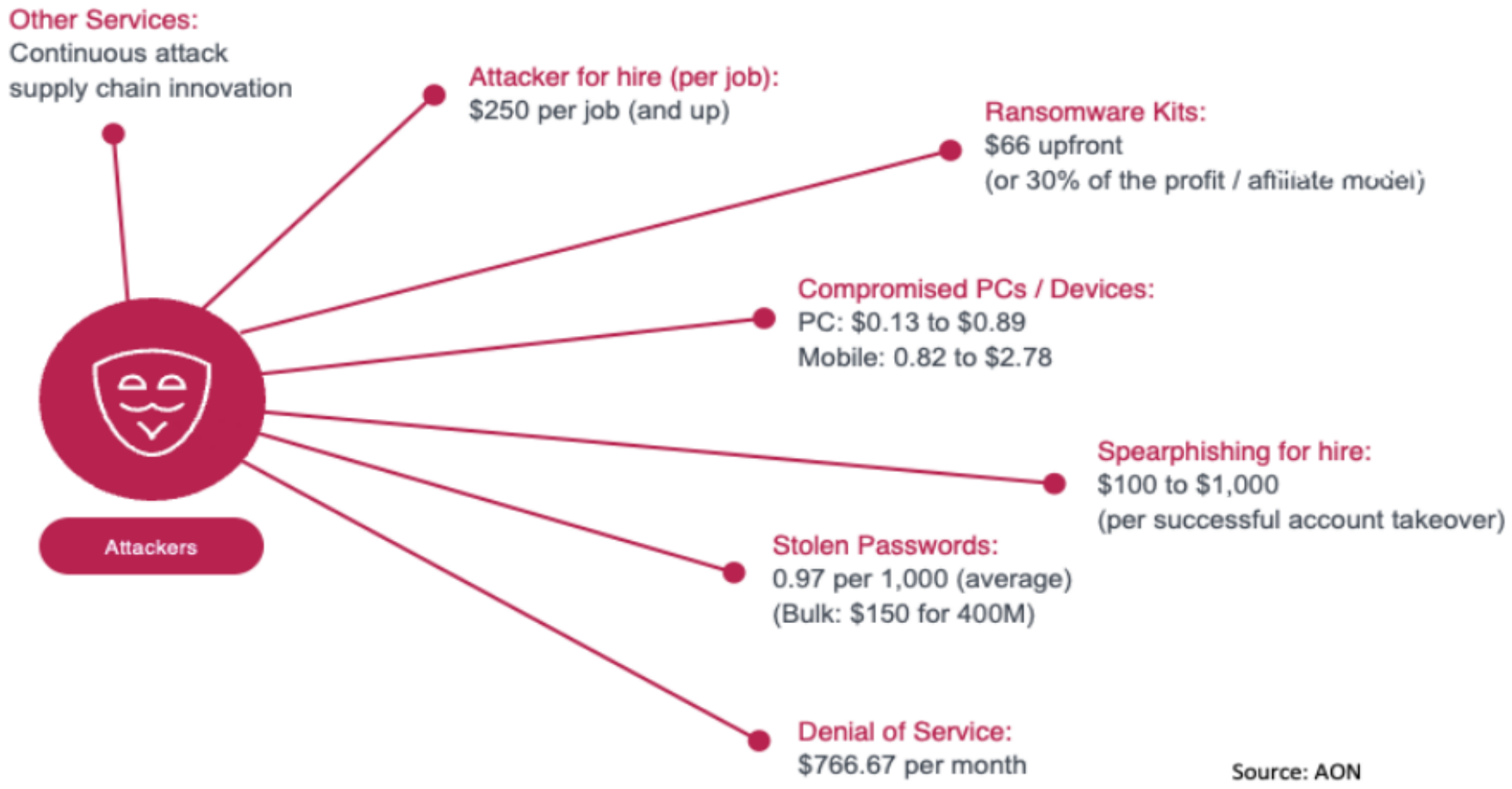
Does the Transit Industry Understand the Risks of Cybersecurity and Are They Being Prioritized?

