NMFTA CYBERSECURITY CARGO CRIME REDUCTION FRAMEWORK

Reducing the Attack Surface by Understanding the Complexities and Interdependencies of the Cargo Crime Ecosystem

Version 1.0

Cargo theft is the multi-headed hydra of threats faced by the transportation sector. Prevention requires a holistic approach to cybersecurity, operational security, and physical security.

NMFTA™ National Motor Freight Traffic Association, Inc. | CYBER

Release date:

6/12/2025

NMFTA Cybersecurity Team

[**This Page Is Left Intentionally Blank**]

Contents

Intended Audience

While this resource is mapped specifically to the cybersecurity guidebooks provided by NMFTA which are targeted at owner operators and fleets, this Cyber-Enabled Cargo Theft Prevention Guide will provide useful information and controls to mitigate the risk of cyber-enabled cargo theft across the transportation sector. Fleets, brokers, and even full-service third-party logistics providers (3PLs) will find that these controls, when properly configured and enforced, reduce their risk of falling victim to cyber-enabled cargo crime.

Assumptions

Assumption 1: Existing Cybersecurity Knowledge

This guide assumes a basic awareness of cybersecurity concepts and overall threats posed to the transportation sector by cyber-enabled cargo theft. While controls are clearly identified, and their impact on the cargo-theft risk faced by an organization are covered in detail, the controls themselves are not fully outlined, nor are implementation strategies or examples provided. For additional information on the controls identified in this resource, please reference the NMFTA Cybersecurity Guidebook – Mid-Sized Fleets.

Assumption 2: Additional Operational Security Controls Required

As discussed in the introduction below, cybersecurity controls alone are not sufficient to protect an organization from cargo theft. Many of the controls in this resource address cyber-operational risks, or cyber-physical risks. However, there are many more operational and physical risks that are not covered in this guide. Additional study of the operational risks and physical risks present in the organization is strongly recommended to fully address the issue of cargo theft in a holistic manner.

While operational security (OPSEC) has evolved as part of a broader, holistic security approach within modern organizations, its roots remain firmly grounded in the United States (U.S.) Department of Defense doctrine. At its core, OPSEC is about identifying sensitive information, understanding the risks associated with its exposure, and implementing controls to mitigate those risks. These principles are directly applicable to both traditional and cyber-enabled threats, including cargo theft, financial fraud, and targeted intrusion campaigns.

Unlike many controls found in formal cybersecurity maturity models, OPSEC practices often manifest as procedural safeguards that don't rely on technical tools—but are no less critical to an organization's overall security posture. For example, instituting a dual-authorization process for changes to banking information—requiring two independent verifications before approval—can be a simple but effective control. This not only reduces the likelihood of falling victim to socially engineered fraud but also addresses the insider threat problem: one malicious actor may succeed; two working in coordination is far less likely.

These kinds of non-technical, behavior-focused mitigations are often overlooked in cybersecurity planning but are essential to creating a layered and resilient defense model. Their relevance is underscored in directives such as NSPM-28 (National Security Presidential Memorandum on United States Government-Supported Research and Development National Security Policy), which reinforces the importance of protecting sensitive information through proactive operational measures.

Assumption 3: Adaptability as a Core Value

Cargo thieves are constantly evolving. Their tactics, techniques, and procedures (TTPs) change constantly to exploit new technologies, fluctuating economic environments, and changes to industry practices and security measures. To successfully mitigate the risks posed by cargo thieves, organizations must maintain an agile and adaptable approach to cargo-theft prevention. This resource is a reference tool to address the common cyber-enabled cargo theft threat vectors that have been observed throughout the transport sector, with the assumption that the reader will remain vigilant for new or additional controls that may be required to address the risk of cargo theft to their organization in the future.

Introduction to Cyber-Enabled Cargo Crime

In August of 2023, two armed criminals took a professional truck driver hostage in their rig at an Ohio truck stop and stole the truck and trailer. This was the start of a seven-hour pursuit and an armed standoff with a SWAT team that ended with two suspects shot dead, and one very lucky driver rescued by law enforcement. This harrowing true story sounds like the plot of an action movie and it's often the kind of story we think of when we think of cargo crime. Fortunately, the reality is that modern cyber-enabled cargo crime does not typically involve high speed chases, or Hollywood style standoffs but this in no way means that it is a threat to be taken lightly.

Cargo crime poses a significant and growing problem in the transportation sector. From small-scale pilfering to the theft of whole trailers, to international strategic cargo theft rings run by sophisticated organized criminal organizations, the methods and the threat actors involved are as varied and diverse as the commodities handled by the transportation industry. While there is no silver bullet to solve this problem, there are common tactics that are shared across many of the different threat actors. Many of these tactics are also shared by common cyber-criminals.

Although cybersecurity controls make up an important part of a cargo theft prevention program and can significantly reduce the risks posed by cyber-enabled (strategic) cargo theft, a holistic approach to reducing an organization's risk from cargo theft and fraud must address three distinct security practices:

- Cybersecurity;
- Operational security; and
- Physical security.

While these are distinct focuses or spheres of responsibility, they overlap in several areas, as illustrated in figure 1.a to the right.

Cybersecurity practices that reduce an organization's risk of falling victim to extortion or a Ransomware as a Service (RaaS) attack can also effectively reduce the risk of falling victim to a successful cyber-enabled cargo theft scheme. However, it is important to remember that the controls detailed in this guide are not designed to be an exhaustive list of the cybersecurity, cyber-operational, or cyber-physical controls available to address the risk of cyber-enabled cargo theft. This document is primarily designed to illustrate the ways in which any control that improves cybersecurity resilience will directly or indirectly improve resistance to cyber-enabled cargo theft.

