# State of Cybersecurity in Arizona

## A Collective Defense Approach

**Ryan Murray**
Deputy Director
Arizona Department of Homeland Security

Interim Chief Information Security Officer for the State of Arizona

**Mission:**
Protect Arizona by providing strategic direction and access to resources that will enable all of the State’s stakeholders to achieve our collective goals protecting the Homeland.

**Statewide Information Security and Privacy Office** which functions as the strategic planning, facilitation, and coordination office for cybersecurity in this state.

# \\The Threats and Vulnerabilities

# National Concern

In recent months, we’ve heard from the top cybersecurity agencies at the federal level, speaking of threats to our critical infrastructure.

Nation State threat actors have been identified as having “deep access into critical infrastructure” - pre-positioning themselves for the early stages of a conflict with the US

Our federal partners at CISA have recently found and eradicated intrusions in multiple sectors including: aviation, water, energy, and **transportation**.

# Nation-State Threats

(Photo by Kevin Dietsch/Getty Images)

“In the event of a conflict China will almost certainly use aggressive cyber operations to go after our critical infrastructure, to go after our pipelines and rail lines, to delay military deployment and to induce societal panic”

This is a world where a major conflict halfway around the globe might well endanger the American people here at home through the disruption of our gas pipelines; the pollution of our water facilities; the severing of our telecommunications; the crippling of our transportation systems—all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will.

# Risk 4: Cybersecurity Threats

As the transportation and logistics industry increasingly relies on digital tools and platforms for operations, it becomes more exposed to cybersecurity threats. From GPS systems to cargo tracking software, the digital landscape offers efficiency but also opens doors to potential cyber-attacks.

## Impact

1. **Data Breaches**: Hackers can access sensitive information, including customer details, shipment data, and financial records. This not only compromises privacy but can also lead to financial losses and damage to reputation.
2. **Disruption of Operations**: Cyber-attacks can halt operations by targeting software systems, causing delays, and affecting the timely delivery of goods and services.
3. **Potential for Sabotage**: In extreme cases, malicious actors might not just steal data but also sabotage operations. This could be by altering shipment details, rerouting goods, or even causing physical harm through the manipulation of digital controls.

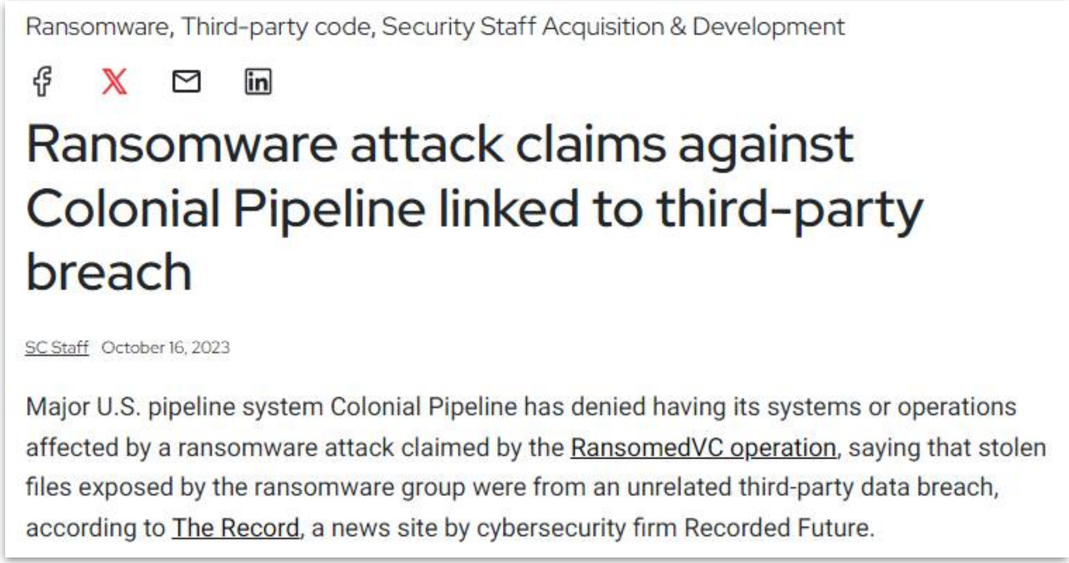
https://safetyiq.com/insight/the-top-5-risks-in-the-transportation-and-logistics-industry/

## Types of Cyber Security Threats in Transportation

QC
Quality Carriers

- Ransomware Attacks
- Supply Chain Compromises
- Unauthorized Access to Control Systems
- Data Breaches

https://qualitycarriers.com/company-news/understanding-cyber-security-threats-and-risk-factors-in-the-transportation-sector/

