Securing Critical Infrastructure in a Connected World

CONTENT PRODUCED BY

ATARC powered by GovExec

HOSTED BY

Deloitte.

This white paper summarizes an off-the-record roundtable discussion among government, industry, operational technology, and critical infrastructure leaders regarding the evolving cyber-physical threat environment facing U.S. critical infrastructure sectors.

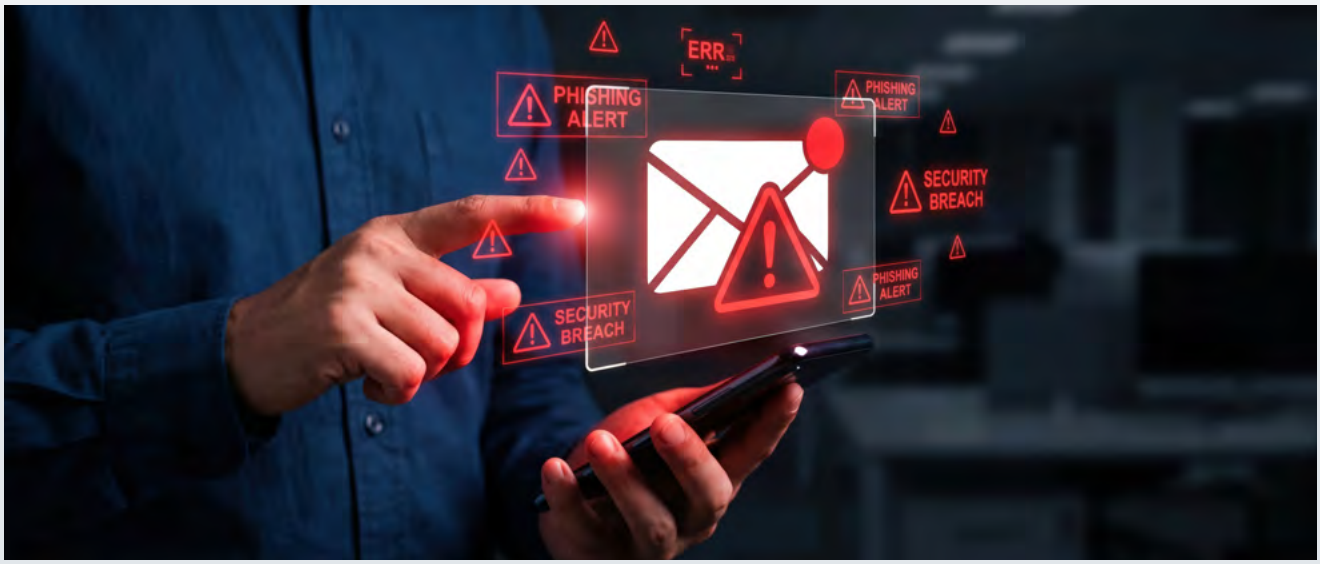
Executive Summary

The United States is entering a new era of critical infrastructure risk defined by persistent, coordinated, and increasingly sophisticated threats across both digital and physical domains. Participants described a rapidly evolving threat environment in which operational technology environments, industrial control systems, and interconnected infrastructure are simultaneously becoming more efficient and more exposed. Water systems, transportation networks, energy systems, communications infrastructure, and industrial environments are increasingly interconnected, creating both operational benefits and expanded attack surfaces.

Roundtable participants emphasized that cybersecurity can no longer be treated as a standalone technical issue. The convergence of cyber and physical infrastructure risk means that digital vulnerabilities now have direct operational consequences, including but not limited to: disruptions to service delivery, safety concerns, economic impacts, and cascading infrastructure failures. Nation-state actors, criminal organizations, and opportunistic threat actors are increasingly operating in parallel, and more frequently in coordination, leveraging common vulnerabilities, internet-exposed systems, supply chain dependencies, and operational complexity.

At the same time, many infrastructure sectors continue to rely on aging operational technology platforms and legacy infrastructure that were not designed for today's connectivity requirements or threat environment. Additionally, participants discussed how workforce shortages, funding limitations, fragmented governance, and uneven visibility across infrastructure ecosystems can further complicate resilience efforts.

Despite these challenges, the discussion was solution-oriented. Participants emphasized the importance of resilience-focused strategies that balance operational continuity with cybersecurity requirements, improve coordination across public and private stakeholders, strengthen visibility and information sharing, modernize aging infrastructure, and address systemic vulnerabilities introduced through integrators and supply chains. The discussion reinforced that resilience depends not only on preventing attacks, but also on improving detection, response, recovery, and operational adaptability across increasingly connected infrastructure environments.



The Evolving Threat Environment

Participants described a threat environment that differs substantially from traditional physical and cybersecurity models. Rather than isolated attacks, critical infrastructure operators now face continuous probing, reconnaissance, positioning, and opportunistic exploitation by a wide range of threat actors. Nation-state actors are increasingly viewed as conducting long-term positioning activities designed to create strategic options during future geopolitical conflicts or periods of instability.

