Cybersecurity Incident Management in the Trucking Industry

Jeremy Daily, Ph.D., P.E.

Urban Jonson

March 13, 2026

Executive Summary

Motor freight transportation has evolved into a highly interconnected cyber-physical system linking commercial vehicles, telematics platforms, cloud services, logistics systems, and regulatory infrastructure. Modern fleets utilize Electronic Logging Devices (ELDs), telematics systems, cloud-based dispatch and fleet management platforms, remote diagnostics, and extensive third-party service providers to enable efficient and compliant operations. While these technologies generate substantial operational and safety benefits, they also introduce systemic cybersecurity risks by tightly coupling vehicle systems, enterprise IT environments, vendors, and regulatory infrastructure. As a result, cybersecurity incidents in the motor freight sector are no longer confined to data loss or traditional IT outages; they increasingly threaten to disrupt vehicle operations, degrade roadway safety, and cascade across supply chains and national borders.

To date, the trucking industry has not experienced a publicly confirmed malicious cyber incident that simultaneously disrupts fleets, vendors, and freight operations at a large operational scale. However, research findings, observed vulnerabilities, and incidents in adjacent sectors demonstrate that the conditions for such an event already exist. Shared technology platforms, homogeneous device deployments, centralized telematics services, and reliance on cloud infrastructure create environments where localized compromises can propagate rapidly across multiple fleets or regions.

This report examines cybersecurity incident management for cyber events that may evolve from subtle technical anomalies into widespread operational disruption. The analysis builds on the NIST Cybersecurity Framework (CSF) 2.0 to evaluate how the Detect, Respond, and Recover functions operate in a distributed environment characterized by fragmented authority, limited operational visibility, and complex vendor dependencies. Particular attention is given to the convergence of information technology (IT) and operational technology (OT), where cyber activity may resemble routine maintenance actions, equipment faults, or driver error. This ambiguity can delay detection and complicate escalation decisions, allowing incidents to persist or expand before coordinated response mechanisms are activated.

A central finding of the report is that large-scale incident response in motor freight is constrained less by technology and more by organizational and systemic factors. Maintenance technicians, fleet operations personnel, and safety staff are often the first to observe operational anomalies, yet escalation pathways are typically designed for isolated mechanical failures rather than correlated cyber events. At the same time, technology vendors and cybersecurity teams may detect digital intrusions without clear visibility into their operational consequences. When incidents span fleets, vendors, or jurisdictions, it is uncertain who possesses the authority, resources, or situational awareness to coordinate an effective response independently.

To address these challenges, the report introduces complementary frameworks designed to strengthen incident response across the motor freight ecosystem. A new **Industry Readiness Maturity Model** provides carriers and technology providers with a structured method for assessing and improving their ability to detect, respond to, and recover from cyber incidents affecting freight operations. Similarly, a **Government Readiness Maturity Model** provides a parallel framework for evaluating how public-sector organizations coordinate responses to large-scale incidents, including incident triage, interagency communication, technical assistance, and cross-border coordination.

Because freight transportation routinely crosses provincial and national boundaries, government coordination is essential for managing systemic cyber incidents. The report highlights how stakeholders can support ecosystem resilience by facilitating information sharing, strengthening sector coordination, and aligning transportation cybersecurity practices with national frameworks such as Canada's Federal Cyber Incident Response Plan (FCIRP). The analysis also emphasizes the importance of compatible U.S.–Canada alerting and coordination mechanisms when incidents affect shared freight corridors, infrastructure providers, or cross-border supply chains.

Ultimately, the report argues that cybersecurity incident management in motor freight must be treated as an operational capability rather than a compliance exercise. Effective preparedness requires shared situational awareness, structured escalation thresholds, practiced coordination mechanisms, and governance frameworks that recognize freight transportation as a distributed cyber-physical system. Largely, these incident response mechanisms already exist, but personnel (both government and industry) may not be aware of the available resources. By developing incident response and coordination plans, industry and government stakeholders can reduce the likelihood that cyber incidents escalate into widespread safety, economic, or national security disruptions.

Table of Contents

Executive Summary i

1 Introduction 1

1.1 Background and Context 1

1.2 Objectives 3

1.3 Intended Audience and Stakeholders 3

2 Motor Freight Cybersecurity Landscape 5

2.1 Key Attack Surfaces for Motor Freight Systems 5

2.2 Regulatory and Policy Drivers 6

2.3 Roles and Responsibilities in Trend Analysis and Incident Response 10

2.4 Cross-Industry and Cross-Border Threat Intelligence Integration 11

2.5 Implications for Carrier, Vendor, and Regulator Practice 13

2.6 Considerations Going Forward 14

3 Framework for Incident Response at Scale 15

3.1 Mapping CSF Functions to Motor Freight Operations 15

3.2 Systemic Challenges in Large-Scale Incident Response 17

3.3 Bilateral Incident Response Frameworks 19

3.4 Governance Models for Scalable Response and Coordination 20

4 Policy and Regulatory Implementation Roadmap 24

4.1 Maturity Model for Cyber Incident Response Readiness 24

4.2 Workforce Training and Capacity Building 30

4.3 Pilot Programs and Data-Sharing Demonstrations 31

4.4 Measuring Response Effectiveness and Return on Investment (ROI) 32

4.5 Roadmap Alignment with International Practices 34

4.6 Incentives for Participation 35

5 Data Collection and Sharing 38

5.1 Data Source Overview 38

5.2 Operational Technology Data Sources 39

5.3 Information Technology Data Sources 40

5.4 Secure Data Collection and Sharing Practices 42

5.5 International Information Sharing Pathways and Mechanisms 43

5.6 Instrumentation Challenges in Mixed Legacy and Modern Fleets 45

5.7 Data Integrity, Timestamping, and Chain-of-Custody Considerations 45

5.8 Potential Incident Response Architecture 46
5.9 Legal and Regulatory Considerations for Data Sharing 47
6 Forensic Analysis and Escalation Criteria 49
6.1 Defining Cyber Incident Severity and Escalation Thresholds 49
6.2 Defining Response Thresholds for Stakeholder Notification 52
6.3 Forensic Readiness: Pre-Incident Planning and Documentation 56
6.4 Investigative Workflows: Evidence Collection, Preservation, and Analysis 59
7 Conclusion 62
7.1 Summary of Key Insights 62
7.2 Long-Term Vision for Cyber Resilience in the Freight Sector 62
Acknowledgements 63
References 64

1 Introduction

The motor freight industry is undergoing a fundamental transformation as trucks, trailers, and logistics operations become deeply integrated with digital systems, cloud platforms, and persistent connectivity. This convergence of information technology, operational technology, and vehicle systems has created a cyber-physical ecosystem in which cybersecurity incidents can directly affect vehicle behavior, roadway safety, regulatory compliance, and supply chain continuity. While a connected ecosystem delivers substantial operational benefits, they also introduce new classes of large-scale cyber risk. This report examines cybersecurity incident management through a system-level lens. By grounding the analysis in real-world operational practices and established frameworks such as the NIST Cybersecurity Framework, the report aims to inform carriers, vendors, regulators, and policymakers on how to strengthen resilience against high-impact cyber incidents in an increasingly interconnected transportation system.

1.1 Background and Context

The trucking industry has adopted connected technologies, including telematics, Electronic Logging Devices (ELDs), cloud-based fleet management systems, and advanced driver assistance systems. Modern motor carriers operate as tightly integrated cyber-physical systems, in which vehicles, drivers, back-office IT infrastructure, third-party vendors, and regulators exchange large volumes of operational and compliance data in near real time. Furthermore, the motor freight carriers operate in a systems-of-systems model where the resources utilized have distributed ownership and cross-organizational dependencies, which challenge effective incident response to a cybersecurity attack.

Motor carriers may be targeted by cybercriminals seeking financial gain through ransomware, fraud, and cargo theft; nation-state actors seeking supply chain intelligence and disruption; insider threats; and opportunistic attackers exploiting weak credentials and outdated systems. Real-world incidents, like ransomware attacks on major freight carriers, show how quickly operations can be disrupted when backend systems, dispatch, or communications are compromised. At the vehicle level, academic research indicates that vulnerabilities in ELDs and telematics systems could enable remote attacks that propagate across fleets, underscoring the risk that cyber incidents can escalate rapidly if not detected and contained early.

Effective cybersecurity incident management in trucking is further complicated by the industry's operational realities and regulatory environment. Many carriers depend on legacy systems, third-party software, and self-certified devices, while cybersecurity expertise and training among drivers and fleet personnel remain inconsistent. Regulatory frameworks covering hours of service, vehicle safety, data privacy, and international operations often focus on data integrity and compliance but do not fully address cyber-physical incident response and recovery. Therefore, this report emphasizes the need for structured incident management systems integrating detection, response, and recovery across both vehicle and backend systems. Without coordinated incident response planning, exercises, and governance, cyber incidents in the trucking industry risk escalating into large-scale safety, economic, and supply chain disruptions.

1.1.1 Logistics IT infrastructure

The information technology ecosystem supporting motor freight and ground freight logistics is broad, complex, and highly interconnected. It extends beyond motor carriers to include third-party logistics providers, telematics vendors, cloud service providers, managed service providers, and a wide range of back-office systems such as human resources, accounting, billing, dispatch, safety, and compliance platforms. These systems are increasingly linked through APIs, software-as-a-service platforms, and direct connections with customers, business partners, and government systems, often across national borders. As a result, what was once a collection of mostly independent systems has evolved into a tightly connected logistics network built on legacy mainframes, client-server environments, cloud infrastructure, SaaS applications, and emerging AI-enabled services.

This growing connectivity has improved efficiency, visibility, and coordination across freight operations, but it has also increased systemic cyber risk. A disruption affecting a single provider or quickly cascade across communications, telematics, billing, dispatch, and other essential services. These risks are especially difficult for small and mid-sized carriers, which often rely heavily on third-party technology and may lack the personnel, visibility, and technical maturity needed to manage cybersecurity across converged IT and operational environments. Common gaps include limited monitoring, weak event correlation, and immature escalation and reporting processes. Coordination is further complicated by organizational structures that still separate enterprise IT from fleet operations, even as the systems themselves converge. Because motor freight is essential to the movement of food, medicine, chemicals, and other critical goods, resilience depends on more than just preventing disruptions. It also requires integrated governance, strong situational awareness, and practiced incident response and recovery plans that can operate effectively at scale.

1.1.2 Trucks and Rolling Assets

A 2025 review paper by Rahimi et al. of the University of Windsor explained cybersecurity vulnerabilities in heavy-duty vehicles and identified major research gaps [1]. Their review argues that heavy-duty vehicles have received less attention for cybersecurity than light-duty vehicles, despite their critical role in commercial transportation and supply chains. It emphasizes that increased connectivity has expanded the attack surface of trucks and other heavy vehicles. Key findings from Rahimi et al. include:

- **Heavy-duty vehicles face distinct cybersecurity challenges** because of different architectures, operational demands, and interfaces.
- **SAE J1939 and related heavy-vehicle communication environments are a central concern**, especially because heavy-duty vehicles often rely on more open and externally accessible network structures for the horizontally integrated nature of heavy-duty vehicle architecture.
- **External connections such as diagnostics, telematics, ELDs, wireless interfaces, and fleet communications substantially enlarge the attack surface**, creating pathways for both local and remote compromise.
- **The literature base is still relatively small**, with the review identifying only a limited set of heavy- and medium-duty cybersecurity publications from 2010 to 2024, underscoring how underdeveloped this field remains compared with light-duty vehicle security research.

This perspective aligns well with FMCSA's 2020 best-practices report [2], which treats telematics and aftermarket devices as major attack vectors in heavy vehicles and frames cybersecurity primarily as a safety and reliability issue. That report provides strong lifecycle guidance for design, integration, deployment, vulnerability response, logging, patching, and incident response, but it is focused mainly on reducing compromise at the level of individual devices, vehicles, or fleets rather than fully addressing cyber incidents that may propagate across many fleets, vendors, or regions at once.

The broader cyber-physical concern is that vehicle operational technology was historically designed for reliability and performance rather than adversarial resilience. As Correnti et al. observe in another safety-critical vehicle domain [3], operators and maintainers often lack the tools and visibility needed to continuously monitor internal networks or distinguish between a cyberattack and a true maintenance issue. In the trucking context, where telematics, ELDs, diagnostics, and aftermarket devices increasingly connect vehicle systems to enterprise IT and external networks, this limited observability raises the risk that abnormal behavior may be misinterpreted, delayed in response, or allowed to escalate into broader safety, compliance, and freight movement disruptions.

1.2 Objectives

The primary objective of this report is to examine cybersecurity incident management in connected motor freight operations through a system-level lens, with particular emphasis on how cyber incidents can emerge, propagate, and scale across vehicles, fleets, vendors, and jurisdictions. Rather than treating cybersecurity solely as an information technology problem, the report frames motor freight as a cyber-physical system of systems in which vehicles, telematics platforms, enterprise IT, third-party services, and regulatory processes interact to shape both risk and response.

Another key objective is to assess how incident detection, response, and recovery responsibilities are distributed across motor carriers, technology vendors, original equipment manufacturers, regulators, first responders, and government coordination bodies. The report evaluates how differences in authority, visibility, and mission affect investigative workflows, evidence handling, information sharing, and decision-making during cyber incidents that span both digital and physical domains.

Finally, the report seeks to outline principles and considerations that can support more resilient and coordinated cybersecurity incident management in motor freight operations. These considerations are informed by established frameworks such as the NIST Cybersecurity Framework, transportation safety practices, and cross-border coordination models, and are intended to help stakeholders improve preparedness, reduce ambiguity during incidents, and limit the operational and societal impacts of cyber events at scale.

1.3 Intended Audience and Stakeholders

This report is intended for a broad set of stakeholders involved in the design, regulation, operation, and oversight of motor freight systems. Primary audiences include motor carriers, fleet operators, vehicle and telematics manufacturers, aftermarket device vendors, and maintenance service providers responsible for deploying and managing connected vehicle technologies. The report is also relevant to cybersecurity professionals and systems engineers tasked with securing cyber-physical transportation systems.

In addition, policymakers, regulators, and standards organizations may use this report to better understand how cybersecurity risks manifest operationally within motor freight operations and how regulatory requirements interact with technical and organizational controls. By addressing cybersecurity from a system-level perspective, the report aims to support informed decision-making across technical, operational, and regulatory domains.

This report makes three primary contributions:

1. a system-of-systems analysis of cyber incident escalation in motor freight operations;
2. proposed readiness maturity models for both industry and government coordination; and
3. a policy and operational roadmap to improve large-scale incident response across the North American freight ecosystem.

2 Motor Freight Cybersecurity Landscape

Cybersecurity in the motor freight sector is shaped by the scale, heterogeneity, and operational complexity of connected fleet environments. Carriers often manage large numbers of vehicles across broad geographic areas while relying on multiple vendors, telematics platforms, aftermarket devices, and shared backend services that operate with uneven security controls and fragmented governance. In this setting, cyber risk is amplified by limited visibility into vehicle operational technology and by the difficulty of distinguishing malicious activity from normal maintenance or system faults, especially when diagnostic traffic, firmware changes, and remote communications are routine parts of operations. These conditions make localized compromise harder to detect and more likely to be misclassified, while also increasing the likelihood that weaknesses in common devices, interfaces, or service providers could propagate across fleets. This section examines that landscape in more concrete terms by identifying the major technical and organizational attack surfaces through which cyber incidents can emerge, spread, and disrupt freight operations at scale.

2.1 Key Attack Surfaces for Motor Freight Systems

Motor freight systems present a dual cyber risk profile spanning vehicle-resident operational technology and enterprise back-office information systems. On the vehicle side, increasing connectivity through diagnostics, telematics, and regulatory technologies exposes legacy in-vehicle networks to remote exploitation via standardized protocols and privileged maintenance interfaces. On the enterprise side, carriers operate complex, highly interconnected back-office environments that rely on remote access, cloud services, and extensive third-party integrations, making them vulnerable to credential abuse, internet-exposed infrastructure flaws, and supply-chain compromise. These attack surfaces blur traditional boundaries between IT and OT, maintenance and intrusion, and isolated incidents versus fleet-wide disruption. Understanding how attackers exploit both domains is essential for assessing cyber risk in modern motor freight operations and for anticipating how localized compromises can escalate into systemic operational, safety, and economic impacts.

2.1.1 Attacks on Trucks, Trailers, Diagnostics, and Telematics

Modern commercial trucks are exposed to multiple cyber attack surfaces through their onboard diagnostics, telematics systems, and vehicle network interfaces. Heavy-duty vehicles rely extensively on standardized protocols such as SAE J1939 and RP1210 to support diagnostics, maintenance, regulatory compliance, and fleet monitoring. These interfaces are essential for legitimate operational use, but they also provide attackers with potential pathways to access in-vehicle networks that were not originally designed with strong security controls. As connectivity has increased, attacks that once required physical access can now be executed remotely through wireless diagnostic adapters, ELDs, and telematics platforms [4].

Diagnostic interfaces represent a particularly critical point of exposure. Vehicle Diagnostic Adapters (VDAs), which bridge external service computers and the vehicle's internal networks, are widely used across the trucking industry for maintenance and troubleshooting. Research has demonstrated that commercially available VDAs often contain wireless capabilities, debug interfaces, and firmware update mechanisms that lack authentication or cryptographic protection. These weaknesses allow attackers to

remotely modify adapter firmware, inject arbitrary CAN or J1939 messages, and manipulate vehicle data such as engine hours or identification information without detection [5]. Because diagnostic traffic is expected during normal operations, malicious activity conducted through these interfaces can closely resemble legitimate maintenance actions, complicating detection and response.

2.1.2 Attacks on Back-Office Systems

Motor freight carriers use complex back-office systems that support dispatch, transportation management systems (TMS), warehouse and yard management systems (WMS/YMS), fleet maintenance platforms, billing and settlement systems, identity and access management (IAM), and extensive third-party integrations with brokers, shippers, fuel vendors, and compliance platforms. These systems are increasingly accessed remotely via VPNs, VDI, cloud portals, and API-driven data exchanges, which expands the attack surface beyond traditional perimeter boundaries.

The Verizon 2025 Data Breach Investigations Report (DBIR), which reports cybersecurity exploits across industries, shows that credential abuse (22%) and exploitation of vulnerabilities (20%) are the most common initial access methods in recent breaches, and servers are involved in about 95 percent of incidents. This underscores the critical role of backend system vulnerabilities in real-world cyberattacks [6]. The convergence of credential abuse, edge infrastructure exposure, and third-party dependency, as detailed in major threat intelligence reports, directly reflects the operational structure of the motor freight logistics chain. Effective cyber risk management, therefore, should focus on implementing strong authentication controls, accelerating patch management for internet-facing systems, and continuously monitoring third-party access points, in accordance with guidance from Microsoft's Digital Defense Report [7].

2.1.3 Attacks At Scale

In motor freight transportation, attacks at scale are best understood through the concept of blast radius, which describes how far the effects of a cyber compromise can propagate once access is achieved. In this sector, blast radius is shaped not only by technical vulnerabilities but also by shared infrastructure, privileged access, and tightly coupled operational dependencies across vehicles, telematics platforms, cloud services, edge devices, and software supply chains. A weakness in a common telematics provider, white-labeled ELD, cloud-hosted identity service, firewall platform, or software update mechanism can extend far beyond a single fleet, enabling disruption across many vehicles, terminals, carriers, or even cross-border freight corridors. Because trucks increasingly function as connected edge nodes within a broader cyber-physical logistics ecosystem, the consequences of compromise are not limited to data loss or isolated outages, but can include degraded dispatch, impaired safety monitoring, delayed shipments, compliance failures, and cascading supply chain effects. In this environment, the scale of cyber risk depends less on any single flaw than on how architecture, trust relationships, deployment homogeneity, and vendor concentration amplify the consequences of compromise, making coordinated detection, response, and recovery a multi-entity challenge rather than a problem any single operator can contain alone.

2.2 Regulatory and Policy Drivers

Regulatory and policy drivers play a central role in shaping how cybersecurity risks are managed in the motor freight sector, particularly as vehicles, telematics, and enterprise systems become increasingly interconnected and as cyber incidents carry safety, economic, and national security implications. Across

jurisdictions, policymakers have largely converged on risk-based cybersecurity principles emphasizing governance, visibility, resilience, and coordination across information technology (IT) and operational technology (OT). However, there are markedly different approaches to enforcement, scope, and accountability. This section examines how the United States, Canada, and the European Union frame cybersecurity expectations for transportation systems, highlighting the predominance of voluntary guidance in North America, the growing role of privacy and critical-infrastructure policy in Canada, and the more prescriptive, lifecycle-oriented regulatory model emerging in Europe. Together, these approaches illustrate both the strengths and limitations of current policy frameworks in driving consistent, scalable cybersecurity outcomes for motor freight operations.

2.2.1 Canada

Cybersecurity obligations for motor freight carriers in Canada arise primarily from privacy law and emerging critical infrastructure policy rather than from transportation-specific cyber regulation. Federal privacy requirements under the Personal Information Protection and Electronic Documents Act (PIPEDA) [8] and provincial regimes, such as Quebec's Law 25 [9] impose mandatory breach notification, recordkeeping, and accountability for incidents involving personal information, indirectly driving improvements in incident detection and governance. At the same time, Canada's Bill C-8 signals a shift toward mandatory cybersecurity programs and incident reporting for designated operators in federally regulated sectors, including transportation [10]. However, the scope and applicability of these obligations to most motor carriers remain under debate and development, creating uncertainty around future compliance expectations.

2.2.2 United States

In the United States, cybersecurity expectations for the motor freight sector are shaped less by mode-specific regulation and more by cross-cutting national cybersecurity policy, critical-infrastructure frameworks, and privacy law. Federal cybersecurity policy has increasingly emphasized incident visibility, information sharing, software supply chain integrity, and zero-trust principles across both information technology (IT) and operational technology (OT) environments. Executive Order 14028, Improving the Nation's Cybersecurity, explicitly recognizes the convergence of IT and OT and establishes federal expectations for prevention, detection, response, and remediation of cyber incidents, with a strong focus on logging, incident reporting, supply chain transparency, and coordination between government and the private sector [11]. While EO 14028 applies directly to federal agencies and contractors, its requirements have had a significant downstream influence on cybersecurity expectations across critical infrastructure sectors, including transportation and logistics.

Complementing this posture, Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, frames cybersecurity risk as a national security issue tied to the provenance, integrity, and trustworthiness of digital technologies used in critical systems [12]. This order provides authority to restrict or mitigate the use of Information and Communication Technology (ICT) products and services linked to foreign adversaries when they pose undue risk to critical infrastructure or the broader digital economy. For motor freight carriers, this policy context reinforces growing scrutiny of telematics platforms, diagnostic tools, cloud services, and network infrastructure that form the backbone of modern fleet operations. Although enforcement actions under EO 13873 typically target vendors rather than carriers, the order elevates supply chain risk management as a core component of cybersecurity governance.

Within the transportation sector, agencies such as DHS (through CISA and TSA) and FMCSA have predominantly issued voluntary, risk-based cybersecurity guidance rather than prescriptive mandates for motor freight carriers. For example, CISA's *Transportation Systems Sector Cybersecurity Framework Implementation Guide* [13] encourages application of the NIST Cybersecurity Framework to reduce risk, but does not establish binding requirements for carriers, TSA's *Surface Transportation Cybersecurity Toolkit* similarly offers best practices based on NIST without enforceable obligations, and FMCSA's publicly posted materials focus on "best practices" for automotive telematics rather than regulatory mandates [2]. As noted by the U.S. Government Accountability Office, TSA's surface transportation cybersecurity efforts have historically relied on guidance and assessments rather than uniform risk management standards across the broader sector.

