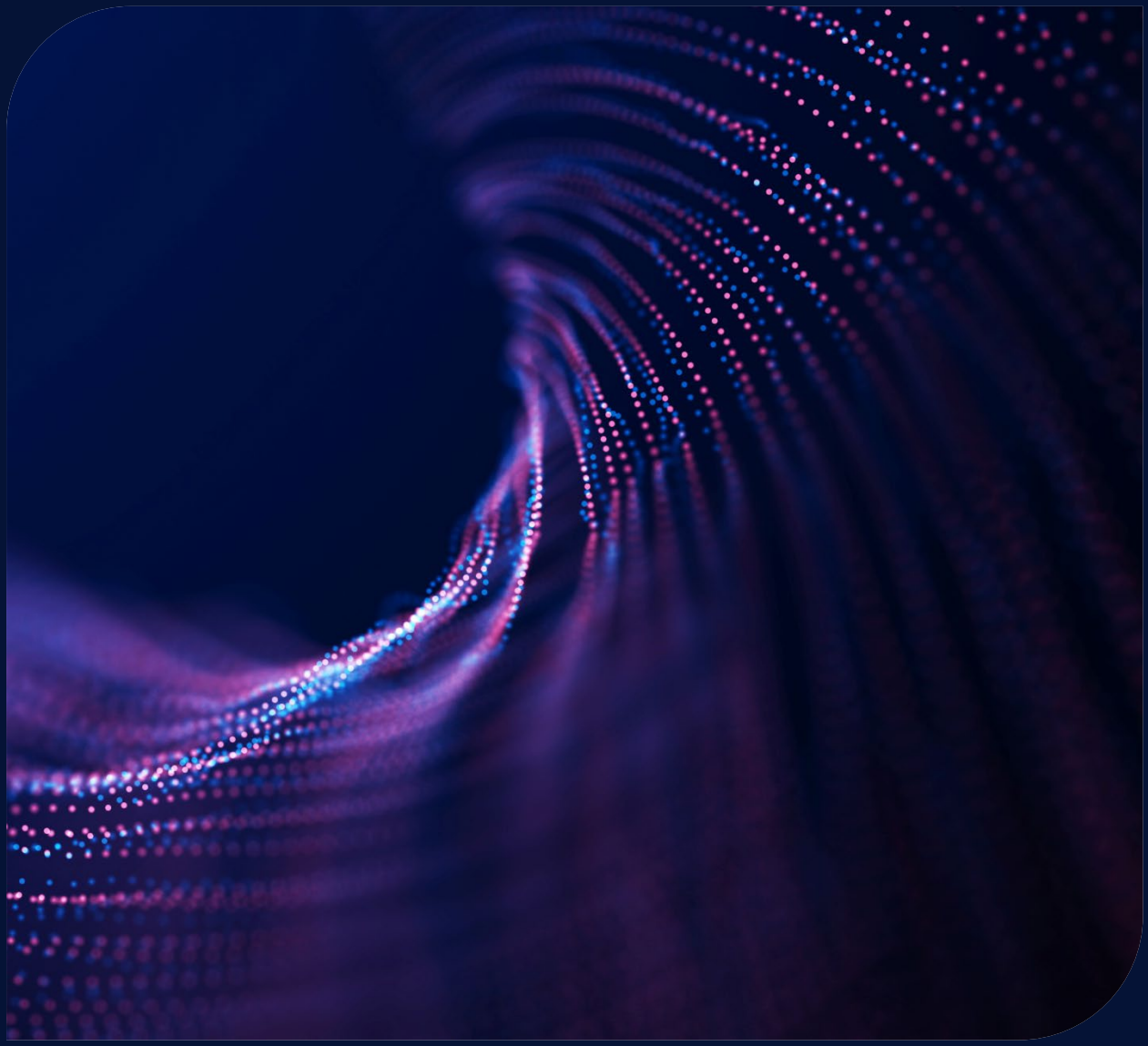
Teneo®

Beyond the Network: Preparing for the Business Impact of Cyber Conflict

Teneo Insights | August 2026



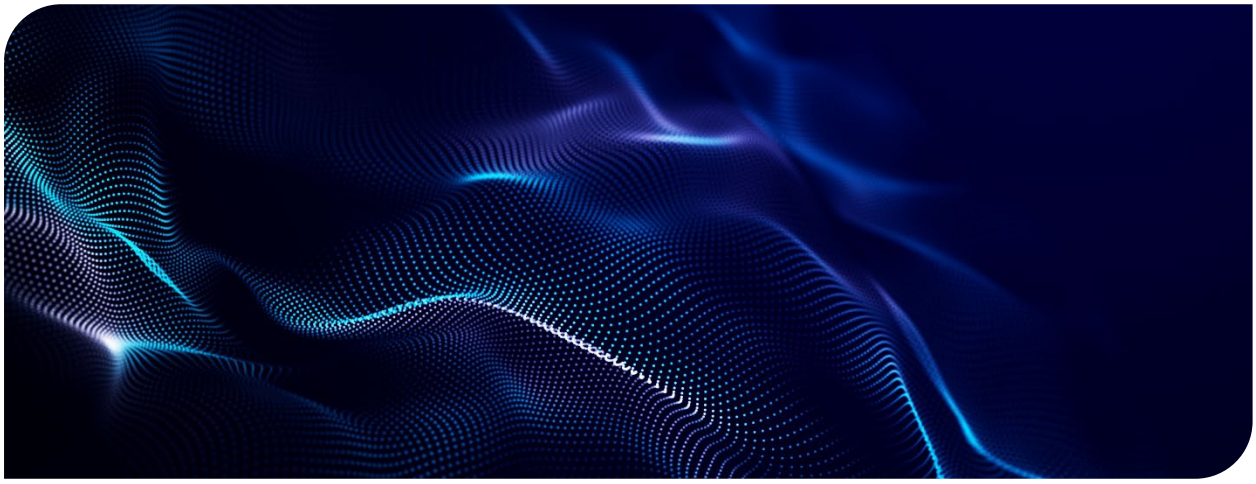
The Cyber Resilience Test for Leaders

Geopolitical conflict rarely remains confined to the battlefield. Cyber activity can extend its effects into corporate networks, operational systems and executive identities, sometimes through deliberate targeting, sometimes through opportunistic spillover.

Leaders do not need to assume their organization is a primary target. They do need to recognize that conflict changes the threat environment and test whether their resilience plans reflect that reality.

Recent cyberattacks affecting more than 30 municipal water systems in Minnesota offer a timely warning. The campaign subsequently widened beyond Minnesota: by July 31, water and wastewater utilities in at least seven U.S. states had reported related incidents to the Federal Bureau of Investigation (FBI).[1] The incidents involved technology used to remotely monitor and control equipment. In Braham, attackers temporarily shut down operating controls at the well and water treatment plant; in Plymouth, crews maintained operations while infrastructure communications were restored.[2]

U.S. agencies have warned that Iran-affiliated actors are exploiting internet-connected operational technology, including programmable logic controllers, across critical infrastructure. Earlier attacks have led to configuration wiping, interference with mechanical sensors and disruption of human-machine interfaces.[3]



[1] FBI and U.S. Environmental Protection Agency, Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions, July 30, 2026.

[2] Associated Press, Cyberattacks targeted Minnesota water systems, July 30, 2026