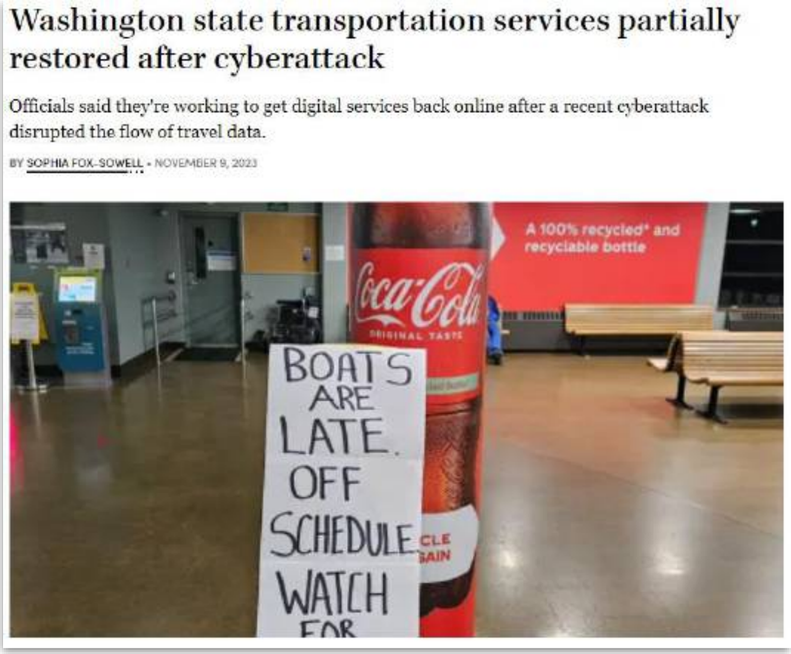


Ransomware, Third-party code, Security Staff Acquisition & Development

## Ransomware attack claims against Colonial Pipeline linked to third-party breach

SC Staff October 16, 2023

Major U.S. pipeline system Colonial Pipeline has denied having its systems or operations affected by a ransomware attack claimed by the RansomedVC operation, saying that stolen files exposed by the ransomware group were from an unrelated third-party data breach, according to The Record, a news site by cybersecurity firm Recorded Future.

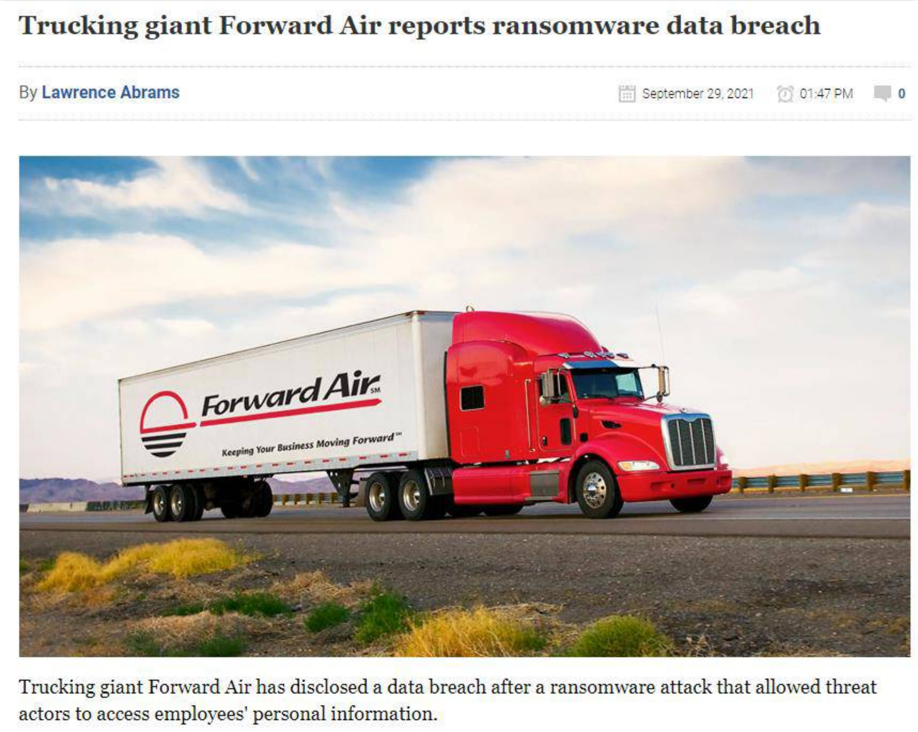


## Washington state transportation services partially restored after cyberattack

Officials said they're working to get digital services back online after a recent cyberattack disrupted the flow of travel data.

BY SOPHIA FOX-SOWELL • NOVEMBER 9, 2023

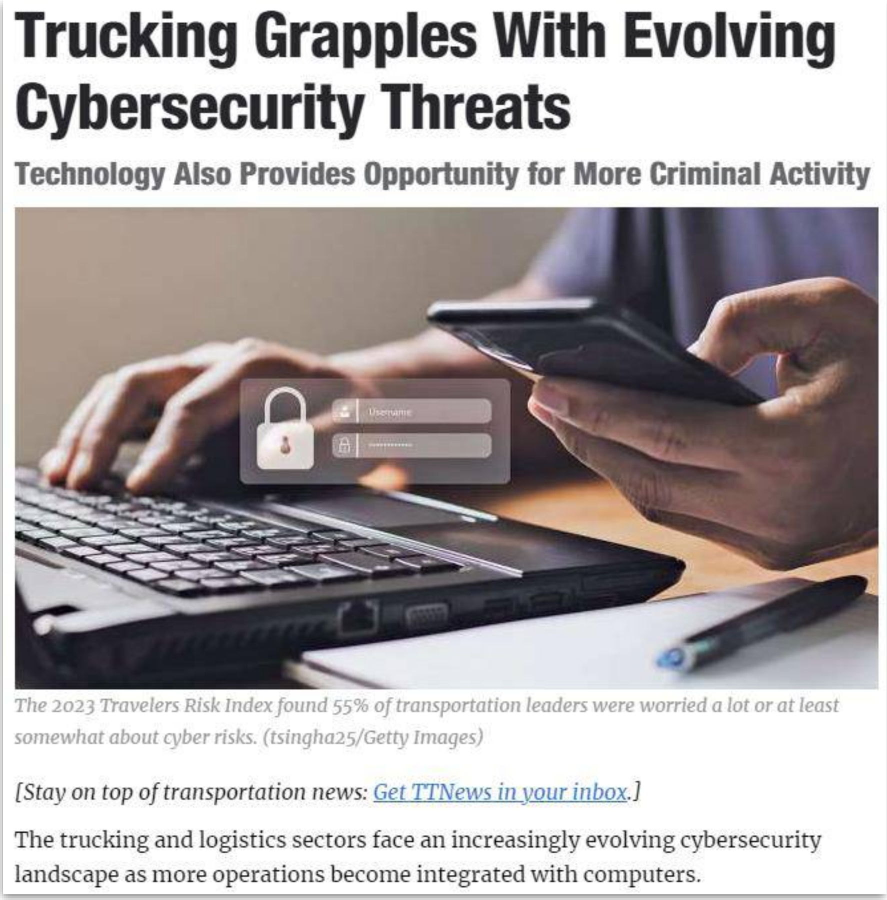
A 100% recycled* and recyclable bottle
Coca-Cola
ORIGINAL TASTE
BOATS ARE LATE. OFF SCHEDULE WATCH FOR



## Trucking giant Forward Air reports ransomware data breach

By Lawrence Abrams September 29, 2021 01:47 PM 0

Trucking giant Forward Air has disclosed a data breach after a ransomware attack that allowed threat actors to access employees' personal information.