The discussion highlighted growing concern surrounding hybrid attack planning, where cyber activities may be coordinated with broader operational disruption efforts targeting physical infrastructure, logistics management systems, communications capabilities, and public confidence. Participants noted that attacks against infrastructure environments are no longer confined to information systems. Instead, they can directly affect pumps, valves, building systems, industrial controls, transportation assets, and operational continuity.

Participants also discussed how opportunistic actors frequently exploit exposed systems without necessarily targeting a specific organization. Internet-connected operational technology devices, particularly within smaller or resource-constrained environments, are often discovered through broad internet scanning activities. In many cases, adversaries are exploiting vulnerabilities that are well-known but remain unaddressed due to operational, financial, or staffing constraints.

This evolving threat environment requires organizations to think differently about resilience. Traditional perimeter-based approaches are increasingly insufficient in environments where infrastructure systems must remain connected, accessible, and operational in order to support modern operational requirements.

The Connectivity Dilemma

One of the central themes of the discussion was the growing tension between operational connectivity and cybersecurity risk. Historically, many operational technology environments remained intentionally isolated from broader enterprise networks and the public internet. However, modern operational requirements increasingly depend on remote access, automation, mobile monitoring, cloud services, centralized visibility, and data-driven operational management.

Participants emphasized that connectivity is often driven by legitimate operational needs. Organizations use connected systems to improve efficiency, reduce operational costs, compensate for workforce shortages, enable remote monitoring, and support geographically dispersed infrastructure environments. In sectors such as water and wastewater management, operators may be responsible for overseeing large regional systems with limited staffing resources. Remote visibility and automated monitoring capabilities therefore become operational necessities rather than optional conveniences.

At the same time, increased connectivity expands the attack surface available to adversaries. Participants described ongoing tensions between operational technology teams focused on reliability and continuity, and cybersecurity teams focused on visibility, monitoring, segmentation, and threat detection. When these perspectives are not aligned, organizations face increased operational and security risk that can limit both resilience and visibility.

Participants stressed that resilience requires integrated decision-making that incorporates operational realities into cybersecurity planning while also recognizing that disconnected systems are no longer practical in many modern infrastructure environments. Connectivity must therefore be managed deliberately, through layered risk management approaches rather than avoided entirely.

Legacy Infrastructure and Modernization Challenges

The discussion repeatedly returned to the challenge of aging infrastructure and outdated operational technology environments. Many critical infrastructure sectors continue to operate systems that were designed decades ago and were never intended to support today's connectivity requirements or cybersecurity expectations or address the ever-evolving challenges associated with the current and emerging threat environments.

Participants described operational environments running legacy operating systems, unsupported hardware, and aging industrial control platforms that cannot easily be upgraded without affecting operations. In many cases, replacing a single component requires broader system-wide modernization efforts because of compatibility limitations and vendor dependencies. Organizations are therefore often constrained to choosing between maintaining vulnerable systems or pursuing expensive multi-year modernization initiatives.

The physical condition of infrastructure itself also emerged as a major concern. Participants discussed how aging water systems, outdated utility infrastructure, and deferred maintenance increase operational fragility while simultaneously complicating cybersecurity modernization efforts. Cyber resilience and infrastructure modernization are increasingly interconnected challenges rather than separate issues.

Funding constraints remain a major hurdle. Although cybersecurity assessments, guidance, and technical assistance may be available, many organizations lack the financial resources required to implement large-scale upgrades. Smaller municipalities and local infrastructure operators are particularly challenged by limited staffing, aging systems, and competing operational priorities.

Participants emphasized that modernization efforts should account for both cyber and physical security and resilience requirements. Investments in connected technologies, automation, and monitoring capabilities should be paired with broader resilience planning that addresses operational continuity, system redundancy, and long-term infrastructure sustainability.

The Supply Chain Challenge

The discussion also highlighted the broader challenge of supply chain visibility. Organizations frequently depend on interconnected technologies, cloud environments, software vendors, operational technology providers, and service contractors whose security practices directly influence operational risk. Participants emphasized that resilience increasingly depends on understanding these interdependencies and improving visibility across the broader ecosystem.

Participants also discussed the lack of consistent reporting and information sharing mechanisms related to vulnerabilities affecting infrastructure supply chains. In many cases, organizations hesitate to disclose incidents or vulnerabilities due to concerns about liability, reputation, or operational impacts. Improving transparency and coordination remains an important component of broader resilience efforts.

Workforce and Operational Realities

Workforce shortages emerged as a persistent challenge across multiple sectors. Participants described environments in which a small number of operators are responsible for managing large and geographically dispersed systems. In some cases, infrastructure organizations struggle to recruit and retain personnel with experience spanning both operational technology and cybersecurity disciplines.

