INFRASTRUCTURE ASSET MANAGEMENT

Defending Critical Public Infrastructure Against New & Evolving Security Threats

How infrastructure owners and operators can strengthen cybersecurity and reduce their vulnerability to cyber attacks

Trimble

Managing risk is nothing new. But a new breed of risk requires more sophisticated approaches.

As an infrastructure owner or operator, you know that critical infrastructure systems are inherently vulnerable to security threats.

You're no stranger to having a plan in place for traditional incidents, like vandalism, structural failures, and natural disasters.

And you're probably all too familiar with the risks these threats present to operations, safety, security, and the environment—not to mention their financial implications.

While managing risk may be nothing new when you're responsible for the safe and uninterrupted operation of public infrastructure assets, new threats have emerged. And they require new approaches.

The threats you must defend against now extend beyond the physical world to the digital.

At the same time, the risks and vulnerabilities that must be proactively and preventatively managed have expanded as well, and in many cases, the stakes are even higher.

You can't disregard that your customers are typical consumers. They've grown to expect that everything from shopping to banking to their interactions with public works providers and government agencies should be both convenient and highly secure.

In today's digital world, secure means cybersecure

The reality is that today's consumers expect all of the entities they interact with to employ current cybersecurity best practices—including yours. If your cybersecurity practices are found to be flimsy, whether through a major breach or a minor inconvenience, you've compromised, if not already lost, the public's trust.

Read on to learn more about these new threats and how you can strengthen the cybersecurity of your critical infrastructure assets.

40%

increase in cyber attacks against the government and public services sector from 1Q23 to 2Q23

Source: BlackBerry Global Threat Intelligence Report, Aug 2023

80%

of critical infrastructure organizations were targeted by ransomware attacks in 2021 alone

Source: "The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption," Claroty, Feb 2022

TOP 4 CYBER TARGET

critical infrastructure is the fourth most popular cyber risk target

Source: BlackBerry Global Threat Intelligence Report, Aug 2023

Trimble

Cybersecurity: Defending critical infrastructure against the rising threat of cyber attack

Technological advances like IoT devices that require the intersection of physical and digital systems have increased the safety, efficiency, and reliability of infrastructure operations. But they've also introduced new security threat vectors.

As our critical infrastructure systems have become increasingly reliant on complex and interconnected digital systems for operations, they've also become attractive targets to cyber criminals.

For bad actors who are politically, financially, or otherwise motivated, the government and public sector systems—particularly those that host sensitive data—provide unique opportunities to profit or wreak havoc.

Motivated cyber criminals aren't your run-of-the-mill petty thieves either. They know that the systems behind infrastructure assets are often interlinked. And they're banking on the probability that a single breach will quickly spread and have widespread impact.

If the security of even one of your assets is compromised, it can create a ripple effect of negative waves across other critical systems—and disrupt the everyday lives of the citizens who rely on them.

Preparing for and defending against these threats must be a top priority for critical public works owners and operators.

5 Types of Cyber Attack that Threaten Critical Infrastructure

Gaining a thorough understanding of the threats and risks you face is the first step to building an effective defense against them. Here are the top types of cybersecurity attacks public works owners and operators need to defend against.

1. Ransomware

Ransomware is a type of malware, which is the most popular form of cyber attack. It "infects" or blocks access to the victim's data, files, or entire systems unless a ransom is paid. While financially motivated, ransomware attacks can also wreak havoc on critical system operations. The Colonial Pipeline incident in May 2021 is an example of a ransomware attack that forced a shutdown of operations and set off a domino effect across the petroleum and transportation sectors, delaying fuel deliveries, creating jet fuel shortages, and inciting panic at the gas pump.

2. Phishing

One of the most effective cyber attack methods, phishing is a type of social engineering attack, typically conducted by email or text. Phishing messages appear to come from a known or trusted sender, making it easier to trick the victim into providing sensitive data (like login credentials or account information) or unwittingly clicking a malware link.

3. Distributed Denial of Service (DDoS) Attacks

A DDoS attack disrupts access to a digital property, such as a website, server, or network, by flooding it with traffic and overwhelming it. An example is the attack waged by the Russian hacking group Killnet in October 2022, which temporarily shut down access to major U.S. airport web sites, including LAX, ATL, and ORD, causing public outcry. Interconnected systems and IoT devices that aren't properly secured are also particularly susceptible to DDoS attacks.