Scott Belcher
Research Associat and Principal Investigator,
Mineta Transportation Institute, and
Co-Founder, Cybrbase

MINETA TRANSPORTATION INSTITUTE

CYBRBASE

Cybersecurity Threat Landscape



Source: Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized? Mineta Transportation Institute May 2025

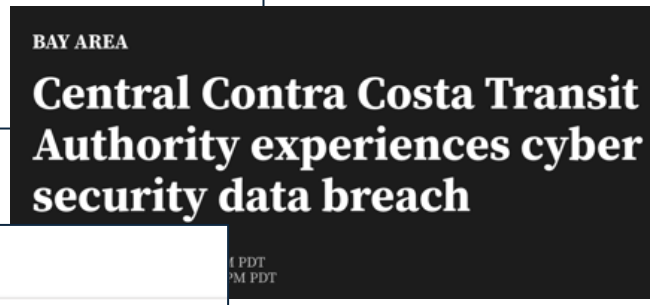
Cybersecurity Attacks Are on the Rise

METRO (WMATA)

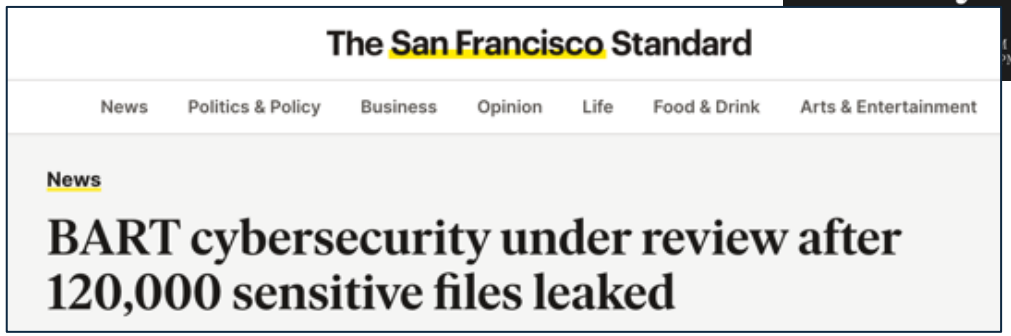
A cyberattack took down Metro's website for two hours. Here's what a cybersecurity expert says

"So what they're trying to do is, hackers are trying to flood your network so you can't operate," cybersecurity expert Steve McKeon told us

By Adam Tuss, News4 Anchor & Transportation Reporter • Published May 14, 2024 • Updated on May 14, 2024 at 7:54 pm


BAY AREA

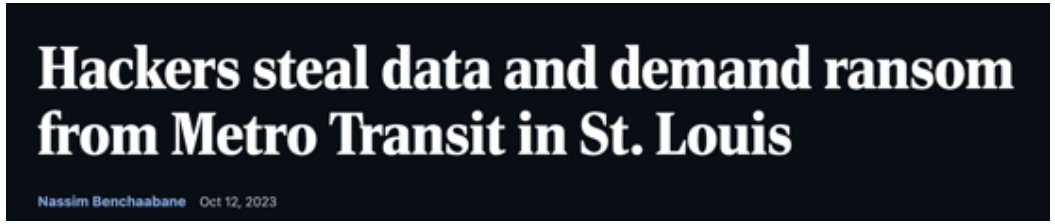
Central Contra Costa Transit Authority experiences cyber security data breach


