Hilco Global
Asset Smarter

SMARTER PERSPECTIVE: SUPPLY CHAIN

Caught in the Crossfire: How Nation-State Cyber Threats Endanger America's Middle Market

By Alexander Niejelow and Hon. Patrick J. Murphy

September 2025 Middle market companies[1] represent a critical but vulnerable segment of the U.S. economy. With over 200,000 such companies collectively generating over $10 trillion in revenue and employing 48 million Americans, they account for one-third of private sector GDP and are continuing to grow in revenue by double digit percentages. This growth trajectory comes with expanded attack surfaces and increased exposure to cyber threats, especially for those reliant on cybersecurity supply chains and operative within critical infrastructure industries. Middle market companies that support critical infrastructure may not realize that by serving as important links in supply chains for larger enterprises they are attractive targets for nation-state actors seeking broader network access. Increased geopolitical tensions have exposed these organizations to a new type of threat actor, as adversarial nation-state actors increasingly target U.S. critical infrastructure using sophisticated methodology that middle market businesses do not have the resources of large enterprises to adequately defend against.

According to the Department of Homeland Security, a compromise in the 16 critical infrastructure sectors could have debilitating effects on national security, economic security, or public health and safety. Within the broader sectors included under "critical infrastructure", recent behavior from cyber attackers associated with foreign nations shows a particular focus on businesses involved in industrial supply and physical infrastructure, such as transportation, utilities, energy, and manufacturing. The interconnectedness of both cyber and physical supply chains, along with third-party vendors, increasingly exposes middle-market businesses in key sectors.

At $9.5 trillion the global cyber crime economy represents the world's third-largest economy by GDP, according to Cybersecurity Ventures, trailing only the US and China.

While all industries are susceptible to these threats, the aforementioned sectors have drawn increased interest in recent years from cybercriminals associated with China, Iran, North Korea and Russia, who focus on collecting information and gaining access to industrial control systems, per DHS. What makes this recent activity even more difficult to understand is that these threat actors prioritize espionage over a one-time attack, often going months or years undetected by the entities they've unauthorizedly accessed. This differs from traditional tactics in which hackers deploy a ransomware attack and demand payment to avoid the release of sensitive information. In May, The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) published a report acknowledged that "Chinese state-sponsored actors have already gained footholds in key sectors of US infrastructure, as public officials and private-sector leadership have raised concerns regarding this activity for several years", explicitly calling out transportation, communications, energy, water and wastewater. Meanwhile, CISA has issued multiple advisories in the last year regarding foreign threats to transportation, manufacturing, and energy systems through VPN exploitation, third-party logistics platforms, industrial control, and fleet management systems.

Sophisticated groups from each of these adversarial countries have unique ways of attacking American businesses. Volt Typhoon, a Chinese Advanced Persistent Threat (APT) group, utilizes various attack vectors such as customer portals, VPN exploitation, and third-party vendors like logistics software to gain persistent access for continued reconnaissance. Volt Typhoon is known to target operational systems in ports, rail control environments, and fleet management infrastructure. Similarly, Check Point, a leading cybersecurity threat intelligence business, said in May that it has observed Chinese threat groups "actively infiltrating the networks of firms that supply components for the manufacturing industry". Iran-linked threat groups such as MuddyWater and APT33 have used vulnerabilities in Microsoft Defender and Fortinet to attempt breaches on at least 10 U.S. companies in recent months, also

[1]*Per The National Center for the Middle Market, businesses generating between $10 million and $1 billion in annual revenue are considered in this segment.*

predominantly in the transportation and manufacturing sectors. According to researchers at Nozomi Networks, there were 28 attempted attacks in May and June alone. These breaches come on the back of multiple attacks in recent years from Iranian-associated groups on small municipal water authorities and industrial equipment controlling water treatment, further demonstrating how smaller entities are caught in the crossfire of geopolitical tensions. Russia's GRU military intelligence group has been seen accessing Western logistics companies, airlines, manufacturers and ports via credential guessing, spear phishing, and CVE usage since May 2022 according to CISA. Unlike Volt Typhoon's focus on undetected surveillance, the purpose here is to cause immediate disruption to supply chains involved in the delivery of military aid to Ukraine.