Figure 1.a – *Security Practice Areas*

This guide specifically addresses the role of cybersecurity controls, as well as some cyber-physical and cyber-operational controls that organizations can utilize as a part of their broader cargo theft prevention strategy. Cybersecurity controls will be discussed that fall either strictly within the cybersecurity sphere or in one of the shared spheres of responsibility. Each control will be clearly identified as either strictly addressing cybersecurity concerns or addressing cybersecurity and one or more additional practice areas. It is critical to address all three of these practice areas in full to effectively minimize the risk of cargo theft.

Cyber-Enabled Cargo Crime Prevention & Response Ecosystem

At the forty-thousand-foot view, there are three clear areas of focus: cybersecurity, operational security, and physical security, as well as law enforcement involvement and criminal prosecution after the event, or "right of bang." However, as we zoom into this issue, we discover the reality is even more complex. There are multiple entities, relationships, controls, and dependencies that exist within each area, many of which overlap and converge with other practice areas and entities within this ecosystem as represented in the illustration below (figure 1.b).

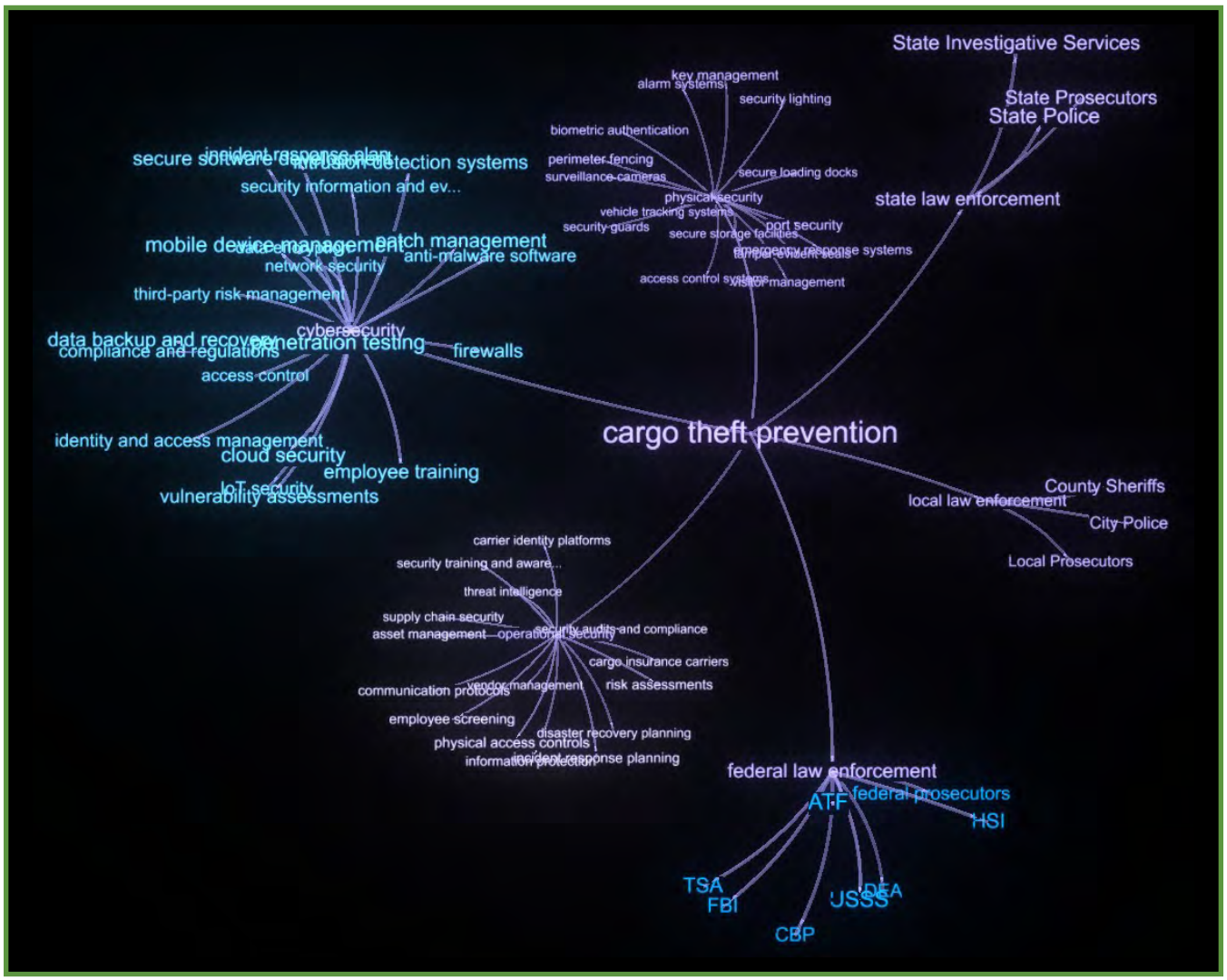

Figure 1.b
A Graphical Representation of the Cyber-enabled Cargo Crime Prevention & Response Ecosystem

To address this issue in a holistic manner, we cannot assume that any one of these entities, or even an entire section of the ecosystem (such as cybersecurity), alone will be enough to solve the problem. While NMFTA specializes in cybersecurity controls that relate to preventing cyber-enabled cargo crime, to effectively design comprehensive mitigation strategies, we have also developed relationships with industry, government,

and law enforcement entities to inform better design of cybersecurity controls that also effectively address cyber-operational security and cyber-physical security issues related to cargo crime.

