Scott Belcher

Research Associate

Mineta Transportation Institute, San Jose State University

House Committee on Transportation and Infrastructure

The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure

November 4, 2021

Enterprise risk management in the U.S. public transit industry needs a twenty-first century upgrade, whereby specific attention is paid to strengthening cyber protections and preparedness across the industry. Risk as defined by most industry providers focuses primarily on the physical risks posed to the organization and its service delivery. Investments have been made for decades to reduce this risk, as it is understood that most threats that are likely to impair transit operations with regularity are physical (*e.g.,* threats against operators and passengers, damage to vehicles, and theft). However, as digital technologies continue to be woven into the operations of even the most conventional public transit agency, any system, process, or function dedicated to reducing physical risk likely includes an array of digital vulnerabilities that need to be managed in concert with current security operations. The increasing frequency and magnitude of cyber threats also increases their potential to negatively impact existing systems designed to reduce physical risk. Risk governance decisions should prioritize potential physical threats, but the design and management of any comprehensive enterprise risk infrastructure in today's world must improve and integrate cybersecurity best practices alongside the physical security priorities.

Based on the findings of the 2020 Mineta Transportation Institute (MTI) Report, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*[1] (hereinafter, the 2020 MTI Report) and research to date, the authors believe transit operators need to elevate their understanding of and preparedness for cyber-related risks to their operations, data, and business infrastructure. Further, given the

[1] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness

dependence transit agencies have on vendors, opportunities exist for the industry to enlist the help of the vendor community to support and in some cases lead the improvement of cyber risk management across the supply chain.

The 2020 MTI Report highlights that some agencies have taken action to protect themselves by seeking technical leadership from outside the transit industry, contracting out the management of personally identifiable information (PII), and seeking support from their supply chain partners. Some include cybersecurity requirements in their contracts with suppliers, one of the more basic and least expensive means to begin maturing an organization's cyber risk posture. And still others have operationalized cybersecurity requirements through actions in partnership with their supply chain, such as annual audits and ongoing monitoring and alerting that is closely coordinated between agency and vendor. Many agencies, however, have not yet embarked on such efforts.

Enterprise Risk Management: The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.[2]

The 2020 MTI Report concludes that for many transit agencies, internal resources for cybersecurity are scarce, as even among those agencies and individuals that recognize the growing threat,

[2] https://csrc.nist.gov/glossary/term/enterprise_risk_management

acquisition of necessary resources is a long, laborious activity. In the view of the authors, there needs to be a collaborative effort between the federal government, the industry, and transit agency leadership to establish, maintain, refine, and support cybersecurity programs. Both carrots and sticks are required to ensure the necessary resources are made available and utilized. The authors emphasize that the Federal Transit Administration (FTA) should require transit organizations to adopt and implement minimum cybersecurity standards prior to receiving federal funding. To date, the U.S. Department of Transportation, and the FTA has largely deferred to the Transportation Security Administration (TSA) in this space. This is about to change.

Transportation infrastructure is a target for nefarious actors seeking to disrupt, be it for personal or political gain. The avenues to exploit this vital infrastructure will continue to evolve along with the technology that enables the industry's core operations and goals. As these technologies are further embedded in operations, new vulnerabilities will arise. Accounting for the risk today will foster greater resiliency and preparedness in the years to come.

The mission of public transit is to move people as safely and efficiently as possible. Public transportation is a multi-faceted, complex, and expansive ecosystem that relies on people, processes, and associated technologies to ensure that it achieves its mission as seamlessly as possible. Security has always been a foundational aspect of public transit operations. Moving people at scale has inherent risk, and every transit agency takes deliberate steps to reduce physical risk wherever possible. An unsafe public transit system impairs the agency in executing its mission, as the public's sense of safety has a direct correlation to their willingness to use the public transit system to move about the community. Digital technologies are playing an increasingly important role in operations security. It is critical that transit agencies understand how their risk profile is changing, and ensure their systems, processes, and procedures engaged to address such risk are effectively resourced and adequately managed.

The transit industry depends on a myriad of technologies, from the physical systems that manage access to the garage to the databases that house operational data or employee information. Technological advancements in general and their expanded application to the transit industry more specifically offer significant advantages for both providers and customers—improved service quality, operational efficiencies, and reduced costs. With each of these advancements, however, comes an additional level of risk that must be weighed and managed by transit providers and their suppliers. Cyber vulnerabilities attributable to the expanding digital ecosystem are prime among these growing risks.

In the 2020 MTI Report, the authors described the unprecedented increase in the volume of data collected and maintained by modern transit operators, the addition of numerous vendors to help manage these growing technology demands on the industry, and the resulting need to spend more time and money securing newly exposed cybersecurity threats. Many transit agencies, the report found, were unprepared to prevent or respond to the broad array of identified threat vectors—ranging from phishing and business email compromise to data breaches to ransomware attacks.