Average breach costs were $4.88 million in 2024, a 10% increase.

Adversarial cyber actors are keenly aware that middle-market businesses have fewer resources to respond to attacks, particularly as they become more sophisticated with the proliferation of AI and have thus shifted from fortifying defenses in large enterprises and governments to easier targets like mid market firms. This is why it is crucial that leaders from businesses of all sizes recognize that they too are exposed to foreign threats and therefore proactively prepare. Middle market companies cannot operate under the false premise that they are safe from the impacts of foreign cyber groups motivated by geopolitical goals. The unified nature of software supply chains and critical dependence on a handful of providers greatly expand the attack surface for all entities. As seen in last year's CrowdStrike outage, if a key third-party cyber supplier is impacted, thousands of companies can see disruptions in business operations – this is particularly relevant with vulnerabilities in cloud providers. The World Economic Forum highlighted supply chain interdependencies and subsequent "systemic cyber security events" as a leading factor in the

increased complexity of cyberspace in 2025. This accentuates the need for middle market organizations to take a proactive approach to defense, as they have less resources to focus on incident response and the impact of an attack on the business is higher.

Supply chain attacks have surged 431% since 2021, indicating growing vulnerability in interconnected business ecosystems.

For middle market companies - protecting against emerging threats requires a strategic and proactive approach utilizing both traditional and evolving security measures. While there are many areas players in the middle market must focus, trends from this year's geopolitical climate suggest four areas are essential:

- Identify evaluate and safeguard valuable assets
- Strengthen defense in depth
- Build resilient supply chains
- Foster executive-level understanding and preparedness and prepare for the attack.

Implement Comprehensive Risk Assessments

According to a 2025 Report, less than half of middle market companies conduct annual cybersecurity risk assessments. This can lead to the presence of less robust or regularized risk management procedures, especially as it relates to simulated incident response or total network visibility. Conducting a risk assessment, and defining an organizational cadence that works for you, is imperative for companies of all sizes, especially companies in the middle market, to proactively manage risk, enable better decision making, beat market trends, and allow companies to adapt faster than competitors.

Establish a Supply Chain Resilience Program

Middle market companies often serve as critical links between small suppliers and large enterprises, making them attractive targets for supply chain attacks. The interconnected nature of modern business ecosystems means that compromising a middle market supplier can provide access to larger, more valuable targets. Fourth party outages are also causes for major business disruptions as well – with major vulnerabilities found in providers such as Microsoft and outages from CrowdStrike. Disruptions to business continuity is now top of mind for executives, with 88% believing that another major incident as large as last year's July global IT outage caused by CrowdStrike will occur in the next 12 months. With these challenges in mind, middle market players must establish a comprehensive program addressing third-party risk that goes beyond just traditional vendor assessments – but wholistically looks at the entire company's supply chain resilience program.

1. *Establish a Governance & Policy Framework:* Define clear ownership for third-party risk management, including roles and responsibilities. Build cross-functional processes involving compliance, procurement, legal, and IT teams – with proper reporting, roles and responsibilities to action quickly.
2. *Inventory & Tier Your Third Parties:* Inventory all vendors and third parties that interact with your organization, documenting the data they access and their business impact. Segment vendors by risk (e.g., critical, high, moderate, low) using criteria like data access, service criticality, past security performance, and compliance posture.
3. *Implement continuous third-party risk monitoring:* Vendor monitoring should be automated as much as possible - using platforms that provide real-time dashboards and alerting. Business specific metrics should determined by key stakeholders and tracked for service performance, regulatory changes, compliance status, and cybersecurity maturity. The level of detail in third party review should be determined by the vendor risk, with high risk vendors requiring more stringent review.

Assess Your Defense Architecture

The global cost of cybercrime is projected to reach $10.5 trillion in 2025, with an annual growth rate of 15%. With the cost of a data breach increasing each year, and new geopolitical factors contributing to annual growth, now is the time for middle market companies to truly assess critical defenses.