In the following sections, we will discuss many of the different entities that exist within this complex ecosystem and the roles and responsibilities that they have in mitigating the risk of cyber-enabled cargo crime, responding to incidents, recovering stolen cargo or fraudulent financial transactions related to cargo crime, and ultimately prosecuting the parties responsible.

Law Enforcement

Law enforcement plays a critical and extremely complex role in response to, and prosecution of, incidents of cargo crime. It is important to understand the differences in responsibility, focus, and capability at the three different levels of law enforcement that may become involved, depending on the specifics of the incident.

Federal

At the federal level, there are several law enforcement agencies that address specific aspects of cargo crime in general, and cyber-enabled cargo crime specifically. However, it is important to understand that the makeup of these agencies can include multiple agency scenarios, joint task forces (JTF), and/ or special task forces (STF) that could have interagency dependencies and differences in communication channels further enhancing the complexities of the problem.

- The Bureau of Alcohol, Tobacco, and Firearms (ATF) - The ATF conducts investigations and arrests in cases that involve alcoholic beverages, tobacco products, and firearms or ammunition. While the focus is narrow, the impact of crimes involving these products can be significant. Any cargo theft incident involving one of the products under the ATF's purview must be properly reported in a timely manner to ensure that the correct resources are assigned to investigate.
- U.S. Customs and Border Protection (CBP) – CBP is directly involved in cargo crimes that occur at or pass through ports of entry (maritime, air, surface transport). They conduct investigations and respond directly to disrupt and apprehend threat actors at points of entry to the U.S..
- The Drug Enforcement Agency (DEA) – The DEA is primarily focused on crimes that involve illicit or prescription drugs. DEA agents become involved in the investigation of cargo crimes that involve the theft of pharmaceuticals, or the cases that involve the trafficking of illicit substances identified as schedule 1 or 2 narcotics.
- Federal Bureau of Investigation (FBI) – The FBI conducts investigations, undercover operations, search and seizure activities, and arrests. There are several cargo-crime JTFs across the country. The FBI also has resources dedicated specifically to internet-facilitated crimes with reporting available via the Internet Crime Complaint Center: www://ic3.gov.

- Federal Prosecutors – Federal prosecution of cyber-enabled cargo crime can vary greatly from region to region based on several factors including local political climate or priorities, criminal caseload, and the perceived impact of the crime, as well as perceived likelihood of a successful prosecution. This last point is heavily dependent on proper reporting and investigation of the original incident as under-reporting, or incorrect scoping of the investigative efforts can reduce the likelihood of successful prosecution.
- Homeland Security Investigations (HSI) – HSI conducts federal criminal investigations into the illegal movement of people, goods, money, contraband, weapons and sensitive technology into, out of and through the United States. HSI also has several cargo crime, and cybersecurity focused tasks forces spread across the country as a part of their "Operation Boiling Point".
- Transportation Security Administration (TSA) – The TSA has several specialized task forces focused on surface transportation security and cybersecurity related to surface transportation. They conduct investigations into incidents of cargo theft and fraud as well as providing preventative resources and education to the public.
- The United States Secret Service (USSS) – USSS conducts investigations into the financial transactions associated with cyber-enabled fraud, extortion, and ransom payments. They can track and potentially reverse transfers of funds (including cryptocurrency) related to crimes when brought in soon enough after an incident.

One of the most significant confounding factors at the federal level can be the difficulty of determining which agency "owns" the crime. Particularly of concern is the lack of clearly identified channels for the public to utilize for their initial reports of cyber-enabled cargo theft, or other types of cargo crimes. This often leads to inadequate follow-up or delayed responses to incidents.

These systemic challenges underscore the sheer complexity of investigating and prosecuting cargo crime, particularly when cyber elements are involved. Jurisdictional overlap among federal agencies, the diverse composition of interagency task forces, and ambiguity in initial reporting channels can all contribute to fragmented investigative efforts and delayed responses. Cyber-enabled cargo crimes often span geographic and bureaucratic boundaries, making it difficult to quickly identify the appropriate lead agency or coordinate a unified law enforcement response. Inconsistent reporting practices, especially when incidents are underreported or misdirected, further diminish the effectiveness of early investigative work, which is critical to building prosecutable cases.

Yet, while these complexities present significant hurdles, they are not insurmountable. Ongoing efforts to formalize interagency collaboration, enhance public-private information sharing, and educate stakeholders on proper reporting mechanisms offer promising avenues for improvement. The growing recognition of cargo crime as both an economic and security issue is catalyzing more focused attention from policymakers and law enforcement leadership alike. With continued investment in coordinated frameworks and a clearer delineation of responsibilities, there is a meaningful opportunity to improve investigative outcomes and increase the rate of successful prosecution. Understanding and addressing these barriers is the first step toward a more resilient and responsive cargo security ecosystem.

State

At the state level, enforcement, investigation and prosecution primarily focus on intrastate incidents. However, these investigations frequently expand to include other jurisdictions and result in a transfer of prosecution and/or investigation to federal agencies.

- State Police – Often one of the first law enforcement agencies to respond to incidents of cargo theft, or to be involved in locating stolen freight. Typically, their jurisdiction is limited by state boundaries, but they are occasionally deputized by federal agencies to provide ongoing assistance as a case expands into federal jurisdiction.
- State Investigative Agencies – Many states have independent investigative agencies or services that will handle complex caseloads and focus on building broader cases for state level prosecution.
- State Prosecutors – State level prosecution is typically pursued in cases that can be clearly identified as falling under state jurisdiction. Therefore, the scope of these cases can be limited to the parties directly involved in the physical theft of freight and may not encompass the broader supporting ecosystem of threat actors that organize and/or facilitate these thefts.