The San Francisco Standard

News Politics & Policy Business Opinion Life Food & Drink Arts & Entertainment

News

BART cybersecurity under review after 120,000 sensitive files leaked


Hackers steal data and demand ransom from Metro Transit in St. Louis

Nassim Benchaabane Oct 12, 2023

RIPTA
RHODE ISLAND PUBLIC TRANSIT AUTHORITY

valley regional transit

MTA

SEPTA

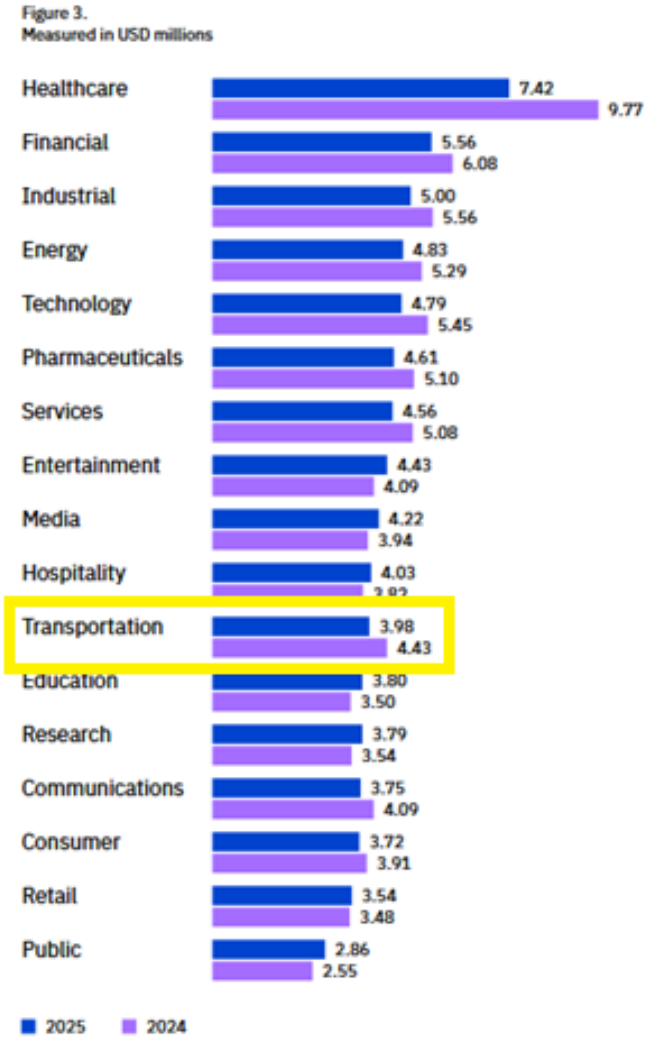
TheBus
HEA

TORONTO TRANSIT COMMISSION

TheRide
Ann Arbor Area Transportation Authority

metro

What is at Stake for Transportation?



Source: IBM 2025 Cost of a Data Breach Report

Public Transportation remains a high target. The average cost of a breach between 2024 and 2025?

$4.2 Million

Since the 2020 MTI study, there have been publicly disclosed cyber incidents in transit, resulting in public distrust, service disruption, and substantial financial loss.

At an average of $4.2 million per breach, this eclipses a small, rural transit agency's **entire annual operating budget**.

Recent MTI Studies Show that Transit Agencies Are Not Cyber Resilient

- Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness, S. Belcher, T. Belcher, Greenwald & Thomas, Mineta Transportation Institute Publications, September 2020.
- Implications of the Sunburst Cybersecurity Attack on the Transit Industry, Belcher & Thomas, Mineta Transportation Institute Publications, January 2021.
- Will the Biden Administration's 'Made in America' Executive Order Present Significant New Cybersecurity Obligations for Transit Operators?, S. Belcher, H. Belcher, Seckman & Thomas, Mineta Transportation Institute Publications, June 2021.
- Personal Data Protection as a Driver for Improved Cybersecurity Practices in U.S. Public Transit, Seckman, Thomas, H Belcher & S Belcher, Mineta Transportation Institute Publications, December 2021.
- Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges, Belcher, Belcher, Seckman, Thomas & Yaqub, Mineta Transportation Institute Publications, July 2022.
- Is There a Light at the End of the Tunnel? The Outlook for Cybersecurity Insurance and Transit in 2024, Belcher & Chollet, Mineta Transportation Institute Publications, April 2024.
- ➢ Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?, S. Belcher, T. Belcher, J. Grimes, L. Holmstrom, A. Souders, Mineta Transportation Institute Publications, May 2025.

The Problem in 2020

44%

Did not have a cybersecurity program in place

59%

Did not conduct cybersecurity assessments at least annually

43%

Did not provide annual cybersecurity training

Source: Mineta Transportation Institute 2020 Study

After the 2020 Study, We Became Evangelists

- Testified before Congress multiple times
- Worked with DOT, DHS, GAO, CISA, APTA, AASHTO, etc.
- Spoke at every transportation conference that would have us
- Created the Cybersecurity Assessment Tool for Transit (CATT) for the FTA
- Urged DOT and Congress to establish a cybersecurity requirements for transportation
- Founded Cybrbase, Inc., where we developed a repeatable, web-based, assessment tool based on NIST CRR
- Helped dozens of transit agencies of all size with their cybersecurity challenges
- Continued to conduct research in the space

The Result . . . Four Years Later

	2020	2024	2024 <$5M
Have a cybersecurity policy	50%	55%	25%
Believe they have the resources to respond to an attack	47%	76%	N/A
Conduct annual security audit or assessment	50%	60%	15%
Either do not have/do not know if they have cybersecurity clauses in their vendor contracts	60%	54%	75%
Provide annual cybersecurity training	47%	55%	<10%

Source: Mineta Transportation Institute 2020 and 2024 Studies

Policy Recommendations

- Dedicated funding for cybersecurity
- A statutory or regulatory mandate
- Attestation requirement
- Procurement language
- Educate about fiduciary obligations of executives and boards
- Educate about available resources

Recommendations for Transit Agencies

- Develop an individualized cybersecurity plan and update it at least annually
- Conduct a cybersecurity assessment at least annually and address the shortcomings identified in that assessment in a timely manner
- Ensure that they have documented cybersecurity policies and procedures in place and that the organization is following them
- Ensure that they have at least one person on staff that is qualified to oversee the overall cybersecurity program and/or cybersecurity vendors

What You Can Do?

