G1VE TECHNOLOGIES

Why AI Speed Threats, Maritime Sabotage Risk, CIRCIA, & Consequence-Based Defense Now Define Critical Infrastructure Leadership

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP

Aug 24, 2026

Original source

https://www.linkedin.com/pulse/keep-harbor-open-w-b-carrington-mba-lssmbb-ctpra-grca-grcp-favye/

I. Last Week Said To Assume Intrusion. This Week Explains Why Continuity Will Be Decided Before The Incident Report Is Filed.

The last article in this vertical made the central posture shift clear. Critical infrastructure leaders have to stop pretending the goal is perfect prevention and start planning for continuity under compromise. That was the right starting point. But this week's facts push the argument further.

The issue is no longer simply whether an operator accepts that breach is plausible. The issue is whether leadership has already made the continuity decisions that determine what stays online, who has authority, and how the mission continues when both digital trust and physical confidence begin degrading at the same time. That is why "Keep The Harbor Open" is not just a port slogan. It is a decision architecture.

It applies to ports, pipelines, water systems, freight rail, electric utilities, fuel storage, and the communications systems that connect them. Once you accept that disruption can arrive through cyber intrusion, vendor unreliability, degraded telecommunications, or even physical sabotage support from maritime or unmanned platforms, you stop asking whether you can prevent every bad day. You start asking whether the system can still function when several assumptions fail at once.

II. The Threat Environment Has Moved From "Protect The Network" To "Preserve The Function."

Senior officials said it plainly this month. Cyber compromise is no longer a black swan. It is just a swan. That line should hit every infrastructure executive in the face. It means the operating environment has changed. AI is helping attackers find and exploit weaknesses faster than defenders can patch them, while years of underinvestment still leave organizations sitting on enormous backlogs of known weaknesses.

That combination is brutal because it compresses time while preserving old fragility. So the leadership question changes. The relevant question is no longer "Are we secure?" in some abstract enterprise sense. The relevant question is "Which functions must continue even if compromise occurs?" That is why the Canadian "Minimum Viable" continuity idea mentioned in the same discussion matters so much.

Infrastructure leaders need their own version. They need a minimum viable port, minimum viable utility dispatch, minimum viable treatment capability, minimum viable movement of goods, and minimum viable public communication plan. If those definitions do not already exist before the incident, they will be improvised during the incident. That is how continuity fails.

III. Ports Are Now An Easy Place To See The New Battlespace Clearly.

The U.S. Coast Guard 's July request for information on technologies to defeat unmanned underwater vehicles was one of the clearest operational warnings of the summer. The agency did not ask only for detection. It emphasized that while there are technologies that can track and detect UUVs, there are far fewer tested and fielded solutions for defeat and mitigation. That distinction matters.

Detection without disruption is not security. It is awareness of approaching failure. The use cases laid out in that notice were not theoretical. Malicious actors could use UUVs for intelligence gathering, surveillance, smuggling, sabotage of critical infrastructure, and kinetic strikes. Put that together with cyber compromise assumptions and the picture gets uglier fast. A port operator does not just have to worry about cranes, gates, and enterprise networks.

It has to think about underwater approaches, channel continuity, fuel movement, service provider reliability, and whether the organization can still make safe decisions if both the data picture and the physical environment start getting weird at the same time. This is why critical infrastructure is now better understood as a live operational battlespace rather than a compliance estate.

IV. The Cybersecurity and Infrastructure Security Agency Has Already Told Operators What Posture To Adopt. Most Organizations Still Have Not Internalized It.

CI Fortify is important because it tells operators to plan on third party connections becoming unreliable during conflict and to assume threat actors may have some access to operational technology networks. That is not normal corporate language. That is wartime continuity language. It tells leaders to focus on isolation and recovery planning, not just perimeter confidence.

In other words, if your strategy still assumes cloud, telecom, upstream vendors, and OT dependencies will all behave normally when the pressure hits, you are planning for peacetime convenience in a wartime environment. The Cybersecurity and Infrastructure Security Agency 's June directive on vulnerability prioritization pushes the same idea from another angle.

Agencies are being told to patch based on consequence and exploitability rather than pretending every vulnerability demands the same urgency. Cybersecurity and Infrastructure Security Agency found that only 1 percent of vulnerability instances at one large agency fell into the three day category, while more than 60 percent could be deferred to a major upgrade cycle.

That is not a call to relax. It is a call to become more disciplined. When AI helps adversaries move faster, consequence based prioritization becomes a necessity, not a luxury. Critical infrastructure leaders should be stealing that logic immediately.