1. *Enforce Zero Trust:* Ensure that all users and devices are subject to continual verification before granting access to resources across all platforms and services. Users and systems should only get the minimum access needed for their role and responsibilities; with periodic reviews and automation in place to update permissions reflecting business changes
2. *Assess your Multi-Factor Authentication (MFA) Coverage:* MFA is now a baseline requirement for cyber insurance policies across nearly all carriers as of 2025 – making it non-negotiable. To be eligible for coverage, or even retain renewal, businesses must demonstrate not just the implementation but often prove operation for robust MFA controls protecting key systems. To ensure proper coverage, assess for MFA across all privileged accounts, identities, and applicable services. Importantly, ensure it is documented and attested to by each group of key stakeholders.
3. *Ongoing Risk Assessment, Modernization and Incident Preparedness:* Your defenses are only as good as your people and enforced by your processes. Cybersecurity should not just be a roadmap item, but a stated business goal woven into the fabric of the enterprise. To meet these goals, it is imperative for middle market organizations to ensure the basics. Conduct audits of key architecture such as network, identity, endpoints and access control mechanisms. Test your defenses with annual penetration tests, vulnerability scans, and simulated phishing attacks. Use lessons learned to patch gaps, modernize legacy systems, eliminate single points of failure and ensure your defenses are layered.

Enhance Playbooks with Critical Infrastructure-Specific Recommendations

Middle Market companies in critical infrastructure sectors face unique resource constraints compared to large enterprises but are increasingly targeted by the same sophisticated threats. These trends can no longer be ignored, requiring middle market companies to consider nation-state level and geopolitical risk factors when creating their incident response playbooks.

1. *Prioritize Essential Controls for Resilience:* Focus on high-impact, feasible actions: Adopt a risk-based approach concentrating on the most critical systems—business operations, safety, and compliance assets. Leverage CISA's Cross-Sector Cybersecurity Performance Goals - These are specifically designed as a practical, prioritized set of practices for small-to-midsize entities.
2. *Build "Operate Through Attack" Capabilities:* Assume system outages - Ensure your playbooks include instructions for continuing operations manually if digital controls fail (e.g., manual override of OT systems, fallback communications). Design playbooks for business continuity, integrate contingency protocols, maintain up-to-date contact rosters, offline process documents, and backup mechanisms.

3. *Update playbooks for Emerging Threats and Sector-Specific Standards:* Review federal guidance (CISA, NSM-22, DHS): Align your policies and contracts with minimum cybersecurity standards, especially regarding IT/OT segregation and incident reporting. Document periodic audits and gap analyses. Use frameworks like NIST Cybersecurity Framework to identify and prioritize remediation actions.

Develop Sophisticated Board-Level Cyber Risk Communication Strategy

A sophisticated board-level cyber risk communication strategy connects cybersecurity metrics and initiatives directly to business and strategic priorities, uses visual and quantifiable reporting, and ensures consistent, transparent engagement. This enables boards to provide informed oversight, allocate resources wisely, and support a resilient, risk-aware organization.

1. *Establish Governance and Clear Oversight Structures:* Assign cybersecurity oversight to a specific committee (risk, audit, or a dedicated cyber subcommittee) to define board roles for cybersecurity. Make sure board-level responsibilities and accountability are explicit. Schedule quarterly cybersecurity briefings to ensure regular engagement with the board and more frequent updates at the committee level. Ad hoc sessions should happen in the aftermath of major incidents.
2. *Align Cybersecurity with Business Objectives and Strategic Risk:* Integrate with Enterprise Risk Management. Cyber risk should be embedded in strategic decision-making - especially mergers, acquisitions, supply chain management, and digital transformation. Frame Cybersecurity as a Business Enabler - Use business outcome driven metrics to illustrate how cyber investments protect operations, reputation, and regulatory standing and drive growth.
3. *Continuous Improvement and Benchmarking:* Use sector-specific frameworks (SEC rules, NIST CSF, FAIR, and CISA's guidelines), not internal frameworks, to demonstrate compliance and improvement relative to peers. Update communication strategies using a stakeholder defined cadence to reflect new threats, regulations, and lessons learned from incidents and exercises.