A key finding from the 2020 MTI Report is that many agencies do not have an accurate sense of their cybersecurity preparedness.

- 81% of responding agencies believe they are prepared to manage and defend against cybersecurity threats, and;
- 73% feel they have access to information that helps them implement their cybersecurity preparedness program

Yet…

- Only 60% actually have a cybersecurity preparedness program;
- 43% do not believe they have the resources necessary for cybersecurity preparedness; and
- Only 47% audit their cybersecurity program at least once per year.[3]

It is essential for transit agencies to develop and maintain mature enterprise risk management systems to mitigate threats to people, operations, and data. This need is neither new nor unique to the transit industry. Part of running any business is taking the necessary steps to protect critical assets. The added challenge organizations face today, however, is the increasing role of digital technologies in all areas of business operations. The resulting need is to have robust cyber risk management practices that span the organization to ensure the continued protection of critical assets.

[3] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness p 32.

Moreover, greater cybersecurity oversight is on its way. The Biden Administration has been vocal about the need for greater engagement in cybersecurity oversight by the federal government. The President on May 12, 2021, issued an Executive Order stating:

> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.[4]

The Executive Order applies specifically to Federal agencies and their suppliers, but it is only a matter of time before the extensive set of requirements included in this Executive Order flow down to recipients of Federal funds.

In a similar vein, the Department of Defense on November 20, 2020, began implementation of the Cybersecurity Maturity Model Certification (CMMC), which is a unifying standard for vendors to ensure they are implementing cybersecurity across the Defense Industrial Base (DIB).

> The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

> level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.[5]

Again, while the CMMC currently only applies to contractors in the DIB, procurement practices that start in the defense arena regularly move into the non-defense arena and procurement and cybersecurity professionals both anticipate this transition.

Finally, Congress has introduced several bills to address cyberattacks against private-sector targets and critical infrastructure, which includes the U.S. transportation sector. The U.S. House Energy and Commerce Committee on July 20, 2021, passed eight cybersecurity bills. The eight-bill package will increase requirements for private companies to report on cybersecurity incidents and provide funding for state and local governments to increase cybersecurity measures.[6] Subsequently, Senator Mark Warner (D-VA) on July 22, 2021, introduced a bipartisan bill that would require the Cybersecurity and Infrastructure Security Agency (CISA) to identify and mitigate threats to the operational technology systems of pieces of critical infrastructure.[7]

[5] https://www.acq.osd.mil/cmmc/faq.html

[6] https://energycommerce.house.gov/newsroom/press-releases/pallone-praises-committee-passage-of-eight-bipartisan-cybersecurity-bills

[7] https://www.warner.senate.gov/public/_cache/files/4/2/422a0de2-3c56-4e56-a4be-0e83af5b0065/F90B3C493BA4FAB09E546FAF40E4B116.alb21b95.pdf

Both the public and private sector have developed a great deal of cybersecurity guidance over the past two decades. Cybersecurity experts will tell you that the tools used to manage cybersecurity and associated threats do not vary greatly across industries but that some industries are more mature in their understanding when it comes to managing cyber risks. Industries such as the financial management industry where billions of dollars are moved digitally every minute have been forced to invest heavily in cybersecurity protection. Other industries such as the transit industry, which has traditionally been a hardware-based industry that relied largely on firmware and closed networks, have not faced the same urgency until recently.

The 2020 MTI Report observes that "[t]he existing cybersecurity guidance for public transit is spread across numerous government and industry entities. . . [and that] federal resources exist for agencies to improve their cybersecurity readiness."[8] The same baseline documents are at the core of every industry cybersecurity program. Despite industry differences, cybersecurity maturity models and the assessment practices used to strengthen policies, procedures, and practices are transferable.

One of the key foundations for cybersecurity programs across any industry comes from the National Institute of Standards and Technology (NIST). NIST is a non-regulatory agency that has no authority to dictate the use of any standard, but its standards carry significant weight. The

[8] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness MTI Report p 35.

work of NIST is defined by federal statutes, executive orders, and policies—including developing cybersecurity standards and guidelines for federal agencies. NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development.[9]

In 2014, NIST released the "Framework for Improving Critical Infrastructure Security" in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[10] which called for a standardized security framework for critical infrastructure in the United States. This guidance is not intended to be a how-to guide for cybersecurity; rather, it is a framework designed to help a wide range of organizations assess risk and make sound decisions about prioritizing and allocating resources to reduce the risk of compromise or failure in their computer networks. For any organization to leverage the NIST Framework, customized implementation is required in ways that are not necessarily obvious from the document. The guidance is equally applicable to public and private industry.