Local

At the local level law enforcement is typically the most restricted by jurisdictional issues. However, the role that they play in investigation of cargo crimes can be pivotal. They are most likely to be the first point of contact in the event of a cargo theft incident, and they often provide vital collection of evidence and critical escalation paths to involve additional law enforcement agencies that may be needed as the scope of a case is determined. As in the case of state level law enforcement, local law enforcement may also be deputized by other agencies to provide them with expanded jurisdiction as a case widens.

Reporting Requirements

Timely reporting of incidents of cargo crime, whether physical or cyber-enabled strategic fraud is critical when it comes to improving the odds of successful recovery of freight and prosecution of the responsible parties. This can only be achieved with a comprehensive understanding of the different law enforcement agencies involved and where they fit into the response efforts. Timely reporting of incidents to the appropriate agencies dramatically increases the likelihood of a positive outcome for the victim organization.

Document Structure

Having outlined the complexity of cyber-enabled cargo theft and the law enforcement response that must occur following an incident, the remainder of this document will focus on specific steps that carriers can take to lower the risk of an incident occurring. The same cybersecurity controls that lower the risk of a successful cyber-attack also have the added benefit of lowering the risk of a successful cyber-enabled cargo theft incident.

There are many possible ways to segment the cybersecurity controls that relate to cyber-enabled cargo theft. The NMFTA Cybersecurity team elected to divide these controls not into maturity levels, but into groups of controls that address common elements of the cyber-enabled cargo theft process. This guide first highlights some of the different types of threat actors involved in cyber-enabled cargo theft and details controls that can specifically aid in uncovering and mitigating activities related to these types of threat actors.

This is followed by the six main elements that contribute to a successful cyber-enabled cargo theft scheme:

- Organized Crime
- Insider Threats and Collusion
- Social Engineering and Deception
- Identity Theft and Fraudulent Carriers
- Online Freight Platform Exploitation
- Telematics and Technology Exploitation

All controls will be identified by the control ID assigned in the related NMFTA Cybersecurity Guidebook – Mid-Sized Fleet to allow for easy reference for further reading and implementation examples. Each control will be identified as strictly a cybersecurity control, or a cyber-operational/cyber-physical control. Once the control has been identified and the sphere of responsibility discussed, the impact on cyber-enabled cargo theft will be provided.

Organized Crime

One of the differentiators between traditional cargo theft and cyber-enabled strategic cargo theft is the involvement of international organized crime. A significant portion of the organized criminal involvement in U.S. cargo theft is based overseas. These sophisticated threat actors often employ the same tactics as traditional cybercrime threat actors, leveraging poor cybersecurity controls, social engineering vulnerabilities, credential harvesting, blackmail, and extortion to gain access to shipment details, freight network data, and internal systems that house shipping documents, shipment tracking details and motor carrier identification data. This access is then used to fraudulently masquerade as a legitimate broker/carrier, map freight networks, track high-value shipments, or to coerce or entice legitimate employees into revealing sensitive information or modifying shipment destinations, documents, or records.

MSF.04.1 - Legal and Regulatory Compliance is Actively Managed

Cyber-Operations Control

Organized criminals are sophisticated and highly adaptive. They will exploit regulatory loopholes, jurisdictional differences, and compliance gaps to facilitate cargo theft, fraud, and money laundering.

By actively managing legal and regulatory compliance, organizations can help to ensure that they meet all relevant industry standards, government regulations and security requirements/best practices. This will reduce the number of weak points that are available for organized criminals to exploit.

MSF.04.5 - Documented Vendor Management Program

Cyber-Operations Control

Organized criminals have the resources and capability to exploit supply chain vulnerabilities by infiltrating vendors, trading partners, and other third-party service providers. They have the resources to potentially do this through collusions, coercion, or by establishing shell companies.

A documented vendor management program can help to ensure that all vendors are thoroughly vetted, regularly assessed for security risks, and contractually obligated to meet cybersecurity standards.

MSF.02.1 - Documented Incident Response Plan (IRP)

Cyber-Operations Control

To effectively manage and recover from an incident of fraud, extortion or cyber-enabled cargo theft, an organization must have a comprehensive and well-documented incident response plan.

IRPs must be regularly tested and kept up to date to reflect any changes in technology or business practices.

MSF.04.6 - Formalized, Documented Cybersecurity Policies

Cyber-Operations Control

Organized criminals may exploit inconsistent or poorly defined security policies or policy enforcement to conduct sophisticated attacks, including social engineering, identity theft and system of record manipulation.

Formalized, documented cybersecurity policies help to standardize security practices across the organization.

Insider Threats and Collusion

Insider threats and collusion can present a significant and difficult to detect risk to all transportation sector businesses, particularly in the context of cyber-enabled cargo theft and fraudulent logistics activities. These threats can come in the form of employees, contractors, or trusted third parties who misuse their access – whether maliciously or under external influence – to facilitate system compromise, fraud or theft.

MSF.01.10 - Implement a Least Privilege Account Access Policy

Cybersecurity Control

The risk posed by an insider threat is increased when employees or contractors have more access than necessary to complete their assigned duties. This over-privileged access can elevate the scope of potential data exfiltration or modification as well as the impact of any collusion with external threat actors.

This attack surface can be significantly reduced by restricting access to the minimum required for each role.

