G1VE TECHNOLOGIES

Assume the Breach. Keep the Harbor Open.

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

Aug 19, 2026

Original source

https://www.linkedin.com/pulse/assume-breach-keep-harbor-open-w-b--pc0ae/

Why Critical Infrastructure Leaders Must Plan for Routine Cyber Compromise, Maritime Disruption, and Operations Under Attack

I. The Warning Has Now Become Operating Guidance

In the last Securing Our Future article, I argued that the next serious homeland disruption would not begin with a cinematic opening strike. It would begin in the seams: ports, pipelines, telecom dependencies, vendor pathways, operational technology, and delayed recognition. That was the warning.

This article moves from warning to operating guidance.

Senior officials are now saying openly that cyber compromise should no longer be treated as a rare shock. At Black Hat , U.S. Department of Homeland Security Assistant Secretary Joseph Alm said cyber compromise is "not a black swan anymore. It's just a swan," and argued that organizations need to prepare to limit damage and continue functioning after attackers get inside. That is a major shift in posture. It means the real leadership question is no longer just how to stop every intrusion. It is how to keep the mission moving once intrusion occurs.

So the governing posture is harder and more realistic:

1️⃣ Assume intrusion,

2️⃣ Reduce harm,

3️⃣ Preserve continuity, and,

4️⃣ Keep the mission moving while the environment is still degraded.

II. AI Is Shrinking The Time Available To Defend

The pressure is increasing because artificial intelligence is compressing attacker timelines. Officials from the United States, Canada, and Britain said this month that AI is helping adversaries find and exploit weaknesses faster than governments can patch them. Joseph Alm added that AI is accelerating exploitation of the weaknesses already buried inside old technology stacks.

That matters for Critical Infrastructure because most operators are not defending greenfield systems. They are defending layered environments full of aging software, mixed vendors, remote access dependencies, and operational technology that was never designed for this threat tempo.

So resilience now has to mean more than "patch more." It has to mean:

1️⃣ Decide faster,

2️⃣ Isolate faster,

3️⃣ Restore faster, and,

4️⃣ Continue essential operations faster.

This is where many organizations are still behind. They are talking about cybersecurity as if the main problem is data theft. In reality, for infrastructure operators, the larger problem is often service degradation, operational delay, and loss of trusted control.

III. The Cybersecurity and Infrastructure Security Agency Has Already Described The Assumptions Leaders Should Use

The Cybersecurity and Infrastructure Security Agency 's CI Fortify initiative is one of the clearest pieces of infrastructure guidance issued this year. The agency told owners and operators to plan for conflict conditions in which telecommunications, internet access, vendors, service providers, and upstream dependencies may be unreliable. It also told them to assume threat actors may already have access to operational technology environments and to focus on isolation and recovery planning.

That should change how executives think immediately. The planning assumptions are no longer comfortable:

1️⃣ Do not assume your provider will be available,

2️⃣ Do not assume your vendor can remote in and fix the problem,

3️⃣ Do not assume your OT environment is still clean when the incident begins, and,

4️⃣ Do assume recovery and continuity are as important as prevention.

This is not theoretical hardening language. It is a practical recognition that in a conflict-linked or high-tempo cyber event, the organization may need to function while parts of its digital ecosystem are unreliable or already compromised.

IV. "Keep The Harbor Open" Is A Real Use Case, Not A Tagline

Ports are one of the clearest examples of why this matters. A harbor is not just a transportation asset. It is a logistics node tied to energy movement, freight flow, emergency response, military support, commercial confidence, and regional stability. If the harbor stops, the consequences travel fast.

That is why the U.S. Coast Guard 's request for technology to defeat unmanned underwater vehicles matters so much. The service said those systems can be used for intelligence collection, surveillance, smuggling, sabotage of Critical Infrastructure, and even kinetic attack. It also made clear that detection alone is not enough. It wants scalable solutions that can actually defeat and mitigate such threats in ports, waterways, and coastal security operations.

So "keep the harbor open" means something concrete:

1️⃣ Keep vessel movement safe,

2️⃣ Keep operators confident enough to make decisions,

3️⃣ Keep throughput from collapsing under uncertainty, and,

4️⃣ Keep continuity plans working even while cyber and physical signals are conflicting.

