Kilpatrick

Insights: Alerts

Beyond the Battlefield: What the Iran Conflict Means for Critical Infrastructure Operators' Cyber and Legal Risk

May 27, 2026

Written by **Anthony D. Glosson** and **Gregory P. Silberman**

On February 28, 2026, the United States and Israel launched coordinated airstrikes on Iran under Operation Epic Fury, triggering the most significant regional military conflict in a generation. The headlines have focused on missile exchanges, the effective closure of the Strait of Hormuz, and surging energy prices. For most U.S. companies, the Gulf feels geographically remote. But the cyber and legal risk implications of this conflict are not confined to the battlefield. They are arriving, with increasing velocity, across the full spectrum of domestic critical infrastructure: energy and utilities, financial services, telecommunications, transportation, healthcare, and defense-adjacent industries. A Pakistan-brokered ceasefire took effect on April 8, but as of the date of this update the Strait of Hormuz remains effectively closed, ceasefire negotiations have stalled, and Iranian state cyber operators and aligned hacktivist groups have stated explicitly that cyber operations will continue.

Iran has a well-documented, decade-long history of targeting U.S. critical infrastructure in cyberspace. Since hostilities began, threat intelligence firms including CrowdStrike, Google's Threat Intelligence Group, Recorded Future, and SentinelOne have observed a surge in reconnaissance and early-stage intrusion activity across critical infrastructure targets consistent with patterns that have historically preceded more significant disruptive operations.

At the same time, the federal cyber defense infrastructure that companies have relied upon to calibrate their security postures is itself under strain. The Cybersecurity and Infrastructure Security Agency ("CISA"), the primary federal body responsible for threat advisories, sector-specific guidance, and incident coordination, is operating with sharply reduced staffing. The agency has lost approximately one-third of its workforce since January 2025 and, even in issuing a joint advisory on April 7, operated as one voice among six co-authoring agencies rather than as the functional lead it was designed to be.

This alert explains the threat landscape, identifies the sector-specific legal and contractual risk implications that warrant attention now, and outlines considerations for organizations across the critical infrastructure ecosystem.

Iran's Cyber Program and Sectoral Targeting

Iran's offensive cyber program, operated through units linked to the Islamic Revolutionary Guard Corps ("IRGC") and the Ministry of Intelligence and Security ("MOIS"), blends state-sponsored espionage, destructive attacks, and criminal activity in ways that deliberately obscure attribution and preserve plausible deniability. Tehran has

historically activated this ecosystem during periods of military conflict, using cyber operations as an asymmetric force multiplier when conventional military options are constrained.

The sectors most consistently identified by threat intelligence firms as primary targets in the current environment are energy and utilities, financial services, telecommunications, transportation and logistics, healthcare, and defense contractors and military suppliers. A June 2025 joint advisory by CISA, the Federal Bureau of Investigation ("FBI"), the National Security Agency ("NSA"), and the Department of Defense Cyber Crime Center ("DC3") warned critical infrastructure organizations across these sectors to remain vigilant against Iranian state-sponsored cyber threats.

The current threat landscape spans several distinct categories. State-sponsored advanced persistent threat ("APT") groups are conducting espionage and pre-positioning operations, establishing persistent access to target networks that can be activated for disruptive purposes at a time of Iran's choosing. Iran-aligned hacktivist collectives, including the Cyber Islamic Resistance Axis, DieNet, and Handala, are conducting distributed denial-of-service ("DDoS") attacks, data theft, and defacement campaigns across energy, financial, transportation, and government targets. Pro-Russian hacktivist groups have also aligned with Iran-linked collectives since the conflict began.

Two recent incidents illustrate how these threat categories translate to operational impact. In March 2026, a MOIS-linked intrusion at the Los Angeles County Metropolitan Transportation Authority ("LACMTA"), claimed by a hacktivist persona calling itself Ababil of Minab, resulted in the exfiltration of at least 700 gigabytes of data and disrupted arrival screens and transit card systems for several weeks; attribution was established by Gambit Security based on forensic evidence tied to prior MOIS-linked campaigns, confirming that Iran-linked actors are willing to accept the operational costs of extended disruption to U.S. transportation infrastructure. Separately, Unit 42 researchers documented an active campaign by the Iran-nexus group Screening Serpens (also tracked as UNC1549 and Smoke Sandstorm) in which operatives posed as job recruiters to target software engineers at aviation, energy, defense, and telecommunications firms through fake job postings and malware-laced videoconferencing software, with Unit 42 assessing that the campaign showed no signs of slowing as of late April 2026.

The ceasefire has not translated into a pause in Iranian cyber activity. On April 7, 2026, the same day ceasefire negotiations were approaching their deadline, six federal agencies (CISA, the FBI, the NSA, the Environmental Protection Agency ("EPA"), the Department of Energy ("DOE"), and U.S. Cyber Command's Cyber National Mission Force ("CNMF")) issued a joint advisory (Advisory AA26-097A) confirming that Iranian-affiliated APT actors have been actively exploiting internet-facing programmable logic controllers ("PLCs") across U.S. critical infrastructure since at least March 2026, with confirmed operational disruptions and financial losses at organizations in the water and wastewater, energy, and government services sectors.