MSF.02.6 - Designate Cybersecurity Roles and Responsibilities

Cyber-Operations Control

Clearly defined cybersecurity roles and responsibilities help to ensure accountability and support shorter detection and response times for insider threats.

Insider threats often exploit such internal ambiguity as unclear responsibilities or insufficient monitoring of employee activity. By clearly defining roles and responsibilities, organizations can ensure accountability and improved incident response.

MSF.02.17 - Access to OT and Vehicle Systems Based on Role and Attribute-Based Access Control (RBAC/ABAC)

Cyber-Operations Control

Insiders with access to either Operational Technology (OT) such as camera systems, access control systems, or vehicle systems and sensors can manipulate or sabotage devices and data to support or enable theft and fraud.

Role-Based (RBAC) and Attribute-Based (ABAC) access controls help to limit access to sensitive OT systems and onboard vehicle electronics to only those who require this access to complete their assigned duties, reducing the opportunity for disruption, destruction, or manipulation of these systems.

MSF.03.2 - Security Incident and Event Management (SIEM) Solution

Cybersecurity Control

A properly configured SIEM system enables efficient detection, investigation and response to insider threats and collusion by aggregating and analyzing security events data across IT and operational environments.

A well designed and properly tuned SIEM can help to identify anomalous behavior which may be indicative of an insider assisting in cargo theft schemes or compromising company systems to facilitate fraud.

MSF.04.5 - Documented Vendor Management Program

Cyber-Operations Control

Insider threats and collusion often involve an external partner as well. These can be contractors and vendors who have legitimate, authorized access to systems and data.

A documented vendor management program helps to ensure that vendors and third parties are thoroughly vetted, monitored, and contractually obligated to meet cybersecurity standards.

Social Engineering and Deception

Social engineering and deception tactics are key enablers of cyber-enabled cargo theft. These threats are in no way unique to cyber-enabled cargo theft but represent one of the most successfully exploited attack vectors for all cyber-enabled attacks, whether cargo-related or orchestrated to facilitate extortion, data theft, RaaS, or some other cyber related event. These tactics do not rely on technical vulnerabilities, instead they exploit weaknesses in human psychology, tricking employees, drivers, or third parties into revealing sensitive information, granting unauthorized access, or making fraudulent transactions. Business processes should include built-in checks and balances to reduce the likelihood of fraud, collusion, or socially engineered actions (e.g. require verification from a second employee and a trusted vendor contact through predefined contact means prior to changing any payment or account details in a vendor's profile).

Data Loss Prevention (DLP) strategies serve as a critical control layer in mitigating the consequences of successful social engineering attacks. When attackers manipulate individuals into divulging sensitive data – such as shipment schedules, account credentials, or proprietary operational details – DLP controls can serve to limit the blast radius of the incident by preventing the unauthorized transmission, storage, or exfiltration of the targeted data. These measures are particularly important for protecting high-value logistics data commonly targeted in cargo theft schemes.

Effective DLP requires comprehensive data inventory and classification, as well as the use of both technical and policy-based safeguards to monitor, detect, and block attempts to move sensitive information outside the authorized channels. These controls include email filtering, U.S.B/media restrictions, network traffic inspection, and the automated enforcement of data classification rules.

MSF.02.3 – Inventory and Classify All Business Data

Cyber-Operations Control

Establishing and maintaining accurate inventory of all business data – especially data that is considered sensitive, regulated, or business-critical – is essential to protecting against social engineering and deception-based threats. By classifying data according to its sensitivity – public, internal, confidential, restricted – organizations can ensure that they apply appropriate safeguards to prevent unauthorized disclosure. Role-Based or Attribute-Based Access Controls (RBAC, ABAC) and DLP solutions can be configured based on these data classifications.

MSF.01.6 - Basic Cybersecurity User Awareness Training Program

Cyber-Operations Control

Cybersecurity awareness training helps to educate employees about social engineering methods and will help them to recognize phishing and other social engineering techniques and deceptive communication methods.

Social engineering schemes rely on the exploitation of human trust and a lack of awareness about the risks. By training employees to recognize suspicious emails, phone calls, text messages and other social engineering tactics, organizations can significantly lower the likelihood of success for these kinds of attacks.

MSF.01.5 - Require Multifactor Authentication (MFA)

Cybersecurity Control

Using MFA significantly reduces the risk of an account being compromised, even if the credentials are stolen or guessed. It provides an additional authentication factor that is more difficult for attackers to bypass.

Social engineers often trick their targets into revealing credentials. MFA ensures that possession of these credentials alone is not enough to access an account. However, special care must be taken to stress to employees the need to protect their MFA codes and to never reveal an MFA code or token to anyone. Authorized support teams will not require this code to assist a user and will have alternative/administrative methods for accessing or recovering accounts when required. Preference should be to use phishing resistant MFA methods where possible.

MSF.02.2 - Document Contractual Requirements

Cyber-Operations Control

Establishing contractual obligation with third-party partners and vendors requiring secure communication channels and the verification of identities before sensitive information is shared reduces the risk of data compromise through social engineering.

Social engineering often involves impersonation or the manipulation of a trust relationship. By requiring identity verification and secure communication requirements in contracts, organizations can reduce the risk of information disclosure by means of deception.

MSF.02.11 - Configure Email Security

Cybersecurity Control

Implementing SPF, DMARC, and Secure Email Gateways (SEGs) helps to reduce phishing attempts by forcing sender authentication.

Email is the primary attack vector for social engineering attacks. By configuring email systems to authenticate senders and filter out many phishing emails, this control will reduce the likelihood of deceptive communications from reaching employees.

