-focused. State-backed and proxy actors seek long-term access to R&D, intellectual property, deal flow, commercial strategy and executive communications, often by engaging individuals rather than attacking systems. Alongside technical compromise, reporting shows sustained use of legitimate-looking engagement routes - CV submissions, contract roles, advisory work, paid "briefings" and expert consultations - to identify, cultivate, or manufacture access. These approaches blend human relationships with identity and access over time, exploiting trust, professional openness, and fragmented oversight across recruitment, consulting and partnerships.[1]

Related activity may look routine in isolation (e.g., invitations to speak on panels, introductions via industry groups, third-party diligence on deals), but cumulatively expose sensitive information or strategic intent, complicating detection and governance.[2]

Implications for corporates

- Assume interest in what makes you competitive. R&D, deal flow and leadership thinking are attractive targets even outside traditional "national security" sectors.
- Expect quiet tactics before noisy ones. Relationship-building, CVs, contracting routes and expert calls often precede any overt compromise.
- Right-size intelligence and investigation capability. Assess how credible the threat is for your sector and calibrate your intelligence, due diligence and investigative depth to match exposure, sensitive assets and partner footprint.

Case study - Google AI trade secrets

2025

Software engineer Linwei “Leon” Ding was charged with stealing confidential Google AI model artefacts and sharing them with People’s Republic of China (PRC)-linked entities, illustrating the espionage risk to high-value tech R&D and the exploitation of remote-work access pathways.

Google Headquarters - Anthony Quintano, Flickr

[1] CISA/NSA/FBI & partners advisory on PRC router compromises (Sept-2025)
[2] Targeting U.S. Technologies 2025 (DCSA)

CORE THREAT AREAS

7. Sanctions risk and geopolitical exposure

The current snapshot

UK sanctions enforcement has tightened. OFSI (Office of Financial Sanctions Implementation) reports higher case volumes, increased use of monetary penalties, expanded sector threat assessments and closer international coordination, including memorandum of understanding between OFSI and the US Office of Foreign Assets Control (OFAC). OTSI (Office of Trade Sanctions Implementation), now operational for trade-related breaches, adds a second line of UK enforcement focused on customs, trade services, licensing and movement-of-goods offences.[1]

In January 2026, OFSI confirmed a revised enforcement framework to clarify expectations and speed case outcomes. From 28 January 2026, the single UK Sanctions List became the authoritative source for designations, simplifying screening but raising the bar on accuracy, governance and auditability.[2]

Recent actions show that even routine service payments can breach sanctions where a designated person ultimately benefits.[3]

Implications for corporates

- Treat sanctions as dynamic. Ownership, routes and beneficiaries change faster than annual reviews.
- Pause when unsure. Stopping a transaction to check is usually safer than trying to fix it afterwards.
- Evidence the decision. Being able to show what you checked and why you proceeded matters as much as the controls themselves.
- Investigate when value flows are unclear. That's where real exposure hides.

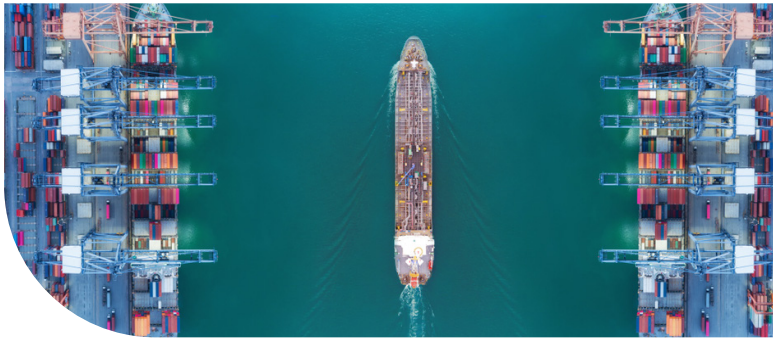
“**Routine service invoices** can carry extraordinary risk when the value flows to a designated person. Sanctions exposure hides in the mundane; evidence your decisions like a regulator will ask tomorrow.”

Matt Horne, Director of Intelligence and Investigations, Clue Software

Case study – £1.1m settlement for export-control breaches

UK exports, **2025**

HMRC concluded a £1.16 million compound settlement with a UK exporter that unlawfully made goods available to Russia in breach of The Russia (Sanctions) (EU Exit) Regulations 2019. The case demonstrates the escalating enforcement posture around sanctions compliance following Russia's invasion of Ukraine, during which UK and international measures have sought to restrict Kremlin access to funding. It highlights how even routine commercial activity can result in significant penalties where firms fail to meet export-control and licensing requirements, reinforcing HMRC's willingness to pursue substantial financial sanctions for breaches.