V. CIRCIA Is Not Just A Reporting Rule. It Is A Leadership Speed Test.

CIRCIA will require substantial incident reporting to the Cybersecurity and Infrastructure Security Agency within 72 hours and ransomware payment reporting within 24 hours. Many organizations still speak about that requirement as a legal or compliance burden. That is far too narrow. In practice, it is a test of whether the organization can establish facts, coordinate legal and operational leadership, preserve evidence, maintain continuity, and communicate externally while the event is still unfolding.

The reporting clock is not just a burden. It is a forcing function that exposes whether your command structure is real. That is why the next stage of infrastructure leadership is not a bigger binder. It is faster decision choreography. If the operations team, cyber team, legal team, executive leadership, and external affairs team have not already rehearsed how the first 24 hours work, then the 72 hour rule becomes a panic amplifier.

And, if you add degraded third party communications or an overlapping maritime or physical disruption scenario, the need for pre delegated authority becomes obvious. Leaders should be asking now which decisions can be made locally, which require central approval, and which cannot wait for perfect information.

VI. The Smartest Operators Are Moving From General Awareness To Sector Specific Continuity Design.

Congressional pressure is moving in the same direction. Proposed legislation would require CISA to refresh sector specific cybersecurity plans across all 16 critical infrastructure sectors because AI enabled threats are evolving faster than outdated plans. That matters because generic cyber language is no longer enough. The practical version of resilience now has to be sector specific.

A port has different priority functions than a power utility. A water system has different tolerances than a freight rail operator. A data center has different dependencies than a fuel terminal. For leadership teams, the right move over the next quarter is brutally clear:

1. Define the minimum viable mission.
2. Identify which dependencies are most likely to go unreliable under conflict or disruption.
3. Separate functions that must survive from functions that can temporarily degrade.
4. Build isolation playbooks.
5. Build recovery priorities.
6. Rehearse reporting, authority, and external communications together.

...And, for operators in maritime, energy, water, and transportation, stop acting as if cyber and physical risk live in separate rooms. They do not. The hostile actor does not care about your org chart.

VII. Thought-Provoking Close: The Final Assessment

The Harbor Is A Metaphor. The Mission Is Not. “Keep The Harbor Open” is about more than maritime infrastructure. It is about what serious critical infrastructure leadership looks like in a

period where compromise is routine, dependencies are unreliable, and consequence now matters more than checkbox confidence.

The organizations that win will not be the ones with the prettiest maturity model. They will be the ones that already know what must remain functioning, who decides, and how the system continues to move under degraded conditions. That is the real pivot from last week.

Last week asked leaders to accept the world as it is. This week asks whether they are structured to lead inside it. Those are not the same thing. And in the next serious incident, everyone will discover the difference very quickly.

✨ Call to Action: Step Into the Arena ✨

Most professionals will read about the future. A select few will shape it.

If you are serious about staying ahead of the curve in Artificial Intelligence, Regulatory Compliance, and Enterprise Risk, this is where you need to be.

📩 Subscribe to Securing Our Future to gain direct access to:

1. Strategic foresight on AI Governance & Ethical Deployment
2. Real-world applications across National Security & Mission Assurance
3. Advanced GRC, TPRM, and Regulatory Compliance frameworks
4. Emerging Fintech and Risk Intelligence innovations

⚔️ The landscape is shifting—fast. The gap between those who understand and those who execute is widening.

This is built for professionals responsible for decisions that carry consequence—not commentary.

📅 Ready to operationalize these insights and move beyond theory?

👉 https://calendly.com/g1ve-technologies

Let us translate insight into measurable, defensible outcomes—and build capability, not just conversation.

🔍 About the Author

W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP is a National Security-aligned Artificial Intelligence Strategist/Tactician and Governance, Risk, and Compliance (GRC) Authority/Subject Matter Expert with over a decade of experience operating at the intersection of National Security, National Defense, Critical Infrastructure, Cybersecurity, AI Governance, Mission Assurance, Mission-Critical Systems, and Predictive Funding/Grant Intelligence.

As Managing Partner at G1VE Technologies, LLC and a Strategic Board Advisor, W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP architects and operationalizes enterprise-scale risk, compliance, and AI governance ecosystems across both Public and Private Sector environments—including Fortune 500/1000 organizations and Federal-aligned missions, where failure is not an option.

His work is centered on delivering Decision Advantage, strengthening Operational Resilience, and enabling organizations to navigate high-stakes, high-uncertainty environments with precision and confidence.

📡 Connect with W.B. Carrington, MBA, LSSMBB, CTPRA, GRCA, GRCP here to stay at the forefront of:

- Artificial Intelligence
- National Security
- GRC
- Cyber Risk
- Regulatory Strategy
- Mission Assurance