Additional Mitigations

In addition to the controls specified above, NIST 800-53 includes several controls that specifically relate to DLP efforts:

- AC-4 – Information Flow Enforcement: Enforces controls on the flow of information between designated sources and destination to prevent unauthorized disclosure or transmission.
- SC-12 through SC-28 – System Communication and Protection: These controls include a range of encryption, boundary defense, and transmission confidentiality requirements that prevent the leakage or disclosure of sensitive data.
- MP-5 and MP-6 – Media Transport Protections and Media Sanitization: Controls to ensure that data is securely handled during transfer and permanently removed from storage devices when no longer needed.
- SI-4(4) - Monitoring for Unauthorized Data Movement: Supports continuous monitoring capabilities to detect data exfiltration attempts.
- IR-4(1) - Incident Handling – Automated Reporting: Enhances DLP by ensuring that incidents related to data loss trigger immediate alerts and predefined responses.

Identity Theft and Fraudulent Carriers

Cybercriminals utilize identity theft and fraudulently masquerade as legitimate carriers or brokers to exploit vulnerabilities in brokerage, dispatch and load management systems. This involves stealing legitimate company or driver identities or even registering new “legitimate” but fraudulent companies with the FMSCA to gain unauthorized access to load boards, freight tenders, shipments data, and payment systems with the goal of facilitating cargo theft and financial fraud.

MSF.01.3 - Use Strong Unique Passwords

Cybersecurity Control

Identity theft and fraudulent carrier schemes typically involve credential stuffing using common username and password combinations or brute-force attacks. The use of strong, unique passwords helps to reduce these threats by making it significantly more difficult for threat actors to guess or crack passwords with these methods.

Using unique passwords for each account also reduces the risk of one compromised password leading to the breach of multiple accounts.

MSF.01.4 - Require Passwords on All Devices

Cybersecurity Control

Requiring passwords on all devices (including mobile devices used by drivers, dispatchers, and maintenance teams) reduces the risk of unauthorized access if a device is lost or stolen.

In identity theft and fraudulent carrier schemes, attackers may attempt to access TMS, telematics or other logistics systems through stolen devices. Requiring passwords creates an easy, and free first line of defense against unauthorized access to sensitive carrier data.

MSF.01.5 - Require Multifactor Authentication (MFA)

Cybersecurity Control

Using MFA significantly reduces the risk of an account being compromised, even if the credentials are stolen or guessed. It provides an additional authentication factor that is more difficult for attackers to bypass.

Identity theft scams frequently rely on stolen credentials. Properly configured MFA (e.g., Phishing-resistant MFA) ensures that credentials alone are not sufficient to gain unauthorized access to systems used to manage carrier identity.

MSF.01.10 - Implement a Least Privilege Account Access Policy

Cyber-Operations Control

Limiting user access to the minimum required to complete assigned duties reduces the overall available attack surface and the potential impact of compromised credentials.

In the context of preventing fraudulent carrier scams, strictly limiting access to systems such as FMCSA accounts, load board accounts, dispatch and telematics systems, etc., ensures that even if an employee's identity or account is compromised, the attacker is more likely to be prevented from accessing systems outside the scope of the compromised employee's specific role.

MSF.02.1 - Documented Incident Response Plan (IRP)

Cyber-Operations Control

A well-documented IRP includes predefined procedures for detecting and responding to and recovering from identity theft of account compromise.

Rapid identification and containment of compromised accounts are critical to preventing unauthorized pickups or financial fraud. An effective IRP ensures a swift and coordinated response.

MSF.02.6 - Designate Cybersecurity Roles and Responsibilities

Cybersecurity Control

Assigns clear roles for identity management, account monitoring, and incident response, ensuring accountability and rapid action in case of identity-related security incidents.

In the context of identity theft and fraudulent carrier schemes, it is crucial to have dedicated personnel responsible for monitoring identity usage, investigating anomalies, and executing incident response protocols to mitigate the impact or fraudulent activity.

Online Freight Platform Exploitation

The rise of online freight matching platforms, digital-native brokerages, and load boards has introduced new cyber-enabled fraud threat vectors. These platforms allow criminals to exploit weak cybersecurity controls, identity verification gaps, and to leverage social engineering to manipulate load assignments, steal cargo and commit financial fraud.

MSF.01.6 - Basic Cybersecurity User Awareness Training Program

Cyber-Operations Control

Cybersecurity awareness training helps to educate employees about the methods used and ways to detect lookalike domains, fraudulent websites, and spoofed communications from threat actors masquerading as official load board representatives.

Understanding how threat actors impersonate legitimate online freight platforms and load boards, will help employees function as a first line of defense against these types of attacks.

MSF.02.2 - Document Contractual Requirements

Cyber-Operations Control

Establishing contractual obligation with third-party partners and vendors requiring secure communication channels and the verification of identities before sensitive information is shared reduces the risk of data compromise through social engineering.

Unexpected changes in the methods of communication from a legitimate third-party load board of online freight service should be flagged for investigation and verification prior to any further interaction with the third-party. Threat actors will often use communication channels that are less secure, or unusual for the legitimate load board or freight service. E.g., SMS messages, encrypted messaging apps, similar/lookalike domain email accounts, private emails accounts, etc. By documenting the normal communication methods authorized for the relationship, organizations can reduce the risk of having their employees fall for these types of attacks.

MSF.04.5 - Documented Vendor Management Program

Cyber-Operations Control

Insider threats and collusion often involve an external partner as well. These can be contractors and vendors who have legitimate, authorized access to systems and data.

A documented vendor management program helps to ensure that vendors and third parties are thoroughly vetted, monitored, and contractually obligated to meet cybersecurity standards.