The North American regulatory environment establishes strong policy signals but limited direct enforcement for motor freight cybersecurity. Federal strategies emphasize resilience, transparency, and coordination across IT and OT, yet leave substantial discretion to carriers regarding implementation. This regulatory posture risks uneven adoption of cybersecurity controls across the sector, particularly among small and mid-sized carriers, despite the motor freight industry's systemic importance to economic stability and supply chain continuity.

2.2.3 European Regulations

UN ECE Regulations R155 and R156, along with the EU Cyber Resilience Act (CRA), collectively set a baseline for cybersecurity and software integrity in transportation systems and their supporting digital products for the European market. R155 links road-vehicle type approval to the manufacturer's ability to operate a Cyber Security Management System (CSMS) that manages cybersecurity risks throughout the vehicle's lifecycle. Meanwhile, R156 highlights governance and traceability for vehicle software updates through a Software Update Management System (SUMS), including over-the-air updates. The CRA extends beyond vehicles to establish horizontal cybersecurity requirements for products with digital components sold in the EU, covering many transportation technologies such as telematics devices, gateways, and other connected edge products, while excluding areas already regulated by specific vehicle, aviation, and marine safety regimes.

2.2.3.1 UN ECE R155

UN ECE Regulation No. 155 sets cybersecurity expectations for road-vehicle type approval by requiring manufacturers to implement and maintain a Cyber Security Management System (CSMS), which is a documented, risk-based framework for identifying, assessing, and managing cyber risks affecting vehicles and their electrical/electronic systems [14]. In practical terms, it requires OEMs to demonstrate the organizational capability to manage threats and vulnerabilities across the vehicle lifecycle, including governance, risk assessment practices, security engineering, verification/validation, and defined incident-handling and continuous-improvement processes.

In the UNECE/EU type-approval framework, vehicles are grouped into standardized categories based on their design and intended use. Category L covers powered two- and three-wheel vehicles and quadricycles (e.g., mopeds, motorcycles, tricycles, and light four-wheelers) [15]. Category M includes vehicles designed to carry passengers (from passenger cars through buses), while Category N covers vehicles designed to carry goods (from light commercial vans to heavy trucks), both further subdivided

by seating capacity and/or maximum mass. Category O applies to trailers, subdivided primarily by maximum mass [16].

For transportation stakeholders, R155 is significant because it formalizes cybersecurity as a requirement for approval and promotes consistent practices across the connected-vehicle ecosystem. It encourages manufacturers and suppliers to identify common vehicle exposure points as part of an overall risk surface that should be managed, tested, and monitored after vehicles are deployed. R155 also highlights the importance of post-production activities, including monitoring for emerging threats, addressing vulnerabilities, and collaborating with suppliers, because compliance depends on demonstrating cybersecurity capabilities not only at launch but throughout the vehicle's supported lifetime.

2.2.3.2 UN ECE R156

UN ECE Regulation No. 156 addresses the safety and integrity of vehicle software updates, including over-the-air updates, by requiring manufacturers to operate a Software Update Management System (SUMS), which is the organizational processes and procedures used to deliver, control, and document updates in accordance with regulatory requirements [17]. It applies to vehicles in categories M, N, O, R, S, and T that permit software updates, covering passenger vehicles, trucks, trailers, and certain agricultural/forestry tractors and towed equipment in the UNECE classification system. In effect, R156 is an “update governance” rule: it requires that updates be managed in a controlled way, with traceability and accountability for what software changed, why it changed, and how it was validated.

From a transportation operations perspective, R156 is important because software now plays a key role in safety, compliance, and uptime. The regulation links organizational update procedures to type-approval readiness. It requires manufacturers to identify approval-relevant software, maintain records, and demonstrate that their update processes reduce the risk of unauthorized or unsafe changes. The rule also creates a compliance framework that includes a Certificate of Compliance for the SUMS, highlighting that authorities assess not only the technical update method but also the manufacturer’s management system for planning, validating, deploying, and documenting updates. This is especially relevant for fleets that rely on over-the-air updates to maintain security and functionality without taking vehicles out of service, while ensuring that updates do not cause safety regressions or interfere with regulated functions.

2.2.3.3 EU Cyber Resilience Act

The EU Cyber Resilience Act, Regulation (EU) 2024/2847, establishes broad cybersecurity standards for “products with digital elements” sold in the EU, hardware and software used or expected to be used in a way that involves a direct or indirect data connection to a device or network [18]. It defines key requirements for secure design and development, vulnerability management, and information disclosure, and establishes a conformity and market surveillance system to ensure products meet basic cybersecurity standards before and after sale. Regarding transportation, the CRA generally applies to many digital products used in operational settings, such as telematics devices sold as standalone products, edge gateways and routers used in depots and yards, maintenance and diagnostic tools, and IoT components supporting fleet, logistics, and charging infrastructure, provided they are marketed in the EU.

Equally important, the CRA defines the situations in which it does not apply, thereby affecting the scope of transportation compliance. It excludes certain products already regulated by other EU frameworks,

including products covered by Regulation (EU) 2019/2144 (the EU's vehicle general safety/type-approval framework), such as UN ECE R155 and R156, as well as products certified under EU aviation rules and certain marine equipment rules. This means road-vehicle OEM cybersecurity typically aligns with vehicle type-approval obligations, while many "around-the-vehicle" digital products used by transport operators may fall under the CRA. The CRA's timeline also shapes procurement and lifecycle planning: it generally applies from 11 December 2027, with earlier applicability for specific elements such as Article 14 and Chapter IV (notified bodies), which may affect how suppliers prepare their compliance programs and how transportation organizations assess vendor readiness.

2.3 Roles and Responsibilities in Trend Analysis and Incident Response

NIST Special Publication 800-12 emphasizes that cybersecurity risk is fundamentally an organizational and management problem, requiring clearly defined roles, shared responsibility, and coordination across technical and operational domains [19]. NIST CSF 2.0 extends this principle by framing cybersecurity as a distributed challenge where no single entity owns all assets, telemetry, or response authority [20]. In the motor freight context, this means that threat and risk trend analysis cannot be centralized within a single organization or sector; instead, it emerges from the combined contributions of multiple actors, each with distinct visibility, authority, and constraints.

Motor freight carriers are primarily responsible for operational detection and impact assessment. They can observe service degradation, dispatch disruptions, driver-facing anomalies, and fleet-level effects, and are best positioned to correlate cyber signals with real-world operational outcomes. However, carriers often lack deep visibility into vehicle internals, telematics firmware, cloud platform internals, or shared software dependencies, which limits their ability to independently attribute root cause during large-scale events. Furthermore, the freight carriers operate as independent businesses, and they will often limit the sharing of internal information.

Original equipment manufacturers (OEMs) and tier-1 suppliers contribute architectural knowledge and component-level insight. Their role in trend analysis includes understanding systemic weaknesses in vehicle platforms, ECUs, update mechanisms, and diagnostic interfaces, and identifying when observed field behavior may indicate exploitation rather than a random fault. OEMs and suppliers are also uniquely positioned to assess safety implications and long-term design risks, but may not see cross-fleet operational patterns without coordinated reporting.

Telematics providers, software vendors, and managed service providers occupy a critical aggregation role. Because they operate shared infrastructure across many customers, they are often the first to detect anomalous patterns at scale, such as coordinated authentication failures, abnormal message flows, or update-related anomalies. Their participation is essential for reducing blast radius during widespread incidents, yet their role is complicated by contractual boundaries, liability concerns, and asymmetric information sharing.

First responders and transportation authorities contribute situational coordination and safety oversight. They rely on structured reporting to assess risks to public safety, infrastructure continuity, and regulatory compliance. Their role becomes especially important when cyber incidents intersect with physical safety, border operations, or emergency logistics.

Finally, **government** cybersecurity organizations provide cross-sector correlation, intelligence fusion, and threat attribution. By aggregating incident reports across industries and jurisdictions, these

organizations identify campaign-level trends, exploited vulnerabilities, and adversary tactics that are invisible to individual operators. Under CSF 2.0, this role aligns with the Govern and Detect functions at the national and sector level, enabling shared defensive action without requiring centralized operational control.

Overall, these roles illustrate why large-scale incident response in motor freight is inherently distributed. No single actor has sufficient visibility or authority to detect, interpret, and respond to systemic cyber events alone. Effective threat and risk trend analysis, therefore, depends on structured information sharing, clearly defined responsibilities, and alignment across organizational boundaries. These are principles that directly inform the cross-industry and cross-border integration mechanisms.

2.4 Cross-Industry and Cross-Border Threat Intelligence Integration

Effective threat and risk trend analysis in motor freight depends on combining technical threat signals, criminal and state-actor insights, and transportation-specific operational context. Because freight systems operate across sectors, vendors, and national borders, the most useful picture comes from integrating government intelligence, law-enforcement reporting, transportation safety guidance, and industry-led sharing mechanisms into a repeatable process for patch prioritization, detection tuning, and risk register updates.

2.4.1 Canadian Government Agencies

Canada's transportation cybersecurity ecosystem supports motor freight through a distributed set of roles spanning technical cyber defense, national coordination, criminal reporting, fraud pattern analysis, and transportation-sector guidance.

- **Canadian Centre for Cyber Security (Cyber Centre / CSE)**: Canada's primary federal source for technical cybersecurity guidance, alerts, threat analysis, and cyber incident reporting support [21], [22], [23].
- **Public Safety Canada**: Leads national cyber policy and coordination, including critical infrastructure resilience and federal cyber incident response expectations through the Federal Cyber Incident Response Plan (FCIRP) and national strategy documents [24] [25].
- **Royal Canadian Mounted Police (RCMP) and the National Cybercrime Coordination Centre (NC3)**: Central reporting and investigative coordination point for criminal cyber incidents, supporting cross-victim pattern recognition and law-enforcement action [26]. This coordination role reflects the convergence of criminal justice and cybersecurity functions identified by Dupont and Whelan [27], who argue that cyber incidents increasingly sit along a continuum between traditional crime and national security concerns.
- **Canadian Anti-Fraud Centre (CAFC)**: Tracks cyber-enabled fraud relevant to freight operations, including payment fraud, account compromise, and social engineering, while supporting broader trend visibility [28].
- **Transport Canada:** Provides transportation-specific cyber guidance, incident awareness resources, vehicle cybersecurity tools, and strategy relevant to connected and software-enabled vehicles [29] [30] [31] [32].

2.4.2 US Government Agencies

In the United States, no single agency owns end-to-end motor freight cyber threat analysis. Instead, insight is distributed across cyber defense, law enforcement, transportation security, vehicle safety, and accident investigation functions.

- **Cybersecurity and Infrastructure Security Agency (CISA)**: Primary federal source for defender-oriented technical intelligence, including the Known Exploited Vulnerabilities (KEV) Catalog, alerts and advisories, the Joint Cyber Defense Collaborative (JCDC), and Automated Indicator Sharing (AIS) machine-readable sharing [33] [34] [35], [36].
- **Federal Bureau of Investigation (FBI)**: Provides criminal threat context through Internet Crime Complaint Center (IC3) reporting, ransomware and extortion trend reporting, private-industry notifications, and InfraGard information sharing [37] [38] [39].
- **Transportation Security Administration (TSA) Surface Operations**: Offers surface transportation cyber toolkits, structured risk-assessment concepts, and an evolving model for sector cyber expectations and reporting [40] [41]. An assessment by the U.S. Government Accountability Office (GAO) of TSA's efforts highlights TSA's initiatives to strengthen cybersecurity and enhance information sharing related to security across surface transportation. The assessment emphasizes that trend analysis should include operational technology and connected-device risks, as well as enterprise IT [42].
- **Federal Motor Carrier Safety Administration (FMCSA)**: Contributes motor-freight-specific cyber risk insight through research and safety analysis related to telematics, ELDs, aftermarket systems, and large-scale commercial vehicle cyber risk .
- **National Highway Traffic Safety Administration (NHTSA)**: Provides lifecycle-oriented vehicle cybersecurity guidance, especially for secure design, coordinated vulnerability disclosure, software integrity, and post-incident learning [43].
- **National Transportation Safety Board (NTSB)**: Supplies post-incident, system-level safety analysis that can identify cyber-physical contributing factors and broader systemic weaknesses when serious transportation events occur.

2.4.3 Industry Information-Sharing Organizations

Industry-led sharing mechanisms complement government sources by providing peer context, operational detail, and transportation-specific defensive practices.

- **Information Sharing and Analysis Centers (ISACs):** Trusted, sector-focused communities that share tactical indicators, operational incident insights, and strategic threat trends across critical infrastructure sectors.
- **Automotive ISAC (Auto-ISAC):** The most relevant existing industry forum for automotive and commercial vehicle cybersecurity collaboration, including heavy-duty OEMs, suppliers, and fleets through its Commercial Vehicle Affinity Group.

- **ISAOs and related sector groups:** Additional communities may support regional, modal, or community-specific sharing where transportation cyber risks overlap with logistics, energy, manufacturing, or public safety operations.

2.4.4 Operational Use in Motor Freight

When combined, these sources support a repeatable cross-border threat intelligence process for motor freight. In practice, this means integrating government alerts, law-enforcement reporting, transportation-sector guidance, and industry peer reporting into a common analytic workflow that supports weekly patch and hunting priorities, monthly threat trend updates, and quarterly risk-register refreshes. The value of this approach is that it reduces blind spots across fleets, vendors, and borders and turns isolated incidents into a more actionable understanding of how cyber risk is evolving in the freight sector. However, there is little evidence available suggesting that an integrated information sharing and workflow is being used.

2.5 Implications for Carrier, Vendor, and Regulator Practice

The threat and risk trends described above imply that motor freight cybersecurity cannot be managed effectively as a traditional "IT security" function alone. The most consequential risks emerge where enterprise systems, telematics platforms, diagnostic tools, and vehicle networks intersect. These are often through vendor-managed services and operational workflows that were never designed for adversarial conditions. For carriers, this shifts the focus from one-time compliance or tool acquisition toward repeatable operational disciplines: maintaining a continuously updated inventory of connected assets and third-party dependencies; enforcing strong identity controls for remote access; segmenting telematics, maintenance, and corporate networks; and establishing minimum telemetry and logging expectations for both IT and OT systems. In practice, carriers should treat telematics and diagnostic ecosystems as tier-1 operational risk, requiring lifecycle management comparable to that of identity systems or financial platforms, including onboarding standards, configuration baselines, and deprovisioning controls.

For motor carrier technology vendors, the primary implication is that security outcomes should be demonstrable, not implied. Fleet operators increasingly depend on vendor systems as operational control points; therefore, vendors are effectively part of the carrier's attack surface and incident response chain. This elevates the need for secure-by-design engineering, hardening of update mechanisms, stronger authentication and authorization models, and transparent vulnerability management practices. Vendors should also support operational defensibility: exporting logs in usable formats, supporting customer detection and response workflows, and providing clear incident communications and recovery playbooks.

For regulators and public-sector partners, these security and detection patterns indicate that existing guidance often falls short in operational specificity. A persistent gap is the lack of clearly defined baseline expectations for event visibility, incident classification, and coordinated response across IT, OT, and third-party stakeholders. Guidance can be made more actionable by focusing on measurable outcomes, such as minimum logging coverage, controls on remote access, and routine recovery testing. Rather than prescribing uniform technical solutions, regulators can strengthen resilience by establishing scalable baseline requirements, incentivizing structured information sharing, and reinforcing supplier accountability, particularly for technologies widely deployed under regulatory mandates or market concentration.

In practice, recurring tabletop exercises such as the US CyberStorm reveal a consistent failure point: participants often struggle to identify who to contact and how to report during an incident [44]. This recurring outcome underscores the need for a well-defined, resilient communication and collaboration framework. Establishing clear escalation paths and trusted points of contact is therefore as critical to effective incident response as technical controls themselves.

2.6 Considerations Going Forward

Future policy and operational guidance should account for the growing concentration of cyber risk in shared platforms and common dependencies. Cloud concentration, telematics platforms, white-labeled ELD ecosystems, common edge devices, and managed services mean that a single weakness can affect many fleets at once. Guidance that treats organizations as isolated units therefore risks underestimating the likelihood and consequences of correlated failure. A more realistic approach to resilience would emphasize shared-service dependencies, coordinated vulnerability response, minimum standards of observability, and contingency planning for multi-party outages and cross-border disruptions.

A second policy consideration is the need for minimum standards of observability and evidence to support incident classification and response. The sector's ability to distinguish cyber events from maintenance actions or component failures depends on having sufficient telemetry and history from vehicle gateways, diagnostic interfaces, telematics backends, identity providers, and remote access infrastructure. Without baseline visibility, detection, and attribution, detection and attribution become guesswork, and incident response becomes reactive after operational harm occurs. Guidance can address this by promoting outcome-based requirements, such as log retention and accessibility, audit trail integrity, and the ability to correlate events across vehicle and enterprise environments.

Finally, policy would ideally align to a risk-based lifecycle model that mirrors NIST Cybersecurity Framework and modern supply-chain realities: governance and accountability for cybersecurity decisions; continuous identification of exposure as fleets and vendors change; protection and segmentation across IT/OT boundaries; detection tuned to operational contexts; and response/recovery plans that include third parties and cross-border reporting pathways. Importantly, future guidance would preferably be designed to be feasible for small and mid-sized carriers through scalable implementation pathways, templates, and shared services because uneven adoption across the long tail of the industry creates systemic weak points that sophisticated adversaries can exploit. The net goal is not only higher average maturity, but reduced variance resulting in the sector becoming harder to disrupt at scale.

3 Framework for Incident Response at Scale

While previous sections examine how cyber incidents emerge and propagate, this section focuses on how organizations should respond once incidents occur. The NIST Cybersecurity Framework provides a useful structure for mapping incident management responsibilities across distributed freight systems. This section explains how the NIST Cybersecurity Framework (CSF) 2.0 can be applied to motor freight operations as a practical, operations-aligned approach to managing cyber risk in a highly distributed, cyber-physical environment. It shows how the CSF functions of Govern, Identify, Protect, Detect, Respond, and Recover map to real-world freight activities spanning vehicles, drivers, terminals, back-office systems, and third-party platforms, and why governance and system-level visibility are foundational to resilience. The discussion highlights that large-scale incidents expose systemic challenges that are not primarily technical, but structural: fragmented ownership, limited cross-system awareness, ambiguous signals, constrained physical recovery capacity, and weak coordination across organizations and borders.

3.1 Mapping CSF Functions to Motor Freight Operations

The NIST Cybersecurity Framework (CSF) 2.0 provides a unifying structure for translating diverse regulatory guidance and voluntary best practices into a coherent, operationally meaningful cybersecurity program. For motor freight carriers, the value of the CSF lies not in prescriptive technical controls but in its ability to align cybersecurity risk management with real-world freight operations across vehicles, drivers, dispatch, terminals, back-office systems, and third-party ecosystems. Unlike traditional enterprise environments, motor freight operations are cyber-physical by nature: failures or compromises in digital systems can directly affect safety, regulatory compliance, and the movement of goods.

Across North America, agencies such as DHS, CISA, TSA, FMCSA, and Transport Canada consistently frame cybersecurity expectations in risk-based, outcome-oriented terms rather than enforceable technical mandates. These expectations map naturally onto the CSF 2.0 core functions, making the framework a practical lens for integrating regulatory guidance, industry standards, and operational realities into a single risk management approach.

3.1.1 Governance as the Anchor for Cyber-Physical Risk

CSF 2.0 elevates Govern to a first-class function, reflecting the reality that cybersecurity outcomes depend heavily on organizational accountability, decision-making authority, and integration with business objectives. In motor freight operations, governance challenges are amplified by the historical separation between IT, fleet operations, safety, and compliance functions. Cyber risks affecting telematics, ELDs, or diagnostics may not be owned by IT teams, while safety and operations leaders may lack visibility into backend system dependencies or third-party cloud risks.

Applying the Govern function in this context requires carriers to define clear ownership for cybersecurity across enterprise IT and vehicle-related systems, establish escalation paths that include safety and operations leadership, and integrate cyber risk into existing safety management systems (SMS), compliance programs, and insurance considerations. Governance also provides the mechanism by which carriers interpret regulatory guidance and translate it into policies that reflect fleet size, operational complexity, and risk tolerance.

3.1.2 Identifying Assets and Dependencies Across the Freight System

The Identify function is particularly critical for motor freight carriers because the attack surface is distributed and dynamic. Assets include not only servers, endpoints, and cloud applications, but also rolling assets such as trucks and trailers, embedded telematics devices, ELDs, diagnostic adapters, yard systems, and mobile driver applications. These assets are frequently introduced through aftermarket installations, leased equipment, or third-party service providers, complicating traditional asset inventory practices.

Mapping CSF Identify activities to freight operations involves understanding how data, credentials, and control signals flow between vehicles, dispatch systems, maintenance platforms, regulators, and external partners. This includes identifying dependencies on cellular networks, GPS services, OEM backends, and SaaS platforms that support routing, compliance, and billing. Without this system-level visibility, carriers cannot assess how a cyber event could propagate across fleets or affect operations at scale.

3.1.3 Protecting Operations Without Disrupting Freight Movement

The Protect function encompasses safeguards designed to limit the likelihood and impact of cyber incidents. In motor freight environments, protective controls should be balanced against operational uptime, driver usability, and regulatory requirements. Measures such as strong authentication, network segmentation, secure configuration, and disciplined patch management apply equally to back-office systems and to connected fleet technologies, but are often implemented unevenly.

For example, carriers may invest heavily in vehicle performance analytics and predictive maintenance while underinvesting in access controls for telematics portals or vendor remote access. CSF-aligned protection emphasizes consistency: applying baseline security expectations across enterprise IT, vehicle interfaces, and third-party integrations, while recognizing practical constraints for smaller carriers. Importantly, protection in this sector often relies on contractual and procurement mechanisms that require vendors to demonstrate secure development practices, vulnerability management, and incident notification, rather than direct technical control by the carrier.

3.1.4 Detecting Anomalies in a Noisy Operational Environment

The Detect function is one of the most challenging areas for motor freight carriers, particularly when distinguishing cyber events from equipment faults, maintenance activities, or environmental effects. Vehicles generate large volumes of operational data, and anomalies may be interpreted as routine mechanical issues rather than potential cyber indicators. At the same time, many carriers lack centralized visibility across telematics platforms, cloud services, and on-premises systems.

Mapping detection to freight operations involves correlating signals across domains: unexpected vehicle behavior, anomalous network traffic, unusual telematics commands, authentication failures in fleet portals, and abnormal dispatch system activity. Effective detection does not require advanced capabilities across all carriers, but it does require clear escalation thresholds and the ability to preserve logs and evidence when anomalies affect safety or compliance.

3.1.5 Responding with Safety, Operations, and IT in Mind

The Respond function highlights the need for coordinated action during cyber incidents. In motor freight operations, response activities should consider driver safety, vehicle control states, regulatory obligations, and customer commitments, which is more than just system restoration. A response plan that focuses solely on IT systems may fail to address real-world impacts, such as vehicles operating in degraded modes or dispatch disruptions affecting time-sensitive cargo.

CSF-aligned response planning encourages carriers to define roles and decision authority across IT, fleet operations, safety, legal, and communications functions. It also supports scenario-based planning for incidents that affect multiple vehicles or third-party platforms simultaneously, recognizing that cyber events at scale may require operational workarounds rather than immediate technical fixes.

3.1.6 Recovering and Sustaining Freight Operations

The Recover function emphasizes restoring capabilities and improving resilience after an incident. For motor freight carriers, recovery may involve reimaging systems, restoring cloud services, revalidating vehicle configurations, or temporarily altering routes and schedules. Recovery planning should account for fleet heterogeneity, vendor dependencies, and the practical limits of taking vehicles out of service.

CSF 2.0 encourages carriers to treat recovery as a learning process, updating risk assessments, improving vendor requirements, and refining incident response procedures based on real events. This aligns closely with Transport Canada's emphasis on continuous improvement and lifecycle risk management, particularly as fleets adopt increasingly connected and software-defined vehicles.