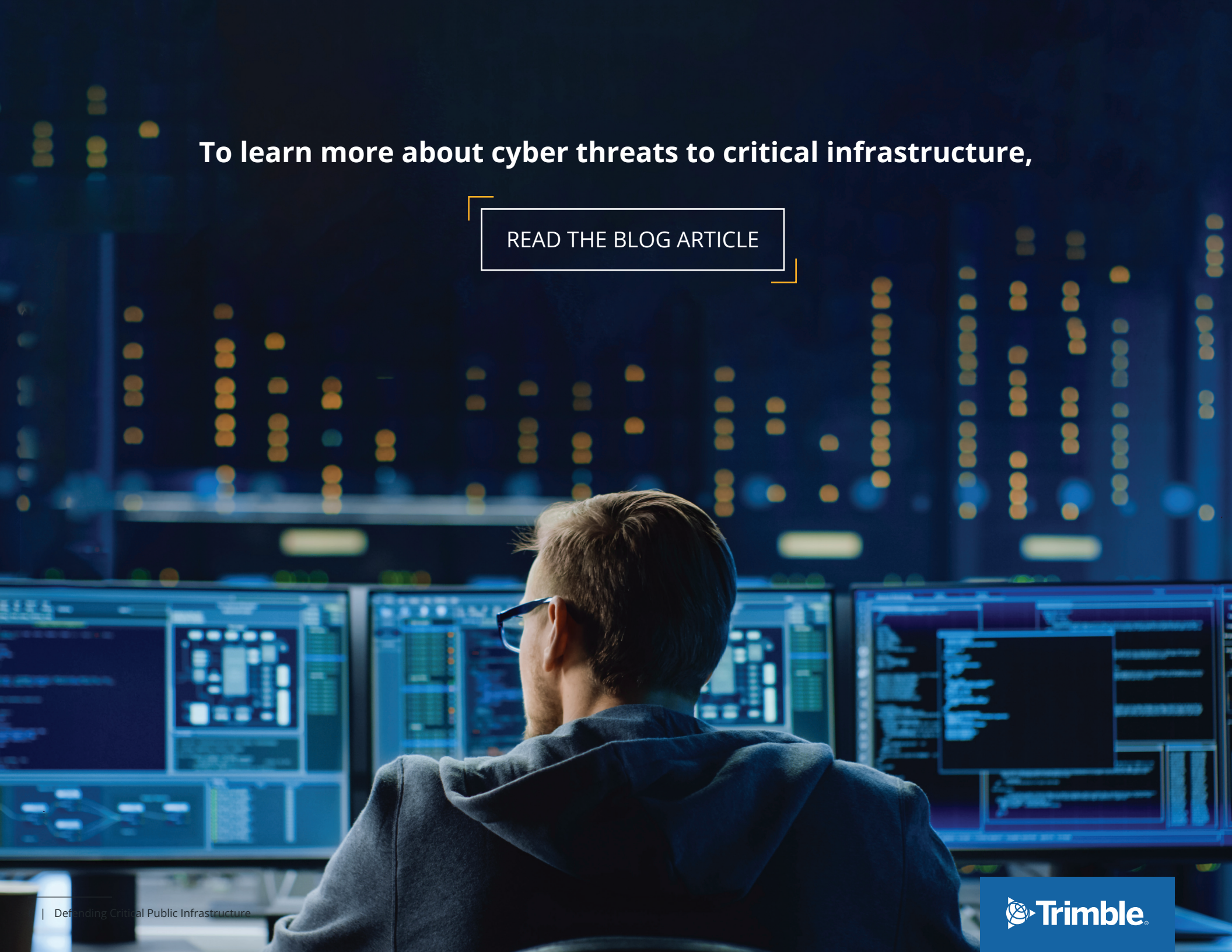
4. Supply Chain Attacks

Growing in popularity, supply chain attacks occur when an attacker infiltrates a third-party supplier, typically preying on software vulnerabilities, to gain access to the supplier's partners or disrupt the supply chain. As private owners and operators—as well as services like Amazon Web Services—are increasingly involved in critical infrastructure, the entry points for a supply chain attack have grown exponentially.

5. Insider Attacks

An insider attack is defined as the use of authorized access by a trusted insider, such as an employee, contractor, or vendor, to do harm, whether intentionally or innocently. Because they can be motivated by malicious intentions or happen by accident or negligence, insider attacks can be especially difficult to detect.

Trimble


To learn more about cyber threats to critical infrastructure,
READ THE BLOG ARTICLE