

Security Program Strategy & Operations > Emerging Issues >

One Operating Picture: How Geopolitics, AI, and Insider Risk Are Converging

For decades, corporate security managed risk in relatively discrete lanes. Geopolitical risk was assessed externally, insider risk was treated as a human or HR issue, and technology risk was delegated to cyber teams. That model is breaking down.

Today, geopolitics, artificial intelligence, and insider risk are converging into a single operating picture, forcing security leaders to reassess how threats emerge, scale, and manifest inside their organizations. When these risks are combined and accelerated by intelligent, machine-driven means, the ability to mitigate them quickly enough to make a difference is growing.

Geopolitical Risk Is No Longer “External” to the Enterprise

Geopolitical competition increasingly targets private organizations directly, not just governments. Global companies are now treated as strategic assets, leverage points, and enforcement mechanisms in national competition. The World Economic Forum notes that geopolitical fragmentation has made companies both *subjects* and *participants* in geopolitical outcomes, requiring firms to develop internal geopolitical intelligence rather than treating it as an external condition. [[World Economic Forum](#)]

This shift is visible at the governance level. Board-level guidance increasingly frames national security, sanctions, export controls, and regulatory compliance as central business risks rather than edge cases. The Harvard Law School Forum on Corporate Governance documents how boards are now expected to govern decisions through a national-interest lens, reflecting the

collapse of the separation between geopolitical and commercial risk. [[Harvard Law School Forum on Corporate Governance](#)]

For security leaders, this means geopolitical pressure increasingly manifests inside the enterprise through workforce exposure, regulatory asymmetry, and localized coercion, rather than only at the perimeter.

AI Has Collapsed the Cost and Skill Barrier for Abuse

Artificial intelligence has fundamentally altered the threat economy. Advanced capabilities that once required skilled teams are now widely accessible, dramatically lowering the barrier to high-impact abuse.

Microsoft Threat Intelligence details how threat actors are operationalizing AI across the full lifecycle of cyber and influence operations—using generative models to accelerate reconnaissance, impersonation, and identity abuse rather than inventing entirely new attack types. [[Microsoft Threat Intelligence blog](#)]. This supports the growing observation that attacks are shifting from “breaking in” to “logging in,” leveraging legitimate access and trusted identities. [[Cloudflare 2026 Threat Intelligence Report](#)]

According to Cloudflare’s 2026 threat analysis report, “An actor who previously lacked the skills to craft a convincing phishing email or write custom malware can now leverage an LLM to generate them rapidly and at scale, significantly lowering the barrier to entry for highly effective operations.” [[2026 Cloudflare Threat Report](#)]

Crucially, these capabilities do not require malicious insiders. They exploit routine access, normal workflows, and human trust—turning ordinary mistakes into strategic exposure.

Insider Risk Has Shifted From “Bad Actors” to “Risky Conditions”

The insider threat model centered on identifying malicious individuals is increasingly outdated. Modern insider risk is driven by conditions, not intent.

A 2025 report produced by Cyber Insiders shows most insider incidents are unintentional rather than deliberate sabotage. Security practitioners report low confidence in detecting insider risk early, despite high awareness of its impact. [[2025 Insider Risk Report](#)].

The problem is compounded by geopolitics. The U.S. National Counterintelligence and Security Center explicitly warns that foreign adversaries now target critical infrastructure, private sector companies and academic institutions to exploit individuals with access to sensitive systems. [[Insider Threat Mitigation for U.S. Critical Infrastructure Entities](#)].

In this environment, outcomes matter more than intent. A well-meaning employee operating under geopolitical pressure, enabled by AI tools, can unintentionally create national-level consequences.

Why These Risks Are Converging Now

This convergence is structural, not cyclical.

The 2025 Aon Global Risk Management Survey documents how geopolitical volatility, cyber risk, workforce disruption, and AI adoption have moved from isolated categories into a set of interdependent, systemic risks. They state, “What stands out in the survey results is how these rapidly rising risks interact, as well as their potential impact on multiple areas of a business. Technology risks intersect with workforce dynamics and challenges in adopting artificial intelligence (AI). Geopolitical instability affects supply chains, influences the regulatory landscape and has an impact on balance sheets.” [[A New Era of Converging Risks and Accelerating Disruption](#)]. Organizations increasingly experience cascading effects across these domains rather than discrete incidents.