3.2 Systemic Challenges in Large-Scale Incident Response

The preceding section mapped motor freight operations to the NIST Cybersecurity Framework (CSF) 2.0, illustrating how governance, identification, and protection activities establish the conditions for resilience. However, the greatest operational stress in the motor freight sector emerges not during steady-state risk management, but during large-scale incidents that require timely detection, coordinated response, and sustained recovery across many independently operated systems. As fleets, telematics platforms, cloud services, and third-party providers become more tightly coupled, the Detect, Respond, and Recover functions increasingly operate in a system of systems context, which is one characterized by distributed ownership, partial visibility, and evolving system behavior.

A fundamental challenge in large-scale detection is the absence of unified system awareness. As noted in systems-aware cybersecurity research, effective detection in cyber-physical systems depends on understanding not just individual component behavior but how that behavior relates to system goals, operational states, and expected interactions [45]. In motor freight operations, no single organization typically has end-to-end visibility into how vehicle networks, telematics gateways, cloud backends, identity services, and regulatory interfaces interact at runtime. As a result, anomalous behavior observed in one domain—such as unexpected in-vehicle network traffic, delayed telematics updates, or backend authentication failures—may appear benign or ambiguous in isolation. Without cross-system correlation, detection degrades into local troubleshooting rather than recognition of a potentially coordinated cyber event.

This lack of holistic system knowledge directly undermines incident response at scale. Traditional response models assume clear ownership boundaries and centralized authority, yet motor freight operations exhibit operational and managerial independence, a defining characteristic of system of systems [46]. Vehicles are owned and operated by carriers; telematics platforms by vendors; cloud infrastructure by hyperscalers; and diagnostic tools by OEMs or service providers. Each organization has distinct priorities, response timelines, and information-sharing constraints. During a large-scale incident, no single actor can unilaterally execute containment actions across the affected systems. Response, therefore, depends on coordination across organizational boundaries that were never designed for real-time cyber incident command and control, leading to delays, fragmented decision-making, and inconsistent mitigation.

The Respond function is further complicated by ambiguity between cyber events and non-malicious failures. As emphasized in system-aware cybersecurity architectures, rapid differentiation between natural faults and adversarial actions is essential for choosing appropriate response strategies [45]. In motor freight operations, where maintenance actions, diagnostics, and software updates are routine and often remote, malicious activity may closely resemble legitimate operational behavior. At scale, this ambiguity creates a dangerous hesitation: aggressive containment actions risk disrupting freight movement and safety, while cautious responses may allow adversarial activity to persist across fleets or propagate through shared platforms.

Recovery at scale introduces additional systemic challenges because a system-of-systems is evolutionary rather than static. Recovery is not simply a matter of restoring systems to a known-good baseline; it often requires adapting to new configurations, vendors, or operational constraints introduced during the incident. System of systems engineering literature highlights that such environments exhibit emergent behavior and continual evolution, meaning that post-incident states may differ materially from pre-incident ones [46]. For motor freight carriers, recovery may involve operating with degraded telematics functionality, replacing compromised devices at scale, rerouting freight, or transitioning to alternate service providers.

A further systemic challenge in large-scale cyber-physical incidents is the limited availability of local resources to execute recovery operations, particularly when vehicle behavior, safety systems, or physical assets are affected. Motor freight recovery relies heavily on geographically distributed, capacity-constrained resources, like roadside technicians, tow operators, dealership service bays, OEM field engineers, inspection stations, and terminal maintenance staff. None of these resources are provisioned to respond to synchronized, fleet-wide anomalies. If a cyber event produces widespread vehicle derates, sensor faults, immobilizations, or safety-related alerts, recovery demand can rapidly exceed regional capacity, leading to cascading delays that amplify operational and safety impacts. Unlike enterprise IT recovery, which can often be centralized or virtualized, cyber-physical recovery requires physical access, specialized tools, and trained personnel at the point of failure. At scale, the saturation of these local resources becomes not only a recovery bottleneck but also a secondary indicator of systemic failure, distinguishing coordinated cyber effects from ordinary mechanical reliability issues. The absence of surge capacity, mutual-aid mechanisms, or preplanned regional recovery coordination further constrains the response, forcing carriers to prioritize which assets to restore first amid uncertainty. This dynamic underscores that resilience in motor freight is inseparable from the availability and coordination of physical recovery infrastructure, and that large-scale cyber incidents can outstrip local response capabilities long before their technical root cause is fully understood.

A final systemic challenge is the misalignment between detection and recovery incentives across stakeholders. Vendors may prioritize restoring service availability, carriers may prioritize safety and regulatory compliance, and government agencies may prioritize attribution and broader risk awareness. Without predefined recovery coordination mechanisms and shared situational awareness, these competing objectives can result in fragmented recovery efforts that restore individual systems while leaving systemic vulnerabilities unaddressed. Furthermore, cybersecurity expertise is fragmented across the industry, which leads to uncertainty in the detection of an incident at scale. NIST SP 800-160 emphasizes that resilience in complex systems requires intentional architectural consideration of recovery pathways, authority, and feedback loops [47]. These elements are often absent in organically evolved freight technology ecosystems.

Ultimately, these challenges show that failures in the Detect, Respond, and Recover functions at scale are not primarily technical shortcomings but vulnerabilities in the system of systems that make up motor freight operations. They arise from fragmented ownership, incomplete system knowledge, weak cross-organizational coordination, and the absence of architectures designed to support cyber resilience as an operational property. Addressing these challenges will require moving beyond tool-centric approaches toward system-aware designs, shared incident frameworks, and governance models that recognize motor freight transportation as a cyber-physical system of systems rather than a collection of independent IT assets.

3.3 Bilateral Incident Response Frameworks

The goal in large-scale motor freight cyber incidents is not for governments to run private-sector response, but to ensure that the broader ecosystem can coordinate quickly when incidents affect shared services, critical freight movement, or cross-border commerce. A potential model would be a standing U.S.–Canada Motor Freight Cyber Resilience Council, organized as a public–private partnership and aligned with each country's national incident coordination doctrine, including the U.S. National Cyber Incident Response Plan (NCIRP) and Canada's Federal Cyber Incident Response Plan (FCIRP). Such a body could provide a stable coordination structure across carriers, vendors, regulators, and government agencies while supporting a consistent minimum level of preparedness across organizations of different sizes.

This model could be organized around two standing functions: one focused on policy and baseline development, including shared definitions, minimum data fields, and model playbooks, and another focused on operational coordination and exercises, including cross-border escalation triggers, communications protocols, and joint exercises. The council's practical outputs should include a harmonized incident taxonomy, a minimum data schema for cross-border incident reporting, a joint coordination playbook, model contractual language to improve ecosystem expectations, and a recurring exercise and after-action program.

An instructive precedent already exists in the Great Lakes binational incident-notification model. The Great Lakes Water Quality Agreement (2012) establishes a notification expectation when either country becomes aware of a pollution incident or an imminent threat of joint concern [48]. That treaty-level expectation is operationalized through the Canada–United States Joint Marine Pollution Contingency Plan (CANUS JCP), which defines roles for notification, coordination, communication, and reporting. Although developed for environmental incidents, the underlying coordination problem is similar to cyber incidents affecting motor freight: multiple independent operators, shared infrastructure, cross-

border impacts, and no single organization with complete authority or visibility. Applied to cyber incidents, this suggests that an effective binational motor freight alerting model should be built around trigger-based notification, a defined cross-border coordination structure, and standardized information packages that allow governments, carriers, and vendors to share partial but actionable information quickly.

At present, no equivalent formalized alerting and coordination framework exists for large-scale cyber incidents affecting motor freight. Instead, reporting and coordination responsibilities are distributed across multiple agencies in both countries, and cross-border awareness often depends on voluntary reporting, informal relationships, and ad hoc communication. In Canada, Transport Canada's Situation Centre and the Canadian Centre for Cyber Security already provide a national intake pathway for transportation cybersecurity incidents, suggesting half of a workable model. A future binational framework would need to pair that pathway with a clearly defined U.S. counterpart and specify when incidents affecting fleets, vendors, freight corridors, or shared digital infrastructure trigger rapid, structured cross-border notification and joint operational coordination.

3.4 Governance Models for Scalable Response and Coordination

Cybersecurity incidents in the motor freight trucking industry rarely remain confined to a single system or company. Dispatch platforms, ELD/telematics, warehouse and terminal systems, fuel/payment networks, and shipper/broker integrations are closely connected, and the operational effects of disruptions can quickly spread across an entire ecosystem. Therefore, responding at scale is both a technical challenge and a business coordination issue, requiring a response capability that is repeatable, auditable, and interoperable across fleets, terminals, and third parties.

The following standards section summarizes the most relevant regulatory requirements, standards, and best practices for incident response across the United States, Canada, and the European Union. Instead of treating these as separate compliance checklists, the report uses them as a unified reference model for how mature programs organize incident management, evidence handling, communications, and recovery, while also complying with jurisdiction-specific notification and reporting requirements. Building on that foundation, the governance section then presents two complementary governance models: one for motor freight carriers to translate standards into enforceable policies, decision rights, and operational procedures across a distributed enterprise and partner network; and a second, bi-national model to support ecosystem-wide coordination and readiness across the U.S. and Canada. Together, these sections aim to ensure that incident response is not only "documented," but also governable, measurable, and executable under stress.

3.4.1 Incident Response Regulations, Standards, and Best Practices

Responding to cybersecurity incidents at scale in the motor freight trucking industry requires more than traditional IT incident handling because the systems that "move freight" are distributed across fleets, terminals, warehouses, and a dense partner ecosystem (brokers/3PLs, shippers, intermodal partners, maintenance networks, and SaaS vendors). As a result, high-performing programs use a single, standards-based incident response (IR) operating model that can be executed consistently across business units and geographies and then layer in jurisdiction-specific reporting and privacy workflows (a "notification wrapper") so containment and recovery work does not stall while regulatory thresholds and timelines are evaluated.

NIST SP 800-61 Rev. 3 offers a structured approach for integrating incident response into broader cybersecurity risk management and serves as a practical blueprint for playbooks, communications, evidence handling, and ongoing processes improvement [49]. ISO/IEC 27035 formalizes information security incident management as a repeatable lifecycle that supports consistent execution across distributed organizations and service provider relationships [50]. Organizations usually combine this incident-management core with an information security management system (ISMS) framework through ISO/IEC 27001 [51] and the associated control guidance in ISO/IEC 27002 [52] so that IR is not "just a plan," but a governed capability with roles, training, logging expectations, supplier requirements, and periodic testing. Because cyber incidents in trucking can cause business interruptions, ISO 22301 business continuity practices are often used to establish recovery goals and fallback operating modes that ensure freight continues to move safely during technology disruptions or outages [53]. Finally, programs that expect litigation, fraud, or cargo theft risk incorporate digital evidence handling and incident investigation guidance, such as ISO/IEC 27037 [54] and ISO/IEC 27043 [55], as well as NIST forensic integration guidance, to ensure evidence is preserved while response actions proceed [56].

Large-scale trucking responses also benefit from industry overlays that link "cyber" decisions to operational realities. Transportation-sector guidance from CISA helps transportation owners and operators apply risk frameworks in ways that reflect transportation operating constraints and dependencies. Fleet operators may also want to incorporate heavy-vehicle guidance for telematics and aftermarket electronic system integration, since the ELD/telematics layer creates unique attack and outage pathways [2]. In parallel, the trucking ecosystem often inherits cargo-security requirements from high-value shippers and global supply chains, making supply-chain security standards and cargo-security requirements a practical component of IR planning, especially for cyber-enabled cargo theft scenarios in which identity spoofing, fraudulent pickups, and tracker manipulation intersect with physical security controls. ISO 28000 [57] offers a management-system approach for supply-chain security, while the Transported Asset Protection Association (TAPA) Trucking Security Requirements (TSR) and Facility Security Requirements (FSR) are frequently referenced in shipper–logistics provider agreements and certification programs for over-the-road and facility security [58].

In the United States, trucking organizations often face a combination of statutory, regulatory, and contractual drivers that influence reporting readiness and executive decision-making. Federal cyber incident reporting expectations are evolving under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) [59], with CISA's rulemaking (including proposed requirements published in the Federal Register) may push many critical-infrastructure-adjacent service providers toward faster incident classification, documentation, and reporting workflows even when they are not certain they are directly "covered." Publicly traded carriers, logistics providers, and technology vendors also need a materiality decision workflow that supports the SEC's cybersecurity disclosure rules [60]. In addition, trucking ecosystems frequently interact with regulated financial services (e.g., through payment processors, banks, and certain insurance/finance partners) and may be required to maintain incident response planning consistent with sector rules, such as New York's cybersecurity regulation for covered financial entities [61]. Card payment environments also commonly shape expectations for incident response planning through the Payment Card Industry (PCI) guidance that emphasizes preparedness and breach response practices [62].

In Canada, incident response obligations for commercial organizations are commonly shaped by privacy breach assessment, notification, and record-keeping requirements under federal privacy law. The Office of the Privacy Commissioner of Canada provides guidance on mandatory breach reporting and notification when a breach of security safeguards poses a "real risk of significant harm," as well as on expectations for keeping records of breaches. These are requirements that materially affect how a trucking organization triages incidents involving driver, employee, customer, or consignee data across dispatch, HR, and claims systems [63].

In the European Union, response-at-scale planning must adhere to strict reporting schedule requirements when an organization falls within scope (or when contractual obligations flow down from in-scope shippers, ports, or logistics partners). The NIS2 Directive outlines structured reporting obligations for "significant incidents," including an early warning within 24 hours, an incident notification within 72 hours, and a final report no later than one month after the incident notification [64]. Separately, the General Data Protection Regulation (GDPR) requires controllers to notify the competent supervisory authority of a personal data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it (unless the breach is unlikely to pose a risk to individuals), which highlights the need for a privacy-aware incident classification process that can run alongside containment and recovery actions [65].

3.4.2 Motor freight carrier governance model

Motor freight carriers may be able to manage incident response effectively at scale by using Control Objectives for Information and Related Technology (COBIT) 2019 as the enterprise governance backbone [66]. This helps to define decision rights, oversight, performance management, and continuous improvement. COBIT's governance system principles aim to deliver stakeholder value, adopt a holistic and end-to-end scope, separate governance from management, and customize the governance framework using design factors [67]. These aims are especially relevant in trucking because "enterprise IT" includes distributed terminals, fleets, ELD/telematics and aftermarket integrations, customer/broker portals, and outsourced service providers that collectively determine whether freight continues to move safely during disruptions. In practice, the carrier should clearly separate governance from management execution, while ensuring the governance system is tailored to the carrier's size, outsourcing mix, cross-border footprint, and risk profile.

A reportable, repeatable carrier model employs a three-tier structure: (1) a board-level risk or audit committee that determines cyber resilience risk appetite, approves the incident response policy framework, and monitors outcome-based metrics; (2) an executive cyber resilience steering committee that owns the cross-functional policy set and resource prioritization; and (3) operational execution through a 24×7 security team (SOC/CSIRT) integrated with major incident management and business continuity leaders. This structure should be clearly defined using "decision rights" language (e.g., who can declare a major incident, authorize operational shutdowns/segmentation, approve customer notifications, and engage law enforcement/insurers) so that the organization can respond swiftly across time zones and under time pressure.

To ensure the carrier actually develops the necessary policies and procedures for scale, governance may suggest a minimum policy and playbook library and align it with COBIT governance and management objectives, such as incident intake, classification, escalation, and resolution processes that match COBIT's "managed incidents" objective, and continuity playbooks consistent with COBIT's continuity

frameworks objective. The playbooks should cover at least the following: ransomware/extortion; identity compromise and privileged access abuse; business email compromise and fraud/cargo theft enablement; TMS/dispatch outages; ELD/telematics outages or vendor compromise; and third-party SaaS compromise scenarios that cascade across multiple terminals or customers. This library should be paired with an evidence-handling and investigation approach that preserves the chain of custody while remediation proceeds, consistent with modern incident response guidance and litigation/insurance expectations.

Since motor freight operates as an ecosystem business, carrier governance must also include ecosystem incident governance: contractually specified notification thresholds and timelines for critical vendors (such as TMS, telematics/ELD, fuel card/payment processors, cloud providers, managed service providers, broker platform integrations), requirements for forensic cooperation and log retention, and a "joint exercise" expectation for tier-1 vendors. This is best implemented through an Ecosystem Coordination Cell that is pre-activated for major incidents and has designated points of contact with key vendors and high-dependency customers (major shippers, brokers/3PLs). This facilitates shared situational awareness and coordinated containment when an incident impacts multiple entities. Meanwhile, a carrier operating in both the U.S. and Canada should develop a "notification wrapper" around the technical response to ensure that privacy and reporting obligations can occur concurrently with containment and recovery, rather than delaying them. In Canada, this includes breach assessment and reporting/notification processes aligned with the "real risk of significant harm" standard, as well as record-keeping expectations [63].

Finally, the carrier governance model may incorporate a measurable assurance and continuous improvement cycle: regular table-top exercises (including at least one tier-1 vendor annually), annual recovery tests for dispatch and billing operations, and post-incident reviews that track corrective actions to completion (such as policy updates, control changes, training, and vendor remediation). This is reinforced by adopting cross-sector baseline practices aimed at reducing the likelihood and impact of common systemic failures (e.g., asset inventory, MFA, logging, vulnerability management, backups, and incident planning), which can serve as a prioritized "minimum set" for critical services and third-party dependencies [68].

4 Policy and Regulatory Implementation Roadmap

This roadmap offers policy and regulatory implementation ideas to enhance cyber incident response readiness for large-scale events across the motor freight ecosystem. It aims to turn incident response governance into repeatable operational outcomes, such as quicker escalations, more reliable continuity decisions, better information sharing, and consistent cross-border coordination when freight disruptions affect both Canada and the United States.

4.1 Maturity Model for Cyber Incident Response Readiness

Motor freight cyber readiness should be evaluated through two complementary perspectives: industry execution readiness and government coordination readiness. Industry focuses on how effectively operators and vendors can respond and recover from a cybersecurity incident. Examples of motor freight security issues include ransomware attacks impacting multiple terminals, fleet-wide credential exposure leading to identity compromise, or shared-vendor breaches affecting dispatch or telematics. Rapid response and recovery require proper escalation procedures, vendor mobilization, evidence preservation, and communication. Government measures success based on how well public-sector agencies can triage, coordinate, and support multi-entity responses at scale.

The newly proposed roadmap in this report uses two separate maturity models to keep expectations measurable and realistic. Both models use a 0-5 scale, where Level 0 represents no meaningful readiness and Level 5 represents an optimized capability with continuous improvement and validated performance. This approach aligns with typical maturity concepts: the NIST Cybersecurity Framework Implementation Tiers depict a progression from reactive practices to adaptive, risk-informed approaches, and COBIT process capability models typically use a 0-5 scale from incomplete to fully capable and optimizing [69], [70].

For industry, the model emphasizes dispatch continuity, terminal operations, fleet and driver enablement dependencies (including ELDs and telematics), and the shared vendor ecosystem (TMS platforms, fuel and payment services, managed IT providers, and cloud identity). For the government, the model emphasizes consistent triage, predictable coordination rhythms, structured information requests, surge technical assistance, and cross-border liaison procedures, because systemic freight disruption frequently becomes multi-jurisdictional.

4.1.1 How to use this model in a policy and regulatory roadmap

The maturity models proposed within this report are created to support phased implementation rather than a one-size-fits-all compliance cliff. A practical approach includes: (1) assessing current readiness, (2) establishing minimum target levels by stakeholder group (and by size/risk), (3) aligning incentives and requirements to promote progression step-by-step, and (4) verifying progress through exercises and performance metrics. The model should be used alongside at-scale escalation thresholds (severity, scope, impact, and cross-border triggers) to ensure that maturity levels drive predictable actions during real-world events.

The roadmap does not require a single framework. Organizations can align internal practices with the Center for Internet Security Controls Implementation Groups (IG1-IG3) [71] for prioritization and resource allocation, and defense-related supply chain entities can map practices to the Department of

War Cybersecurity Maturity Model Certification (CMMC), where relevant [72]. The goal is consistent readiness outcomes and coordinated execution.

4.1.2 Industry Readiness Maturity Model for Motor Freight Operators

The Industry Readiness Maturity Model serves as both an assessment and planning tool for motor freight operators looking to understand and enhance their operational and incident-response readiness. To apply the model, organizations start by defining the assessment scope, which may include enterprise-wide operations or specific areas such as dispatch, terminals, vendor coordination, and continuity of operations. They then evaluate their current state by comparing existing practices to the criteria at each maturity level, from No Readiness to Optimizing. This evaluation relies on evidence such as documented response plans, well-defined roles and escalation procedures, on-call coverage availability, visibility into critical systems, and established vendor coordination mechanisms. The target maturity level should reflect the lowest level that is consistently demonstrated across the assessed scope, rather than aspirational or partially implemented capabilities.

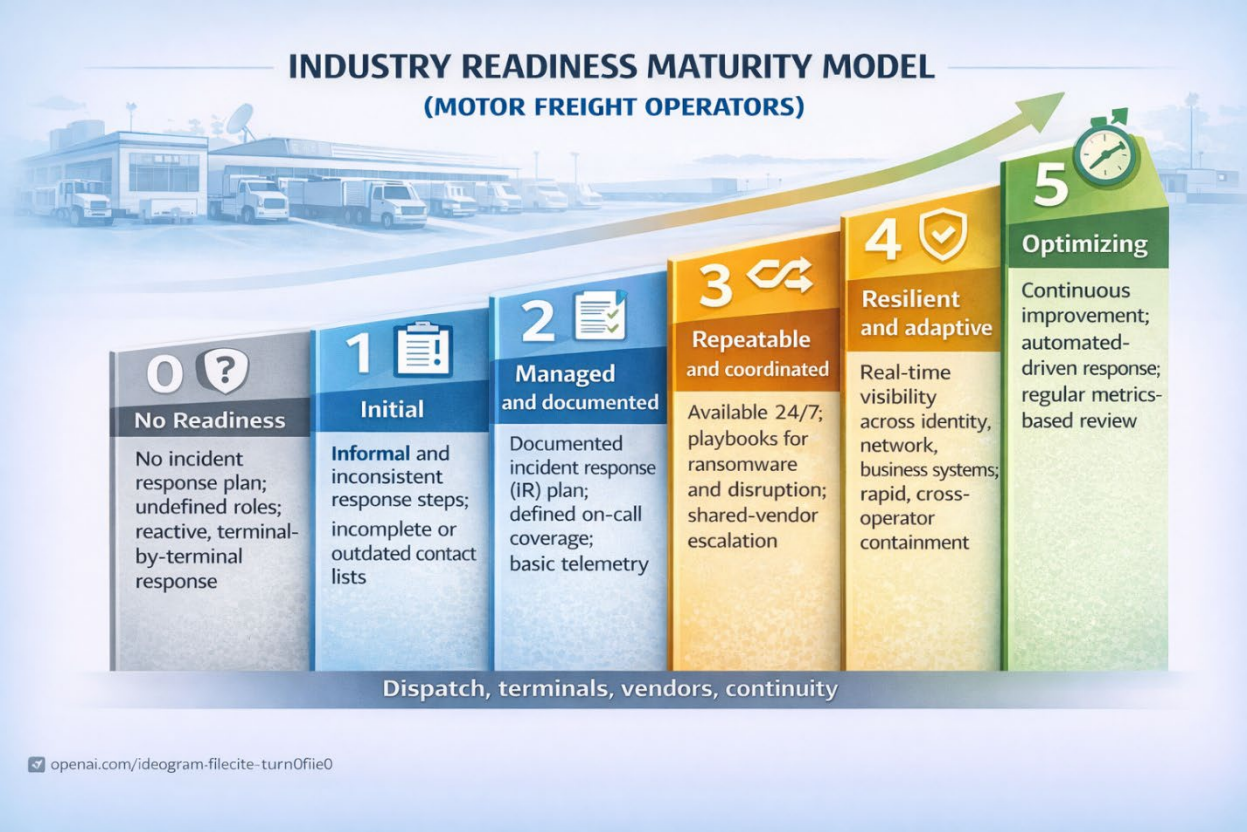


Figure 1: Industry Cyber Incident Response Readiness Maturity Model for Motor Freight Operators.