Sign outside HMRC in Whitehall - Howard Lake, Flickr

[1] Sanctions Enforcement Action (GOV.UK) [gov.uk]
[2] New and Updated Enforcement Framework – a message from Giles Thomson (OFSI Blog, 29 Jan 2026)
[3] OFSI Enforcement Actions: Decisions and Monetary Penalties (GOV.UK Collection)

CORE THREAT AREAS

8. Protest, activism and physical security

The current snapshot

Protest and activism affecting corporates in 2025-26 are increasingly shaped by a fast-moving, fragmented information environment. Campaigns mobilise quickly online, often driven by emotive narratives, misinformation and wider geopolitical events, before translating into on-site activity with limited warning. Issues can escalate rapidly from digital discourse to physical disruption, targeting offices, retail premises, infrastructure, AGMs, executives and associated partners.

Campaigns are fluid, decentralised and multi-issue. Pro-Palestine mobilisation remained prominent through much of 2025, frequently extending beyond direct protest to pressure on corporates, landlords, clients and suppliers perceived to have indirect links or associations. Climate groups adapted tactics following Just Stop Oil's public pause, shifting towards commercial disruption, reputational pressure and shareholder activism. Right-wing and anti-migration activity persisted into 2026, often characterised by flash mobilisation and heightened risk of confrontation.

For corporates, the risk lies in persistence, proximity and amplification. Activity may recur, spread across locations, or migrate between physical sites, online spaces and governance forums, creating operational disruption, reputational harm and duty-of-care challenges for organisations and their affiliates.

More broadly, physical security risk is increasingly shaped by how quickly organisations see and connect early signals across their estate. Initial indicators of emerging threats are often subtle and distributed: unusual loitering, repeated filming, suspicious vehicles, changes in access patterns, or low level staff concerns. These signals are typically observed first by frontline staff, facilities teams, guarding, control rooms or suppliers, rather than central security functions. Where reporting is fragmented, informal or slow, organisations lose the opportunity to intervene early and proportionately before risks escalate, converge or spread.

Implications for corporates

- Expect activity to move. Issues rarely stay online or on-site; they often move between platforms, locations and people.
- Listen to the front line. Early signs are usually spotted by staff, facilities, guarding or suppliers, not central teams.
- Focus on proximity and persistence. Repeated presence, reconnaissance or amplification matter more than protest size.
- Join the dots afterwards. Bringing together reports, CCTV and site observations helps reduce future exposure

“**Protest rarely arrives** as a surprise; it arrives as a pattern. The organisations that cope best keep people safe in the first five minutes and reputations safe in the first five hours.”

Matt Horne, Director of Intelligence and Investigations, Clue Software

Case study - Palestine Action campaigns

UK protests, **2021-25**

UK-based activist group Palestine Action conducted sustained on-site protests, occupations and direct action against companies linked to Israel-related defence and security activity. Campaigns combined online mobilisation with repeated physical disruption of offices, factories and supplier sites, alongside reputational pressure on clients, landlords and financial partners. Activity escalated to property damage and site shutdowns, creating operational, legal and duty-of-care risks and prompting heightened policing and legislative response.

Palestine Action Protest, London, September 6 - Indigo Nolan

CORE THREAT AREAS

9. Safeguarding and exploitation

The current snapshot

Modern slavery and exploitation remain material risks for corporates, particularly deep within global supply chains. Global estimates suggest around 27.6 million people remain in forced labour [1], concentrated in sectors such as agriculture, mining, manufacturing and seafood, with persistent risk signals linked to regions and commodities including Xinjiang cotton and parts of Southeast Asian fisheries.

Corporate transparency continues to lag underlying exposure. Only a small proportion of companies disclosed forced-labour incidents under UK and Australian reporting frameworks between 2016 and 2024, pointing to gaps in due diligence, detection or disclosure rather than low prevalence. UK guidance tightened in 2025, with updated expectations around content, action, and implementation in modern slavery statements.[2] EU due-diligence reforms likewise raise expectations around risk-based checks, including upstream suppliers, and remediation, supported by the EU's new Forced Labour Regulation (EU 2024/3015).[3]

Beyond supply chains, exploitation risk can also sit closer to home within operations or contractor networks, creating safeguarding risks for employees, agency staff and customers. Sexual harassment, and predatory behavior including through abuse of positions of trust are also a significant threat within the workforce. Having appropriate policies, structures, confidential reporting channels and effective investigative functions are vital to protect staff and instill confidence in corporate integrity.