The aging workforce within critical infrastructure sectors further complicates this challenge. Many experienced operators possess decades of institutional knowledge regarding legacy systems and operational processes. As these individuals retire, organizations risk losing critical know how that is difficult to replace through traditional hiring pipelines.

Participants emphasized that workforce shortages are directly influencing operational technology decisions. Remote monitoring, automation, mobile access, and centralized management capabilities are increasingly necessary to maintain operational continuity with limited staffing. However, these same technologies can introduce additional exposure if not implemented securely.

The discussion also highlighted the lack of formalized training pipelines focused specifically on operational technology cybersecurity. Traditional IT cybersecurity training often does not adequately address industrial control systems, physical operations, safety considerations, and operational continuity requirements associated with infrastructure environments.

Addressing workforce challenges therefore requires more than simply increasing hiring. Participants stressed the importance of cross-disciplinary training, operationally informed cybersecurity practices, workforce development programs, and technologies that can augment human capabilities without introducing unnecessary risk.

Visibility, Coordination, and Information Sharing

Participants repeatedly emphasized the importance of coordinated visibility across infrastructure ecosystems. Although many organizations are capable of detecting vulnerabilities or suspicious activity within their own environments, there remains significant inconsistency in how information is shared across sectors, jurisdictions, and operational communities.

The absence of standardized reporting requirements and information-sharing mechanisms can create situations where similar vulnerabilities are repeatedly discovered and mitigated independently.

Improving visibility requires both policy and cultural change. Participants discussed the need for stronger coordination among government agencies, infrastructure operators, sector risk management agencies, and private-sector partners. Information sharing should support actionable operational outcomes rather than simply distributing threat intelligence.

Participants also emphasized the need for broader situational awareness regarding interconnected infrastructure dependencies. A vulnerability affecting one infrastructure sector or integrator may have downstream impacts across multiple operational environments. Improving ecosystem-level visibility therefore becomes increasingly important as infrastructure systems become more interconnected.

The discussion reinforced that resilience depends on collective awareness and coordination rather than isolated organizational efforts. Participants consistently emphasized that no single organization can effectively manage infrastructure risk independently within today's interconnected operational environment.

From Compliance to Resilience

Traditional physical security and cybersecurity programs often prioritize compliance with standards, frameworks, and regulatory requirements. While participants acknowledged the value of these activities, they also emphasized that compliance alone does not guarantee resilience within today's threat environment.

Organizations may effectively meet regulatory requirements while still remaining vulnerable to sophisticated adversaries, operational disruptions, or cascading infrastructure failures. Participants therefore advocated for a broader resilience-based approach focused on prevention, detection, response, recovery, and operational adaptability.

Resilience requires organizations to assume that some disruptions will occur despite efforts at prevention. As a result, organizations should prioritize continuity planning, operational redundancy, rapid recovery capabilities, and adaptive response mechanisms. Participants emphasized that resilience should be embedded across governance, operations, workforce planning, technology modernization, and supply chain management activities.

Several participants also highlighted the importance of scenario-based exercises and operational simulations that incorporate both cyber and physical disruptions. These exercises help organizations better understand cascading operational impacts, decision-making priorities, and cross-functional coordination requirements during complex incidents.

The discussion ultimately reinforced that resilience is not solely a technical objective. It is an operational capability that depends on coordination, adaptability, leadership, workforce readiness, infrastructure modernization, and ecosystem-wide collaboration.

Conclusion

The roundtable discussion highlighted the growing complexity of securing critical infrastructure within increasingly connected operational environments. Participants consistently emphasized that critical infrastructure resilience can no longer be viewed through a purely cybersecurity lens. The convergence of physical infrastructure challenges, operational demands, workforce constraints, supply chain dependencies, and cyber threats requires a broader and more integrated approach to resilience.

Modern infrastructure systems should remain connected in order to support operational efficiency, automation, remote monitoring, and service continuity. At the same time, this connectivity expands exposure to increasingly sophisticated adversaries operating across both digital and physical domains. Organizations are therefore being asked to modernize aging infrastructure, strengthen cybersecurity, reduce physical security vulnerabilities, improve operational visibility, and address workforce shortages simultaneously.

Despite these challenges, participants expressed cautious optimism that meaningful progress is possible through stronger coordination, more deliberate risk management, targeted modernization investments, improved information sharing, and resilience-focused operational planning. Participants emphasized that resilience ultimately depends on recognizing the interconnected nature of today's infrastructure environment and adopting approaches that integrate physical and cybersecurity, operational continuity, workforce development, and physical infrastructure modernization into a unified strategy.

The threat environment is already evolving rapidly. The organizations and sectors well positioned for long-term effectiveness will be those capable of adapting quickly while maintaining the operational resilience required to support essential services, public trust, and national security.