Once the current maturity level is established, the model identifies capability gaps and associated operational risks by highlighting differences between the current state and the next maturity level. These gaps provide a clear basis for prioritizing improvements, focusing on steady progress rather than jumping levels, since each stage of maturity builds the essential capabilities needed for greater resilience and adaptability. The gap analysis can be used to develop a phased improvement plan aligned with organizational goals, risk tolerance, and resource availability, including assigned ownership, timelines, and performance metrics. Over time, the model also enables tracking progress through

quantitative measures such as detection, containment, and restoration times, and supports regular reassessments following incidents or drills. In this way, the model functions not only as a diagnostic tool but also as a common reference for coordinating efforts among operational leaders, technical teams, and external partners around readiness objectives and ongoing improvement

Table 1: Levels of Readiness for Motor Carriers

Level	Readiness name	Operator characteristics (dispatch, terminals, vendors, continuity)
0	No Readiness	No incident response plan, undefined roles, unmanaged logging, lacking vendor escalation paths, and reactive, terminal-by-terminal response; no dispatch/TMS continuity procedures.
1	Initial / Ad Hoc	Informal response steps exist but are inconsistent; point-of-contact lists are incomplete or outdated; evidence is not systematically preserved; restoration depends on individual staff and vendor goodwill.
2	Managed / Documented	Documented IR plan and escalation thresholds; defined on-call coverage (may be limited to business hours); baseline telemetry for key systems; maintained vendor escalation contacts; established basic communication workflow and internal notification tree.
3	Repeatable / Coordinated	Available 24/7 for core functions; has playbooks for ransomware, identity compromise, shared-vendor issues, and terminal disruption; follows standardized evidence preservation; conducts routine exercises; and practices dispatch continuity procedures during degraded operations.
4	Resilient / Adaptive	Real-time visibility across identity, endpoint, and network, plus critical business systems; pre-negotiated vendor surge support; rapid containment that minimizes operational disruption; quantified continuity decision framework; repeatable cross-operator coordination steps.
5	Optimizing	Drive continuous improvement through metrics and after-action reviews; automate enrichment, triage, and notification workflows; conduct regular exercises including vendor participation; proactively test shared-vendor and cross-border scenarios; achieve measurable reductions in detection, containment, restoration times, and blast radius.

4.1.3 Proposed Government Readiness Maturity Model for Coordination of Large Motor Freight Incidents

The proposed Government Readiness Maturity Model helps public-sector organizations evaluate, coordinate, and enhance their preparedness for large-scale motor freight incidents, particularly those involving cyber threats or systemic operational disruptions. Governments could adopt the model by initially defining the scope of coordination, including relevant agencies, levels of government, cross-border partners, and industry interfaces. The assessment would ideally focus on coordination functions, including triage, information collection, assistance pathways, interagency synchronization, and cross-border notification and escalation mechanisms.

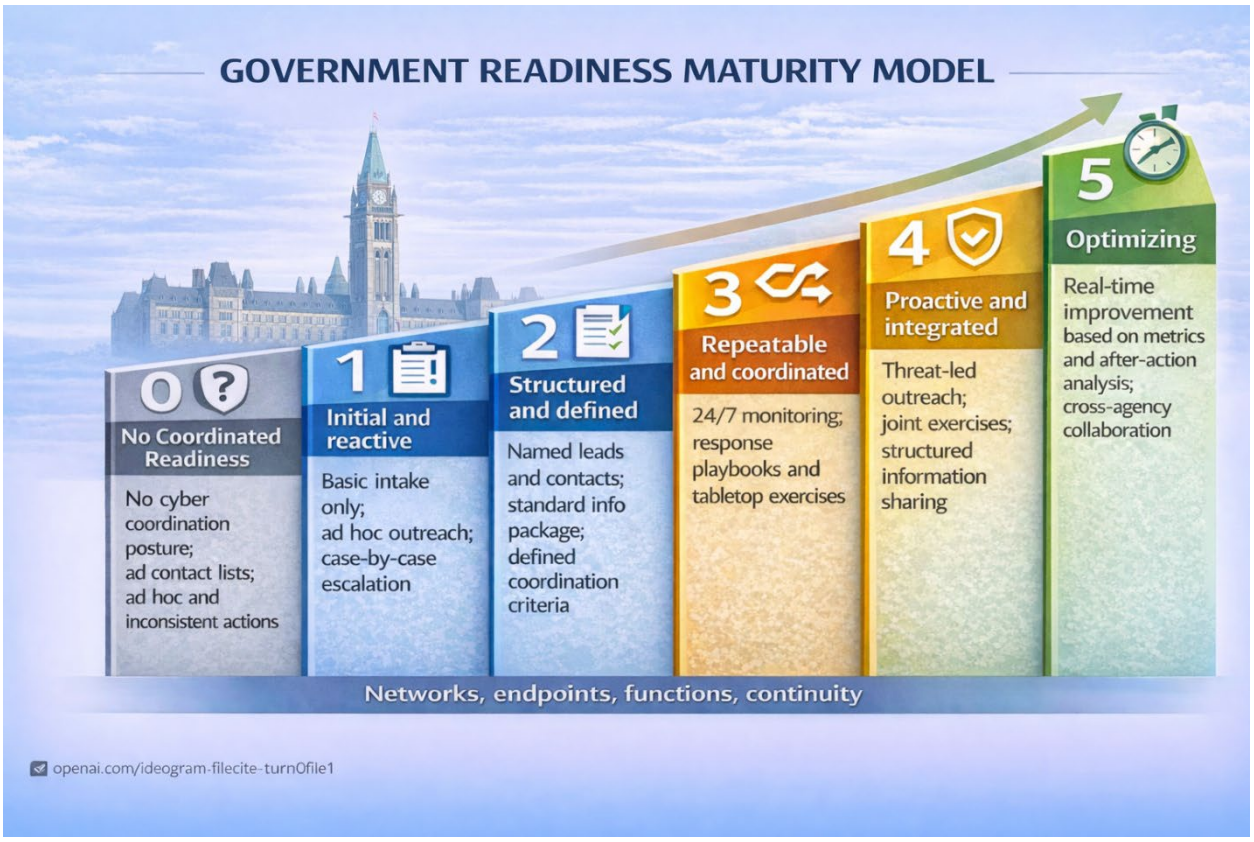


Figure 2: Graphical Representation to Quantify proposed Readiness Maturity for Government

Governments could assess their current posture by comparing existing practices against the characteristics defined at each maturity level, from No Coordinated Readiness to Optimizing. Ideally, this assessment would be based on evidence and reflect routinely demonstrated capabilities rather than informal relationships or ad hoc successes. Indicators could include maintained contact rosters, standardized information request templates, defined triggers for convening coordination calls, documented assistance pathways, and practiced cross-border coordination procedures. The assigned maturity level would ideally match the lowest level that is consistently achieved across the assessed coordination functions.

Once the current maturity level is assessed, the model would help identify coordination gaps and systemic risks that could obstruct a timely or effective response during large-scale freight disruptions. These gaps provide a clear basis for prioritizing improvements, emphasizing gradual progress rather than aiming to achieve advanced capabilities immediately. Governments could use the model to develop a phased roadmap that aligns policy development, operational procedures, training, exercises, and partner engagement with clearly defined readiness goals.

Over time, the model would encourage continuous improvement by using metrics, after-action reviews, and trend analysis to refine coordination triggers, guidance products, and information-sharing mechanisms. Regular reassessment coupled with real-world incidents would allow governments to evaluate progress, verify assumptions, and strengthen collaboration with industry and international partners. In this way, the model would serve as both a diagnostic framework and a shared reference to align government stakeholders around consistent, repeatable, and resilient coordination practices.

Table 2: Proposed Government Readiness Levels and Descriptions

Level	Readiness name	Government/coordination characteristics (triage, assistance, coordination, cross-border)
0	No Coordinated Readiness	No established freight-sector cyber coordination posture; no maintained contact rosters; no standard information request templates; coordination remains improvisational and inconsistent.
1	Initial / Reactive	Basic intake exists, with ad hoc outreach to the industry. Playbooks are limited, and coordination relies on personal relationships. Cross-border escalation is handled case-by-case without defined triggers.
2	Structured / Defined	Named coordination leads and maintained contact lists; standard initial information request package; defined criteria for convening calls; documented pathways for technical assistance and law enforcement/regulator engagement; basic cross-border notification triggers documented.
3	Repeatable / Operational	Established coordination rhythm (sitrep cadence, recurring calls when triggered); practiced multi-agency coordination; standardized guidance products; repeatable cross-border liaison procedures; ability to recognize shared-vendor/cascade risk patterns from reports.
4	Proactive / Integrated	Threat-led outreach and preparedness activities; surge playbooks to mobilize assistance; consistent cross-border information sharing procedures; routine joint exercises with industry and partner agencies; metrics-driven evaluation of response timeliness and effectiveness.
5	Optimizing	Ongoing improvement through lessons learned and trend analysis; near-real-time sharing of actionable guidance; refined escalation triggers based on pilot data; well-established binational coordination pathways routinely tested; clear reductions in systemic freight disruption.

4.1.4 Minimum outlooks by organization size and role

Achievable goals for cybersecurity incident management should scale with an organization's size, operational complexity, and role in the motor freight ecosystem. Industry guidance consistently recognizes that carriers and brokers operate under widely different constraints in staffing, budget, and technical maturity, and that cybersecurity posture should be outcome-based rather than prescriptive. The goal is not uniform tooling or identical processes, but a shared baseline of preparedness that ensures incidents can be detected, escalated, and coordinated without introducing systemic risk to freight movement.

For small carriers and small brokers with limited resources, a minimum target of Level 2 (Managed/Documented) is both realistic and necessary. Guidance for owner-operators and small fleets assumes limited human resources, minimal technical complexity, and constrained budgets, often relying on part-time staff or third-party service providers rather than dedicated security teams [73]. At this level, essential outcomes include clearly defined escalation triggers (for example, ransomware indicators, loss of dispatch access, or suspected account compromise), verified contact information for critical vendors and service providers, and baseline logging for identity systems and core business

platforms. A documented yet simple dispatch-continuity plan and a basic incident communications workflow ensure that even a small operation can maintain safety and operational control while seeking external assistance. These measures are the minimum required to prevent silent failure or unmanaged disruption during an incident.

Mid-size carriers, regional fleets, or 3PLs with multiple terminals should operate at a minimum of Level 3 (Repeatable/Coordinated). At this scale, organizations typically support 24/7 operations, manage multiple facilities, and rely on shared platforms for dispatch, billing, telematics, and identity management. As a result, incidents can propagate across terminals or vendors if not rapidly identified and contained. Minimum expectations at this level include continuous escalation coverage, documented and exercised playbooks for high-impact scenarios such as ransomware and shared-vendor compromise, and routine tabletop exercises that involve both IT and operations leadership. Log retention, snapshotting, and chain-of-custody awareness are examples of evidence preservation steps to support recovery, insurance, and potential regulatory reporting. Terminal-level recovery sequencing plans further ensure that restoration decisions are deliberate and coordinated, rather than improvised under pressure.

Large national carriers and critical logistics providers should aim for at least Level 4 (Resilient/Adaptive) given their systemic importance and potential national-level impact. At this scale, incidents are unlikely to remain localized; shared identity platforms, cloud providers, telematics services, and fuel or payment vendors create natural aggregation points for cascading failure. Essential outcomes, therefore, include real-time cross-domain visibility across IT, operational platforms, and key third-party services; pre-negotiated surge support and notification arrangements with critical vendors; and the ability to make quantified continuity decisions (for example, when to isolate systems versus maintain limited operations). Structured information-sharing packages for regulators, law enforcement, and sector partners enable coordinated response without exposing unnecessary sensitive data. Routine joint exercises with major vendors and cross-border escalation triggers for operations involving ports of entry or binational corridors help ensure readiness for incidents that exceed a single organization’s control.

Critical vendors supporting motor freight, including transportation management system (TMS) providers, electronic logging device (ELD) providers, telematics vendors, fuel and payment platforms, and identity or managed service providers, should meet at least Level 3 and have a clear trajectory toward Level 4 maturity. Because these vendors inherently serve many customers simultaneously, their incident-management capabilities directly affect the sector’s ability to respond to events at scale. Minimum expectations include tested customer notification service-level agreements, rapid identification of affected customers and functions, and the ability to produce evidence packages that support downstream investigations by carriers and authorities. Surge support capacity is essential during widespread events, as the quality of vendor response often determines whether an incident remains manageable or escalates into a sector-wide disruption.

Finally, government coordination entities involved in transportation cybersecurity would ideally operate at a minimum of Level 3 (Repeatable/Operational). Their role would not be deep forensic analysis within individual environments, but convening stakeholders, enabling cross-organizational correlation, and providing coordinated guidance during significant events. Therefore, outcomes would include clearly defined convening triggers, structured and repeatable information-request templates, an established situation-report cadence, and regularly tested contact rosters. For incidents affecting border crossings,

ports of entry, or binational freight corridors, repeatable cross-border liaison procedures would be essential to ensure timely coordination between U.S. and Canadian authorities and industry partners.

Across all organization types, these minimum capabilities reinforce a central principle: incident-management maturity should be sufficient not only for self-recovery but also to avoid becoming a weak link in a tightly coupled transportation system. By defining realistic, role-appropriate baselines, the sector can improve resilience without imposing uniform requirements that do not account for operational realities.

4.2 Workforce Training and Capacity Building

A key consideration for policy and regulatory implementation is that workforce capacity is foundational to effective cybersecurity incident management in motor freight, particularly as fleets adopt increasingly connected, software-defined, and cyber-physical technologies. Across government, industry, and academia, guidance consistently emphasizes that cybersecurity outcomes depend not only on tools and policies, but on personnel who understand how digital threats manifest in physical systems and operational contexts. For transportation systems, this requires a workforce that is conversant in both information technology (IT) and operational technology (OT), and capable of reasoning about safety, reliability, and cybersecurity as interdependent concerns rather than isolated disciplines [74].

Federal vehicle cybersecurity guidance highlights workforce development as a prerequisite for sustained risk reduction. The National Highway Traffic Safety Administration (NHTSA) states that continually educating both the existing workforce and future professionals is critical to improving the cybersecurity posture of modern vehicles, particularly as connectivity and automation increase [75]. This emphasis reflects the reality that many vulnerabilities in transportation systems arise not from unknown technologies, but from misunderstandings of system interactions, legacy protocols, and maintenance interfaces that are well known within engineering communities but poorly understood by traditional IT security staff.

One of the most effective mechanisms for addressing this gap is experiential, system-focused training that exposes participants to real operational assets. Challenge-based education models, such as the CyberTruck Challenge, demonstrate how hands-on interaction with vehicles, telematics units, diagnostic tools, and backend systems accelerates learning and builds durable expertise across sectors. These challenge events combine structured instruction with supervised assessment of real equipment, enabling participants to understand how vulnerabilities emerge from the interaction of hardware, software, protocols, and operational practices rather than from abstract attack scenarios. Importantly, this model supports both talent generation and community building, creating networks of practitioners who can share insights and coordinate responses long after the training event concludes.

From a systems engineering perspective, this approach aligns directly with INCOSE's vision that cybersecurity should become as foundational to system design and operation as performance and safety. The referenced challenge-based education model addresses the need for “cyber-informed engineers” who can operate within constrained, safety-critical, and regulated environments where conventional IT security controls may not be feasible [74]. For the motor freight sector, this is particularly relevant given the long vehicle lifecycles, the prevalence of legacy communication protocols, and the operational need for remote diagnostics and maintenance access.

Continuing education is equally important for the existing workforce. Many fleet operators, maintenance personnel, dispatchers, and operations managers entered the industry before cybersecurity became a core operational concern. As a result, effective capacity building should include recurring training that focuses on recognizing abnormal system behavior, understanding escalation thresholds, and coordinating with IT, vendors, and government partners during incidents. The vehicle cybersecurity best-practice literature stresses that awareness training alone is insufficient; personnel should be trained to interpret cyber events in an operational context, including how cyber activity may masquerade as equipment faults, sensor failures, or maintenance anomalies [76].

Finally, workforce development should be viewed as a shared responsibility across carriers, vendors, academia, and government. No single organization can train the full spectrum of skills required to secure modern motor freight operations at scale. Challenge events, professional short courses, sector-led guidance, and cross-industry collaboration collectively form a workforce multiplier that expands both the number of trained professionals and the depth of system-specific knowledge available to the sector. As incident response increasingly requires coordinated action across fleets, vendors, and borders, investments in workforce training and capacity building are not optional enhancements, but core enablers of national and economic resilience.

4.3 Pilot Programs and Data-Sharing Demonstrations

Pilot programs should validate the policy and regulatory roadmap in controlled environments before wider adoption across a diverse motor freight ecosystem. Consistent with modern exercise doctrine, pilots should not be treated as isolated events; they should produce reusable operational outputs and documented lessons learned that translate into continuous improvement actions over time. Each pilot should generate measurable outcomes such as refined escalation thresholds, standardized reporting packages, verified points of contact, and repeatable coordination workflows with key vendors and government partners [77].

A useful portfolio includes industry-only tabletops, government-only tabletops, and joint exercises, implemented as a progressive exercise cycle that builds in scope and complexity, culminating in higher-fidelity coordination demonstrations. Industry-only tabletops validate dispatch continuity, terminal recovery sequencing, and vendor escalation under operational constraints. Government-only tabletops validate convening triggers, structured information requests, and coordination rhythms. Joint exercises validate the interface between these environments: what gets reported, when, in what format, how consent and sensitivity are handled, and how technical assistance and public messaging are coordinated under real time pressure. This portfolio aligns with the Federal Cyber Incident Response Plan (FCIRP) [25] that is articulated in the Public Safety Canada's 2024-to 2025 Departmental Plan [78].

Cross-border pilots should be explicit because motor freight operations depend on border hubs, binational carriers, and shared vendors. Modern Canadian policy framing explicitly emphasizes partnership-driven cyber resilience and faster information sharing across critical infrastructure communities, including cross-border resilience with the United States. Likewise, contemporary U.S.–Canada bilateral messaging recognizes cybersecurity cooperation as a shared priority for protecting North American critical infrastructure, reinforcing the need for compatible cross-border procedures and liaison pathways in high-impact incidents [24].

Data-sharing demonstrations should transition from ad hoc exchanges to structured, reviewable packages with defined timelines, handling expectations, and analyst validation checkpoints. Recent

exercise after-action analysis for Canadian cyber-physical preparedness found that delays in sharing sensitive information and the lack of interoperable platforms can impede coordinated decision-making, emphasizing the need to rehearse both the timing and mechanisms of information flow. [79]. Where appropriate, pilots should test interoperable, machine-readable formats. Examples of these formats include STIX for structured cyber threat and observable information and TAXII for transporting threat intelligence over HTTPS [80].

The following are preliminary considerations for activities that foster communication and planning to address incident response challenges at scale.

- **Carrier dispatch continuity tabletop** (industry-only): ransomware or destructive disruption of TMS/dispatch; verify manual fallbacks, restoration priorities, and customer/shipper communication cadence.
- **Terminal operations + identity compromise tabletop** (industry-only): compromise of identity provider or privileged access tools; verify rapid containment without stranding drivers or disrupting yard operations.
- **Shared vendor compromise tabletop** (industry-only): telematics or fuel/payment vendor events impacting multiple fleets; verify vendor notification SLAs, affected-customer scoping, and mitigation distribution.
- **Freight disruption coordination tabletop** (government-only): multi-carrier service disruption; verify convening triggers, information request templates, and situational awareness products.
- **Joint U.S.-Canada cross-border exercise** (joint): incident affecting border throughput or binational carriers; verify liaison procedures, compatible information dissemination, and coordinated messaging.
- **Minimum viable indicator sharing demonstration** (joint): exchange a small set of validated indicators, affected product versions, and mitigations in a structured format with handling markings and analyst review gates.

4.4 Measuring Response Effectiveness and Return on Investment (ROI)

When evaluating policy and regulatory outcomes, measuring incident response effectiveness in motor freight requires metrics that connect cybersecurity outcomes to freight mission outcomes and stakeholder expectations. NIST CSF 2.0 frames cybersecurity as a set of high-level outcomes used to understand, assess, prioritize, and communicate cybersecurity efforts, and its implementation guidance emphasizes organizational context such as mission objectives, dependencies, and contractual requirements. In practice, this means pairing technical measures (e.g., time to detect, contain, and restore) with freight-impact indicators that reflect service delivery objectives so that cyber disruptions can be translated into operational and supply chain consequences that leadership can act on.

A balanced scorecard should include both quantitative metrics (time, coverage, volume, and cost) and qualitative benchmarks (decision quality, coordination effectiveness, and execution maturity). Industry benchmarking and incident response practice commonly emphasize time-based performance measures spanning compromise-to-detection, detection-to-containment, and containment-to-remediation, while also tracking the operational burden of false positives and triage workload. For qualitative benchmarking, CSF 2.0 Tiers provide an established model for describing progression from informal, ad hoc behaviors to repeatable and continuously improving approaches, which makes a simple 0–5 scale

defensible when used consistently. To reduce subjectivity, qualitative benchmarking should be calibrated over time through exercises, assessments, and after-action reviews, consistent with CSF improvement guidance that calls for identifying improvements from tests and exercises and with incident response guidance that emphasizes lessons learned and continuous improvement. This approach is consistent with the SANS 2023 Incident Response survey, which notes that organizations increasingly assess incident response effectiveness using internal metrics, exercises, and public frameworks such as NIST [81]. In this report, those established IR measures are extended into the motor freight context by linking them to operational continuity, coordination quality, and freight-specific outcomes at scale.

Return on investment (ROI) should be presented in terms of both loss prevention and capability enhancement, and expressed as a credible range (best/expected/worst) rather than a single point estimate. Loss prevention includes productivity and service-delivery losses avoided through faster containment and recovery. These measures include reduced downtime at terminals, fewer missed loads, and fewer penalties. Capability enhancement includes governance and coordination outcomes that reduce systemic exposure over time (shorter escalation times, reduced blast radius, improved reporting quality, and better vendor performance). This framing aligns with enterprise risk management guidance for leadership decision-making and with quantitative risk standards [82]. It is also consistent with cost benchmarking that links faster identification and containment with reduced breach impacts and costs, reinforcing the value of investments that measurably shorten incident lifecycles [83].

Metrics should be designed to be shared in aggregate (anonymized) across industry and government pilots to enable collective learning while protecting sensitive operational details. Canadian incident reporting guidance [84] explicitly encourages organizations to pre-decide what contextual and technical information they can share to inform next steps, support rebuild and recovery, and improve broader ecosystem resilience, while also stating that raw or identifying victim data will not be shared externally. Using consistent definitions among U.S. and Canadian stakeholders also improves cross-border situational awareness and decision-making during multi-entity incidents, aligning with Canadian federal response and event management frameworks that prioritize timely coordination, stakeholder situational awareness, and regular review/testing of processes.

4.4.1 Quantitative metrics

Using the 2023 SANS Incident Response Survey for inspiration, the following examples of quantitative metrics can be used to measure effective response and return on investment [81]. Separately, IBM's Cost of a Data Breach Report 2024 provides an evidence-backed economic basis for treating detection and containment speed as financially meaningful [85].