To further support organizations in the face of a growing cyber threat, Congress established the CISA at the U.S. Department of Homeland Security (DHS) through the Cybersecurity and Infrastructure Security Agency Act of 2018.[11] According to DHS, "CISA is the Nation's risk

[9] https://www.nist.gov/cybersecurity

[10] Barack Obama. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11737, February 19, 2013, https://www.federalregister.gov/ documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[11]https://www.congress.gov/bill/115th-congress/house-bill/3359

advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[12] CISA coordinates a collective defense to identify and vet procedures to manage and reduce the impact from disruption to critical infrastructure. In this role, the organization builds and coordinates relationships across industries working with sector specific agencies, such as the U.S. DOT, the FTA, the TSA, among others.

CISA's role is to unite government and private sector partners, with a particular focus on 16 Critical Infrastructure Sectors:

> There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[13]

The public transit industry is part of the Transportation Security Sector (TSS), which is one of the 16 critical sectors. As such, the industry has direct access to CISA's capabilities and resources, such as intelligence analysis, data assessment, response methods development, and assistance to manage risks to critical infrastructure that often spike from emerging threats. CISA

[12] https://www.cisa.gov/about-cisa

[13] https://www.cisa.gov/critical-infrastructure-sectors

leads a systematic approach to manage and reduce cyber risk that includes providing services, cyber training, support to critical infrastructure operators, and risk analysis.

The TSA is another critical cybersecurity player. TSA's origins date back to the days after September 11, 2001, when it was formed as part of the Aviation and Transportation Security Act. Its "mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce."[14] Given its provenance, TSA's original orientation centered on physical security, but the agency "is responsible for securing the nation's transportation systems from all threats, including both physical and cyber."[15] In this latter role, TSA overlaps with CISA. TSA explains the division of labor as follows:

> Although TSA has responsibility for oversight of both the physical security and cybersecurity of the [TSS], TSA is not directly responsible for the defense of the private sector portion of TSS information technology infrastructure. Rather, TSA serves a vital role in ensuring the cybersecurity resilience of the TSS infrastructure and will work with the Cybersecurity and Infrastructure Security Agency (CISA), with its mission to protect the critical infrastructure of the United States.[16]

[14] Transportation Security Administration (TSA), "Mission," https://www.tsa.gov/about/ tsa-mission (accessed March 13, 2020).

[15] TSA, "TSA Releases Cybersecurity Roadmap," December 4, 2018, https://www. tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap (accessed March 13, 2020).

[16] TSA, "Cybersecurity Roadmap 2018," 4 November 2018, https://www.tsa.gov/sites/ default/files/documents/tsa_cybersecurity_roadmap.pdf (accessed March 13, 2020).

DHS in 2015 built upon the NIST Framework and issued a document "to provide the TSS guidance, resource direction, and a directory of options to assist a TSS organization, [including public transit agencies], in adopting an industry-compatible version of the NIST Framework."[17] This guidance was designed both for transit agencies that have an existing risk-management program and for agencies that do not yet have a formal cybersecurity program.[18] The TSS Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector[19] owners and operators to apply the tenets of the NIST Cybersecurity Framework to help reduce cyber risks.

Recent events have demonstrated the need to be proactive when it comes to cybersecurity. Major attacks such as SolarWinds, Colonial Pipeline, JBS Foods, and Acer have caused significant interruption and cost to the global economy. The transit industry has experienced a number of high-profile attacks as well. Cyber-attacks have involved the Metropolitan Transportation Authority (MTA) in New York City, the Martha's Vineyard Ferry in Massachusetts, and the Southeastern Pennsylvania Transportation Authority (SEPTA) in Philadelphia. Between June of

[17] Department of Homeland Security (DHS), Transportation Systems Sector Cybersecurity Framework Implementation Guidance, 2 June 26, 2015, https://www.cisa.gov/sites/ default/files/publications/tss-cybersecurity-framework-implementation-guide-2016- 508v2_0.pdf (accessed February 24, 2020).

[18] DHS, Transportation Systems Sector Cybersecurity Framework Implementation Guidance, June 26, 2015, 3, https://www.cisa.gov/sites/default/files/publications/ tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf (accessed February 24, 2020).

[19] CISA, "Transportation Systems Sector," https://www.cisa.gov/transportation-systemssector (accessed March 13, 2020).

2020 and June of 2021, the global transportation industry witnessed a 186% increase in weekly ransomware attacks.[20]

This flood of activity and associated attention has raised a level of alarm throughout the government and the transit industry. Working with industry experts from other more mature fields such as financial management and defense, the researchers learned that the executives of these industries have come to treat cybersecurity threats as they treat the many other high-profile threats that the organizations' executive teams must evaluate, prioritize, and manage on an on-going basis.

