Atlas Initiative for Critical Infrastructure

Strategy Essentials

# Cyber Security for Civil Infrastructure

Author: Gerald (Jerry) Buckwalter
Atlas International Director of Innovation and Strategy Essentials President

June 24, 2025

We are not prepared. We are not aware of how unprepared we are. We are not aware of the cost to prepare. We are not aware of how damaging our unpreparedness could be.

Cyber security is simply another risk management issue. When designing and building infrastructure, we are familiar with risk management trade-offs applied to materials selection, earthquake design, hurricane design, monitoring for infrastructure decay, and so forth. But infrastructure has new risks associated with the digital age. We design and build using digital tools. And most infrastructure systems are now controlled by, monitored by, and personalized by, digital equipment. And that equipment includes centralized computer systems, algorithms in the cloud, and devices at the edge (imbedded in the physical world at the point of user engagement).

Therefore, digital/cyber security is now an integral part of our risk management ecosystem. Military infrastructure is more secure than civil infrastructure. Warfighting systems are highly digital and highly secure – by necessity for national security reasons. So that mindset is applied more naturally to military infrastructure. And the Department of Defense (DoD) has the budget to cover the cost of that security. Civil infrastructure has not had the same imperative.

There are three criteria that should guide us in how we assess and plan for digital security:

1. **The Threats and Their Methods of Attack:** The threats are numerous, and preparation for zero-day attacks are difficult. National intelligence agencies, some Department of Energy Labs, and the DoD continue to protect us in this global cat and mouse game but can't share all the details with the civil sector. However, the Department of Homeland Security (DHS), and their Cybersecurity and Infrastructure Agency (CISA) component, has the responsibility to collect and share this information with all levels of government and all civil infrastructure

stakeholders. The U.S. must maintain and make this a vibrant on-going activity. Civil infrastructure stakeholders should become familiar with this database.

2. **The Consequence of an Attack:** We have become familiar with the typical action of hackers who penetrate our IT systems, hold our data hostage, and demand ransom payments for the release of that information. Most companies feel helpless, have not prepared with adequate backup systems, and pay the ransom – thereby fueling the profitable market for hacking. In addition, we are not hardening the digital devices in the operational technology (OT) systems associated with infrastructure. This leaves us vulnerable to hacking into our electrical grid, our water systems, and our electronically controlled transport systems.

3. **The Cost of Resilience Measures:** There is no silver bullet. Most civil engineering companies and public agencies have begun to create some IT redundancy so they can recover more quickly. Protective measures are used infrequently. This should be no surprise since protective measures can become prohibitively expensive, interfere with normal business systems, and must be updated as frequently as each new hacking vector is discovered. OT systems are predominantly part of the built environment and redesigning those involve repair and replacement activity which will disrupt existing services.

I have worked in, or for, the government (intelligence, defense, and civilian agencies) and the private sector (both the defense industrial base (DIB) and commercial companies). I witnessed the measures that the intelligence agencies, military components, and the DIB implemented to address the cyber threat. And I witnessed the lack of those measures in federal civil agencies, state and local governments, and civil engineering companies.

Historically, it was thought that this difference was justified. National security components of a country were the obvious and most frequent targets of cyber threats. Now, we know differently. Any criminal or nation-state actor can adversely impact the digital assets of banking, water, transportation, or energy. In doing so, they can cripple a country just as fast as digital degradation of our military systems. And with the advancements in AI, we have created a new cyber vector for them to attack.

Yet, the civil vs military digital security differences remain. To address this, civil engineers must close three primary gaps in our current approach.

- **Attention to Natural versus Manmade Threats:** Investments for long-term resilience have been limited and mostly directed to threats associated with earthquakes, climate change, extreme weather, and other natural challenges. The danger associated with manmade threats have been limited to hardening against bomb threats and active shooters. The threat associated with cyber threats have been culturally relegated to the federal government. But the solution will

need to be an all-of-government, an all-of-society, and an all-of-nations effort. It's a global problem and any point of weakness defeats us all.

- **Separation of IT versus OT:** We have relegated the responsibility of cyber security to our IT departments. Very few are thinking about the power switches in the grid, the valves in the water pipes, the electronic controls of our transit systems, and now the electronic controls of our electric vehicles. Those points of cyber penetration defy counting. And many devices are archaic since they are old. Fixing them is troublesome and expensive. They require the expertise of our operational systems people, not just our IT staff. Cyber-trained operational device expertise must become a new skill set.

- **Relationship Between Designers/Builders and Owners/Operators:** Design and build players want to deliver a quality piece of infrastructure within cost and on time. That's a big enough challenge. They have little time, and no incentive, to think about the cyber hardness or resilience level of that infrastructure. Owners and operators worry about it. They are blamed if the systems go down. But the systems have already been built and delivered, and they don't have trained staff to modify them. It's time for the design phase to include cyber security specifications mutually understood and agreed to by both parties.

The DHS has defined our nation's critical infrastructure elements, including Health Care and Public Health, Energy, Information Technology, Transportation Systems, Defense Industrial Base, Emergency Services, Government Facilities, Critical Manufacturing, Chemical, Dams, Nuclear Reactors, Materials and Waste, Water and Wastewater, Food and Agriculture, and Financial Services. Digital failures in any of them have enormous consequences for daily life. It's time to protect some of them and make all of them more resilient to cyber-attacks – which will demand more of our time, training, and money.

The risks are very high. Total protection is unaffordable and often impossible. Resilience is the answer. And resilience in the face of digital risks is the same as with physical risks – balanced measures of protection, graceful degradation, swift repair, rapid recovery, and systems reconstitution. As with all risk management considerations, the cost of resilience measures will need to be balanced with affordability for the ultimate users of the infrastructure – our citizens. However, I'm suggesting the balance point will change once we properly assess the danger.