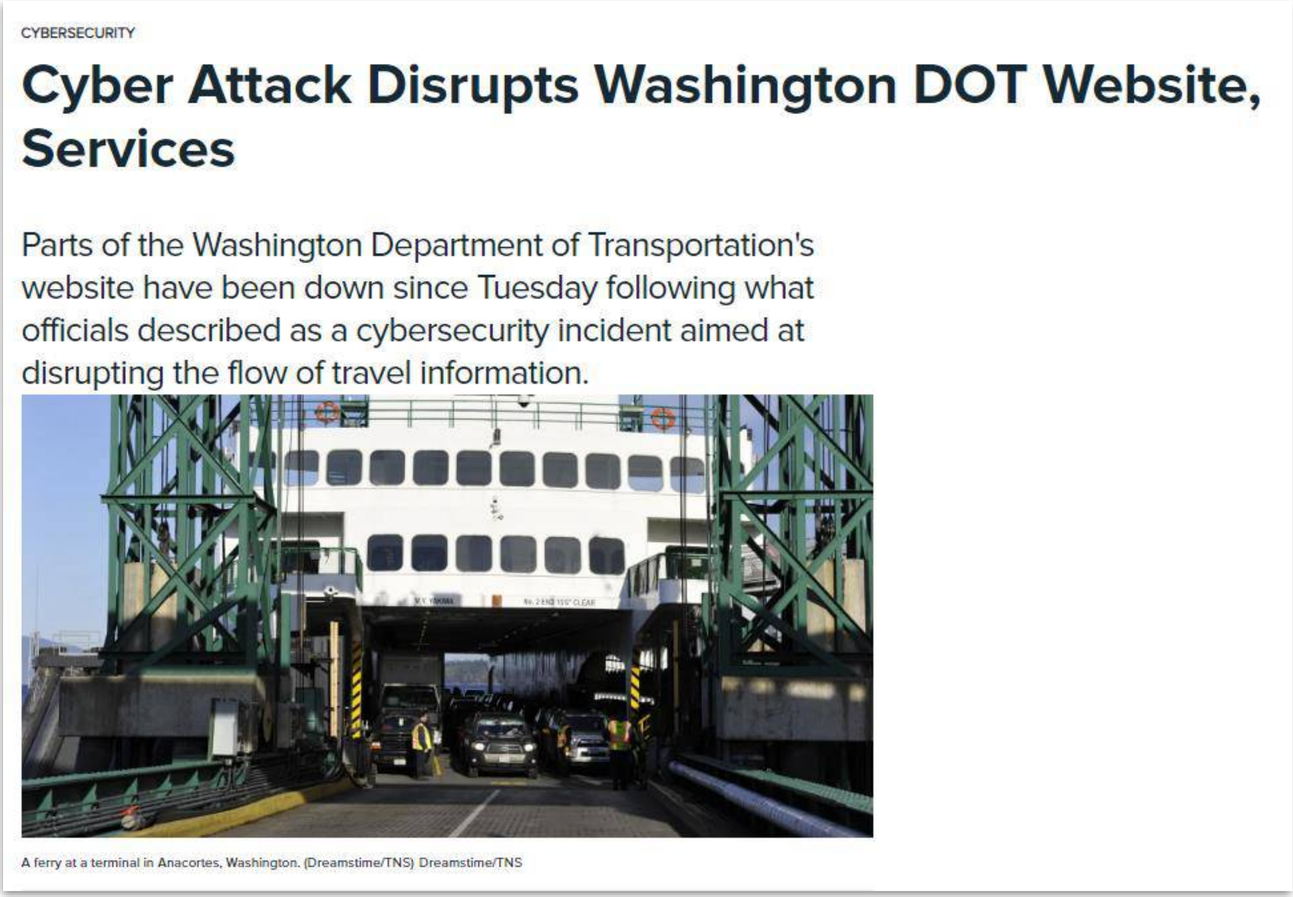
# Trucking Grapples With Evolving Cybersecurity Threats

## Technology Also Provides Opportunity for More Criminal Activity

*The 2023 Travelers Risk Index found 55% of transportation leaders were worried a lot or at least somewhat about cyber risks. (tsingha25/Getty Images)*

*[Stay on top of transportation news: Get TTNews in your inbox.]*

The trucking and logistics sectors face an increasingly evolving cybersecurity landscape as more operations become integrated with computers.

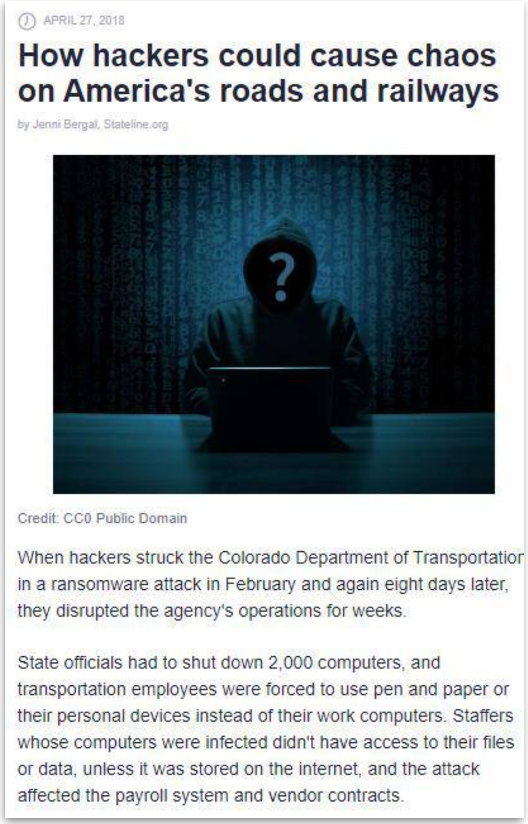


CYBERSECURITY

# Cyber Attack Disrupts Washington DOT Website, Services

Parts of the Washington Department of Transportation's website have been down since Tuesday following what officials described as a cybersecurity incident aimed at disrupting the flow of travel information.