- **Detection and triage:** mean time to detect (MTTD), time to triage, false positive rate, percentage of alerts with automated enrichment.
- **Containment and recovery:** mean time to contain (MTTC), mean time to restore (MTTR) for dispatch and terminal-critical functions, percentage of endpoints isolated within the target time, and restore-time variance by terminal.
- **Scope control:** number of terminals affected, total critical business systems impacted, privileged accounts affected, vendor systems involved, and evidence completeness rate.

- **Operational freight impact**: shipment delay hours, missed loads, reduction in terminal throughput (percent), driver idle hours, customer SLA penalties, and border throughput impacts where applicable.
- **Readiness coverage:** percentage of terminals with end point detection response (EDR) coverage, percentage of critical systems centrally logged, log retention days, percentage of critical vendors with tested escalation paths, and exercise completion rates.

4.4.2 Qualitative benchmarks (simple 1-5 scales)

NIST IR 8286r1 frames cybersecurity risk as an enterprise risk management (ERM) input and states that enterprises should ensure cybersecurity risk receives appropriate attention within ERM, enabling risks to be identified, assessed, and managed in the context of broader mission and business objectives, of which examples are shown in Table 3 [82].

Table 3: Qualitative measures mapped to a 1-5 scale.

Dimension	1 (Ad hoc)	3 (Repeatable)	5 (Optimizing)
Escalation decisions	Inconsistent and personality-driven	Rule-based with documented overrides	Risk-based, fast, audited, continuously refined
Vendor coordination	Contacts unclear; slow engagement	Tested contacts; defined SLAs	Surge contracts; rehearsed; measured performance
Cross-border notifications	Improvised case-by-case	Triggered and documented	Practiced; fast liaison and compatible products
Evidence readiness	Limited; inconsistent chain of custody	Standard collection and tracking	Automated where appropriate; validated; high completeness
Lessons learned	Minimal follow-up	Post-incident actions tracked	Trend-driven continuous improvement with metrics

4.5 Roadmap Alignment with International Practices

The roadmap aligns with widely adopted U.S. incident response and risk management guidelines. NIST SP 800-61 Rev. 3 describes incident response as a lifecycle capability that should be integrated into broader cybersecurity risk management and continuously refined [49]. This supports the roadmap's focus on repeatable playbooks, governance, exercises, and performance metrics. The maturity framework also complements NIST Cybersecurity Framework Implementation Tiers, which depict a progression from informal, reactive practices to adaptive, risk-informed approaches [20].

Where motor freight stakeholders handle regulated or government-linked information, NIST SP 800-171 Rev. 3 provides a recognized control baseline that includes incident response requirements and emphasizes the need to track, document, and report incidents in line with applicable laws and contractual obligations [86]. While many carriers are not directly within scope for such requirements, the control logic offers a solid template for internal and external notification procedures, as well as for evidence and recordkeeping expectations when third-party dependencies are involved.

As motor freight operations increasingly rely on software-defined vehicles and telematics systems, vehicle cybersecurity standards such as ISO/SAE 21434 become more important for the makers and suppliers of these systems. ISO/SAE 21434 specifies engineering requirements for managing cybersecurity risks throughout the lifecycle of road vehicle electrical and electronic systems, emphasizing vendor escalation, coordination of software supply chains, and structured information sharing in incidents involving telematics or embedded platforms [87].

For organizations operating in markets affected by UN vehicle regulations, UNECE UN Regulations Nos. 155 (cybersecurity management systems) and 156 (software update management systems) strengthen managed processes for cybersecurity and controlled updates [14], [17]. Even when these regulations primarily apply to manufacturers and type approval, fleets benefit by aligning vendor requirements and incident escalation workflows with the expectations they set for managing cyber risk and software updates. The EU Cyber Resilience Act [18] sets broad cybersecurity requirements for products with digital elements. Motor freight operators using EU-sourced digital products (e.g., telematics units, IoT components, software services) can adopt CRA-aligned supplier practices to improve vulnerability management and security-by-design standards across their vendor ecosystem.

4.6 Incentives for Participation

When analyzing policy and regulatory implementation, it is crucial to understand the incentives for data sharing within the ecosystem. Sharing data after incidents is particularly challenging in motor freight because the involved parties—such as carriers, brokers, OEMs/telematics providers, insurers, and multiple government agencies—often face misaligned incentives, asymmetric risks, and unclear ownership of evidence. Common barriers include fear of reputational damage, legal or regulatory risks, competitive disadvantages, and the simple cost of developing high-quality, deconflicted, shareable incident reports while operations are under stress. Koepke emphasizes that participation is limited by trust and governance issues (who can see what, and how it will be used), liability concerns, and "free-rider" behavior, where organizations benefit from others' disclosures while withholding their own. [88]. Those barriers are heightened in freight because incidents often involve shared vendors and interconnected networks; in practice, a carrier may lack the forensic visibility to confidently identify the root cause when the compromise could be in a cloud identity platform, a managed service provider, or an ELD/telematics portal.

4.6.1 Sharing Incentives for Fleets

For motor carriers, the most concrete incentive for sharing cybersecurity incident data is operational: sharing can reduce downtime by accelerating pattern recognition (e.g. "this looks like that campaign"), enabling faster containment guidance, and surfacing workable recovery paths that peers have already tested. In the United States, motor carriers do have industry focused information-sharing avenues today, but they are spread across the Auto-ISAC [89], CISA Incident Reporting System [90], and the American Trucking Association's Fleet CyWatch [91], rather than consolidated into a single dominant carrier-only ISAC. In Canada, Koepke notes that credible value is strongest when sharing produces actionable outputs (timely indicators, mitigations, and coordination) rather than abstract calls for collaboration [88].

In Canada, motor carriers do not appear to have a single dominant trucking-only cyber information-sharing program. Instead, they rely on a distributed set of mechanisms: official reporting channels through the Canadian Centre for Cyber Security [92], the RCMP's NC3/Canadian Anti-Fraud Centre system [26], and Transport Canada's Situation Centre [93]; and broader information-sharing communities such as the Canadian Cyber Threat Exchange (CCTX) [94] and Auto-ISAC, the latter of which Transport Canada explicitly identifies as relevant to commercial vehicle companies.

In freight, where service continuity is the business, better collective detection and containment translates directly into fewer missed loads, less terminal congestion, and shorter "manual operations" periods. Even when reputational risk exists, there's also a pragmatic upside: if multiple fleets disclose consistent indicators and tactics, vendors and governments can corroborate and publish higher-confidence advisories, which gives carriers political/contractual cover to take disruptive defensive actions (e.g., shutting down integrations, rotating credentials, forcing MFA resets) that would otherwise be second-guessed.

A second fleet incentive is risk transfer and post-incident defensibility. Cyber insurance can (sometimes) formalize response steps and provide access to specialized response services that improve decision quality under pressure. MacColl et al. describe how insurance can provide crisis-management structure and access to response expertise that many organizations would not otherwise have readily available, and that these relationships can sometimes encourage reporting through better-connected response workflows [95]. However, this is inconsistent across the market, and victims still face strong commercial and reputational disincentives to transparency.

4.6.2 Incentives for Governments to Encourage Sharing

From a government perspective, incident reporting and sharing could create a national "early warning" and "learning" system aimed at turning scattered victim experiences into trend detection, prioritized mitigation, and coordinated disruption of criminal ecosystems. But Busetti & Scanni emphasize that incident reporting often fails to deliver those benefits because the system tends to treat reporting as a compliance artifact rather than an operational feedback loop; they frame effective reporting as needing to support both threat detection and policy learning, and they point out that many organizations hesitate because reporting consumes scarce resources and doesn't reliably return value to the reporter [88]. In transportation, that "return value" problem is acute: if a carrier reports but gets little timely technical help, the experience reinforces the belief that reporting is overhead, not resilience.

At the geopolitical level, governments also would ideally be inclined to care because ransomware and systemic compromises can degrade essential services and create strategic leverage for hostile actors. Iwasaki explicitly connects ransomware payment and disclosure regimes to national-security considerations (e.g., sanctions risk and the idea that ransom flows can enable broader criminal/terrorist activity), while also warning that blunt policy tools can backfire by changing victim incentives in undesirable ways, like hiding attacks [96]. The national-security incentive to encourage reporting competes with the private-sector incentive to minimize attention and preserve business continuity unless governments can create safe, predictable channels that reduce the downside of reporting incidents.

4.6.3 Anti-patterns for data sharing

1) **“Share only when forced”** (compliance minimalism). When reporting is framed as a checkbox, organizations provide vague timelines, incomplete indicators, and low-fidelity impact descriptions. That undermines correlation and reduces the value of the shared dataset, exactly the policy-learning problem Busetti & Scanni warn about [97].

2) **“PR-first disclosure”** (optics over utility). A fleet may disclose only broad statements (“cyber incident, no impact”) while suppressing the technical details peers actually need (identity artifacts, vendor touchpoints, exploitation path). This can protect the reputation in the short term, but increases sector-wide exposure.

3) **“Vendor scapegoating” and “vendor silence.”** In motor freight, shared-service providers rely on telemetry to confirm whether a compromise is single-tenant or multi-tenant. When contracts don’t require timely, structured evidence packages, carriers and governments get stuck in ambiguity. That ambiguity delays containment across the ecosystem.

4) **Ransom-payment policy distortions.** Both insurance and payment restrictions can unintentionally shape reporting behavior. MacColl et al. note persistent limits in reporting mechanisms and that victims are often not incentivized to be transparent due to commercial, regulatory, and reputational considerations. Iwasaki argues that strict bans may unintentionally reduce investment or encourage concealment, and proposes approaches that pair clearer standards and notification requirements with conditional safe harbors to realign incentives [96].

4.6.4 Challenges in sharing for motor freight carriers

Freight is an availability-driven business. During an incident, leadership pressure usually prioritizes “get dispatch back, keep trucks moving” over “produce a clean, shareable incident package.” When operations are brittle (relying heavily on TMS, email, identity, and shared vendor portals), the perceived cost of disclosure increases because leaders worry that disclosing specifics will trigger customer churn, contract penalties, or regulatory scrutiny at the worst possible moment. Koepke’s barriers of risk, trust, and the fear of harm become more binding when downtime is existential, and margins are thin [88].

At the same time, the systemic upside of sharing is unusually high in freight because campaigns reuse the same access paths (identity takeover, MSP compromise, vendor-side credential abuse) across many similarly-structured operators. That creates a strong “collective defense” argument: sharing is one of the few levers that can improve fleet resilience at scale, by turning isolated incidents into early warnings that keep other fleets from going down the same week.

5 Data Collection and Sharing

For cybersecurity events at scale, especially in transportation, incident response requires organizations to consistently gather high-quality telemetry, maintain its integrity, and quickly share the necessary subset with trusted partners. Modern incident response guidance treats it as a core component of cybersecurity risk management and operational practice, rather than a separate activity. This integrated approach is especially important and challenging for the transportation ecosystem, which has complex supplier, partner, and cross-border operational dependencies.

5.1 Data Source Overview

Data requirements can be defined by mapping use cases to investigation questions. This allows responders to quickly and confidently determine what happened, when it began, how far it spread, who and what were affected, what containment measures are safe, and what needs to be reported or shared externally. In practice, this involves creating a requirements catalog that lists critical event types, identifies the authoritative source systems for each event type, and outlines the minimum fields required for correlation. Example events include authentication, privilege changes, administrative actions, malware execution, data access, data egress, and configuration changes. The goal is not to collect everything, but to gather enough information to enable consistent scoping, investigation, and defensible reporting [98].

For transportation companies, requirements may enable identity-to-action traceability. Collection data for IT networks may include:

- stable asset IDs
- identity IDs
- timestamps
- session/request IDs
- system-of-record references
- identity-provider logs (SSO/MFA),
- VPN and remote access logs
- privileged access management (PAM) logs
- directory changes

Requirements may also include consistent time normalization (time zones, drift tolerances, and handling of authoritative timestamps) to enable reconstruction of multi-system timelines during emergencies. Without these correlation keys and time controls, organizations end up with large volumes of telemetry that may not answer the most critical questions under pressure [26].

Transportation requirements should include telemetry at IT/OT interfaces, such as segmentation devices, remote access brokers, and jump hosts, as well as telemetry for dispatch, yard, terminal, maintenance, and fueling systems, and interfaces between operational platforms and corporate IT. Even when OT systems have limited native logging, requirements can specify compensating controls, such as boundary monitoring, remote access audit trails, and configuration-change logging at managerial points. This approach helps determine whether an event is contained within enterprise IT or has spread to systems that could threaten operational stability and public safety.

Government organizations typically require a different data "shape" during large-scale incidents, as their primary value lies in cross-organizational correlation and coordinated guidance rather than deep forensic reconstruction within a single victim environment. Often, their view starts with what organizations submit through reporting channels, which include incident summaries, indicators, affected products/versions, observed tactics/techniques, and impact descriptions that enable cross-sector pattern matching. This is why a scalable program benefits from a two-tier output model: (1) a full-fidelity internal investigation package that supports ground truth and remediation, and (2) an external coordination package that is sanitized, sensitivity-labeled, and structured for quick sharing and correlation. Simply put, the organization that owns the telemetry should be designed to answer, "exactly what happened here?" while government partners should be able to answer, "how does this pattern relate across the country and what should everyone do next?"

5.2 Operational Technology Data Sources

Operational data sources form the foundation for detecting, scoping, and responding to cybersecurity events that originate in or affect motor freight vehicles. These devices include telematics, ELDs, ECUs, GPS, and diagnostics. Unlike enterprise IT systems, where logging and telemetry are relatively standardized, vehicle and fleet operational data is fragmented across onboard components, aftermarket devices, and vendor-managed backends. Effective incident response depends on understanding which operational data sources exist, what visibility they provide, and how they can be correlated with enterprise and identity telemetry to reconstruct events involving vehicles, drivers, and remote services.

Telematics units and ELDs are among the most critical operational data sources because they act as persistent gateways between vehicles and external networks. These systems typically collect and transmit location, speed, engine status, driver activity, fault codes, and compliance records, while also supporting remote configuration, firmware updates, and diagnostics. From an incident detection perspective, telematics and ELD telemetry support visibility into device connectivity state, authentication and authorization events, configuration changes, command execution, firmware or software updates, and anomalous message patterns sent to or received from vehicle networks. Because many telematics platforms are centrally managed across large fleets, backend logs from vendor cloud services often provide the earliest indication that an issue may be affecting multiple vehicles or customers simultaneously.

Electronic Control Units (ECUs) and in-vehicle networks are a more constrained yet essential data source for cybersecurity analysis. Most heavy-duty vehicle ECUs were not designed to generate security logs, and direct access to internal ECU telemetry is often limited by OEM design and safety considerations. As a result, data requirements should focus on what can be realistically observed: network-level indicators such as message rates, error frames, address claiming behavior, diagnostic session initiation, and changes in operational modes. Where direct ECU logging is unavailable, requirements should emphasize monitoring at aggregation points that can observe and record interactions with the vehicle network without interfering with safety-critical functions.

GPS and positioning data provide additional context that is particularly valuable for scoping and response. Location data can help determine whether anomalous behavior correlates with specific geographic regions, border crossings, facilities, or maintenance events, and whether multiple vehicles exhibit similar patterns in time and space. During large-scale incidents, GPS-derived timelines can also support operational decision-making, such as identifying which vehicles may need to be routed to safe

locations, removed from service, or isolated from remote connectivity until containment actions are validated. Because GPS data is often processed through telematics backends and shared with dispatch and logistics systems, maintaining consistent identifiers and timestamps across these platforms is critical for correlation.

Diagnostic interfaces and tools are a particularly sensitive operational data source because they blur the boundary between legitimate maintenance activity and potential adversarial action. Diagnostic adapters, service laptops, mobile applications, and remote diagnostic services generate records of diagnostic session initiation, parameter reads and writes, firmware flashing, and configuration changes. For incident analysis, it is essential that these events be logged with sufficient detail to establish who initiated the action, from where, using which tool or account, and against which vehicle or subsystem. In environments where diagnostic tooling lacks native logging, compensating controls become critical for reconstructing events and distinguishing faults from cyber activity.

Across all operational data sources, correlation hinges on a small set of shared reference points: stable vehicle identifiers (VINs or internal asset IDs), device identifiers, driver or technician identities, and synchronized timestamps. Without these anchors, even rich telemetry cannot reliably answer core incident-response questions at scale. For this reason, operational data sources should be integrated into the broader incident data architecture, with clear ownership, retention expectations, and interfaces for sharing sanitized summaries with trusted partners. When operational telemetry is treated as first-class incident data, it becomes possible to detect fleet-wide patterns, respond proportionately, and recover safely in the face of cyber incidents.

5.3 Information Technology Data Sources

The primary sources that most consistently support large-scale incident response include endpoint detection and response (EDR) telemetry, operating system and application logs, and identity and access records from identity providers, VPNs, PAM, SaaS audit trails, and directory services. These sources collectively answer “who did what from where?” but only if they are integrated with consistent schemas, stable identifiers, time normalization, and clear ownership for each log source so responders know what is authoritative during triage and scoping. Since account compromise and privilege misuse are common attack vectors, identity logs and administrative audit trails should be treated as primary evidence.

Network telemetry provides scalable evidence of communications and egress and remains valuable even when endpoint visibility is limited by attacker tampering, agent outages, or incomplete endpoint coverage. Flow and DNS data help develop hypotheses about command-and-control activity, lateral movement pathways, and data egress points, while proxy and secure web gateway logs offer more detailed information about outbound requests and destinations. Selective packet capture at critical choke points can further support investigations by confirming protocol misuse and reconstructing exfiltration attempts, but packet captures usually require a carefully defined scope and retention due to volume and sensitivity.

Application and data-layer audit logs are often crucial in transportation because significant outcomes, such as reservation disruptions, cargo or manifest manipulation, fraud, or exposure of customer and operational data, often occur at the application or database layer rather than solely at the endpoint. Logging at API gateways, cloud providers, email servers, databases, message buses, object storage, and administrative consoles can determine whether records were accessed, modified, or exported, and can

help establish the evidence trail needed for breach assessments and stakeholder communication. In safety-adjacent or OT environments, device-level logs may be limited by design or legacy constraints; in such cases, the most practical bulk evidence may come from boundary controls and management-plane systems, including remote access brokers, jump servers, configuration management tools, and segmentation devices that show whether access paths to operational networks were used and whether configurations were changed.

In large operational environments, Security Information and Event Management (SIEM) systems serve as the central analytical platform within security operations centers (SOCs), enabling the collection, normalization, correlation, and storage of security telemetry from diverse enterprise systems and sensors [99]. By aggregating logs from networks, endpoints, applications, identity services, and cloud infrastructure, SIEM platforms make large volumes of security data manageable at scale and provide a unified view for detection and investigation. Event data is enriched with contextual information such as asset metadata, identity attributes, and network intelligence, allowing correlation across domains that would otherwise appear unrelated. The resulting searchable event store supports both rapid triage and detailed forensic reconstruction of incidents, helping analysts identify affected entities, detect similar activity across systems, determine initial access points, and reconstruct early stages of an intrusion. In this way, SIEM systems transform continuous monitoring data into actionable detection and response capabilities rather than serving solely as log repositories.

Architectural design decisions in SIEM deployments significantly influence incident response effectiveness at scale [100]. Therefore, high-value telemetry sources should be onboarded using consistent schemas and reliable parsing so that correlation rules and analytic workflows operate on complete and accurate data. Storage strategies typically balance real-time analysis with longer-term retention: short-window “hot” data supports rapid investigation and threat hunting, while longer-term archival storage enables forensic analysis of incidents discovered after the fact or developing slowly over time. Because SIEM platforms often serve as the evidentiary backbone of incident investigations, deployments should also preserve audit records of administrative access and configuration changes and protect critical event datasets against tampering. These design considerations ensure that security telemetry can support both operational response and defensible post-incident analysis.

Security Orchestration, Automation, and Response (SOAR) technology enhances SIEM by coordinating and automating repeatable response steps across security tools and business processes [101]. This reduces triage and containment time and ensures more consistent responses in high-pressure situations. SOAR capabilities typically include playbook-driven automation such as enrichment, ticketing, notifications, endpoint isolation, account disablement, token revocation, and indicator blocking. It also offers case management features like evidence collection, timeline notes, and approvals, along with workflow governance that tracks who approved what and when. While SOAR is not primarily about automatically resolving incidents at scale, it is valuable because it handles high-volume, low-variance tasks that could otherwise overwhelm responders. SOAR also maintains a structured record of actions, supporting repeatability and auditability, which are crucial in incident response guidance.

The most effective approach for large transportation operators is to treat SIEM and SOAR as a connected system: SIEM provides detection, correlation, and investigative search, while SOAR transforms validated detections into governed actions with documentation. For example, a SIEM correlation that links anomalous Multi-factor Authentication (MFA) events, suspicious remote access locations, and privileged role changes can activate a SOAR workflow that retrieves recent authentication

history, checks endpoint posture, queries Endpoint Detection and Response (EDR) platforms for matching behaviors, and routes the case for approval-based containment (such as account lock, token revocation, endpoint isolation). This division of responsibilities is important when incidents are extensive: SIEM reduces uncertainty across multiple sources, and SOAR minimizes operational friction by standardizing response, documentation, and escalation. For large-scale events requiring external coordination, SOAR can also help create a consistent external coordination package (including sanitized indicators, affected products, timelines, mitigations, and impact summaries) as part of a playbook, supporting rapid sharing with proper controls without forcing analysts to manually reassemble outputs during high-pressure situations.

Government organizations typically do not ingest or hold a private company's full-fidelity telemetry by default. Instead, their situational awareness typically relies on reports and artifacts from formal channels and trusted exchanges. During a large-scale event, the shared subset, such as indicators, affected products, technique descriptions, high-level timelines, and impact summaries, can be extremely valuable when multiple organizations quickly report similar artifacts. This facilitates cross-incident correlation and speeds up the dissemination of mitigations. For transportation operators, the practical takeaway is that their external-facing package should be designed to be comparable and easy to consume, while their internal bulk sources (and the SIEM/SOAR backbone that makes them actionable) remain the authoritative source for ground truth and recovery decision-making.

5.4 Secure Data Collection and Sharing Practices

Guidance for secure data collection practices should focus on ensuring telemetry is reliable for investigation and defensible for future reporting, which requires large-scale integrity, availability, and auditability. This includes consistent time synchronization, preservation of original records, tamper resistance, cryptographic file hashes for file integrity validation, and strict administrative controls and comprehensive audit trails for access and modifications. When incident responders need to justify conclusions to executives, regulators, insurers, or courts, the ability to demonstrate that evidence was collected consistently and protected from modification becomes a crucial requirement, not just a best-effort feature.

The technical mechanisms that enable the flow of log and application data into SIEMS and other event aggregation systems, commonly called log pipelines, should be treated as critical infrastructure because they are high-value targets for intruders. Encryption in transit and at rest should be standard; collectors and forwarders should be strongly authenticated; and telemetry systems should be segmented to reduce the likelihood that a compromise in one zone enables attackers to disable or poison monitoring. Unnoticed issues such as missing events, time mismatches between systems, data that cannot be interpreted, changes in data structure, or monitoring tools going offline, can create blind spots that are only revealed when an incident escalates into a crisis. Organizations may want to implement continuous assurance of telemetry completeness (asset-class coverage, log-source freshness, volume baselines) and establish escalation criteria when monitoring fidelity degrades.