The Reasonable Security Standard and the CISA Gap

The legal significance of the CISA staffing situation extends beyond operational cybersecurity. Most regulatory frameworks governing critical infrastructure security, including the Health Insurance Portability and Accountability Act ("HIPAA") for healthcare, NERC CIP for energy, NYDFS cybersecurity regulations for financial services, and the Federal Trade Commission ("FTC") data security standards, use some form of reasonableness or adequacy standard that is calibrated, at least in part, by the threat environment and available

government guidance. CISA advisories, sector-specific alerts, and coordination frameworks have served as a practical benchmark for what “reasonable” security looks like in a given threat environment.

With CISA operating at reduced capacity, companies should not assume that federal cybersecurity advisories will provide the same level of timely threat intelligence or practical guidance that they may have provided in prior incidents. Reports of workforce reductions, suspended interagency threat bulletins, and leadership and staffing constraints suggest that CISA may be less able to serve as a central, real-time government backstop during periods of heightened Iranian cyber activity. Companies that have built their security programs primarily around CISA frameworks, alerts, and advisories should therefore assess whether they have sufficient independent sources of threat intelligence, incident response readiness, and escalation protocols to address fast-moving nation-state and proxy cyber threats.

Across sectors, organizations and their counsel should be asking whether current security investments and governance frameworks are calibrated to the current threat environment, rather than the one that prevailed when those frameworks were last reviewed.

Vendor Agreements and Supply Chain Exposure

Across critical infrastructure sectors, the most consequential near-term legal vulnerability for many organizations is not a direct attack on their own systems. Iranian APT groups have historically and systematically used third-party vendor access as a primary intrusion vector, compromising a software provider, a managed services vendor, an operational technology supplier, or a cloud infrastructure partner, and moving laterally into target organizations that would be difficult to penetrate directly. The vendor ecosystems of energy companies, financial institutions, telecommunications providers, and transportation operators are extraordinarily complex, and the contractual frameworks governing third-party access are frequently legacy instruments not designed with nation-state threat actors in mind.

Most vendor agreements and technology contracts across these sectors contain security representations calibrated to routine commercial risk: general obligations to maintain “industry standard” or “commercially reasonable” security, notification obligations triggered only upon confirmed breaches, and audit rights that are rarely exercised in practice. Few of these agreements contemplate the specific obligations, response timelines, or vendor-side security investments appropriate to a threat environment in which Iranian state-sponsored actors are actively conducting reconnaissance.

The gap between what existing agreements require of vendors and what the current threat environment demands is a real and measurable liability exposure, both in the event of a breach and in the context of regulatory scrutiny that follows.

Organizations should treat the current environment as a prompt to assess the adequacy of their vendor agreement security posture, with particular attention to third-party access rights to sensitive systems and data, incident notification timelines and thresholds, audit and assessment rights, and the allocation of liability in the event of a vendor-side compromise. For organizations in regulated sectors, this review should account for sector-specific regulatory requirements around third-party risk management, including NERC CIP supply chain risk management standards for energy, Office of the Comptroller of the Currency (“OCC”) guidance for financial institutions, and Federal Communications Commission (“FCC”) requirements for telecommunications providers, which may themselves impose heightened obligations in an elevated threat environment.

Ransomware and OFAC Sanctions

Organizations across critical infrastructure sectors have developed ransomware response frameworks over the past decade, often centered on data recovery and, in some cases, payment as a business continuity option. In the current environment, it is particularly important to note that ransomware payments to Iran-nexus threat actors implicate the Office of Foreign Assets Control ("OFAC") sanctions regime. OFAC has issued clear guidance that facilitating payments to sanctioned Iranian entities, including through ransomware intermediaries, may constitute a sanctions violation regardless of the payer's knowledge of the ultimate recipient. In a conflict environment in which Iranian state and criminal cyber capabilities are increasingly converging, and in which attribution may be uncertain at the time a payment decision must be made, the sanctions analysis that must precede any ransomware payment consideration is considerably more complex than it would be in a non-conflict period. Organizations and their counsel should ensure that incident response plans explicitly address the OFAC analysis and engage appropriate sanctions counsel as part of any ransomware response, well before a payment decision is required under operational pressure.

Incident Reporting Obligations: CIRCIA, SEC Disclosure, and the Coordination Challenge

A significant cyber incident involving an Iran-nexus threat actor will trigger multiple overlapping reporting obligations with compressed and potentially conflicting timelines. Organizations across the critical infrastructure ecosystem must understand these obligations now, before an incident forces real-time legal triage under operational pressure.

The Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") requires covered entities to report substantial cyber incidents to CISA within 72 hours, and to report ransomware payments within 24 hours of payment. For organizations facing an Iran-nexus ransomware event, the 24-hour CIRCIA payment reporting window runs concurrently with the OFAC sanctions analysis described above, creating acute tension between the operational pressure to restore systems, the legal obligation to report a payment within 24 hours of making it, and the sanctions compliance analysis that must be completed before any payment can lawfully be authorized.