A ferry at a terminal in Anacortes, Washington. (Dreamstime/TNS) Dreamstime/TNS



APRIL 27, 2018

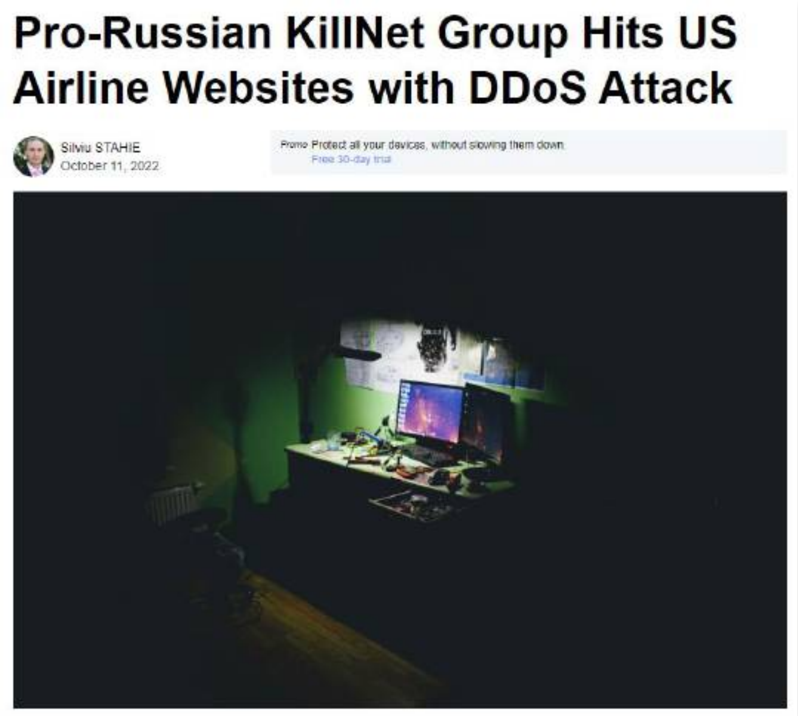
# How hackers could cause chaos on America's roads and railways

by Jenni Bergal, Stateline.org

Credit: CC0 Public Domain

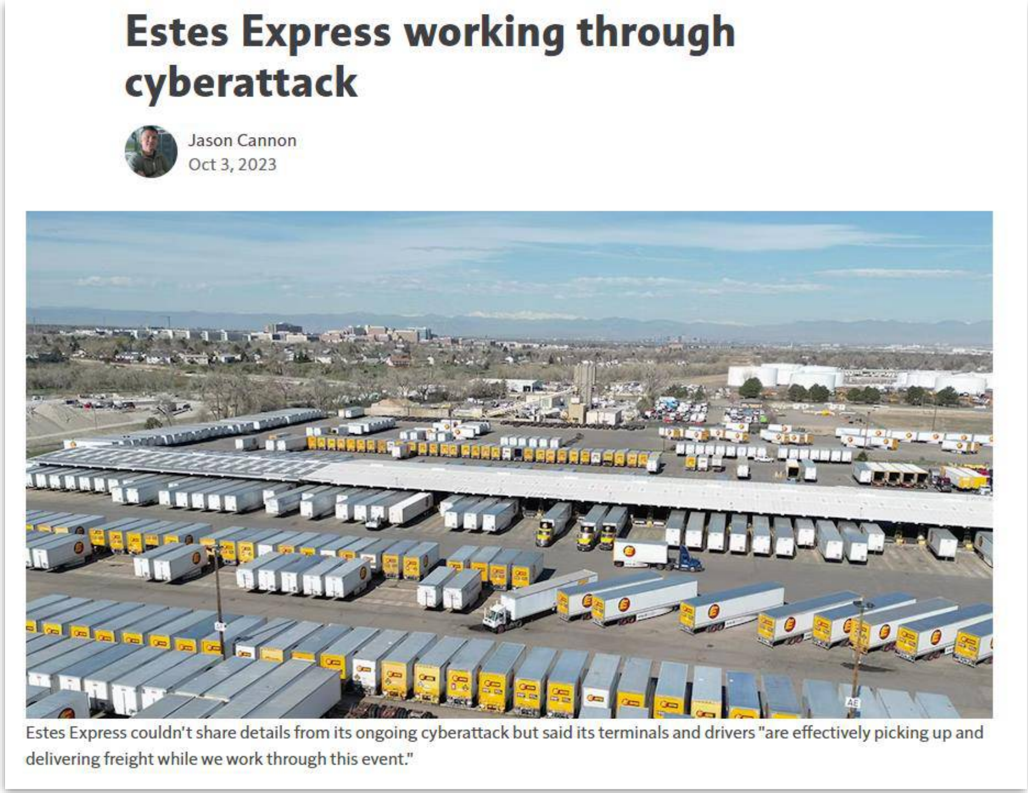
When hackers struck the Colorado Department of Transportatior in a ransomware attack in February and again eight days later, they disrupted the agency's operations for weeks.

State officials had to shut down 2,000 computers, and transportation employees were forced to use pen and paper or their personal devices instead of their work computers. Staffers whose computers were infected didn't have access to their files or data, unless it was stored on the internet, and the attack affected the payroll system and vendor contracts.



