Enhanced Good Practice

Issue	**Civil Unrest**
Practice	**Crisis Preparedness**
Enhancement	**Improving Organizational Resilience with Security Intelligence**

International SecurityLigue

SUMMARY

Social unrest now spreads faster and farther than before, enabled by social media and democratized communications. Businesses face a systemic threat: protests and disorder that can cross borders and rapidly escalate. Advanced security intelligence — upstream monitoring, real-time alerts, contextual analysis, and integrated operational response — materially reduces the risk of property damage, loss, and business disruption.

ISSUE

Episodes of civil disorder are increasingly systemic: movements can ignite in one city and quickly appear in many others. Social media accelerates transmission of information and coordination, compressing the timeline from initial incident to mass mobilization. Companies often lack the internal capacity to detect, contextualize, and act on early signals. Without timely, actionable intelligence, firms are forced into reactive decisions—sometimes hourly—that increase exposure to property damage, supply-chain disruption, reputational harm, and legal liability.

BENEFITS

Security intelligence delivers timely, contextualized warnings and actionable analysis that enable businesses to protect people and assets, make informed operational decisions, and reduce physical, financial, and reputational harm.

PROCESS OR APPROACH

- Establish upstream monitoring — Deploy continuous, 24/7 monitoring of social media, local news, community channels, and open-source indicators to detect early signals of unrest and trending narratives that could mobilize crowds.
- Contextualize and triage — Use analysts and automated tools to assess credibility, geographic relevance, likely escalation pathways, and potential impact on company assets and personnel; assign risk levels and confidence scores.
- Map assets to threats — Maintain an up-to-date inventory of critical sites, supply routes, and personnel locations; overlay intelligence to identify which assets are at immediate risk and prioritize protective actions.
- Integrate real-time alerting — Ensure intelligence platforms can push concise, actionable alerts to decision-makers and field teams (mobile devices, dashboards, and command centers) with recommended mitigations and escalation steps.
- Activate contingency playbooks — Pre-defined, scenario-based playbooks (curfews, temporary closures, asset hardening, evacuation, liaison with authorities) must be ready and rehearsed; intelligence triggers specific actions.
- Coordinate with local authorities and partners — Share verified intelligence with law enforcement and local stakeholders where appropriate; establish liaison protocols to avoid duplication and ensure timely support.
- Leverage capacity-rich providers — Engage professional security firms that offer threat monitoring, analyst support, and operational integration; prefer providers with proven platforms and 24/7 operations.
- Monitor misinformation and reputational threats — Extend monitoring to disinformation, rumor, and negative sentiment that can amplify unrest or target the company; prepare rapid communications and mitigation strategies.
- Continuous learning and scenario testing — Run stress-test scenarios (including cross-border contagion cases) and after-action reviews to refine indicators, thresholds, and response playbooks.

IMPERATIVE

Social unrest is now a systemic, transnational risk that can rapidly threaten operations, people, and reputation. Companies must move from ad-hoc reaction to intelligence-led prevention: invest in upstream monitoring, integrate real-time alerts with operational teams, and adopt scenario-tested contingency plans. Where internal resources are insufficient, partner with professional security firms that provide continuous threat platforms, analyst expertise, and mobile operational support. Early, contextual intelligence is not optional — it is a business-critical lifeline that preserves safety, continuity, and corporate resilience.