[3] U.S. Environmental Protection Agency, EPA, FBI, CISA, NSA Issue Joint Cybersecurity Advisory to Water System Regarding Iranian-Affiliated Cyber Attacks, April 7, 2026

Cyber Conflict Rarely Respects Organizational Boundaries

The cyber dimension of geopolitical conflict is often less visible than military activity, sanctions or diplomatic action. It can, however, reach organizations far removed from the immediate confrontation.

State-linked groups pursue espionage, disruption, influence or the theft of strategically valuable information. Hacktivists amplify claims and target organizations associated with one side of a conflict. Criminal groups use heightened anxiety, public attention and newly available access to launch fraud or ransomware campaigns. These activities do not always occur independently. The FBI has described a threat environment in which the boundaries among nation-state, hacktivist and criminal actors are increasingly indistinct.[4]

For business leaders, the practical question is not whether every organization will be targeted directly because of a conflict. It is whether a more active and permissive threat environment increases the likelihood that the organization, an executive or a critical supplier will be affected.

Exposure is likely to be heightened for organizations connected to energy, shipping, infrastructure, manufacturing, public services, government and defense. But sector alone is not determinative. An organization's technology, data, geographic footprint, public positions, customers, leadership profile and third-party relationships can all make it relevant to an adversary.

Operational Technology Turns Cyber Risk Into Continuity Risk

For many boards, cyber risk is still framed primarily around data loss, privacy and enterprise technology. Those issues remain important, but attacks on operational technology change the nature of the consequence.