## Pro-Russian KillNet Group Hits US Airline Websites with DDoS Attack

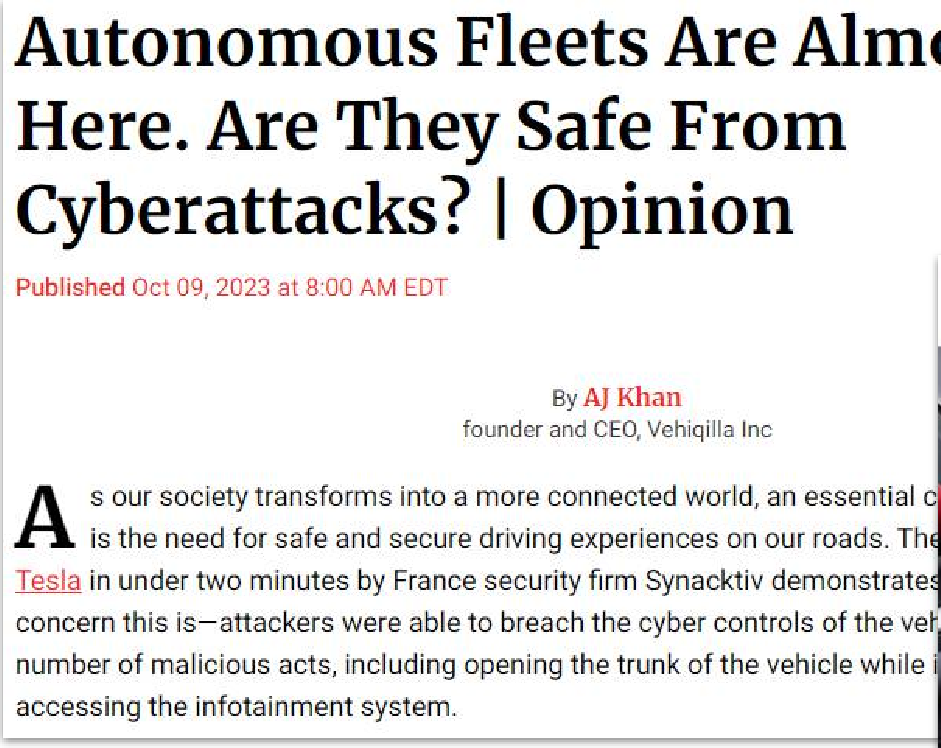
Silviu STAHIE
October 11, 2022



## Estes Express working through cyberattack

Jason Cannon
Oct 3, 2023

Estes Express couldn't share details from its ongoing cyberattack but said its terminals and drivers "are effectively picking up and delivering freight while we work through this event."

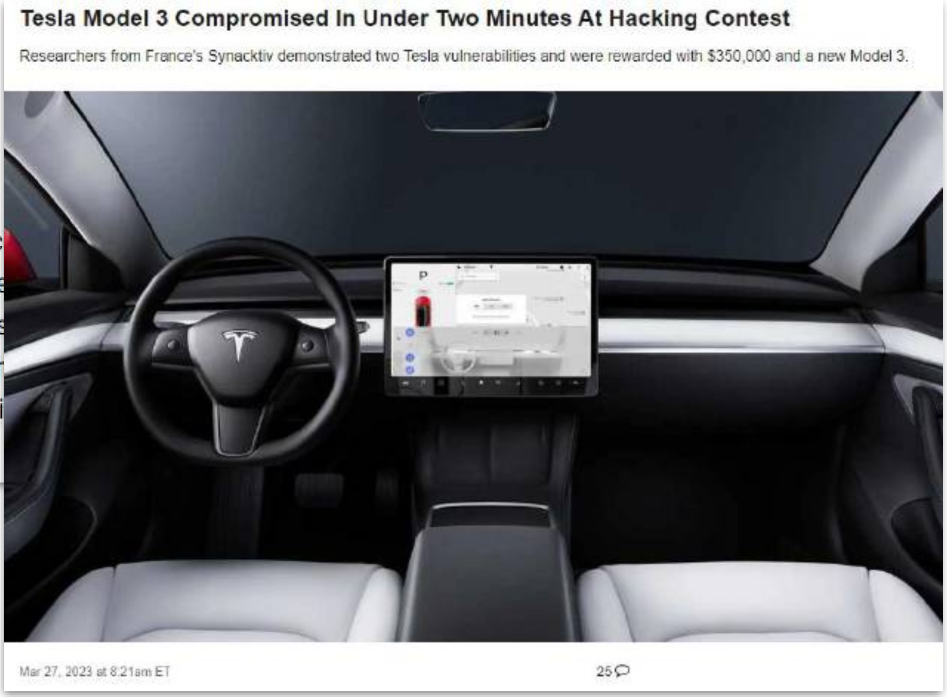


# Autonomous Fleets Are Almost Here. Are They Safe From Cyberattacks? | Opinion

Published Oct 09, 2023 at 8:00 AM EDT

By AJ Khan
founder and CEO, Vehiqilla Inc

As our society transforms into a more connected world, an essential c
is the need for safe and secure driving experiences on our roads. The
Tesla in under two minutes by France security firm Synacktiv demonstrates
concern this is—attackers were able to breach the cyber controls of the veh
number of malicious acts, including opening the trunk of the vehicle while i
accessing the infotainment system.



## Tesla Model 3 Compromised In Under Two Minutes At Hacking Contest

Researchers from France's Synacktiv demonstrated two Tesla vulnerabilities and were rewarded with $350,000 and a new Model 3.