MSF.02.4 - Document Service Inventory

Cyber-Operations Control

Maintaining an updated inventory of all online freight platforms, cloud services, and third-party integrations used by the organization will aid in managing the exposure to potentially fraudulent load boards and online freight platforms.

Fake load board schemes often involve manipulating or hijacking legitimate platforms or using lookalike domains to impersonate legitimate services. By maintaining an inventory of authorized load boards and online freight platform URLs/APIs as well as the related accounts, exposure that can be mitigated on the customer end will be reduced.

Telematics and Technology Exploitation

The integration of telematics, fleet management systems, and IoT-enabled vehicle technologies enabled operational efficiency gains that have clearly benefited the transportation sector. However, these same advances have introduced potential cybersecurity risks if systems are not properly secured. Cybercriminals and fraudsters regularly exploit vulnerabilities in remote access protocols, SaaS portals, and data transmission mechanisms to gain unauthorized access, manipulated data, or facilitate fraudulent activity.

MSF.01.1 - Keep Software and Operating Systems Updated

Cybersecurity Control

Keeping software and systems updated reduces the likelihood of easily compromised vulnerabilities in the organization's technology platforms and systems. Exploitation of unpatched applications and operating systems is one of the most common attack vectors for cyber criminals engaged in general cybercrime or cyber-enabled cargo theft.

MSF.02.19 - Special Purpose Devices are Isolated from Enterprise Networks

Cybersecurity Control

Ensuring that devices with direct access to, or connections with, TMS systems, telematics systems or maintenance software (such as warehouse or dock handheld scanners, mobile devices belonging to drivers and logistics personnel, maintenance diagnostics laptops, etc.) are isolated from the main enterprise network will reduce the risk that one of these devices is compromised by a threat actor who gains access to another portion of the network. This can help to reduce the risk of lateral movement within the network resulting in direct access to telematics portals or sensitive cargo or vehicle-related information.

MSF.02.17 - Access to OT and Vehicle Systems Based on Role-Based/Attribute-based Access Control (RBAC/ABAC)

Cybersecurity Control

Utilizing RBAC/ABAC helps to ensure that only authorized personnel and devices can access telematics systems and diagnostics/maintenance applications. Telematics data and onboard systems access can be used to track/reroute shipments to facilitate cargo theft. Implementing RBAC/ABAC reduces the risk of unauthorized access, reducing the risk of data breaches and cargo tracking/rerouting.

MSF.02.10 - Proactive End of Life (EOL) Management Policies

Cybersecurity Control

Ensuring that telematics devices, maintenance tools, diagnostic laptops, and all associated software are kept up to date, patched, and replaced before they reach end of support life helps to reduce the risk of successful compromise of these systems. Attackers commonly target outdated systems with known vulnerabilities, by proactively managing EOL devices and software, the risk of exploitation is reduced.

MSF.02.15 - Encrypt all Devices

Cybersecurity Control

By encrypting all devices, including mobile devices, the risk of sensitive data being compromised in the event of the theft or loss of a device is reduced. Data at rest should be in an encrypted state and secure communication protocols should be utilized whenever data is transmitted.

Conclusion

Cyber-enabled cargo theft is a dynamic and complex threat, but it is not insurmountable. This guide has illustrated that effective prevention requires a holistic, layered defense encompassing cybersecurity, operational safeguards, and physical security measures. There is no single silver bullet – threat actors will continue to adapt with new tactics, from phishing schemes and ransomware to identity theft and insider collusion. Yet, by proactively implementing the practical mitigations discussed, transportation sector organizations can significantly reduce their risk exposure. Every security control put in place – whether it's enforcing multifactor authentication, vetting business partners, training staff on fraud awareness, or hardening IT systems – is a meaningful step toward protecting your fleet and freight.

Now is the time for action. We encourage carriers, brokers, shippers, and all supply chain partners to take ownership of the solutions presented in this guide. Treat cybersecurity and cargo security with the same rigor as safety and compliance. Create clearly defined communication plans, specifically identifying the proper incident reporting processes and contact points, both internally and with external law enforcement agencies and insurance contacts. Conduct regular assessments and drills, update incident response plans, and ensure leadership supports a culture of security. Collaborate with law enforcement and industry initiatives (such as information-sharing networks and the NMFTA cybersecurity community) to stay ahead of emerging threats. Report incidents and suspicious activities promptly – this not only aids investigations but also helps the whole industry learn and strengthen defenses. Remember that building resilience is an ongoing journey: review and refine your security measures continuously as the threat landscape evolves.

Despite the complexity of the challenge, the tone of this conclusion is intentionally optimistic: cyber-enabled cargo theft can be mitigated with vigilance and collective effort. The transportation sector has a long history of overcoming adversity through innovation and cooperation. By embracing best practices and frameworks, investing in robust security programs, and working together across organizations, we can thwart even the most organized and tech-savvy thieves. The payoff for this hard work is tangible – safer supply chains, preserved profits and reputations, and increased trust from customers and partners. In an era where criminal tactics are growing more sophisticated, our industry's commitment to security must grow stronger still. Armed with knowledge from this guide and the resources referenced, you have the tools to act. The National Motor Freight Traffic Association stands with you in this effort. Together, let's harden our defenses and take back control from cyber-enabled criminals. The future of secure and resilient freight transport depends on what we do next – so let's get to work.