When systems used to control equipment or physical processes are disrupted, a cyber incident can threaten operational continuity and create broader safety and public confidence risks. The affected organization may need to maintain essential services manually, make decisions with incomplete technical information and communicate before the cause or attribution is known.

This requires a different level of preparedness. Leaders need to know which operational systems are connected to the internet, which vendors can access them remotely and where legacy or unsupported technology creates dependency. They also need to understand whether teams can operate critical processes safely if automation or communications are unavailable.

The test is not simply whether the organization can prevent an intrusion. It is whether it can continue to function when technology is degraded.

[4] FBI, Worldwide Threats to the Homeland, December 11, 2025

Innovation and Leadership Are Part of the Attack Surface

Strategically important technology has become an intelligence target in its own right. U.S. counterintelligence guidance warns that emerging technology companies, which, as startups,often have weaker security controls, can attract state actors, competitors and criminals seeking intellectual property, technical expertise or commercial advantage. The risks extend beyond networks to investment, insiders, supply chains, overseas expansion, international travel and pitch competitions.[5]

This matters for companies working in areas such as artificial intelligence, semiconductors, autonomy, biotechnology, defense technology and cybersecurity. Engineers and other specialists can possess valuable knowledge long before a product becomes public. Conferences, investor meetings and collaborative projects can expose both people and information outside the controls of the normal workplace.

Senior executives also require specific attention. Their public visibility, decision-making authority and access make them useful targets for impersonation, social engineering and account compromise. An attacker does not always need to breach a hardened system if a convincing message, voice or request can cause a trusted employee to act.

Cyber resilience must therefore protect both infrastructure and authority: the systems through which the organization operates and the people whose instructions others trust.



[5] Office of the Director of National Intelligence, National Counterintelligence and Security Center

Five Priorities for Leaders

This environment calls for an integrated leadership response rather than a purely technical one.



Identify What Must Not Fail

Map the systems, people, vendors and facilities required to sustain critical operations. Include operational technology, executive communications and dependencies that sit outside the direct control of the organization.



Prepare to Operate in a Degraded Environment

Test manual workarounds, alternative communications and decision rights. Crisis exercises should assume that some technology is unavailable and that the cause, duration and attribution remain uncertain.



Protect Executives and High-Value Teams

Strengthen personal account security, travel protocols and verification procedures for sensitive instructions. Ensure employees know how to challenge an unusual request without slowing legitimate decisions unnecessarily.



Integrate Cyber Into Enterprise Crisis Management

Cyber, operations, legal, communications, security and executive leadership should not develop separate understandings of the incident. Plans must establish how technical facts become business decisions and how the organization will communicate credibly as the situation evolves.



Establish Escalation Before an Incident

Clarify when and how to engage the board, law enforcement, regulators, insurers, external advisors and critical partners. Preserving evidence, reporting quickly and coordinating decisions are much easier when relationships and thresholds are defined in advance.

Resilience Before Attribution

Cyber activity during geopolitical tension may not announce itself as an act of war. It may look like an offline control panel, a compromised vendor connection, an exposed client document or a convincing instruction from a senior executive.

The organizations best positioned to withstand this environment will not be those that attempt to predict every attacker or scenario. They will be those that understand what matters most, can operate through disruption and have integrated technical response with leadership, governance and communications.

Resilience is not the absence of disruption. It is the ability to maintain critical operations, make sound decisions with incomplete information and communicate credibly while the facts emerge.

Teneo supports organizations in assessing how cyber risk intersects with operational resilience, executive protection, governance and communications, and in translating that assessment into practical preparation.

Authors



Elizabeth Buckley
Managing Director



Abhi Arora
Global Head of
Information Security

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance and ESG.

The firm has more than 1,800 employees located in 50+ offices around the world.

teneo.com

© 2026 Teneo. All rights reserved. This material was produced by Teneo for use solely by the recipient. This communication is intended as general background research and is not intended to constitute advice on any commercial investment or trade matter or issue and should not be relied upon for such purposes. The views expressed here represent opinions as of this date and are subject to change without notice. The information has been obtained from sources believed to be reliable but no guarantees can be given as to its accuracy, completeness or reliability. AI-enabled tools may have been used in the preparation of this report to assist with data analysis, content structuring, and editorial refinement. Where used these tools did not operate autonomously and did not replace expert judgment. All outputs were reviewed, validated, and finalized by the report authors, who retain full accountability for the accuracy and integrity of the work. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or otherwise, without the prior consent of Teneo.