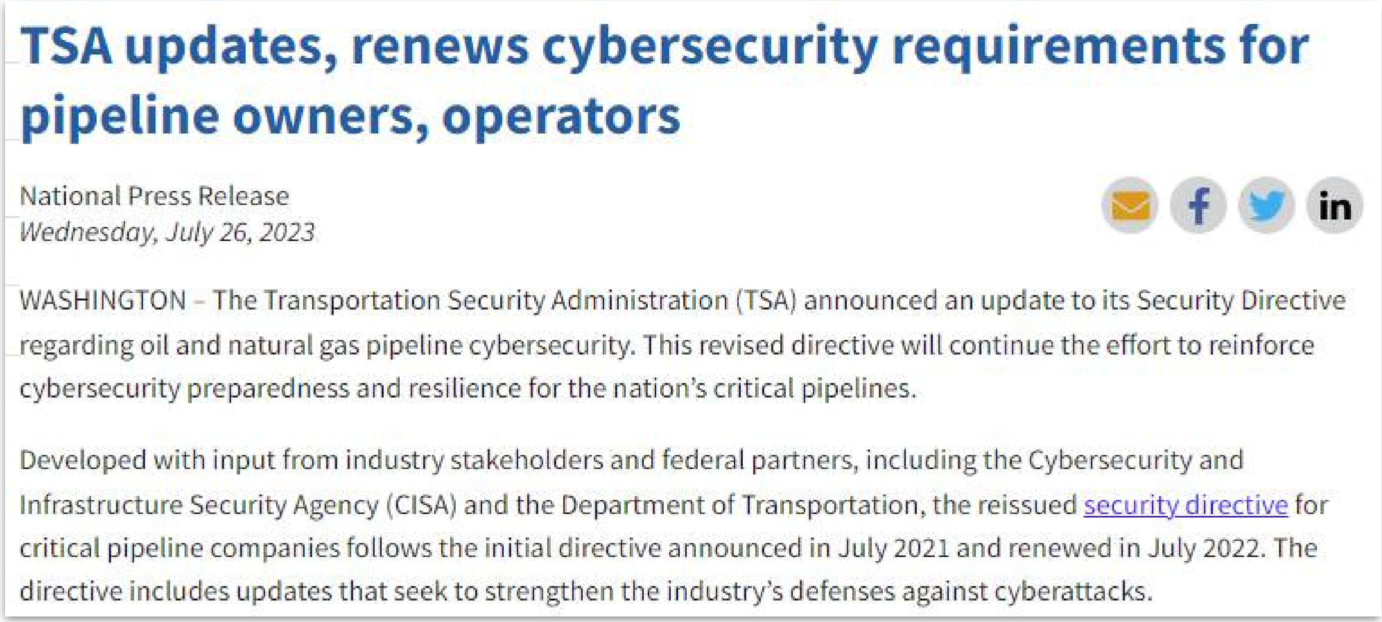
Mar 27, 2023 at 8:21am ET

25

ARIZONA COUNTER TERRORISM
ACTIC
INFORMATION CENTER
GREAT SEAL OF THE STATE OF ARIZONA
DITAT DEUS
1912
ARIZONA INFORMATION SHARING
AND ANALYSIS CENTER

# \\Our Response - Collective Defense

TRANSPORTATION SECURITY ADMINISTRATION
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEPARTMENT OF PUBLIC SAFETY
GREAT SEAL OF THE STATE OF ARIZONA
DITAT DEUS
1912
STATE TROOPER
ARIZONA
Arizona Department of Emergency and Military Affairs



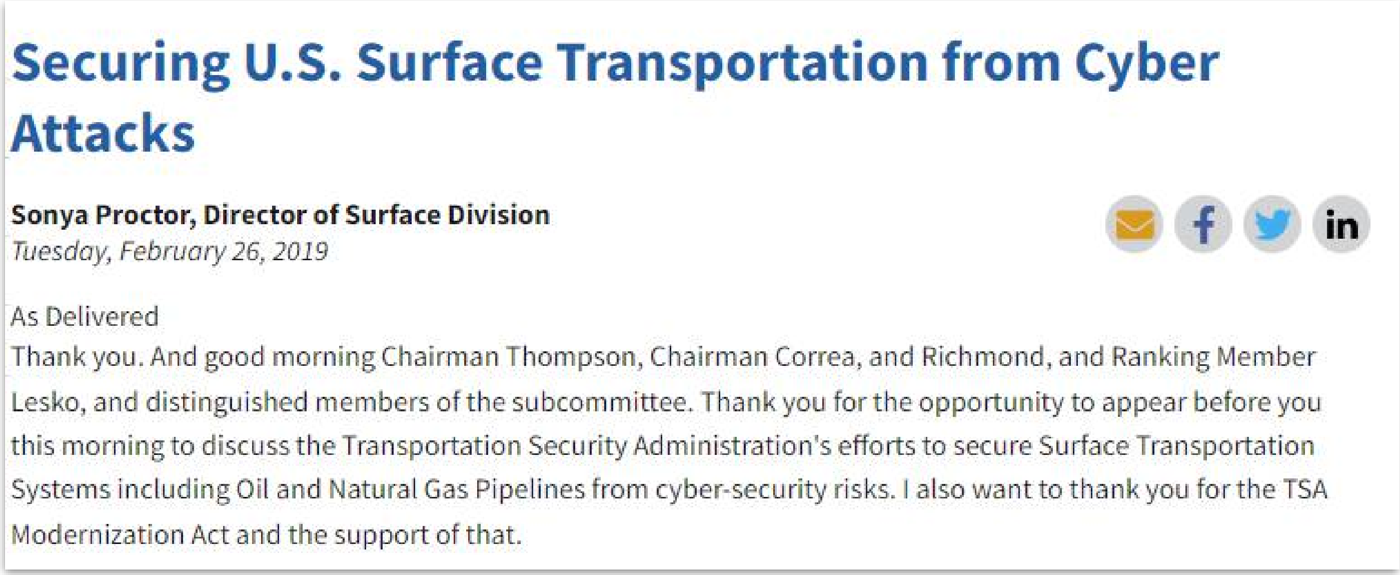
# TSA updates, renews cybersecurity requirements for pipeline owners, operators

National Press Release
*Wednesday, July 26, 2023*

WASHINGTON – The Transportation Security Administration (TSA) announced an update to its Security Directive regarding oil and natural gas pipeline cybersecurity. This revised directive will continue the effort to reinforce cybersecurity preparedness and resilience for the nation's critical pipelines.