The International Telecommunication Union states that 74% of the world’s population are online. [[ITU](#)] It’s been an upward trend and does not seem to show signs of slowing down. This massive expansion of the digital landscape has unfortunately made internet crime a global issue.

At the same time, digital work has embedded trust into platforms and identities that were never designed to withstand synthetic impersonation or large-scale manipulation. This collapse of implicit trust is the accelerant binding these risks together.

Security Ramifications for Corporate Leaders

Contemporary intelligence collection routinely draws on organizational and employment records, travel and movement data, communication and access logs, and other digital traces to build detailed “human maps” of organizational structures, professional networks, and individual behavior. [[newstrail.com](#)]

Government guidance emphasizes that effective insider threat mitigation requires contextual and behavioral indicators, not just transactional monitoring. [[dni.gov](#)]

Across multiple 2026 threat outlooks, a consistent picture emerges: cybercrime is no longer driven by novel exploits or isolated actors, but by the large-scale industrialization of techniques that already work. Fortinet’s 2026 Cyberthreat Predictions emphasize a decisive shift away from innovation toward throughput, where success is measured by how quickly attackers can move from reconnaissance to monetization rather than by technical creativity. [[Fortinet](#)] This

same acceleration is echoed in Mandiant’s M-Trends 2026 findings, which show threat actors operating as coordinated, professionalized ecosystems. Initial access is increasingly brokered and handed off between specialized groups, sometimes in under 30 seconds, allowing attacks to escalate rapidly from minor footholds into ransomware deployment or mass data exfiltration. As a result, defender response windows are shrinking dramatically, forcing organizations to rethink security models that assume linear, human-paced attack timelines. This blurs the line between cyber, physical, and human risk in ways most organizational structures are not designed to manage. [[Mandiant M-Trends 2026 Report](#)]

At the same time, the economic engine behind this industrialization is becoming more precise and automated. Ransomware-as-a-Service has evolved from indiscriminate volume attacks into targeted, intelligence-driven campaigns focused on high-value organizations, supported by tailored reconnaissance and rapid execution. Google’s Cybersecurity Forecast 2026 further highlights how artificial intelligence is accelerating this shift, with threat actors moving from experimental AI to embedding it across the entire attack lifecycle. AI is now used to streamline reconnaissance, enhance social engineering, automate decision-making, and scale operations with minimal human involvement. [[Preparing for Threats to Come: Cybersecurity Forecast 2026](#)]

Together, these trends point to a future where cyber risk is defined less by the sophistication of individual tools and more by speed, coordination, and automation—placing pressure on defenders to adopt equally integrated, machine-speed detection and response capabilities.

This blurs the line between cyber, physical, and human risk in ways most organizational structures are not designed to manage.

Operating in a Converged Risk Environment

Gaining Traction Identifying risks as connected is gaining traction but there is a long way to go. It’s a complicated process given all the interdependences. Statistics generated from polls during a KPMG 2025 webcast revealed: Only 27% of professionals believe that interconnected risks management in their organization is mature and effective. And nearly 40% believe that the biggest challenge in managing interconnected risks within the organization is the lack of integrated systems and risk data sharing. Success factors included a shared purpose and strategic alignment; clear guardrails and role clarity; and building equity and trust. [[KPMG](#)]

The Dual Nature of AI in Security It is becoming increasingly clear, AI doesn’t care who uses it. The same capabilities that make it powerful and transformative also introduce new forms of risk. For example, attackers can use AI to scale and automate malicious operations while defenders can use AI to detect, prioritize, and respond faster than human teams alone. The tension between these two forces is shaping modern security strategy.

The Leadership Imperative

The convergence of geopolitics, AI, and insider risk is not a future scenario. It is the current operating environment.

Security leaders who continue to manage these domains independently will remain reactive. Those who succeed will be the ones who integrate intelligence across human, technical, and geopolitical dimensions, and who can articulate that picture clearly to executive leadership. However, part of the problem also lies in Boards of Directors not recognizing the connected picture. The notion of a reliable holistic enterprise security assessment for business remains largely unshared.

The question is no longer whether these risks intersect, but whether your organization is structured to see them as one.

Visit the **Security Executive Council** web site to view more resources in the [Security Program Strategy & Operations : Emerging Issues](#) series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our [3-minute video](#) to learn more.

Contact us at: contact@secleader.com

Website: <https://www.securityexecutivecouncil.com/>