Implementation Checklist

Implemented	Date	Control ID	Control Description	Control Type	Threat Vector(s)
		MSF.01.1	Keep Software and Operating Systems Updated	Cybersecurity Control	Telematics and Technology Exploitation
		MSF.01.10	Implement a Least Privilege Account Access Policy	Cybersecurity Control	Insider Threats and Collusion Identity Theft and Fraudulent Carriers
		MSF.01.3	Use Strong Unique Passwords	Cybersecurity Control	Identity Theft and Fraudulent Carriers
		MSF.01.4	Require Passwords on All Devices	Cybersecurity Control	Identity Theft and Fraudulent Carriers
		MSF.01.5	Require MFA	Cybersecurity Control	Social Engineering and Deception Identity Theft and Fraudulent Carriers
		MSF.01.6	Basic Cybersecurity Awareness Training Program	Cyber-Operations Control	Social Engineering and Deception Online Freight Platform Exploitation
		MSF.02.04	Document Service Inventory	Cyber-Operations Control	Online Freight Platform Exploitation
		MSF.02.1	Documented Incident Response Plan (IRP)	Cyber-Operations Control	Organized Crime Identity Theft and Fraudulent Carriers
		MSF.02.10	Proactive End of Life (EOL) Management Policies	Cybersecurity Control	Telematics and Technology Exploitation
		MSF.02.11	Configure Email Security	Cybersecurity Control	Social Engineering and Deception
		MSF.02.15	Encrypt All Devices	Cybersecurity Control	Telematics and Technology Exploitation
		MSF.02.17	`Access to OT and Vehicle Systems Based on RBAC/ ABAC	Cyber-Operations Control	Insider Threats and Collusion Telematics and Technology Exploitation
		MSF.02.19	Special Purpose Devices are Isolated from Enterprise Networks	Cybersecurity Control	Telematics and Technology Exploitation

Implementation Checklist Cont.

Implemented	Date	Control ID	Control Description	Control Type	Threat Vector(s)
		MSF.02.2	Document Contractual Requirements	Cyber-Operations Control	Social Engineering and Deception Online Freight Platform Exploitation
		MSF.02.3	Inventory and Classify All Business Data	Cyber-Operations Control	Social Engineering and Deception
		MSF.02.6	Designate Cybersecurity Roles and Responsibilities	Cyber-Operations Control	Insider Threats and Collusion Identity Theft and Fraudulent Carriers
		MSF.03.2	Security Incident and Event Management (SIEM) Solution	Cybersecurity Control	Insider Threats and Collusion
		MSF.04.1	Legal and Regulatory Compliance is Actively Managed	Cyber-Operations Control	Organized Crime
		MSF.04.5	Documented Vendor Management Program	Cyber-Operations Control	Organized Crime Insider Threats and Collusion Online Freight Platform Exploitation
		MSF.04.6	Formalized, Documented Cybersecurity Policies	Cyber-Operations Control	Organized Crime
		NIST 800-53 AC-4	Information Flow Enforcement	Cybersecurity Control	Social Engineering and Deception
		NIST 800-53 IR-4(4)	Incident Handling – Automated Reporting	Cybersecurity Control	Social Engineering and Deception
		NIST 800-53 MP-5 and MP-6	Media Transport Protections and Sanitization	Cyber-Operations Control	Social Engineering and Deception
		NIST 800-53 SC-12 to SC-28	System Communication Protection	Cybersecurity Control	Social Engineering and Deception
		NIST 800-53 SI-4(4)	Monitoring for Unauthorized Data Movement	Cybersecurity Control	Social Engineering and Deception

Notes

Notes

Acronyms

ABAC – Account Based Access Control

API – Application Programming Interface

ARP – Address Resolution Protocol

ATF – Bureau of Alcohol, Tobacco, and Firearms

BCP – Business Continuity Plan

CBP – Customs and Border Protection

CIS – Center for Internet Security

CPG – Cybersecurity Performance Goals

CSF – Cybersecurity Framework

DEA – Drug Enforcement Agency

DKIM – Domain Keys Identified Mail

DLP – Data Loss Prevention

DMARC – Domain based Message Authentication, Reporting, and Conformance

DRP – Disaster Recovery Plan

EDR – Endpoint Detection and Response

EOL – End of Life

FBI – Federal Bureau of Investigations

FMCSA – Federal Motor Carrier Safety Administration

HSI – Homeland Security Investigations

IoC – Indicator of Compromise

IRP – Incident Response Plan

IRT – Incident Response Team

IT – Information Technology

JTF – Joint Task Force

MAC – Media Access Control

MDM – Mobile Device Management

MFA – Multifactor Authentication

MSP – Managed Services Provider

MSSP – Managed Security Services Provider

NIDS – Network Intrusion Detection System

NIPS – Network Intrusion Prevention System

NIST – National Institute of Standards and Technology

NMFTA – National Motor Freight Traffic Association

OPSEC – Operational Security

OS – Operating System

PII – Personally Identifiable Information

RBAC – Role-Based Access Control

SaaS – Software as a Service

SEG – Secure Email Gateway

SIEM – Security Incident and Event Management

SMB – Small to Medium Business

SMS – Short Message Service

SPF – Sender Policy Framework

STF – Special Task Force

SWAT – Special Weapons and Tactics

TMS – Transportation Management System

TSA – Transportation Security Administration

TSP – Telematics Service Provider

TTP – Tactics, Techniques, and Procedures

TTX – Tabletop Exercise

URL – Uniform Resource Locator

USSS – United States Secret Service

VPN - Virtual Private Network

ZTA – Zero Trust Architecture

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

1001 N. Fairfax Street, Suite 600

Alexandria, VA 22314-1798

(866) 411-6632

www.nmfta.org