Developed with input from industry stakeholders and federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Transportation, the reissued security directive for critical pipeline companies follows the initial directive announced in July 2021 and renewed in July 2022. The directive includes updates that seek to strengthen the industry's defenses against cyberattacks.

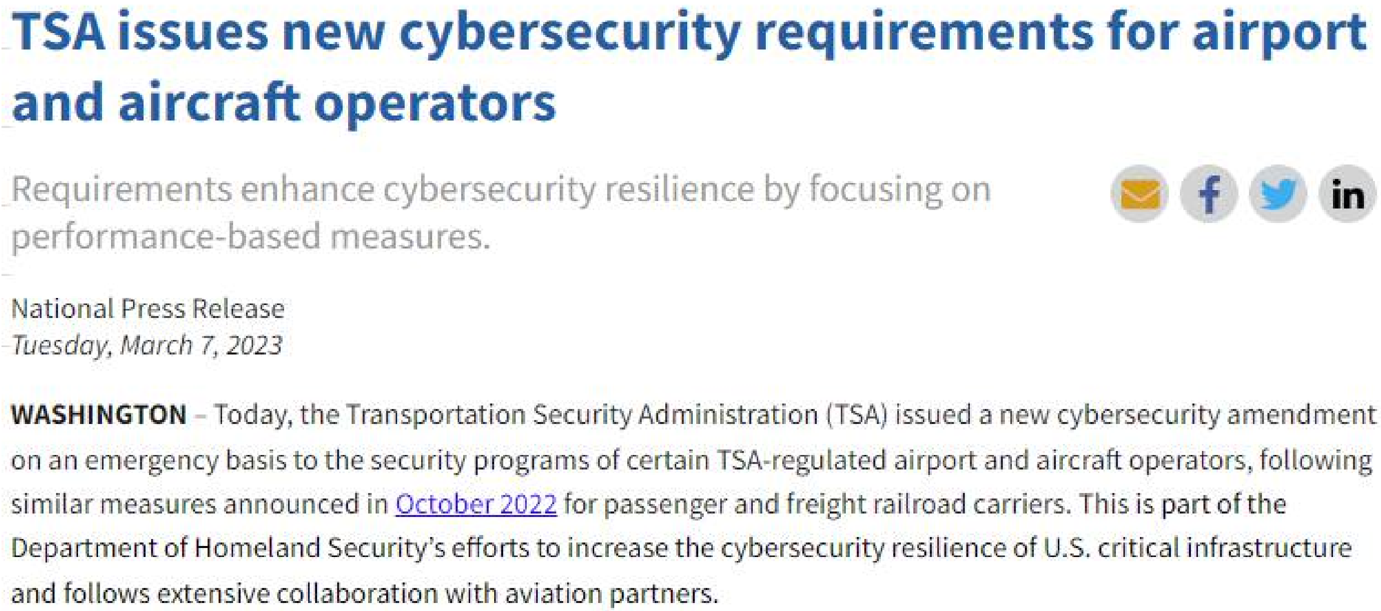
https://www.tsa.gov/news/press/releases/2023/07/26/tsa-updates-renews-cybersecurity-requirements-pipeline-owners



# Securing U.S. Surface Transportation from Cyber Attacks

**Sonya Proctor, Director of Surface Division**
*Tuesday, February 26, 2019*

As Delivered
Thank you. And good morning Chairman Thompson, Chairman Correa, and Richmond, and Ranking Member Lesko, and distinguished members of the subcommittee. Thank you for the opportunity to appear before you this morning to discuss the Transportation Security Administration's efforts to secure Surface Transportation Systems including Oil and Natural Gas Pipelines from cyber-security risks. I also want to thank you for the TSA Modernization Act and the support of that.

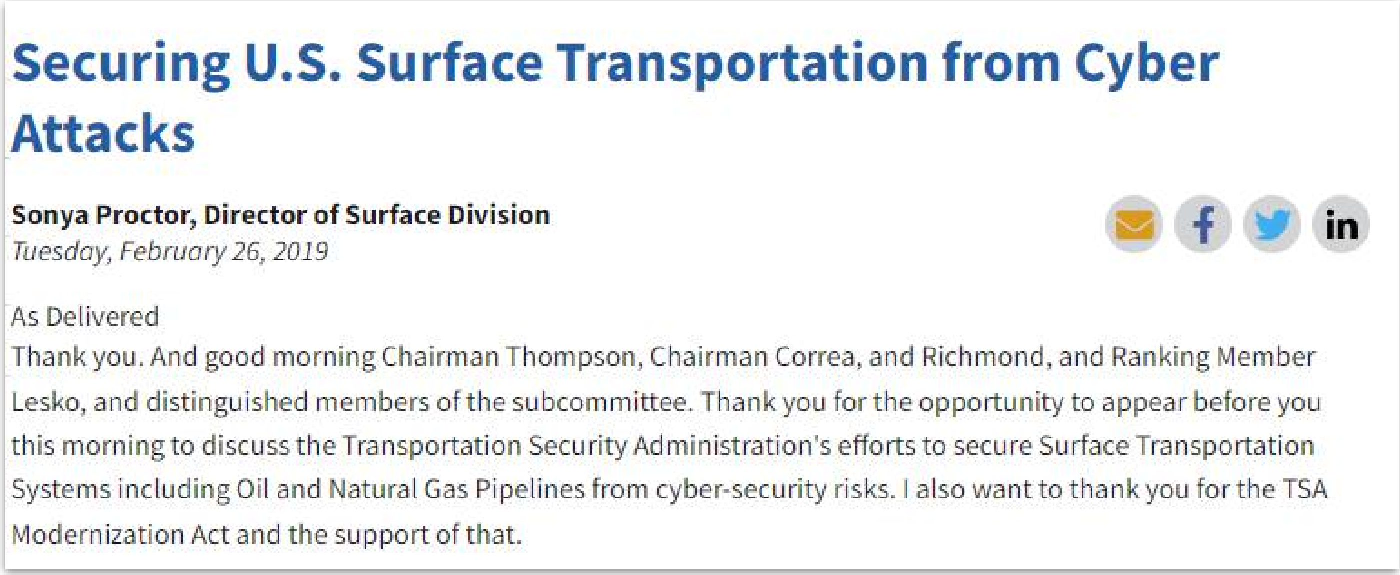


# TSA issues new cybersecurity requirements for airport and aircraft operators

Requirements enhance cybersecurity resilience by focusing on performance-based measures.

