MCX

CMAA
Construction Management Association of America

Member Communication Experience

America's Infrastructure Is Only As Strong As Its AI Governance

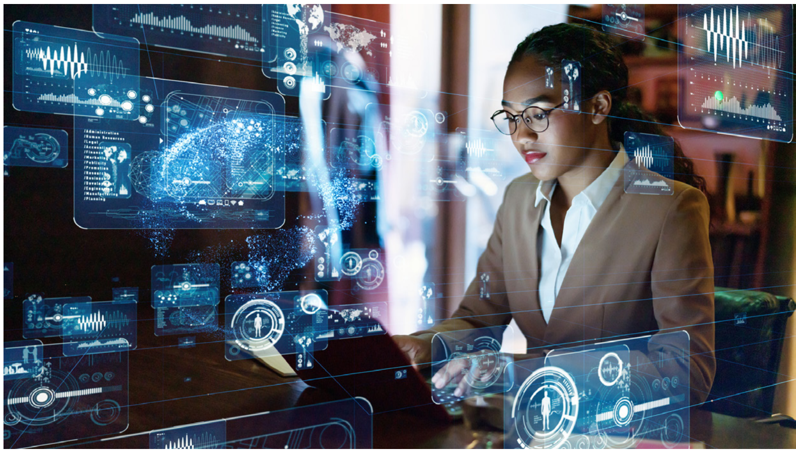
Written by: Lalitha Krishnamoorthy, Vice President, Artificial Intelligence and Digital, Stantec

America's civil infrastructure is at a pivotal moment. While the rise of artificial intelligence has introduced new challenges, it also brings powerful tools and fresh opportunities to strengthen our systems. Recent surges in cyberattacks have highlighted vulnerabilities, but have also galvanized leaders to innovate and adapt, so our infrastructure remains robust and secure. AI-enabled attacks have made absolute protection impossible, meaning internal digital policies and governance are all the more critical to minimize system vulnerabilities.

American utility owners have long recognized the challenges of maintaining and modernizing the nation's civil infrastructure systems. The highly exposed nature of electrical grids, water treatment facilities, and gas lines make them prime targets for attacks. Over the last decade, there have been hundreds of reported incidents of cybercriminals and foreign actors hacking into some of America's most vital infrastructure systems to wreak havoc and cause potential danger. Through August of 2024, cyberattacks on U.S. utilities surged by nearly 70% year over year.

AI has only proliferated more since then.

The advent of widespread, commercially available AI has created an entirely new headache for utility operators by dramatically lowering the technical savvy required to mount an attack. At the same time, utility operators now have access to advanced technologies that can both detect and defend against threats more effectively than ever before. So on one hand, hackers don't need in-depth knowledge anymore — just a ChatGPT subscription and a Wi-Fi connection. On the other hand, it is now possible for teams to respond swiftly and intelligently to emerging risks due to AI-assisted programs democratizing security.



UPDATING LEGACY SYSTEMS

Even the best protections and most advanced security systems can no longer defend against the scale of attack that AI enables. Deepfakes have proven quite capable of bypassing the knowledge-based authentication systems that banks and government agencies rely on, with the global financial sector reporting a 393% increase in deepfake-enabled phishing attacks in one year. If that's their effort against top-tier security systems, then imagine the vulnerability of the legacy systems more often used by civil infrastructure.

This shift means security teams must move from trying to eliminate every spark to making sure that, if something does ignite, its impact is contained and recovery is swift.

Part of that is done through using properly installed firewalls and fail-safe systems. When bad actors inevitably do gain access to a system, these walls can close off their point of entry. Just because one system is exposed doesn't mean the whole network of systems needs to go down with it.

Ironically, identifying a breach is where AI can actually help companies defend themselves. AI trained on the right usage data can leverage pattern recognition skills to detect anomalies and early warning signs of an attack. Odd or unusual user behavior, such as a user trying to access higher security information or making unusual changes to a system, can either alert IT teams or automatically isolate the affected area until security teams can assess the threat.

It's a time-intensive, though worthwhile, security upgrade civil infrastructure teams can make. In the era of sensors and IoT systems, infrastructure's digital footprint has expanded enormously — and with every expansion comes an increase of vulnerability. Having the ability to isolate each component is like having a gate valve on a leaking pipe; water can be shut off to the affected pipe before flooding causes even more damage.

AI GOVERNANCE AND THE ROLE OF EMPLOYEES

Even before an attack, improved governance and more diligent digital policies can limit the risk an organization faces. As much as limiting exposure for companies means creating internal firewalls and emergency shut-offs, it also means training and upskilling their workforce on data hygiene and AI use, including prompt engineering, detecting AI-generated phishing attempts, and secure model deployment practices.

Having a workforce that understands what AI is (and what it isn't) is vital to using AI correctly and safely. Adopting frameworks like the NIST AI Risk Management Framework and conducting regular audits supports compliance and builds a culture of trust.

One of the most prominent threats organizations face as a result of AI isn't a traditional attack per se, but rather an accidental data breach — one caused by lax policies and employee awareness. An analysis by the House Committee on Homeland Security estimated that one in 10 intrusions the U.S. faced in 2023 were due to improper access to credentials rather than any complex hack.

AI creates even greater potential for this sort of opportunistic breach as workers use large language models for their day-to-day tasks. Without clear policies governing AI use, the risk that sensitive data will be shared with a third-party source is significant. Workers may have little understanding of what's happening with that data and how it could be used in the future to make the system more vulnerable. All it takes is the wrong data being pasted into a large language processor for highly sensitive information to become exposed.

Organizations need to focus on reducing damage and recovering more quickly when attacks occur. Figuring out how to integrate technologies such as voice recognition, deepfake detection, and biometric recognition will be an essential part of creating safer infrastructure systems. Incorporating robust testing, continuous monitoring, and clear guidelines for responsible use will aid these technologies in enhancing security rather than introducing new vulnerabilities.

It's not that AI shouldn't be used in civil infrastructure. But understanding the risks to data privacy and the new vulnerabilities any new technology systems create is critical to understanding the risk. As crucial as updating legacy systems to modern standards is, minimizing the impact of human error when interacting with AI is equally vital.

The path forward is clear: When we embrace innovation, invest in people, and foster a culture of proactive governance, America's infrastructure can not only withstand today's threats, but thrive in tomorrow's opportunities.

About the Author

Lalitha Krishnamoorthy is vice president of AI and digital at Edmonton, Canada-based global engineering, architecture, and environmental consultancy Stantec.

About the Article

Republished from Construction Dive online. Construction Dive is a leading industry publication operated by Industry Dive. Their business journalists spark ideas and shape agendas for 10+ million decision makers in the most competitive industries. The daily email newsletter and website cover topics such as commercial building, residential building, green building, design, deals, regulations, and more.

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.