Implications for corporates

- Assume risk sits below the surface. Harm is more likely in deeper tiers, labour brokers and contractor networks than in policy documents.
- Act on indicators, not certainty. Waiting for definitive proof often means acting too late.
- Investigate to protect people. The purpose of investigation is to remove harm and prevent recurrence, and may require producing a package of information for law enforcement to progress.
- Check outcomes, not paperwork. Improvement should be visible in real conditions for workers and customers.

Case study - Forced-labour and exploitation risks

UK consumer goods sector, **2024**

Unilever acknowledged heightened forced-labour and exploitation risks across parts of its manufacturing, services and agricultural supply chains, strengthening supplier oversight, worker-voice mechanisms and remediation - illustrating the expectation that large corporates move beyond compliance statements toward active identification, safeguarding and remedy.

Unilever building in Hong Kong - Wikimedia Commons

[1] Data and Research on Forced Labour (International Labour Organization)
[2] UK Government Publishes Updated Guidance on Modern Slavery Reporting: What This Means for Businesses (Linklaters Sustainable Futures)
[3] EU: New Law Requires Companies to Tackle Forced Labour (Human Rights Watch)

Taking an intelligence-led approach to readiness

An intelligence-led approach is less about frameworks and more about habits. The principles below reflect what consistently works in practice: bringing information together early, making proportionate decisions under uncertainty, and investigating properly when patterns or harm emerge.

Build one shared picture. Bring threat and risk intelligence from people, identity, suppliers, sites and systems into a single place where patterns can be seen.

Make reporting easy. Encourage staff, facilities teams, guarding and suppliers to share early concerns, even when information is incomplete.

Decide proportionately. Use intelligence-led triage and risk assessment to choose when to monitor, when to intervene, and when to investigate.

Investigate when it matters. Escalate to structured investigation for repeated patterns, threats to sensitive assets, indicators of criminality, or safety and legal risk.

Keep evidence as you go. Record why decisions were taken, what was checked and how issues were resolved. Collate threat and risk reporting centrally to enable evidential integrity within follow on action by investigations teams, HR, security, regulators or law enforcement.

Learn deliberately. Track how quickly issues were spotted and acted on, and feed lessons back into detection and controls.

Over time, organisations that consistently collect intelligence, assess risk in context and investigate properly develop a much clearer understanding of their real exposure - and respond with greater confidence and less disruption.

Final thoughts

Resilience is the capacity to recognise what matters, make sense of it quickly and act with purpose. Organisations that do this well see risk in context, connect signals early, and coordinate decisions across people, identity, suppliers and public narrative. The threats in this assessment will continue to change. What does not change is the need to notice weak signals sooner, respond proportionately, and sustain trust with employees, customers and partners.

Underpinning this approach is a secure, evidentially sound capability for accumulating intelligence, assessing risk and managing investigations over time. Consistent reporting, linked data and case history build an organisational memory that allows risks to be assessed more accurately and responses to become more confident and proportionate.

"Becoming intelligence-led and developing robust investigative rigour to respond to corporate security threats does not mean doing more. It means seeing more, sooner - and ensuring insight moves to the right people at the right time," comments Matt Horne, Director of Intelligence and Investigations at Clue Software. "It means delivering investigations and due diligence with the necessary depth and rigour to match the risk. When teams share the same picture, rehearsed choices become confident action."

Ultimately, resilience is measured not only by what an organisation prevents, but by how it anticipates, communicates, responds and recovers. By applying the principles in this report, corporates can navigate a converged threat landscape with clarity, agility and confidence.

If you would like to discuss any of the threats and implications featured in our Corporate Security and Integrity Threat Assessment or discuss how our intelligence and investigation management software can support intelligence-led resilience, contact our **Director of Intelligence and Investigations, Matt Horne. Matt.horne@cluesoftware.com**

CLUE

© 2026 Clue Computing Co. Ltd
Clue House, Petherton Road, Hengrove, Bristol, BS14 9BZ, UK.
Company Number 01715616
Company registered in England & Wales.