A practical example makes this real. Imagine a port authority facing three things at once: degraded scheduling systems, suspicious OT activity, and a maritime security alert involving possible underwater interference near a key access channel. That is not an IT incident with a side problem. That is an executive command problem involving continuity, safety, reporting, and National Security implications all at once.

V. Consequence Based Defense Is Now The Mature Operating Model

The Cybersecurity and Infrastructure Security Agency's June vulnerability directive points in the right direction. The agency changed remediation timelines to focus on consequence and exploitability, with deadlines ranging from three days for the highest-risk vulnerabilities to sixty

days for lower-priority issues. It explicitly said the change responds to a threat environment in which AI can help attackers find and exploit weaknesses faster. Source

The most useful statistic in that article is operational, not rhetorical. In one initial analysis, only 1% of vulnerability instances fell into the three-day category, while more than 60% could be deferred until the next upgrade cycle.

That is the adult answer to infrastructure defense in 2026. Not all vulnerabilities matter equally. Not all systems matter equally. Not all downtime hurts equally.

So the real questions are:

1️⃣ Which weaknesses create the fastest path to operational loss,

2️⃣ Which systems are mission essential,

3️⃣ Which dependencies create the biggest cascading consequences, and,

4️⃣ What can be deferred without increasing real-world risk?

That is what consequence based defense actually means.

VI. Reporting Discipline Is Now Part Of Operational Readiness

The coming CIRCIA regime makes this even harder. The Cybersecurity and Infrastructure Security Agency has said it expects the final rule in September, requiring substantial incidents to be reported within 72 hours and ransomware payments within 24 hours. That is not just a compliance shift. It is a readiness test.

Why? Because reporting does not happen in a calm environment. It happens while leadership is still trying to understand the event, stabilize operations, preserve evidence, manage communications, and determine whether the incident is local, sector-wide, criminal, geopolitical, or some combination of all four.

A realistic infrastructure decision cycle now has to handle:

1️⃣ Event classification,

2️⃣ Operational stabilization,

3️⃣ Internal escalation,

4️⃣ External reporting, and,

5️⃣ Continuity execution

...at the same time.

That means organizations that still separate legal, cyber, operations, and executive decision-making into clean stovepipes are going to struggle badly when time compresses.

VII. The Real Divide Is Between Organizations That Can Operate While Hurt And Those That Cannot

This is the point many leaders still resist. The biggest difference in the next round of infrastructure disruption will not be which organization bought the most tools. It will be which organization designed itself to keep functioning while trust is degraded.

That requires a harder set of internal questions:

1️⃣ What is our minimum viable operation,

2️⃣ What services absolutely must stay live,

3️⃣ Which manual workarounds are real rather than theoretical,

4️⃣ Which third parties can fail without collapsing us, and,

5️⃣ Who has decision authority when continuity and reporting pressures collide?

Canada's cyber leadership framed a version of this at Black Hat by describing work around what government services must still exist during extreme disruption, even in a scenario involving prolonged loss of internet access. That logic applies directly to infrastructure. Every serious operator now needs its own version of a minimum viable port, minimum viable utility, minimum viable transit authority, or minimum viable health network.

VIII. Thought-Provoking Close: The Final Assessment

The breach is no longer the real shock. The real shock is when an organization discovers, under pressure, that it:

1️⃣ Cannot keep operating,

2️⃣ Cannot identify what matters fastest,

3️⃣ Cannot trust key dependencies,

4️⃣ Cannot separate disruption from strategic threat, and,

5️⃣ Cannot move quickly enough to preserve continuity and meet reporting obligations.

That is why the title holds.

Assume the Breach. Keep the Harbor Open.

The last article said the war begins before the first shot. This one completes the logic. Once that reality is accepted, continuity becomes the command priority.

So the operating standard is clear:

1️⃣ Assume compromise,

2️⃣ Reduce harm,

3️⃣ Preserve continuity,

4️⃣ Maintain essential functions, and,

5️⃣ Keep the harbor open.

✨ 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