For public companies, the SEC's cybersecurity incident disclosure rules require disclosure of material cybersecurity incidents on Form 8-K within four business days of a materiality determination. In a nation-state intrusion scenario, the materiality analysis is itself complex: the scope of compromise may not be fully understood within the disclosure window, ongoing incident response may be jeopardized by premature public disclosure, and national security considerations may support a delayed filing. Organizations should ensure that the process for making a materiality determination, and for seeking a national security delay if warranted, is documented and operationalizable before an incident occurs. State data breach notification laws add a further layer: if an Iranian APT group exfiltrates personal data, organizations may face notification obligations across dozens of jurisdictions with varying timelines, which must be coordinated with CIRCIA and SEC reporting requirements within a unified incident response workflow.

Cyber Insurance: War Exclusions and Coverage Uncertainty

Organizations should evaluate whether their cyber insurance policies contain war exclusions, hostile-act exclusions, or government-act exclusions that could be triggered by a cyber operation linked to an active military conflict between the United States and Iran. The insurance industry has been refining cyber war exclusions

since the NotPetya litigation, and many current-generation policies contain exclusions for cyber operations that are “directly or indirectly” attributable to a state actor during a period of armed conflict.

In the current environment, a ransomware attack or destructive operation attributed (even provisionally) to Iranian state-affiliated actors could fall squarely within such exclusions, potentially leaving organizations without coverage for business interruption losses, forensic investigation costs, regulatory defense expenses, and third-party liability. The attribution uncertainty that characterizes Iranian cyber operations, in which state actors deliberately use criminal intermediaries and hacktivist proxies to obscure responsibility, compounds this risk. Insurers may invoke war exclusions based on circumstantial attribution even where definitive state attribution has not been established.

Legal and risk management teams should engage with brokers and coverage counsel to review existing policy language, assess whether current exclusions could be invoked in an Iran-nexus cyber event, and evaluate whether supplemental coverage or policy endorsements are available to address identified gaps. Completing this review before an incident helps avoid negotiating coverage during an active cyber event, when coverage positions are more likely to become adversarial.

Considerations for Critical Infrastructure Organizations

The following considerations are offered to assist boards, general counsel, and compliance leadership across the critical infrastructure ecosystem in assessing their organizations' exposure in the current environment. They are not intended as legal advice applicable to any specific organization's circumstances, and organizations are encouraged to seek qualified counsel regarding their particular situations.

Organizations should evaluate whether their security program documentation reflects a current assessment of the threat environment, including nation-state threat actors with documented interest in their sector, and whether that assessment has been updated since the conflict began on February 28, 2026. A security program whose risk assessment predates the current threat elevation may be difficult to defend as meeting applicable legal standards in the event of a regulatory inquiry following an incident. Organizations that rely heavily on CISA frameworks and advisories should consider whether the current reduced capacity of that agency warrants supplemental engagement with private-sector threat intelligence resources.

In light of the developments described above, organizations should focus on the following near-term actions:

1. **Update threat environment risk assessments.** Review and revise enterprise risk assessments to reflect the April 7 joint advisory (AA26-097A), the ongoing conflict, and the specific Iranian APT groups and hacktivist collectives identified as targeting your sector. Document this review to establish a defensible record that the organization's security posture accounts for the current threat elevation.
2. **Audit critical vendor agreements.** Identify all third-party vendors with privileged access to operational technology, cloud administration platforms, or sensitive data environments. Review governing agreements for adequacy of security representations, incident notification timelines (ensuring notifications are triggered by suspected intrusions and reconnaissance activity, not only confirmed breaches), audit and assessment rights, and the allocation of liability in the event of a vendor-side compromise.
3. **Stress-test incident response plans against an Iran-nexus scenario.** Conduct a tabletop exercise simulating a ransomware event attributed to an Iranian state-affiliated actor, incorporating the OFAC

sanctions analysis, the CIRCIA 24-hour payment reporting obligation, the SEC four-business-day materiality determination, and applicable state notification deadlines into a single integrated response timeline. Pre-identify OFAC sanctions counsel, forensic investigators, and law enforcement contacts (including FBI) who can be engaged on short notice.

4. **Review cyber insurance coverage.** Engage brokers and coverage counsel to assess whether existing cyber policies contain war exclusions, hostile-act exclusions, or attribution-based limitations that could be invoked in connection with an Iran-linked cyber event. Evaluate available endorsements or supplemental coverage to address identified gaps.

5. **Confirm reporting obligation readiness.** Map all applicable incident reporting obligations, including CIRCIA (72 hours for covered incidents, 24 hours for ransomware payments), SEC Form 8-K (four business days from materiality determination), sector-specific frameworks (NERC CIP, HIPAA, NYDFS, TSA directives), and state data breach notification laws, into a unified response playbook with designated responsible personnel, pre-drafted notification templates, and documented escalation procedures. Confirm that these obligations are operationalizable within the compressed timelines a significant incident would impose.

Related People

Anthony D. Glosson

t 202.508.5842

tglosson@ktslaw.com

Gregory P. Silberman

t 650.462.5310

gsilberman@ktslaw.com