- Visit Cybrbase.com and click “Take Our Quiz!”
- Create a culture of awareness – this starts at the top
- Regularly assess your cybersecurity resilience
- Train staff regularly
- Know your critical services
- Develop an asset inventory and start tracking your risks
- Determine your risk appetite and risk tolerance
- Run vulnerability scans
  - Free resources through CISA

After the 2024 Study, We Were Challenged by the FTA and MTI to Try Something New

- Working with Illinois DOT and six of its partners, Cybrbase developed the Cohort-Based approach to conducting cybersecurity assessments
- Replicable, group-based cybersecurity assessment methodology
- Scalable across industry
- Drives down cost
- Fosters shared learning and best practices

How Does it Work?

State groups agencies into smaller cohorts that work together (6-10)

Initial policies and procedures workshop

Facilitated cohort assessment on replicable platform

Post-assessment workshop to identify common problems and actions

Follow-on support

Second facilitated assessment to determine progress

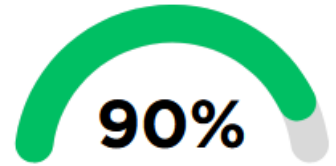
Referrals to technical support

Participants Have Seen Great Value

- Peer engagement and collaboration
- Strong buy-in from management
- Eliminates many excuses
- Heightened cybersecurity awareness within agencies
- Agency silos broken down
- Insurance milestone

Strong Impressions Thus Far

Of attendees found these sessions **beneficial**.



Found in-person assessment and common solutions workshop **very beneficial**.

Have begun discussions with internal/external teams to **tackle risks**.

States are Taking Cybersecurity Measures Into Their Own Hands

Ohio: Cybersecurity Mandate

Ohio recently passed legislation on June 30th regarding a cybersecurity mandate, making it so local and state agencies must now align their cybersecurity programs with the NIST CSF and/or CIS controls. This also includes annual cybersecurity training, mandatory incident reporting, and MFA, among others.

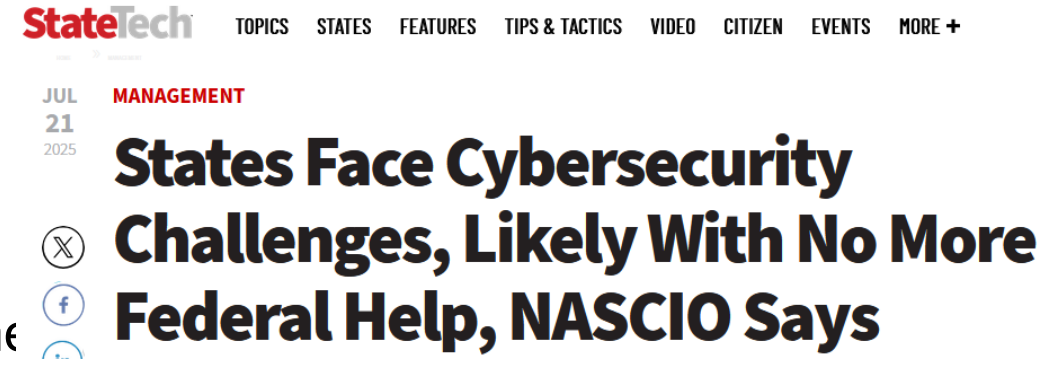
North Dakota: Whole-of-State Approach

Cybersecurity strategy, leveraging the state's long-established STAGEnet network, which connects all state agencies and SLED. This allows the state to centrally manage threat detection, security standards, and responses.

Texas: Launch of Texas Cyber Command

Established with $135 million in state funding:

- Anticipating and responding to cyber threats
- Pre-attack coordination and post-attack recovery
- Cyber awareness training and leadership developme



What Can Michigan Do?

- Create a centralized cyber authority
- Invest in state-funded cyber infrastructure
- Support coordination across local governments and sectors
- Create mandates to ensure minimum levels of cybersecurity assurance
- Support small and mid-sized transit agencies in putting the basics in place

Questions?

Scott Belcher
scottfbelcher@gmail.com
(703) 447-0263

MINETA TRANSPORTATION INSTITUTE

CYBRBASE