Provide Geopolitical Intelligence to Anticipate and Act on Risks and Opportunities

In a changing world order and increasingly volatile geopolitical fronts, global policy developments and regional factors directly impact business priorities, supply chain resilience, and growth objectives. Robust geopolitical intelligence enables executive teams to anticipate disruptions, align operations with evolving regulations, and position the organization to seize opportunities during periods of volatility. Hilco Global's Geopolitical Unit (HGU) delivers the intelligence, analysis, and playbooks that middle market companies need to operate with confidence in complex global environments.

1. *Policy Alignment and Geopolitical Foresight:* Integrate geopolitical analysis into your corporate strategy. Utilize HGU's annual and quarterly publications to stay informed on high-level policy and market dynamics. Deepen decision-maker insight with tailored engagements providing a mix of monthly updates, commissioned research, and market-specific briefings to understand developments that directly affect your company. Apply Senior Advisor expertise to translate complex policy, trade, and military shifts into actionable strategies for market entry, compliance alignment, and risk avoidance, ensuring your business is positioned ahead of regulatory and geopolitical inflection points.
2. *Supply Chain Security:* Map and assess supplier risk exposure: conduct supply chain vulnerability assessments that integrate political, economic, and operations factors. Use HGU's market research, competitive benchmarking, and scenario modeling to understand how sanctions, trade restrictions, or regional instability may impact procurement and distribution. Implement resilience strategies. Develop mitigation plans that address supplier diversification, alternative sourcing, contingency logistics, ensuring continuity during global or regional disruptions.
3. *Geopolitical Playbooks:* Develop action plans for scenarios by creating targeted playbooks covering

everything from regulatory changes, military conflict, to macroeconomic shifts. Define clear escalation plans: establish decision trees and procedures for swift action during identified geopolitical events. Enable cross-functional readiness by embedding these playbooks into core business processes, ensuring leadership, risk, and operation teams are prepared to act decisively to protect continuity and capture market opportunities when geopolitical events manifest.

33% of middle-market companies have five or fewer data security and privacy employees.

The Bottom Line

Middle market companies, especially those integrated with critical infrastructure sectors, stand at the intersection of economic importance and cybersecurity vulnerability. The key to success lies not in matching the resources of large enterprises, but in implementing innovative, scalable security strategies that leverage automation, deception, and strategic partnerships to create asymmetric advantages against adversaries.

Companies that embrace these forward-thinking approaches will not only protect their own assets but contribute to the overall resilience of America's critical infrastructure ecosystem.

The Hilco Global Cyber and Geopolitical teams help organizations strengthen their defenses, safeguard continuity, and turn risk into resilience. Whether you're navigating sophisticated cyberattacks, supply chain disruption, or volatile geopolitical dynamics, our experts provide the intelligence, strategy, and execution support you need to operate with confidence in today's high-stakes environment.

Sources:

Middle Market Center
Cybersecurity & Infrastructure Security Agency
US Department of Homeland Security
NJCCIC
Cybersecurity & Infrastructure Security Agency
Infosecurity Magazine
Nozomi Networks
Cybersecurity & Infrastructure Security Agency
World Economic Forum
PYMNTS
Microsoft
CrowdStrike
SecureFrame
Bloomberg
IBM
Cowbell
RSMiddM

ALEXANDER NIEJELOW
EXECUTIVE DIRECTOR
CYBERSECURITY ADVISORS
PROFESSIONAL SERVICES

Alexander can be reached directly at aniejelow@hilcoglobal.com or 917.952.8315.

HON. PATRICK J. MURPHY
EXECUTIVE DIRECTOR
GEOPOLITICAL ADVISORS
PROFESSIONAL SERVICES

Patrick can be reached directly at pmurphy@hilcoglobal.com or 646.535.8918.