National Press Release
*Tuesday, March 7, 2023*

**WASHINGTON** – Today, the Transportation Security Administration (TSA) issued a new cybersecurity amendment on an emergency basis to the security programs of certain TSA-regulated airport and aircraft operators, following similar measures announced in October 2022 for passenger and freight railroad carriers. This is part of the Department of Homeland Security's efforts to increase the cybersecurity resilience of U.S. critical infrastructure and follows extensive collaboration with aviation partners.



# Securing U.S. Surface Transportation from Cyber Attacks

**Sonya Proctor, Director of Surface Division**
*Tuesday, February 26, 2019*

As Delivered
Thank you. And good morning Chairman Thompson, Chairman Correa, and Richmond, and Ranking Member Lesko, and distinguished members of the subcommittee. Thank you for the opportunity to appear before you this morning to discuss the Transportation Security Administration's efforts to secure Surface Transportation Systems including Oil and Natural Gas Pipelines from cyber-security risks. I also want to thank you for the TSA Modernization Act and the support of that.

1. **Report** Cyber Incidents
2. **Establish a relationship** with their local CISA team and State and Local Partners
3. **Use the services** available to drive necessary investment in cyber hygiene, including throughout their supply chains
4. Double down on their **commitment to resilience**
5. Finally, every technology manufacturer must build, test, and ship products that are **secure by design.**

# Whole-of-State Cybersecurity

| | | | |
|---|---|---|---|
| Cyber Command | AZ-ISAC | Cyber Joint Task Force | Statewide Cyber Readiness Program |

# Critical Partners

AZ DoHS Cyber Command has several critical partners that provide and assist with complementary services to help conduct our essential functions across our whole-of-state cybersecurity mission.

**Arizona Information Sharing and Analysis Center (AZ-ISAC)**

**Department of of Emergency and Military Affairs(DEMA) Cyber Joint Task Force**

# Cyber Command Center/ ACTIC Integration

# Statewide Cyber Readiness Program

- Anti-Phishing / Security Awareness Training(SAT)
- Advanced Endpoint Protection/EDR (AEP)
- Multi-Factor Authentication/IDAM (MFA)
- Web Application Firewall (WAF)
- Converged Endpoint Management (XEM)
- Security Assessments

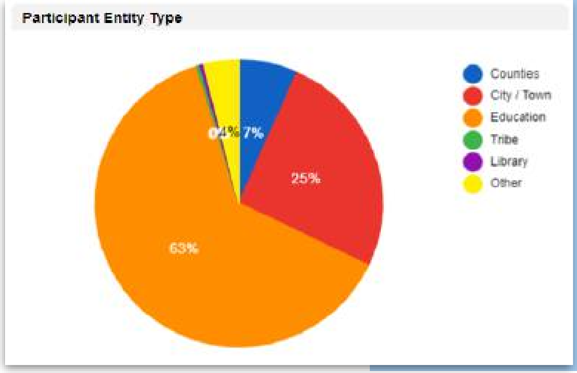
https://azdohs.gov/statewide-cyber-readiness-program

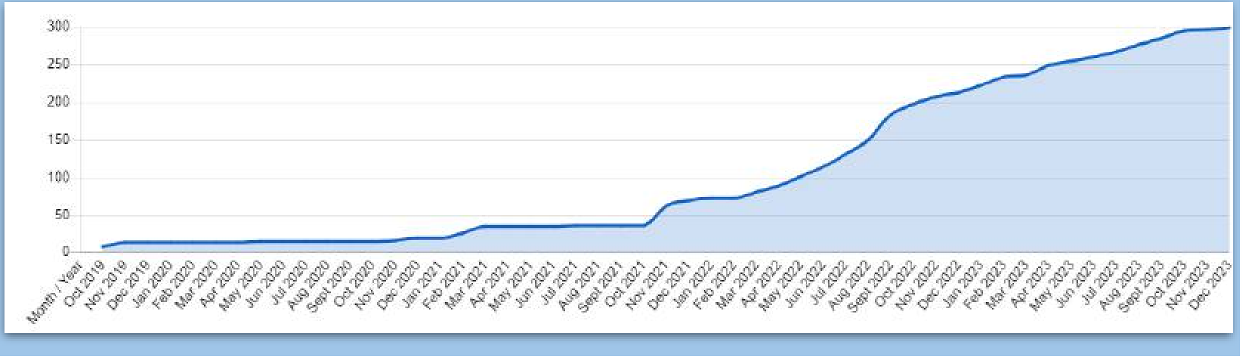
# Cyber Readiness Program

The State of Arizona has allocated funding to provide cyber resources to local and tribal government entities in Arizona.

To provide these resources, the State works with local and tribal government entities that do not currently have the cyber capabilities and priority is given to smaller and less-resourced organizations with the greatest need for support.

The Program is governed by the multi-agency, multi-jurisdictional Statewide Cyber Readiness Planning Committee which provides strategic planning and guidance on the tools that are provided to Arizona Local Governments.





ARIZONA DEPARTMENT OF HOMELAND SECURITY

# Contact me!

**Ryan Murray**

rmurray@azdohs.gov

https://www.linkedin.com/in/ryan-murray-az/