Of the risk management priorities identified by transit executives, business continuity and data protection are the two areas most immediately at risk to cyber threats. The good news is that there are steps that transit providers can take—with the participation and support of vendors—to mature existing risk management practices and implement industry-specific cyber defenses.

People Safety

Creating and maintaining a safe environment for customers, employees, and the communities in which transit agencies provide services is essential for general risk mitigation and continuity of operations. Whether the safety incident involves a bus or train encountering another vehicle or an obstruction, or it involves a physical threat posed to a passenger, the transit operating system and its digital assets have rarely been directly involved. The increasing connectivity of vehicles both to other networked systems and to the internet is changing this dynamic.

[20] https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/

Until recently, the potential for digital tools to access physical operating systems among most public transit agencies was not feasible, as most systems were safely segregated from the internet. The advent and exponential growth of internet-enabled devices has stripped most systems of this protection. Applications enabling automatic vehicle locator (AVL) or global positioning systems (GPS) technologies to track vehicles in real time, for example, are also generally reliant on connected and networked operating systems. Even the transition to electric buses brings with it a whole new level of cyber exposure and other security risks not previously anticipated.

Connected vehicle technologies that enable communication among vehicles on the road, infrastructure, and personal devices, can connect to the internet and vital operating systems — creating new access points for disruption. Transit operators have been piloting and, in some cases, deploying this new safety technology, which brings with it a new cybersecurity threat vulnerability that must be managed. Similarly, as transit operators test and deploy new levels of autonomy, whether it is for bus rapid transit or for first and last mile shuttles, they are exposing their operating systems and their passengers to new cyber risks. Fortunately, to date, there are no known recorded instances of malicious actors exploiting these vulnerabilities to remotely hijack or otherwise disrupt public transit vehicles. The access points to do so, however, are there and have been breached by researchers.

Business Continuity

Interruptions to day-to-day business operations face the most pronounced cyber risk because an increasing amount of transit operations relies on digitally connected systems. Everything from when a bus is scheduled to depart a yard to which operator should be driving it are managed by internet-enabled devices and systems. Yard management and operator scheduling software are increasingly commonplace in public transit agencies. These systems, in turn, feed into public-facing route-planning services on which customers rely to complete their journeys. The public schedules also live on an increasing array of digital systems and services, from the agency's website and mobile applications to third-party services like Google Maps and Uber. A disruption to any one of these systems and the transmission of the data they produce can impair or halt service delivery. For example, SEPTA, suffered a ransomware attack resulting in severe network disruption in August 2020. Vancouver, Canada's TransLink transportation suffered a similar attack in December 2020. Like SEPTA, the services and systems

Operational Technology (OT) is the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.

Information Technology (IT) is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.[21]

[21] https://www.gartner.com/en/information-technology/glossary

on which TransLink relied to conduct day-to-day business operations were disrupted or sidelined. TransLink suffered from deactivated ticket kiosks and metro card readers, phone and internet outages, and offline GPS, tracking, and reporting services.

Personal and Financial Data

The acquisition and exploitation of personal and financial data is a common goal of cyber criminals because it can be easily monetized in forums where individuals and organizations are willing to trade or pay for the information. Transit agencies are in possession of employee and customer data, specifically personal and financial information, which can hold appeal to nefarious actors. The previously cited Vancouver TransLink ransomware attack resulted in a lawsuit against TransLink by employees who accused the company of not doing enough to protect their personal and banking information—much of which was compromised during the attack.

As transit providers adopt new systems to augment and improve service—mobile pay, advanced trip planning, on-board Wi-Fi, etc.—they are increasingly likely to be in possession of more high-value customer data. Special services for older adults and paratransit services for individuals unable to use fixed route services may also require communication or documentation about sensitive health information—none of which the transit agency nor the customer wishes to have in the hands of a nefarious actor. Without implementing robust protection systems, the transit provider is likely to be risking the security of their passengers' data and may not even be in the position to know if or when a system is breached.

Most transit operators outsource fare management and the associated passenger data to PCI compliant vendors, which helps them to manage one of their biggest cybersecurity risks. Operators are now becoming more sophisticated in the contractual requirements that they impose upon their fare management partners to ensure that these vendors have a mature and comprehensive cyber protection system in place.

Transit operators are entering into a challenging new world where digital technology increases their cyber threat risks exponentially. Simultaneously, the Federal Government is increasing its focus on cybersecurity. As such, the transit industry will need to sharpen its focus, take advantage of available resources, and rely increasingly on its partners for support as it elevates its response to these dual pressures. It will have to address these challenges while it is also called upon to respond to growing pressure to address congestion, emissions, and social equity. No easy task.