Secure sharing practices should focus on minimal necessary disclosure while enhancing actionability. This is best achieved by combining sensitivity labeling with structured technical formats. The Traffic Light Protocol (TLP) [102] provides a shared language for managing expectations and information boundaries, enabling sensitive information to flow swiftly within trusted circles without uncontrolled dissemination. Using a structured representation with Structured Threat Information eXpression (STIX) [103] and

standardized transport methods, such as Trusted Automated eXchange of Intelligence Information (TAXII) [80], supports consistent machine ingestion of indicators and related context, including relationships, sightings, and technique mappings. This improves correlation and reduces ambiguity in fast-paced environments. Clear handling rules paired with structured content transform informal indicators of compromise (IoC) into scalable, governed information exchange.

A clear difference between transportation company capability and government capability is the level of sharing: a company can analyze complete bulk sources (endpoint process trees, identity linkage, application audits, and sensitive operational and customer datasets), while government partners typically receive a shareable subset designed for coordination and cross-entity correlation. The key artifact that connects the two is a deliberately designed external coordination package that includes indicators, affected products, observed tactics/techniques, detection guidance, and high-level impact summaries, labeled under TLP and, when possible, encoded for automated exchange. In other words, the company uses depth to establish ground truth and generate reliable outputs; government organizations use breadth to correlate, prioritize, and communicate mitigation measures broadly without requiring everyone's raw logs.

To ensure coordination and data exchange remain effective during a large-scale event, transportation operators may consider adding information sharing into their playbooks rather than improvising. This involves defining who is authorized to release information, pre-approving fields and templates for sharing, and maintaining a shareability matrix that links data types to recipients and their sensitivity levels. It also requires planning for quick resolution of both internal and external conflicts. This governance framework supports faster reporting to national channels while safeguarding sensitive operational and personal information.

Owner-operators and smaller fleet operators face unique challenges in meeting the data collection, data integrity, and data sharing requirements outlined in this section. These challenges are primarily due to scale, cost, and staffing limitations rather than a lack of effort or awareness. Many depend on vendor-managed fleet management, maintenance, and telematics platforms that are mainly designed for operational efficiency rather than strict evidence standards. Data flows through SaaS dashboards and APIs, instead of through secure, dedicated collectors and monitors, make it hard to verify data completeness, identify gaps, or prove tamper resistance later. These issues complicate efforts to justify data when dealing with insurers, regulators, or law enforcement, even if operators act responsibly. For smaller operators, readiness depends on strategic choices: understanding what telemetry their vendors already store, negotiating access and retention terms, using maintenance and fleet systems as unofficial aggregation points, and adopting simplified data sharing practices (like TLP labeling and structured summaries) that enable coordinated responses without revealing raw operational data or requiring extensive security infrastructure.

5.5 International Information Sharing Pathways and Mechanisms

Since transportation systems are inherently cross-border and increasingly rely on shared suppliers and cloud infrastructure, large-scale cyber incidents often require rapid, well-organized international information sharing. Effective communication typically involves multiple channels rather than a single one; it uses layered pathways that transmit different types of information, such as technical indicators, victim impact reports, and operational details, at various speeds and levels of sensitivity. In practice, for

a transportation-sector event, cross-border sharing should be planned so that technical data can be sent swiftly while sensitive operational and personal information stays protected.

On the Canadian side, the *Federal Cyber Incident Response Plan* designates the Canadian Centre for Cyber Security as Canada's technical authority for cybersecurity and information assurance for critical systems [25]. It covers prevention, mitigation, preparedness, response, and recovery. The Cyber Centre also serves as a centralized source of expert advice, guidance, services, and support, delivered through incident reporting channels and engagement mechanisms [92]. In practice, this creates a consistent Canadian process during major events: organizations gather their own data, then share a curated set of indicators, observed tactics/techniques, affected products, and impact summaries through national channels so the Cyber Centre can analyze multiple reports and distribute information guidance.

U.S. policy recognizes that the global nature of the Internet requires, where appropriate, coordination with international partners in handling cyber incidents and designates the Cyber Unified Coordination Group (UCG) as the primary interagency body for major incidents [104]. The Presidential Policy Directive 41 and CISA doctrine outline how major cyber incidents are coordinated across federal agencies [105]. At the same time, CISA's *National Cyber Incident Response Plan* details a national approach that includes federal agencies, state/local/tribal/territorial entities, the private sector, and international partners in responding to significant incidents [106].

For operational exchange at scale, CISA also manages collaboration mechanisms such as the Joint Cyber Defense Collaborative (JCDC) [107], which aims to unify cyber defense capabilities and synchronize incident management and campaign response through shared processes and playbooks with federal, industry, and international partners.

Cross-border information sharing between U.S. and Canadian agencies is most evident through jointly developed advisories, shared technical analyses, and coordinated messaging, especially when campaigns threaten critical infrastructure in both countries. Public reports illustrate joint advisories and analyses involving U.S. agencies and the Canadian Centre for Cyber Security regarding sophisticated malware activity [108], demonstrating how the two nations can align on technical findings, defensive strategies, and public communication during high-risk situations. In incident operations, this joint approach typically relies on receiving compatible artifacts from affected organizations and on channels to validate and resolve sensitive details before broader dissemination.

This is where the suggested joint working group described in the report's governance section could serve as a binational counterpart to U.S. UCG-style coordination, focused on cross-border transportation continuity and actionable technical exchange. Instead of copying every agency authority, a joint working group could establish a repeatable process that brings together Canadian and U.S. leadership, as well as sector regulators, sector leads, and critical infrastructure owners/operators as needed. The benefit is creating a regular process that quickly achieves shared situational awareness, aligns technical guidance, and reduces friction about what can be shared, at what sensitivity, and through which dissemination channels.

Operationally, a binational working group could serve as the bridge between company-level data and government oversight by standardizing the minimum data package that transportation operators provide during large events (confirmed indicators, affected products/versions, observed techniques, detection logic, prioritized mitigations). It can align terminology and formats so both countries can quickly correlate information and agree on how outputs are produced and published. This approach

reflects the intent of UCG and NCIRP frameworks to unite efforts while respecting separate responsibilities and partner processes to ensure information exchange remains timely and actionable. Implemented effectively, the joint working group becomes the channel through which U.S. and Canadian agencies share knowledge and public statements on a schedule that matches large-scale incident dynamics, without either side needing to obtain or store full raw telemetry that remains under company control.

5.6 Instrumentation Challenges in Mixed Legacy and Modern Fleets

Motor freight fleets typically operate a heterogeneous mix of legacy and modern vehicles, creating significant instrumentation challenges for cybersecurity detection, response, and recovery. Newer vehicles may support richer telematics, remote diagnostics, over-the-air updates, and limited security logging, while older platforms often expose only basic fault codes and operational signals through unsecured diagnostic interfaces. This uneven instrumentation landscape results in inconsistent visibility across the fleet, where cyber-relevant indicators, such as anomalous network traffic, unauthorized configuration changes, or suspicious diagnostic activity, may be observable in some vehicles but entirely opaque in others. Compounding this challenge, aftermarket devices are frequently used to retrofit legacy vehicles, introducing additional gateways into vehicle networks without standardized telemetry, authentication, or logging controls. As a result, fleets are forced to infer system-wide risk from partial, fragmented data, complicating correlation across vehicles, terminals, and vendors. In large-scale incidents, these visibility gaps delay detection, hinder scoping, and obscure whether observed anomalies represent isolated faults or coordinated malicious activity. Addressing instrumentation challenges in mixed fleets, therefore, requires compensating controls that acknowledge legacy constraints while enabling fleet-level situational awareness aligned with modern cybersecurity expectations.

5.7 Data Integrity, Timestamping, and Chain-of-Custody Considerations

Effective incident response at scale in motor freight operations depends on the integrity, temporal accuracy, and evidentiary defensibility of the data collected. In distributed cyber-physical environments, logs, telemetry, diagnostic records, and sensor data are generated across vehicles, telematics platforms, cloud services, and third-party systems, each with its own clock, retention policy, and trust boundary. Inconsistent timestamping can severely undermine the ability to reconstruct event sequences, correlate activity across domains, or distinguish cause from effect during rapidly evolving incidents. Equally critical is maintaining a chain of custody for digital evidence, particularly when data may later be used in regulatory inquiries, civil litigation, insurance claims, or criminal investigations. At scale, evidence frequently transits multiple organizations, including carriers, OEMs, telematics providers, managed service providers, and government agencies, increasing the risk of unintentional alteration, loss, or contamination. Without predefined standards for evidence handling, validation, and documentation, organizations may face challenges defending investigative conclusions or demonstrating due diligence. Addressing these risks requires deliberate governance: synchronized time sources, immutable logging where feasible, clear provenance metadata, defined retention windows, and role-based authority for evidence access and transfer. In large-scale transportation incidents, data integrity and chain of custody are foundational to trust, accountability, and coordinated response across organizational and jurisdictional boundaries.

5.8 Potential Incident Response Architecture

A scalable incident response architecture for motor freight transportation should be designed as a system-of-systems capability, not a single organizational platform. As emphasized in OT Digital Forensics and Incident Response (DFIR) research, effective response in cyber-physical environments depends less on centralized control and more on clearly defined roles, data flows, escalation logic, and preservation of evidence across many independent stakeholders [109]. In the freight sector, this architecture should bridge enterprise IT systems, vehicle-level electronics, telematics platforms, roadside operations, and public safety authorities, which are often under conditions where no single actor has complete authority or visibility.

From an actor and stakeholder perspective, the architecture should account for the diverse participants involved in incident detection, response, and recovery. Fleet owners and operators retain responsibility for operational decision-making and service continuity, while authorized IT and OT support personnel manage containment and technical remediation. Drivers and technicians often serve as the first observers of anomalous behavior, particularly in cyber-physical incidents that manifest as breakdowns, diagnostic anomalies, or crashes. Law enforcement and first responders control the scene during safety-critical events, regulators and government agencies provide coordination and oversight, and OEMs, telematics service providers, and upfitters control critical portions of the technical stack and data. Consistent with OT DFIR guidance, the architecture should assume distributed authority and staged escalation, rather than a single incident commander with end-to-end control [109].

Functionally, architecture should support the full incident lifecycle: planning, data acquisition, analysis, detection and notification, response execution, and recovery. Pre-incident planning establishes decision rights, escalation thresholds, and evidence-handling procedures before an event occurs. Data acquisition spans multiple domains, including vehicle networks, diagnostic adapters, telematics streams, identity systems, cloud services, and maintenance records. Analysis should integrate forensic methods from IT, OT, and vehicle systems research, recognizing that cyber incidents in transportation may not present as malware but as protocol misuse, message injection, or anomalous control behavior. Detection and notification extend beyond SOC alerts to include maintenance anomaly reporting, safety investigations, and cross-organizational pattern recognition. Response and recovery then execute predefined plans that balance containment, safety, evidence preservation, and service restoration.

Structurally, a reference architecture should be organized around six core layers. First, a common data schema is required to normalize heterogeneous evidence sources, enabling patterns to be correlated across fleets and vendors. Second, data pipelines should support both continuous ingestion (for monitoring and baselining) and burst collection during incidents, with explicit controls to preserve data integrity and chain of custody. Third, analytic tools should support both real-time triage and offline forensic analysis, consistent with OT DFIR principles that separate time-critical response from deeper investigation. Fourth, notification infrastructure should enable structured, machine-readable sharing of indicators and context using established standards such as STIX for content and TAXII for transport, while still supporting existing operational communication mechanisms (phone, radio, email, safety bulletins). Fifth, incident response plans should define how actors coordinate containment and escalation decisions across organizational boundaries. Sixth, system recovery plans should address both data restoration (backups, configuration baselines) and operational recovery (device replacement, manual fallbacks, degraded operations).

The effectiveness of this architecture cannot be evaluated solely by technical performance metrics. Consistent with resilience engineering and OT DFIR guidance, measures of effectiveness should include Recovery Time Objective (RTO) for restoring essential functionality, Recovery Point Objective (RPO) for data loss tolerance, detection time from first anomaly to incident recognition, and false positive and false negative rates that reflect the system's ability to distinguish malicious activity from routine failures.

Overall, this architecture does not assume that cyber incidents in motor freight will resemble traditional enterprise breaches. Instead, it reflects the reality described in vehicle forensics and OT DFIR literature: cyber-physical incidents are often ambiguous, distributed, and safety-adjacent, requiring coordination across actors who were not historically part of cybersecurity response. By explicitly modeling stakeholders, functions, data flows, and performance measures, this architecture provides a foundation for incident response at scale that prioritizes safety, preserves evidence, and enables coordinated recovery across the freight transportation ecosystem.

5.9 Legal and Regulatory Considerations for Data Sharing

Legal and regulatory constraints govern what can be collected, retained, and shared, especially when large datasets include employee, passenger, customer, or partner personal information. For private-sector transportation companies subject to Canada's private-sector privacy law, guidance emphasizes mandatory breach reporting and notification when a breach poses a real risk of significant harm, and stresses the importance of maintaining breach records, including those that have not been reported. These rules underscore the need for careful evidence preservation and thorough documentation, and they also encourage organizations to limit data collection and implement role-based access to sensitive telemetry, enabling investigators to work effectively while minimizing unnecessary exposure.

The compliance reality for transportation operators is that legal and operational needs should coexist. Organizations should set retention periods aligned with investigation requirements and privacy expectations, implement access controls that distinguish between need-to-know investigative access and broader operational visibility, and establish legal-hold triggers to ensure evidence is preserved when necessary. This is especially crucial in large-scale events where an initial operational disruption may later be identified as a data exposure or a supply chain breach, requiring more comprehensive preservation and documentation than a routine outage.

For Canadian federal institutions, the Privacy Act governs the collection, use, and disclosure of personal information and limits collection to data directly related to an operating program or activity [110]. This has practical implications for open-ended bulk collection and how incident-related data can be shared. This is a key reason government organizations often rely on purpose-limited incident reports and technical artifacts rather than broad ingestion of private-sector raw data: the legal basis for collection and the mandate should align with a specific program or function [111].

The Government of Canada's incident management guidance distinguishes pathways for cyber incidents, threats to national security, and suspected criminal activities, affecting what information is shared, with whom, and under what authority. In large-scale events, these pathways matter because they influence how transportation operators route different categories of information (e.g., technical indicators and incident summaries versus evidence of criminal extortion or national security implications) [112]. The practical result is that organizations benefit from a predefined decision framework that connects information types to recipients and authorities, rather than leaving routing decisions to ad hoc judgment during a crisis.

These legal realities support a best-practice operating model that links company depth to government breadth: the transportation company conducts a thorough internal investigation to establish ground truth using its full-fidelity data. It then produces an external-sharing subset that is lawful, minimal, and operationally useful for technical correlation and coordination. When more detailed information is needed beyond that subset, it is usually obtained through purpose-driven sharing arrangements, regulatory mechanisms, or case-specific legal processes, rather than through assumed bulk access. Designing for this model from the outset improves speed, reduces legal risk, and increases the likelihood that shared information is both actionable and appropriately handled.

6 Forensic Analysis and Escalation Criteria

To date, there has been no publicly confirmed cybersecurity incident that has disrupted motor freight or surface transportation at a true national scale through direct cyber-physical effects on vehicles or fleets. Unlike sectors such as energy or finance, transportation has not yet experienced a cyber event in which coordinated malicious activity simultaneously degraded vehicle operations, caused widespread crashes, or halted freight movement across regions. Most large transportation cyber incidents discussed in policy and academic literature remain hypothetical, modeled, or extrapolated from other sectors. Where "at-scale" cyber impacts are cited, they typically involve enterprise IT disruptions (e.g., ransomware affecting dispatch or billing systems) rather than systemic manipulation of vehicle operations.

However, the absence of a confirmed catastrophic event should not be interpreted as evidence that escalation frameworks are unnecessary. In transportation, escalation logic should account not only for confirmed malicious activity but also for operational stress patterns that exceed normal failure modes. Traditional maintenance and operational response models already include escalation pathways: roadside technicians request assistance from regional maintenance teams, OEM support lines, or specialized diagnostic groups; unresolved issues are elevated to national fleet engineering, vendors, or manufacturers. This tiered support structure assumes that failures are independent, stochastic, and resolvable through additional expertise or parts. When similar anomalies occur simultaneously across many vehicles, terminals, or regions, those higher-level resources can become saturated, an outcome that may itself indicate coordinated or systemic causes rather than coincidental mechanical failures.

Transportation operations further complicate escalation because fleets vary widely in how maintenance and diagnostics are performed. Some large carriers operate internal service centers with centralized diagnostic visibility, while others rely heavily on dealerships, OEM-authorized repair networks, or third-party service locations such as truck stops. This fragmentation means that early warning signals may be dispersed across many independent organizations before anyone recognizes a pattern. These signals may be repeated unexplained faults, identical diagnostic symptoms, or inconsistent vehicle behavior. At scale, the challenge is not simply technical analysis but recognizing when routine escalation pathways are being stressed in abnormal ways. This section establishes criteria for distinguishing localized operational issues from potential cyber incidents, defining when saturation, correlation, and repeated anomalies should trigger forensic preservation and broader escalation, even in the absence of definitive proof of malicious intent.

6.1 Defining Cyber Incident Severity and Escalation Thresholds

Because large-scale transportation cyber incidents remain largely theoretical, escalation thresholds should be grounded in risk-informed severity assessment rather than historical precedent. Other sectors provide instructive analogs. The SolarWinds supply chain compromise demonstrated how a single, stealthy intrusion into a trusted software provider could propagate silently across thousands of organizations, evade traditional perimeter defenses, and remain undetected for months, despite limited immediate operational disruption. While SolarWinds did not directly impair transportation operations, it illustrates how scale, trust relationships, and delayed detection can transform a technically modest intrusion into a nationally significant incident. For transportation, severity should be assessed not only by observed impact, but by proximity to operational control, potential blast radius, and the degree to which failures correlate across otherwise independent systems. Escalation thresholds should account for uncertainty, incomplete evidence, and the possibility that benign explanations may later prove

insufficient. This ensures early forensic preservation and coordination occur before decisive proof is available, rather than after critical evidence has been lost.

6.1.1 Overview of the CISA National Cyber Incident Scoring System (NCISS)

NCISS is CISA's repeatable approach for estimating incident risk, enabling responders to triage and prioritize consistently across multiple entities [113]. It is intended to translate observed technical facts and business impacts into a structured risk rating that drives urgency, resource allocation, and escalation decisions.

CISA NCISS is based on NIST SP 800-61 Rev. 2 and is tailored to incorporate potential impact categories, enabling analysts to evaluate severity at the national level [49]. In practice, organizations often represent NCISS outputs as a score that maps into named priority levels. NCISS materials describe priority labels such as Emergency (Black), Severe (Red), High (Orange), Medium (Yellow), Low (Green), and Baseline, with narrative definitions for each. These labels align well with the U.S. Cyber Incident Severity Schema (Levels 0-5), which standardizes incident severity language across federal coordination [114].

Canada does not publish a universal NCISS-equivalent scoring scale for all non-government operators, but it offers national coordination resources that serve similar functions for escalation and response posture. The Federal Cyber Incident Response Plan establishes coordination protocols and notes that incidents should be reported to the Canadian Centre for Cyber Security (Cyber Centre), which supports situational awareness and coordinated response for incidents affecting the systems of essential non-government entities [25].

Table 4: Summary of the National Cyber Incident Scoring System

NCISS-style score band	Priority/severity label (lexicon)	Practical interpretation for transportation environments
0-9	Baseline - Negligible	Routine or benign activity; monitor and close.
10-24	Baseline - Minor	Suspicious activity; validate and contain locally if needed.
25-44	Low (Green)	Confirmed incident with limited scope; handle via standard IR.
45-64	Medium (Yellow)	Material risk; activate incident management and cross-functional coordination.
65-79	High (Orange)	Credible near-term risk to service or trust stores; war room posture.
80-94	Severe (Red)	Likely significant impact; crisis management posture and senior coordination.
95-100	Emergency (Black)	Imminent threat to wide-scale critical services or life safety; emergency operations posture.

NCISS-style scoring also facilitates quick government coordination. CISA's Federal Incident Notification Guidelines explain how CISA assigns a tracking number and risk rating using a scoring system after receiving a report, emphasizing the role of scoring in triage and decision-making [115].

6.1.2 Applying NCISS to a transportation cybersecurity event at scale

In motor freight operations, an at-scale event is defined by its operational impact and potential to cascade across the network, not by a single technical indicator. Examples include disruptions to dispatch and load-planning systems, telematics and ELD platforms, cross-border clearance processes, terminal and yard operations, or shared-service providers whose failure can affect multiple carriers simultaneously.

Transportation scoring should consider proximity to operational and safety systems as an escalation factor. Even if user-facing disruption has not yet begun, compromises of identity, privileged access, remote access tools, or operational technology boundary controls should be treated as a high priority, as they can enable rapid operational disruption.

At-scale response requires repeated reassessment. Initial scoring should monitor what is confirmed and what remains uncertain (spread, dwell time, persistence), and scores or tiers should be updated when major findings change (privilege escalation, destructive tools, exfiltration confirmation, or OT footholds).

Major transportation incidents often require concurrent coordination with cyber authorities and law enforcement agencies. In Canada, the RCMP NC3 handles national cybercrime coordination and promotes reporting to law enforcement and NC3, while the Cyber Centre offers technical support and is not a law enforcement agency [116].

6.1.3 Defining escalation thresholds for carriers and government agencies

Scoring becomes valuable when it is linked to specific thresholds that trigger definite actions. Operator thresholds should map score or tier levels to actions such as activating a war room, engaging safety leadership, initiating vendor surge contracts, and making service-reduction decisions. In Canada, FCIRP offers a structured national activation and response framework for incidents impacting critical non-government systems. Aligning internal tiers with FCIRP standards helps operators coordinate with the Cyber Centre and Public Safety Canada consistently during major incidents. Cross-border escalation must be explicit because transportation routes often depend on binational cooperation (ports, rail interlines, border crossings, bridges/tunnels, and shared IT services). The Public Safety Canada–DHS Cybersecurity Action Plan highlights improved partnership and coordinated incident response between the two nations. The crosswalk below maps score ranges to tiers consistent with the U.S. severity schema language and incorporates cross-border expectations at Tier 3+. Organizations should also establish strict override protocols (privileged identity compromise, OT boundary access, destructive tooling) that mandate escalation even if the score is still stabilizing.

Table 5: Mapping of Incident Tiers to Escalation Thresholds.

Tier	Severity Schema	Illustrative score band	Operator escalation (examples)	Government escalation (examples)
Tier 0	Level 0 (Baseline)	0-19	SOC handles; ticket only	None / info-only
Tier 1	Level 1 (Low)	20-39	IR lead notified; internal assessment	Sector ISAC/ISAO optional
Tier 2	Level 2 (Medium)	40-59	Activate incident management; vendor escalation	U.S.: consider CISA; Canada: notify Cyber Centre as appropriate
Tier 3	Level 3 (High)	60-79	War room; cross-operator coordination	U.S.: CISA coordination; Canada: Cyber Centre + Public Safety coordination
Tier 4	Level 4 (Severe)	80-94	Crisis management; service curtailment decisions	Federal-level coordination; activate cross-border procedures
Tier 5	Level 5 (Emergency)	95-100	Emergency operations; safety-first shutdown protocols	National-level coordination; cross-border emergency mechanisms

To operationalize the crosswalk, many transportation organizations maintain a separate notification gate checklist. These gates ensure that specific findings, such as compromised trust stores or OT boundary systems, trigger immediate senior notification and cross-border liaison engagement, regardless of the current numeric score.

