CYBERSECURITY CHALLENGES: ARE TRANSPORTATION AGENCIES READY?

The fundamental role of executives and senior managers of state departments of transportation (DOTs), transit agencies, and other transportation-related organizations, is the management of assets to fulfill the public-service mission of providing safe and secure modes of transportation. This includes managing their agency's prevention of, response to and recovery from a major emergency, event, or disaster involving transportation systems and operational technology (OT).

In the first decades of the 21st Century the disruptive and sweeping change resulting from the rapid adoption of innovative digital technologies in all sectors of the economy has extended into the realm of transportation. The profound impact of emerging, advanced transportation technologies has created both revolutionary opportunities and existential threats, prompting the need for transportation-sector leaders to re-examine the capabilities required to support their fundamental roles.

The adoption of the new tools of OT and IT hold the promise of vast benefits to both the general public using the transportation networks and systems and to the leaders that manage them. However, it has also given rise to new and frightening levels of public danger in the form of cybersecurity risk and threats to the OT and IT systems upon which transportation-sector leaders now rely.

The current era of ongoing technological advances has been characterized as "a never-ending, escalating competition between developers and users of systems that employ cyber technology and those who seek to do harm. Each generation of cybersecurity solutions is countered by ever-more sophisticated threats; each potential threat spawns additional layers of defense. This Darwinian struggle takes place around the clock and around the globe, involving many thousands of adversaries targeting millions of cyber-components."

As managers and guardians of vital infrastructure, public trust demands that transportation-related organizations meet the critical risks posed by ongoing cybersecurity threats. Whether perpetrated by an individual, a local group, or a foreign power, and regardless of whether a transportation system is the intended target or an unfortunate bystander, cybersecurity attacks can severely undermine the integrity of public transportation infrastructure and systems. Beyond the possibility of substantial loss of life and injury, such attacks can have catastrophic consequences for economic activity, transportation, mobility and communication networks, and public confidence in the ability of public entities to maintain safety, order and rule of law. Such threats are existential, immediate and persistent and can come from virtually anywhere in the world.

The necessity for transportation agencies to immediately adopt effective mitigation policies to protect critical infrastructure is clear and absolute. They need the right tools and guidance to help them assess, classify, and respond to cybersecurity risks with respect to incident prevention, response and recovery. But while substantial emphasis has been given to the protection of IT systems against such threats, less guidance has been devoted to the risks to OT and to the equipment and protecting transportation business operations. Transportation leaders need more information and guidance around how they can prevent such incidents affecting OT, what to do when they occur, and how to recover.

Global Dynamic Group, LLC
40 Wall Street, 28th Floor
New York, NY 10005

GDG

+1 (347) 767-5453
info@GDGIoT.com
www.GDGIoT.com