6.2 Defining Response Thresholds for Stakeholder Notification

Notification thresholds should be progressive and multi-trigger. Transportation incidents often start as subtle compromises and escalate quickly; thresholds should scale based on severity, proximity to mission-critical systems, and impact size. Cross-border dependencies add an extra trigger dimension. A single-operator incident may require binational notification if it affects cross-border flows or shared dependencies (e.g., shared vendors, border operations, ports, rail interlines, tunnels/bridges, or shared identity services). On the Canadian side, thresholds should include reporting to the Cyber Centre per FCIRP, and parallel reporting to RCMP NC3 (and police of jurisdiction) when criminal activity is suspected. Privacy obligations can also impose mandatory notification requirements if a breach poses a real risk of significant harm, according to guidance from the Office of the Privacy Commissioner of Canada [117]. On the U.S. side, thresholds should include reporting to CISA using the pathways in the Federal Incident Notification Guidelines and CISA reporting resources [118]. For cross-border incidents, thresholds should align with bilateral expectations for compatible cross-border alerts and coordinated dissemination [119], [120].

Repeated, inexplicable breakdowns are often the earliest operational signals that something is wrong, and they often surface first among maintenance staff rather than cybersecurity personnel. From a mechanic's perspective, the initial facts are practical and pattern-based: a cluster of roadside

breakdowns with similar symptoms (e.g., repeated limp-mode activation, intermittent sensor faults, unexpected warning lights, unexplained derates, spurious diagnostic trouble codes that clear and reappear, or repeated “no fault found” outcomes after component replacement). In a connected fleet, these symptoms can plausibly arise from benign causes, poor harness connections, marginal sensors, software regressions, power quality issues, or environmental effects, but they can also be consistent with cyber-enabled manipulation of diagnostics, spoofed signals on vehicle networks, or compromised aftermarket/telematics devices that inject or suppress messages. Because modern troubleshooting increasingly depends on electronic evidence (scan-tool sessions, calibration states, ECU snapshots, update histories, and gateway logs), the response threshold should include “maintenance anomaly triggers” that escalate when the same failure mode repeats across vehicles, terminals, or time windows without a defensible mechanical root cause. Practically, this means treating repeated, correlated “mystery failures” as a cue to preserve artifacts (adapter logs, telematics event streams, ECU configuration states, firmware versions, and work-order timelines) and to elevate the case from a local repair workflow to a fleet-level reliability and security investigation.

A similar but higher-stakes escalation problem emerges when multiple roadway crashes occur with unexplained causes that are not well explained by driver error, mechanical failure, or roadway design. Individual crashes are investigated under safety and legal frameworks, and litigation concerns can limit what a carrier can access or share early, especially when evidence is controlled by law enforcement, insurers, and counsel. However, the notification challenge changes when multiple incidents exhibit a recurring operational signature: the same vehicle subsystem appears implicated, similar driver reports recur (e.g., sudden loss of instrumentation, unexpected braking/derating behavior, erratic warnings, or inconsistent ADAS alerts), or event timing clusters around shared dependencies (a recent software update, a new telematics configuration, a common diagnostic adapter, or a vendor outage). In this scenario, the threshold for stakeholder notification should include a “pattern-of-harm trigger,” in which the occurrence of repeated events becomes an indicator in its own right, regardless of whether any single crash can be conclusively attributed to cyber causes. The operational objective is not to litigate root cause in the moment, but to rapidly constrain potential blast radius: preserve data sources before they roll off retention windows, coordinate with OEMs and telematics providers to check for common-mode faults or malicious activity, and alert sector/government partners when the pattern suggests a systemic hazard that could affect additional vehicles, fleets, or cross-border corridors.

These notifications are intended to support timely, risk-informed decision-making during transportation incidents. Their purpose is to help leadership determine when broader notification, coordination, and escalation are warranted based on potential safety, operational, regulatory, and reputational impact. The thresholds are guidance rather than rigid rules and are designed to be applied with executive judgment, particularly when information is incomplete or evolving.

These thresholds apply to both physical and technology-driven incidents. For example, a vehicle crash involving hazardous materials that closes a critical corridor for several hours may warrant escalation due to safety risk, sustained disruption, and cascading logistics impacts, even in the absence of a cyber component. Similarly, a cyber or OT intrusion affecting rail signaling systems may justify early escalation due to latent safety and systemic risk, even if no immediate service outage is observed. In both cases, escalation is driven by impact and potential consequence rather than by the nature of the initiating event.

Assessments of severity and scale are inherently subjective and will evolve as additional information becomes available. Severity reflects potential impact, not only current conditions, and scale often expands or contracts as investigations progress. No single function has a complete view of an incident at the outset. Operations and safety teams are best positioned to assess physical and service impacts, while IT, OT, and cybersecurity teams are best positioned to assess system integrity and threat propagation. Enterprise risk, emergency management, or incident command leadership is best suited to aggregate these inputs into an integrated picture that supports executive decision-making. These thresholds should therefore be viewed as decision-support tools that enable timely coordination and leadership engagement, with the objective of reducing uncertainty, protecting safety, and maintaining trust as the situation develops.

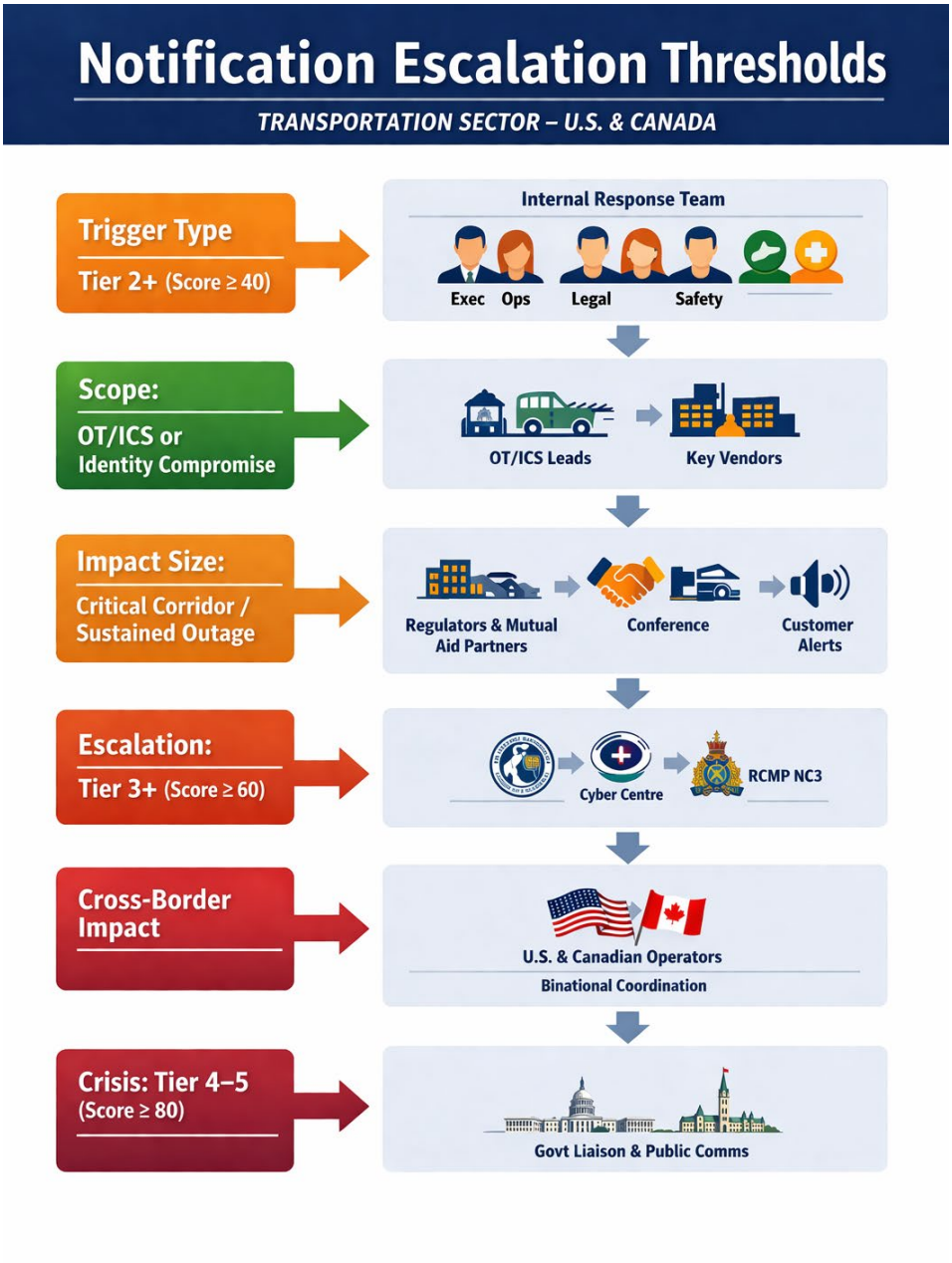


Figure 3. Illustrative Notification Escalation Flow for Transportation Incidents in the United States and Canada.

6.2.1 Transportation company notification thresholds

The operator notification thresholds should be interpreted holistically, with incidents assessed across severity, scope, and impact rather than against a single criterion. Severity tiers reflect increasing levels of organizational risk and are driven by potential consequences, not certainty or root cause. Trigger types such as confirmed OT/ICS involvement, privileged identity compromise, sustained service disruption, or impacts to critical corridors should be viewed as cumulative risk signals. Early involvement of executive on-call leadership, legal and privacy, communications, and safety and operations is intentional, as early coordination reduces downstream risk even when facts are still emerging. Any credible cross-border impact is treated as a risk multiplier due to regulatory complexity, shared dependencies, and heightened public confidence considerations.

Table 6: Incident Response Thresholds for Motor Carrier Response Escalation

Trigger type	Threshold	Minimum stakeholder notifications
Severity	Tier 2+ (Level 2+ / score >= 40)	Executive on-call; Legal/Privacy; Communications; Safety/Operations
Scope	Confirmed OT/ICS involvement OR privileged identity compromise	OT/ICS leadership; critical vendors; affected units; safety leadership as applicable
Impact size	>= 1 critical corridor/hub affected OR > 2 hours sustained disruption	Regulator/oversight as required; mutual aid partners; customer messaging readiness
Escalation	Tier 3+ (Level 3+ / score >= 60)	External partner sharing (ISAC/ISAO); engage CISA (U.S.) and/or Cyber Centre (Canada)
Cross-border impact	Any credible impact on U.S.-Canada cross-border operations or shared dependencies	Notify counterpart operator(s); activate binational liaison; coordinate with CISA and Cyber Centre
Crisis	Tier 4-5 (Level 4-5 / score >= 80)	Public communications cadence; surge contracts; activate compatible cross-border alert/warning procedures

6.2.2 Government agency notification thresholds (sector coordination lens)

Government agency notification thresholds apply a sector-level coordination lens rather than an individual operator perspective. Escalation to agency engagement generally begins at Level 3 or higher, or when national response frameworks are activated. Agency actions are driven by multi-operator or shared-vendor impacts, potential safety risks, or critical service interruptions, and rapidly evolving conditions that require shared situational awareness. Cross-border triggers prioritize alignment between U.S. and Canadian authorities to avoid conflicting guidance, delayed response, or inconsistent public messaging. Agency engagement is intended to enable coordination and risk reduction and should not be viewed as inherently regulatory or punitive.

Table 7: Incident Response Thresholds for Government Response Escalation

Trigger type	Threshold	Agency actions/notifications
Severity	Level 3+ (High) or FCIRP escalation	Coordinated situational awareness; enable CISA/Cyber Centre engagement
Scope	Multi-operator impact or shared-vendor compromise	Notify sector partners; coordinate with ISAC/ISAO
Impact size	Safety risk or critical service interruption potential	Joint coordination calls; engage transportation regulators and public safety partners
Time sensitivity	Rapidly evolving incident	Rapid triage and prioritization using NCISS principles / FCIRP assessment
Cross-border trigger	Cross-border critical infrastructure, services, or shared dependencies affected	Activate joint U.S.-Canada channels and compatible alert/warning procedures; coordinate dissemination

6.3 Forensic Readiness: Pre-Incident Planning and Documentation

6.3.1 Pre-incident planning and readiness tasks

Governance is the foundation of forensic readiness because it determines whether evidence can be preserved and contained quickly enough. Transportation organizations should predefine decision rights across IT, OT, and safety-adjacent domains, including those who can authorize containment actions that may affect service availability and what safety validation is required before restoration.

Policies should establish standards for logging, retention, and evidence handling. Identity and OT boundary systems typically warrant longer retention because they become pivotal during major investigations, and chain-of-custody expectations should cover both internal and third-party evidence (including managed service providers and cloud audit logs).

Procedures should be written as repeatable, step-by-step guides for collection and preservation. This includes time-synchronization checks, minimum-evidence datasets for each environment zone, and clear rules for live response, imaging, and targeted log capture. Transportation OT guidance highlights that organizational planning, policy, and best-practice controls are key to OT cyber readiness.

Templates and playbooks reduce cognitive load during real events. Standardized intake forms, executive briefs, partner-sharing packages, and scenario playbooks (ransomware, privileged access compromise, OT boundary breach, shared-vendor compromise) help teams move quickly while preserving evidence quality.

6.3.2 Communication plans with verified points of contact

During major incidents, coordination failures are often communication failures. A communication plan should define who communicates, via which channels, with what approvals, and at what cadence for each severity tier, covering internal, vendor, regulator, and government communications.

Points of contact should be role-based rather than person-based because duty officers and vendor teams change frequently. Role-based contacts reduce single-point-of-contact dependency and simplify off-hours escalation, and should include primary and secondary numbers and escalation ladders.

Contact lists should be tested. Annual validation should confirm 24/7 reachability, exercise end-to-end escalation ladders, and test alternative channels when primary systems (email, SSO) are impacted.

Cross-border plans should align with bilateral coordination intent. The Cybersecurity Action Plan and the Canada–United States Action Plan for Critical Infrastructure both emphasize collaboration and the use of compatible cross-border information-sharing procedures.

6.3.3 Proposed RACI matrix

A Responsible Accountable Consulted and Informed (RACI) matrix clarifies roles by assigning responsibility and accountability for key incident lifecycle activities, including declaration, containment, evidence preservation, external sharing, notifications, public communications, and lessons learned. It is especially useful when incidents involve IT, OT, and safety-related systems.

Ideally, the matrix would accurately reflect transportation realities: OT containment decisions can influence safety and service continuity, and communication decisions are closely linked to operational impacts. Therefore, safety leadership and OT engineering would preferably have clear roles in OT containment and restoration.

The RACI would optimally also include cross-border notifications and government engagement. A Government Liaison role could manage external sharing and initiate cross-border notifications to CISA and the Cyber Centre when thresholds are reached, while Legal/Privacy would remain responsible for ensuring compliance. The proposed RACI below includes this Government Liaison role and could be extended with a dedicated Binational Liaison designation (primary/alternate) for organizations with cross-border operations.

Table 8: RACI Matrix for Incident Response

Activity	Responsible	Accountable	Consulted	Informed
Declare incident / set initial tier	IR Lead	Executive Sponsor	SOC, Safety, Legal	All leads
Containment actions (IT)	IT Ops Lead	IR Lead	SOC, Vendor	Executive, Gov Liaison
Containment actions (OT)	OT Engineering Lead	Safety Officer	IR Lead, Vendor	Executive, Gov Liaison
Evidence preservation and collection	SOC + DFIR Vendor	IR Lead	Legal/Privacy, OT/IT	Executive
External data sharing (IOCs/TTPs)	Gov Liaison	Legal/Privacy	IR Lead, Communications	Executive
Public communications	Communications	Executive Sponsor	Legal/Privacy, IR Lead	All
Stakeholder notifications (regulators, partners)	Gov Liaison	Executive Sponsor	Legal/Privacy, Communications	SOC/IR/OT/IT
Post-incident report/lessons learned	IR Lead	Executive Sponsor	All leads	Organization-wide

6.3.4 Technical infrastructure for forensic readiness

Technical readiness begins with the ability to generate, retain, and correlate telemetry sufficient to reconstruct events and support timely decision-making. Transportation environments should, at a minimum, capture logs and signals from endpoints, identity and access systems, network infrastructure, cloud and SaaS platforms, and operational technology sources such as engineering workstations, remote access gateways, and OT monitoring sensors. The goal is not exhaustive visibility but defensible coverage of systems that influence safety, service continuity, and operational control.

The scale and sophistication of telemetry collection vary depending on operator size. Large fleets typically have centralized security and IT operations that can handle high-volume data across multiple domains. Medium and small owner/operators may lack dedicated security infrastructure, but can still achieve significant readiness by focusing on high-value data sources and leveraging existing operational systems. Specifically, fleet management and maintenance platforms already gather detailed operational data, including vehicle health, fault codes, work orders, access records, and service histories. These serve as effective points for incident reconstruction when combined with basic identity and network logs.

Security information and event management (SIEM) capabilities enable normalization, correlation, and retention of telemetry across identity, endpoint, network, and OT domains. For larger operators, this usually involves a centralized SIEM that supports consistent access controls and regulatory retention requirements. For smaller fleets, similar results can be achieved through managed SIEM services, cloud-native logging platforms, or vendor-hosted fleet and maintenance systems that provide structured audit

trails and exportable data. The focus should be on ensuring that data can be accessed, preserved, and shared when needed, rather than on deploying enterprise-grade tools.

A security orchestration, automation, and response (SOAR) capability further enhances readiness by enabling repeatable workflows for enrichment, evidence preservation, containment actions, and stakeholder notification. While large operators may deploy full SOAR platforms, smaller owner/operators can implement lighter-weight playbooks embedded in maintenance, safety, or incident management systems to ensure that critical steps are consistently executed during an event.

6.4 Investigative Workflows: Evidence Collection, Preservation, and Analysis

Effective cybersecurity incident management depends not only on detection and containment, but on disciplined investigative workflows that preserve evidence, support attribution, enable recovery, and satisfy legal and regulatory obligations. In the motor freight sector, these workflows should bridge two fundamentally different response paradigms: traditional information technology (IT) incident response and operational transportation incident response involving vehicles, infrastructure, and human safety. Understanding how these paradigms differ, and where they should be integrated, is helpful for responding to cyber incidents that may span enterprise systems, connected vehicles, and real-world physical outcomes.

6.4.1 Responding to IT Breaches: NIST Incident Response Model

For enterprise IT environments, NIST provides a well-established, widely adopted framework for incident response, most notably articulated in NIST SP 800-61 (Computer Security Incident Handling Guide) and reinforced by broader guidance in NIST SP 800-53, SP 800-92, and CSF 2.0. NIST frames incident response as a lifecycle process rather than a linear checklist, emphasizing preparation, coordination, and learning as much as technical containment.

Under the NIST model, the organization that owns and operates the affected systems is the primary first responder. This is typically the motor carrier, broker, or logistics provider. The core phases include:

Preparation: Organizations are expected to establish incident response policies, defined roles and authorities, communication plans, logging and monitoring capabilities, evidence-handling procedures, and relationships with external partners (law enforcement, regulators, insurers, and service providers). Preparation includes ensuring that logs, backups, and forensic artifacts are generated and retained in a manner that supports investigation.

Detection and Analysis: Incidents are identified through alerts, anomalies, user reports, or third-party notifications. The emphasis is on rapidly determining whether an event is a true incident, scoping affected systems, identifying indicators of compromise, and assessing potential impact. Evidence collection during this phase focuses on volatile data (memory, active sessions), logs, authentication records, endpoint telemetry, and cloud or application audit trails.

Containment, Eradication, and Recovery: NIST stresses the need to balance containment actions with evidence preservation. Actions such as isolating systems, disabling accounts, or blocking network access should be coordinated to avoid destroying forensic artifacts. Recovery includes restoring systems from known-good backups, validating integrity, and monitoring for reinfection or persistence.

Post-Incident Activity: Lessons learned, root cause analysis, reporting, and control improvements are integral to incident response. Evidence gathered during the investigation supports internal governance decisions, external reporting obligations, insurance claims, and, when applicable, law-enforcement investigations.

Across all phases, NIST emphasizes chain of custody, time synchronization, documentation, and role clarity. Evidence is typically digital, centrally collected, and analyzed by security, IT, or third-party incident response teams operating under organizational authority.

6.4.2 Responding to Operational Vehicle Incidents: Crashes, Failures, and Worse

Operational incidents involving trucks and trailers follow a markedly different investigative model rooted in transportation safety, emergency response, and criminal or civil investigations rather than enterprise cybersecurity. In these cases, the motor carrier is not the first responder. Instead, responsibility initially lies with public safety authorities whose primary mission is to protect life and secure the scene.

In the extreme case of a serious crash or roadway fatality, investigative priorities unfold in a distinct order:

1. **Life Safety and Scene Control**

First responders (law enforcement, fire, emergency medical services) are responsible for saving lives, preventing secondary hazards, and securing the crash scene. Scene preservation is critical, but it is subordinate to immediate safety needs. Vehicles, trailers, cargo, and surrounding infrastructure may be moved or altered as necessary to protect responders and the public.

2. **Legal and Safety Investigation**

Once the scene is stabilized, authorities gather physical evidence to determine cause and responsibility. This includes vehicle positioning, damage patterns, skid marks, roadway conditions, driver statements, witness accounts, and compliance artifacts (licenses, hours-of-service records, inspection status). Evidence collection is governed by criminal procedure, traffic law, and safety investigation standards—not cybersecurity frameworks.

3. **Technical and Data Extraction**

Increasingly, digital evidence plays a role: engine control modules (ECMs), event data recorders (EDRs), telematics records, GPS history, ELD data, and sometimes video footage. Access to this data may require warrants, subpoenas, or formal requests, and timelines are often dictated by investigative authorities rather than the carrier.

4. **Carrier and Vendor Involvement**

Only after the initial response and scene control are complete does the motor carrier typically fully engage, supporting data requests, preserving internal records, and coordinating with insurers, legal counsel, and technology providers. At this stage, cybersecurity considerations (such as whether data integrity was compromised or systems behaved abnormally) may emerge, but they are secondary to the safety investigation unless clear malicious activity is suspected.

This operational response model assumes that physical evidence and human safety are paramount, and that authority resides with public institutions rather than private system owners. Evidence is distributed, often partially analog, and collected across multiple organizations with independent mandates.

6.4.3 Bridging the Two Models

The growing cyber-physical nature of motor freight systems challenges the historical separation between IT incident response and transportation accident investigation. A cyber event affecting telematics, diagnostics, or vehicle control systems may initially manifest as an operational anomaly or a crash, which places first responders, not security teams, at the front line of evidence handling. Conversely, an enterprise IT breach may later require coordination with regulators or law enforcement if it has safety or cross-border implications.

This divergence underscores the need for predefined integration points between NIST-style IT incident response workflows and transportation safety investigation processes. Without shared expectations around evidence preservation, authority, timing, and data access, critical information may be lost, misinterpreted, or siloed, which complicates both cybersecurity response and public safety outcomes.

7 Conclusion

7.1 Summary of Key Insights

This report demonstrates that cybersecurity risk in the motor freight sector is no longer confined to isolated IT failures or individual vehicle vulnerabilities. Instead, risk increasingly emerges from the interactions among connected vehicles, enterprise systems, telematics platforms, cloud services, and third-party dependencies, operating as a cyber-physical system of systems. In this environment, the most consequential threats arise not from single technical flaws, but from correlated weaknesses in trust relationships, visibility, governance, and incident response coordination. Existing cybersecurity vulnerabilities may manifest as localized anomalies in systems like diagnostics, maintenance, or backend systems. If those vulnerabilities are exploited and expanded, then they may scale into fleet-wide or ecosystem-wide disruptions.

A central insight is that cyber incidents in motor freight are likely to appear operationally before they are recognized as cybersecurity events. Maintenance technicians, dispatchers, and safety personnel may encounter repeated unexplained breakdowns, anomalous diagnostics, or inconsistent vehicle behavior long before a security team identifies a root cause. Similarly, crashes or safety incidents may initially be investigated under traditional transportation and legal frameworks, even when underlying digital systems are involved. Without structured escalation thresholds, shared situational awareness, and integrated investigative workflows, these early signals risk being misclassified as routine failures rather than indicators of coordinated malicious activity.

The report also highlights that large-scale incident response is constrained by systemic factors rather than purely technical ones. Fragmented ownership of vehicles, platforms, and infrastructure; limited end-to-end system knowledge; and uneven resource availability make coordinated detection, response, and recovery inherently difficult. Existing regulatory and policy frameworks in North America emphasize risk-based guidance and voluntary best practices, but they fall short of establishing consistent, scalable incident-response mechanisms. As a result, responsibility for managing systemic cyber risk remains diffuse, even as the potential consequences grow.

Finally, the analysis underscores the importance of cross-border coordination. Freight transportation is inherently binational, and cyber incidents affecting shared vendors, corridors, or services can quickly cross jurisdictional boundaries. Effective response, therefore, depends on aligned alerting, reporting, and information-sharing pathways between operators and government agencies in both the United States and Canada, supported by predefined thresholds and trusted relationships established before a crisis.

7.2 Long-Term Vision for Cyber Resilience in the Freight Sector

Looking ahead, cyber resilience in the motor freight sector should be treated as an operational property of the transportation system, rather than as a standalone cybersecurity function or a compliance obligation. Resilience at scale requires deliberate system-aware design: architectures that limit blast radius, governance models that clarify authority during crises, and data strategies that enable rapid correlation across IT, OT, and physical operations. It also requires acknowledgement that no single organization can manage large-scale cyber incidents alone; resilience should be built collectively across carriers, vendors, OEMs, regulators, and governments as a core capability.

A mature future state is one in which maintenance anomalies, safety incidents, and cybersecurity alerts are integrated into a common situational picture; where escalation decisions are informed by both severity and cascade potential; and where incident response workflows bridge enterprise security practices and transportation safety investigation norms. In such a system, repeated, unexplained operational failures are treated as strategic signals rather than isolated inconveniences, and recovery planning accounts for vendor concentration, resource saturation, and cross-border dependencies.

Achieving this vision will require sustained investment in workforce training, information sharing, forensic readiness, improved governance, and joint exercises that reflect realistic at-scale scenarios rather than isolated incidents. It would also require the continued evolution of policy and regulatory frameworks to reinforce industry-led resilience efforts, ensuring that guidance, incentives, and expectations align with the sector's systemic importance.

The absence of a catastrophic cyber incident in motor freight to date should be viewed as an opportunity rather than reassurance. The conditions that enable attacks at scale already exist. By adopting system-level approaches now, before those conditions are exploited, the motor freight sector can strengthen its ability to detect emerging threats, respond decisively under pressure, and recover in ways that preserve safety, economic stability, and public trust.

Acknowledgements

The authors acknowledge using different AI tools for research and editing support. Any AI-generated material was critically evaluated, validated against authoritative sources, and extended by the authors, who retain full responsibility for the content, interpretations, and conclusions presented.

The authors also appreciate the contributions of the authors and organizations cited in the references. Without the existing quality work in the literature, the findings and considerations presented herein would not be possible.

References

[1] N. Rahimi, B.-A. Schuelke-Leech, and M. Mirhassani, “A comprehensive review of security vulnerabilities in heavy-duty vehicles: Comparative insights and current research gaps,” *Comput. Secur.*, vol. 154, p. 104452, Jul. 2025, doi: 10.1016/j.cose.2025.104452.

[2] D. Klinedinst, “Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles,” Carnegie Mellon University, FMCSA-RRT-19-013, May 2020. Accessed: Dec. 22, 2024. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/49248

[3] J. Correnti, J. Lospinoso, M. Weigand, and K. Kramer, “Hidden Vulnerabilities: Operational Technology Cybersecurity Shortfalls,” in *Proceedings of the 2020 Ground Vehicle Systems Engineering and Technology Symposium (GVSETS)*, Novi, MI: NDIA, Aug. 2019. doi: https://doi.org/10.4271/2024-01-3863.

[4] J. Jepson, R. Chatterjee, and J. Daily, “Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms,” in *Symposium on Vehicles Security and Privacy (VehicleSec) 2024*, San Diego, CA: NDSS, Feb. 2024. doi: 10.14722/vehiclesec.2024.23047.

[5] E. Larson, W. Ford, S. Lerner, and J. Daily, “Vehicle Diagnostics Adapter Cybersecurity Concerns with Wireless Connectivity,” presented at the WCX SAE World Congress Experience, Detroit, Michigan, United States, Apr. 2023, pp. 2023-01–0034. doi: 10.4271/2023-01-0034.

[6] Verizon, “2025 Data Breach Investigations Report,” Verizon Business. Accessed: Mar. 09, 2026. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[7] Microsoft, “2025 Microsoft Digital Defense Report (MDDR).” Accessed: Mar. 09, 2026. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

[8] Office of the Privacy Commissioner of Canada, “The Personal Information Protection and Electronic Documents Act (PIPEDA).” Accessed: Mar. 12, 2026. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[9] National Assembly of Quebec, *An Act to modernize legislative provisions as regards the protection of personal information*, vol. Bill 64. 2021. Accessed: Mar. 12, 2026. [Online]. Available: https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/latest/sq-2021-c-25.html

[10] Parliament of Canada, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, vol. C–8. 2025. Accessed: Mar. 12, 2026. [Online]. Available: https://www.parl.ca/LegisInfo/en/bill/45-1/c-8

[11] “Improving the Nation’s Cybersecurity,” Federal Register. Accessed: Jan. 04, 2024. [Online]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[12] “Securing the Information and Communications Technology and Services Supply Chain,” Federal Register. Accessed: Mar. 02, 2025. [Online]. Available: https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[13] “Transportation Systems Sector | Cybersecurity and Infrastructure Security Agency CISA.” Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

[14] *UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2025/5]*. Accessed: Mar. 01, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500005

[15] *Regulation (EU) No 168/2013*, vol. L60/52. 2013. Accessed: Mar. 01, 2026. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2013/168/oj/eng

[16] *REGULATION (EU) 2018/858*, vol. Document 32018R0858. 2018. Accessed: Mar. 01, 2026. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/858/oj/eng

[17] *UN Regulation No. 156 - Software update and software update management system | UNECE*. Accessed: Mar. 01, 2026. [Online]. Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[18] *Regulation (EU) 2024/2847*. 2024. Accessed: Mar. 01, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

[19] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-12r1, Jun. 2017. doi: 10.6028/NIST.SP.800-12r1.

[20] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[21] Communications Security Establishment Canada, "National cyber threat assessment 2025–2026", Accessed: Mar. 09, 2026. [Online]. Available: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

[22] "Report a cyber incident," Canadian Centre for Cyber Security. Accessed: Mar. 01, 2026. [Online]. Available: https://www.cyber.gc.ca/en/incident-management

[23] Communications Security Establishment Canada, "Alerts and advisories," Canadian Centre for Cyber Security. Accessed: Mar. 01, 2026. [Online]. Available: https://www.cyber.gc.ca/en/alerts-advisories

[24] "Canada's National Cyber Security Strategy: Securing Canada's Digital Future." Accessed: Mar. 01, 2026. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

[25] "Federal Cyber Incident Response Plan." Accessed: Mar. 01, 2026. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fdrl-cbr-ncdnt-rspns-pln-2023/index-en.aspx

[26] "Report cybercrime and fraud," Royal Canadian Mounted Police. Accessed: Mar. 01, 2026. [Online]. Available: https://rcmp.ca/en/federal-policing/cybercrime/national-cybercrime-coordination-centre/report-cybercrime-and-fraud

[27] B. Dupont and C. Whelan, "Enhancing relationships between criminology and cybersecurity," *J. Criminol.*, vol. 54, no. 1, pp. 76–92, Mar. 2021, doi: 10.1177/00048658211003925.

[28] R. C. M. P. Government of Canada, "Report fraud and cybercrime." Accessed: Mar. 01, 2026. [Online]. Available: https://antifraudcentre.ca/report-signalez-eng.htm

[29] Transport Canada, "Cybersecurity Incidents." Accessed: Mar. 01, 2026. [Online]. Available: https://tc.canada.ca/en/binder/66-cybersecurity-incidents-transport-canada

[30] Transport Canada, "Vehicle cyber security," 17792661. Accessed: Mar. 01, 2026. [Online]. Available: https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/vehicle-cyber-security

[31] Transport Canada, "Canada's Vehicle Cyber Security Assessment Tool (VCAT)," 17792668. Accessed: Mar. 01, 2026. [Online]. Available: https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/canada-s-vehicle-cyber-security-assessment-tool-vcat

[32] Minister of Transport, *Transport Canada's Vehicle Cyber Security Strategy*. Transport Canada, 2021. Accessed: Mar. 01, 2025. [Online]. Available: https://tc.canada.ca/sites/default/files/2021-08/transport-canada-vehicle-cyber-security-strategy.PDF

[33] "Known Exploited Vulnerabilities Catalog." Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[34] "Cybersecurity Alerts & Advisories." Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories

[35] "Joint Cyber Defense Collaborative." Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

[36] "Automated Indicator Sharing (AIS)." Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais

[37] FBI, "Internet Crime Complaint Center (IC3)." Accessed: Mar. 01, 2026. [Online]. Available: https://www.ic3.gov/

[38] Federal Bureau of Investigation, "Private Industry Notification." Accessed: Mar. 01, 2026. [Online]. Available: https://www.ic3.gov/CSA/2023/230928.pdf

[39] Federal Bureau of Investigation, "InfraGard Fact Sheet," Accessed: Mar. 01, 2026. [Online]. Available: https://www.fbi.gov/file-repository/infragard_factsheet.pdf

[40] TSA, "Surface Transportation Cybersecurity Toolkit," U.S. Department of Homeland Security Transportation Security Administration. Accessed: Mar. 01, 2026. [Online]. Available: https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit

[41] Transportation Security Administration, "TSA announces proposed rule that would require the establishment of pipeline and railroad cyber risk management programs," U.S. Department of Homeland Security Transportation Security Administration. Accessed: Mar. 01, 2026. [Online]. Available: https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and

[42] "Surface Transportation: TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed | U.S. GAO." Accessed: Mar. 01, 2026. [Online]. Available: https://www.gao.gov/products/gao-25-107947

[43] NHTSA, "Cybersecurity Best Practices for the Safety of Modern Vehicles, Updated 2022," Sep. 2022. [Online]. Available: https://www.nhtsa.gov/document/cybersecurity-best-practices-safety-modern-vehicles-2022

[44] "Cyber Storm: Securing Cyber Space." Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/resources-tools/programs/cyber-storm

[45] R. A. Jones and B. Horowitz, "A System-Aware Cyber Security architecture," *Syst. Eng.*, vol. 15, no. 2, pp. 225–240, 2012, doi: 10.1002/sys.21206.

[46] M. Jamshidi, "System of systems engineering - New challenges for the 21st century," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 23, no. 5, pp. 4–19, May 2008, doi: 10.1109/MAES.2008.4523909.

[47] R. Ross, M. Winstead, and M. McEvilley, "Engineering Trustworthy Secure Systems," National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 1 Rev. 1, Nov. 2022. doi: 10.6028/NIST.SP.800-160v1r1.

[48] *Great Lakes Water Quality Agreement*. Accessed: Mar. 01, 2026. [Online]. Available: https://binational.net/agreement/full-text-the-2012-great-lakes-water-quality-agreement/

[49] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident response recommendations and considerations for cybersecurity risk management : a CSF 2.0 community profile," National

Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-61r3, Apr. 2025. doi: 10.6028/NIST.SP.800-61r3.

[50] "ISO/IEC 27035-1:2023," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/78973.html

[51] "ISO/IEC 27001:2022," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/27001

[52] "ISO/IEC 27002:2022," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/75652.html

[53] "ISO 22301:2019," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/75106.html

[54] "ISO/IEC 27037:2012," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/44381.html

[55] "ISO/IEC 27043:2015," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/44407.html

[56] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology, NIST Special Publication (SP) 800-86, Sep. 2006. doi: 10.6028/NIST.SP.800-86.

[57] "ISO 28000:2022," ISO. Accessed: Mar. 01, 2026. [Online]. Available: https://www.iso.org/standard/79612.html

[58] "Trucking Security Requirements (TSR) Standard." Accessed: Mar. 01, 2026. [Online]. Available: https://www.tapaonline.org/trucking-security-requirements-tsr-

[59] "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking; Town Hall Meetings," Federal Register. Accessed: Mar. 01, 2026. [Online]. Available: https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings

[60] "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Federal Register. Accessed: Mar. 01, 2026. [Online]. Available: https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

[61] "N.Y. Comp. Codes R. & Regs. Tit. 23 § 500.16 - Incident Response Plan," LII / Legal Information Institute. Accessed: Mar. 01, 2026. [Online]. Available: https://www.law.cornell.edu/regulations/new-york/23-NYCRR-500.16

[62] "Responding to a Cardholder Data Breach." Accessed: Mar. 01, 2026. [Online]. Available: https://listings.pcisecuritystandards.org/documents/Responding_to_a_Cardholder_Data_Breach.pdf

[63] O. of the P. C. of Canada, "What you need to know about mandatory reporting of breaches of security safeguards." Accessed: Mar. 01, 2026. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/

[64] *Directive (EU) 2022/2555*, vol. L 333. 2022. Accessed: Mar. 01, 2026. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj

[65] *Regulation (EU) 2016/679*, vol. L 119. 2016. Accessed: Mar. 01, 2026. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj

[66] "COBIT® | Control Objectives for Information Technologies®," ISACA. Accessed: Mar. 01, 2026. [Online]. Available: https://www.isaca.org/resources/cobit

[67] “Industry News 2019 COBIT Design Factors,” ISACA. Accessed: Mar. 01, 2026. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2019/cobit-design-factors

[68] CISA, “Cross-Sector Cybersecurity Performance Goals, Version 2.0,” Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/sites/default/files/2025-12/CPG_Report_2.0_508c.pdf

[69] “Industry News 2020 Effective Capability and Maturity Assessment Using COBIT 2019,” ISACA. Accessed: Mar. 07, 2026. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019

[70] “Cybersecurity Framework FAQs Framework Components,” *NIST*, Sep. 2015, Accessed: Mar. 07, 2026. [Online]. Available: https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components

[71] “CIS Critical Security Controls Implementation Groups,” CIS. Accessed: Mar. 07, 2026. [Online]. Available: https://www.cisecurity.org/controls/implementation-groups/

[72] “CIO - About CMMC.” Accessed: Mar. 07, 2026. [Online]. Available: https://dodcio.defense.gov/CMMC/About/

[73] NMFTA, “Cybersecurity Best Practices Guidebook: Owner Operator and Small Fleet,” National Motor Freight Traffic Association, Inc., 1.1, Jan. 2025. Accessed: Jan. 29, 2026. [Online]. Available: https://nmfta.org/wp-content/media/2025/01/031025-SmallFleet-CyberGuideBook.pdf

[74] J. Daily and M. (Trae) Span, “A Model for Cybersecurity Education through Challenge Events,” *INCOSE Int. Symp.*, vol. 34, no. 1, pp. 944–957, 2024, doi: 10.1002/iis2.13187.

[75] National Highway Traffic Safety Administration, “Cybersecurity best practices for modern vehicles,” DOT, Washington, D.C., DOT HS 812 333, Oct. 2016. Accessed: Jan. 29, 2026. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[76] AutoISAC, “Cybersecurity Awareness and Training Best Practice Guide,” Automotive ISAC, https://automotiveisac.com/bpg2. Accessed: Jan. 29, 2026. [Online]. Available: https://static1.squarespace.com/static/618a9a805a5be466f28052a2/t/67b77e747905a721309de2c1/1740078710792/2024-12-18-BPG2-Cybersecurity+Awareness+and+Training_4Web.pdf

[77] Federal Emergency Management Agency (FEMA), “Homeland Security Exercise and Evaluation Program,” Jan. 2020. Accessed: Mar. 08, 2026. [Online]. Available: https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

[78] “Public Safety Canada’s 2024 to 2025 Departmental Plan.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2024-25/index-en.aspx

[79] “Cyber-Physical Capstone Exercise After-Action Report.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cpstn-xrcs-ftr-ctn-rprt-2024/index-en.aspx

[80] “What is STIX/TAXII?” Accessed: Mar. 06, 2026. [Online]. Available: https://www.cloudflare.com/learning/security/what-is-stix-and-taxii/

[81] M. Roddie and T. Williams, “SANS 2023 Incident Response,” SANS, 2023. Accessed: Mar. 08, 2026. [Online]. Available: https://www.devo.com/wp-content/uploads/2023/10/Survey_IR-2023_Devo.pdf

[82] S. D. Quinn *et al.*, “Integrating cybersecurity and enterprise risk management (ERM),” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8286r1, Dec. 2025. doi: 10.6028/NIST.IR.8286r1.

[83] FAIR Institute, “Factor Analysis of Information Risk (FAIR) Standard v3.0.” Jan. 2025. Accessed: Mar. 08, 2026. [Online]. Available: https://www.fairinstitute.org/hubfs/Standards%20Artifacts/Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20Standard%20v3.0%20%28January%202025%29.pdf

[84] Communications Security Establishment Canada, “Cyber incident reporting guidelines: Key information sharing requirements – ITSM.00.140,” Canadian Centre for Cyber Security. Accessed: Mar. 08, 2026. [Online]. Available: https://www.cyber.gc.ca/en/guidance/cyber-incident-reporting-guidelines-key-information-sharing-requirements-itsm00140

[85] IBM, “Cost of a Data Breach Report 2024.” 2024. Accessed: Mar. 06, 2026. [Online]. Available: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

[86] R. Ross and V. Pillitteri, “Protecting controlled unclassified information in nonfederal systems and organizations,” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-171r3, May 2024. doi: 10.6028/NIST.SP.800-171r3.

[87] “ISO/SAE 21434: Road Vehicles - Cybersecurity Engineering - SAE International.” Accessed: Dec. 08, 2021. [Online]. Available: https://www.sae.org/standards/content/iso/sae21434/

[88] P. Koepke, “Cybersecurity Information Sharing Incentives and Barriers,” Massachusetts Institute of Technology, Cambridge, MA, Jun. 2017. Accessed: Mar. 08, 2026. [Online]. Available: https://web.mit.edu/smadnick/www/wp/2017-13.pdf

[89] “Automotive ISAC,” Automotive ISAC. Accessed: Mar. 08, 2026. [Online]. Available: https://automotiveisac.com

[90] “Incident Reporting System.” Accessed: Mar. 08, 2026. [Online]. Available: https://myservices.cisa.gov/irf

[91] “Fleet CyWatch,” American Trucking Association. Accessed: Mar. 08, 2026. [Online]. Available: https://trucking.org/fleet-cywatch

[92] Communications Security Establishment Canada, “Contact the Cyber Centre,” Canadian Centre for Cyber Security. Accessed: Mar. 08, 2026. [Online]. Available: https://www.cyber.gc.ca/en/contact-cyber-centre

[93] Transport Canada, “National Incident Response and Management.” Accessed: Mar. 08, 2026. [Online]. Available: https://tc.canada.ca/en/corporate-services/transparency/briefing-documents-transport-canada/2025-2/minister/national-incident-response-management

[94] “Canadian Cyber Threat Exchange (CCTX),” Canadian Cyber Threat Exchange. Accessed: Mar. 08, 2026. [Online]. Available: https://cctx.ca/

[95] J. MacColl *et al.*, “Cyber Insurance and the Ransomware Challenge.” Accessed: Jan. 29, 2026. [Online]. Available: https://www.rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-ransomware-challenge

[96] M. Iwasaki, “Banning ransomware payments: unintended effects on cybersecurity investment and incident reporting,” *Int. Cybersecurity Law Rev.*, vol. 6, no. 1, pp. 17–27, Mar. 2025, doi: 10.1365/s43439-025-00137-5.

[97] S. Busetti and F. M. Scanni, “Evaluating incident reporting in cybersecurity. From threat detection to policy learning,” *Gov. Inf. Q.*, vol. 42, no. 1, p. 102000, Mar. 2025, doi: 10.1016/j.giq.2024.102000.

[98] K. Dempsey *et al.*, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-137, Sep. 2011. doi: 10.6028/NIST.SP.800-137.

[99] M. Cinque, D. Cotroneo, and A. Pecchia, “Challenges and Directions in Security Information and Event Management (SIEM),” in *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Oct. 2018, pp. 95–99. doi: 10.1109/ISSREW.2018.00-24.

[100] S. Bhatt, P. K. Manadhata, and L. Zomlot, “The Operational Role of Security Information and Event Management Systems,” *IEEE Secur. Priv.*, vol. 12, no. 5, pp. 35–41, Sep. 2014, doi: 10.1109/MSP.2014.103.

[101] B. Kovacevic and N. DiCola, *Security Orchestration, Automation, and Response for Security Analysts: Learn the secrets of SOAR to improve MTTA and MTTR and strengthen your organization’s security posture*. Packt Publishing Ltd, 2023.

[102] “Traffic Light Protocol (TLP),” FIRST — Forum of Incident Response and Security Teams. Accessed: Mar. 01, 2026. [Online]. Available: https://www.first.org/tlp/

[103] “STIX Version 2.1,” OASIS Open. Accessed: Mar. 01, 2026. [Online]. Available: https://www.oasis-open.org/standard/stix-version-2-1/

[104] “Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) — FBI.” Accessed: Mar. 02, 2026. [Online]. Available: https://www.fbi.gov/news/press-releases/joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-and-the-office-of-the-director-of-national-intelligence-odni

[105] “PPD-41 on United States Cyber Incident Coordination.” Accessed: Mar. 08, 2026. [Online]. Available: https://irp.fas.org/offdocs/ppd/ppd-41.html

[106] “National Cyber Incident Response Plan (NCIRP),” Department of Homeland Security, Dec. 2016. Accessed: Mar. 01, 2026. [Online]. Available: https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[107] “Joint Cyber Defense Collaborative.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

[108] A. J. Vicens and A. J. Vicens, “Chinese-linked hackers use back door for potential ‘sabotage,’ US and Canada say,” *Reuters*, Dec. 04, 2025. Accessed: Mar. 08, 2026. [Online]. Available: https://www.reuters.com/world/china/chinese-linked-hackers-use-back-door-potential-sabotage-us-canada-say-2025-12-04/

[109] E. Salfati and M. Pease, “Digital Forensics and Incident Response (DFIR) framework for Operational Technology (OT),” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8428, Jun. 2022. doi: 10.6028/NIST.IR.8428.

[110] “The Privacy Act in brief.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/

[111] “Modernizing Canada’s Privacy Act – Learn more about the Privacy Act.” Accessed: Mar. 08, 2026. [Online]. Available: https://justice.canada.ca/eng/csj-sjc/pa-lprp/res.html

[112] “Management of Security Incidents.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/management-security-incidents.html

[113] “CISA National Cyber Incident Scoring System (NCISS).” Accessed: Mar. 08, 2026. [Online]. Available: https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

[114] “FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination,” whitehouse.gov. Accessed: Mar. 08, 2026. [Online]. Available:

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1

[115] “Federal Incident Notification Guidelines.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.cisa.gov/federal-incident-notification-guidelines

[116] “National Cybercrime Coordination Centre,” Royal Canadian Mounted Police. Accessed: Mar. 08, 2026. [Online]. Available: https://rcmp.ca/en/federal-policing/cybercrime/national-cybercrime-coordination-centre

[117] “What you need to know about mandatory reporting of breaches of security safeguards.” Accessed: Mar. 09, 2026. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/

[118] CISA, “Reporting a Cyber Incident.” Accessed: Mar. 09, 2026. [Online]. Available: https://www.cisa.gov/reporting-cyber-incident

[119] CISA, “Canada-U.S. Action Plan for Critical Infrastructure.” Accessed: Mar. 09, 2026. [Online]. Available: https://www.cisa.gov/resources-tools/resources/canada-us-action-plan-critical-infrastructure

[120] “Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security.” Accessed: Mar. 08, 2026. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx