NMFTA CYBERSECURITY BEST PRACTICES GUIDEBOOK

Mid-Sized Fleet

Version 1.0

As with any journey, your path to a hardened cybersecurity posture must start where you are today. No matter where that is, there are steps you can take now to protect yourself and the operation that you have built from cyberthreats.

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

[This Page Is Left Intentionally Blank]

Table of Contents

Introduction 6

Intended Audience 6

Assumptions 7

Document Structure 8

Prerequisites: Mid-Sized Fleet Controls - Tier One 9

MSF.01.1 - Keep Software and Operating Systems Updated 9

MSF.01.2 – Back Up Important Files 10

MSF.01.3 – Use Strong, Unique Passwords. 11

MSF.01.4 – Require Passwords on All Devices 12

MSF.01.5 – Require Multi-Factor Authentication 13

MSF.01.6 – Basic Cybersecurity User Awareness Training Program 14

MSF.01.7 – Deploy Endpoint Detection and Response Software 15

MSF.01.8 – Documented Hardware and Software Inventory Management 16

MSF.01.9 – Secure Wireless Networks 17

MSF.01.10 – Implement a Least Privilege Account Access Policy 18

Initial: Mid-Sized Fleet Controls - Tier Two 19

MSF.02.1 – Documented Incident Response Plan 20

MSF.02.2 – Document Contractual Requirements 21

MSF.02.3 – Inventory and Classify All Business Data 22

MSF.02.4 – Document Service Inventory 23

MSF.02.5 – Software Version Controls 24

MSF.02.6 – Designate Cybersecurity Roles and Responsibilities 25

MSF.02.7 – Replace MFA with Windows Hello or Similar 26

MSF.02.8 – Prevent Remote Administrative Access to Systems 27

MSF.02.9 – Restrict Admins to Privileged Access Workstations. 28

MSF.02.10 – Proactive End-of-Life Management Policies 29

MSF.02.11 – Configure Email Security 30

MSF.02.12 – Layered Network Access Controls 31

MSF.02.13 – Internal Network Segmentation 32

MSF.02.14 – Operational Technology Segregated from Information Technology 33

MSF.02.15 – Encrypt All Devices 34

MSF.02.16 – Enable Detailed Security Logging 35

MSF.02.17 – Access to OT and Vehicle Systems Based on Role and Attribute-Based Access Control 36

MSF.02.18 – Preventative Maintenance Cycles Include Checks for Tampering with Onboard Electronics on Power Units and Trailers. 37

MSF.02.19 – Special Purpose Devices are Isolated from Enterprise Networks 38

MSF.02.19.A - Maintenance Facilities: Diagnostic Laptops 38

MSF.02.19.B - Warehouse and Dock: Handheld Scanners and Portable Devices 38

MSF.02.20 – Diagnostics Laptops are Physically Controlled to Prevent Unauthorized Access or Tampering. 39

Intermediate: Mid-Sized Fleet Controls – Tier Three 40
MSF.03.1 – Bring Your Own Device Policies and Restrictions are Actively Managed 41
MSF.03.2 – Security Incident and Event Management Solution 42
MSF.03.3 – Secure Baseline Configurations or Device Images 43
MSF.03.4 – Port Security Enabled on All Network Access Ports 44
MSF.03.5 – Policy and Technical Controls to Enforce Connection Medium (Wi-Fi/Wired) 45
MSF.03.6 – Deploy Application Security Software 46
MSF.03.7 – Fully Implement Zero-Trust Architecture 47
MSF.03.8 – Network Intrusion Detection System 48
MSF.03.9 – Network Intrusion Prevention System 49
MSF.03.10 – Secure Communication Between Telematics Systems and Telematics System Providers 50
Advanced: Mid-Sized Fleet Controls – Tier Four 51
MSF.04.1 – Legal and Regulatory Compliance is Actively Managed 51
MSF.04.2 – Regular Assessments and Exercises 52
MSF.04.3 – Mobile Device Management Solution 53
MSF.04.4 – Prioritized Risk Register 54
MSF.04.5 – Documented Vendor Management Program 55
MSF.04.6 – Formalized, Documented Cybersecurity Policies 56
MSF.04.7 – Documented Change Control Process 57
MSF.04.8 – Documented Access Control Lists 58
MSF.04.9 – Formalized, Documented Disaster Recovery Plan 59
MSF.04.10 – Formalized, Documented Business Continuity Plan 60
Goal – Security-Minded and Empowered Culture is Universally Accepted 61
Additional Resources 63
Acronyms 65
Appendix A 67

Introduction

This guidebook contains an actionable list of cybersecurity control best practices, divided into four distinct maturity levels. These controls are based on a selection of industry standard cybersecurity frameworks, such as The National Institute for Standards & Technology's Cybersecurity Framework (NIST CSF 2.0) and the Center for Internet Security's 18 Critical Security Controls (CIS 18 v8.1) that have been tailored to the specific needs of the trucking industry as well as controls specifically designed for the requirements of trucking operations and their mobile assets.

While these controls represent the best-practice recommendations of the NMFTA cybersecurity team and provide a strong starting point for organizations to pursue their path to cybersecurity maturity, they are not designed to be an exhaustive list of all cybersecurity controls available to the trucking industry, nor do they provide any guarantee of complete or impenetrable defense from cyberattacks. For example, many systems and services within the modern enterprise come with several levels of optional security "out of the box" (e.g., SSL, TLS, and PKI security for transport layer protocols). The optimal configurations for these types of service options are not explicitly stated in this guide. The general rule should be to configure the most secure option that is practical in an organization's business environment. Cybersecurity programs and their individual requirements vary greatly from business to business, and depend largely on the specific operating infrastructure, business processes, staffing levels, and education, as well as the overall business risk tolerance of the business. Where applicable, this document contains references to additional resources and control frameworks that may be used to augment this best-practice guidebook, and to develop additional layers of controls for any business

This content and additional information can be found on the NMFTA cybersecurity website: www.nmfta.org/cybersecurity.

Intended Audience

This document is intended for mid-sized fleets (approx. 50–3,000 assets). Complex operations with 50 or fewer assets may find this guidance applies to their operation as well. However, most small fleets (under 50 assets) will find that the related *NMFTA Cybersecurity Best Practices Guidebook: Owner Operator and Small Fleet* is a better fit for their needs. Visit https://nmfta.org/whitepapers to download a copy.

Larger fleets (more than 3,000 assets) or organizations with established cybersecurity programs will find this document a valuable refresher on essential security controls. For more in-depth guidance, they may refer to the upcoming *NMFTA Cybersecurity Best Practices Guidebook: Large Fleet* document for additional insights and recommendations.

Assumptions

Several assumptions were made in the creation of the included list of controls regarding this guidebook's intended audience. These assumptions are as follows:

Assumption 1: Small In-House Team or Outsourced IT and Cybersecurity

This guidance assumes that a mid-sized fleet owner either assigns information technology (IT) and/or cybersecurity tasks to a specific employee who either manages a small team or contracts these responsibilities out to a third-party managed service provider (MSP) or managed security services provider (MSSP).

Assumption 2: Moderate Operational and Technical Complexity

This guidance assumes that a mid-sized fleet will have a moderate to significant amount of network complexity in their operation, and will likely have a significant number of computers, tablets, mobile phones, network hardware, cloud assets, vehicles, telematics units, and Software as a Service (SaaS) platforms to consider when building out their cybersecurity program.

Assumption 3: Included Maintenance and/or Warehousing Facilities

This guidance assumes that the organization includes maintenance or warehousing facilities and staff. Both business units introduce distinct security challenges that must be carefully assessed when developing a cybersecurity program.

Document Structure

This document is divided into four sections, each representing a distinct cybersecurity maturity level as a mid-sized fleet progresses in developing their cybersecurity program. The top recommended controls for each maturity level are included in each section. For every control listed, there will be an identification number, followed by a brief description, and the intended purpose or benefit of each respective control. Controls will be clearly identified as to their applicability to back office, maintenance facilities, and physical assets (power units and trailers). Once the control is defined, several example implementations will be given. These do not represent, nor are they intended to include all possible implementations for the given control, but are included with the intent of providing insight into the many ways in which the control *could* be implemented if applicable in the specific operating environment of the business following this best practice guide. The last item included in each control section will be a cross-reference to any related NIST CSF 2.0 controls or CIS 18 v8.1 safeguards for further information.

Prerequisites: Mid-Sized Fleet Controls - Tier One

The cybersecurity control requirements to reasonably protect a mid-sized fleet from common threats are substantially greater than those required to protect individuals or smaller fleets due to the complexity and the scale of these businesses. It is vital to start with a solid foundational level of cybersecurity throughout the organization on which to build out a robust cybersecurity program with comprehensive protection for all aspects of the business. While many of the controls in this section overlap with the guidance found at multiple maturity levels for smaller operations, the expectation for mid-sized fleets is that all controls in this first section are considered prerequisites for the rest of their cybersecurity program.[1]

MSF.01.1 - Keep Software and Operating Systems Updated

Keeping your operating systems and software updated is crucial for safety, reliability, and smooth functionality. Updates protect against potential security risks by fixing known issues that threat actors might try to exploit. They also improve performance, helping systems run better and avoid crashes, while often adding new features to keep your tools current. By staying up-to-date, you reduce the chances of unexpected issues, stay in line with industry standards, and avoid potential risks. In short, you can think of software and operating system updates like a preventative maintenance program for your computer assets.

Implementation Examples

Example 1: Turn on auto-updates for software and operating systems whenever it is an option.

Example 2: Apply all recommended patches released by software vendors, especially those related to new vulnerabilities and those designed to enhance security.

Example 3: Limit what software gets installed on your work computers and mobile devices to work-related software. Uninstall and remove unauthorized software and services.

Example 4: Decide on, document, and follow through with an action plan to address software and operating systems that are reaching the end of manufacturer's support.

Example 5: Replace end-of-life software and service versions with supported, maintained versions.

Mappings to External Control Standards

- NIST PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.
- CIS 18 v8.1 Safeguard 2.2: Ensure Authorized Software is Currently Supported.

1 This level of cybersecurity maturity maps to NIST maturity level: Partial

MSF.01.2 – Back Up Important Files

Backing up important files is crucial to protect against data loss, and the "3-2-1" backup rule makes it easy to remember a smart approach: Keep **3 copies** of your data, store **2 copies on different types of media** (like an external drive and a cloud service), and keep **1 copy offsite** for added security. This strategy reduces the potential impact of hardware failure, accidental deletion, and cyberthreats. Backup schedules and formats must be developed with an awareness of maximum tolerable outage (MTO) ranges, recovery time objectives (RTO) and recovery point objectives (RPO) to ensure that the maximum downtime and maximum data loss expected in a worst-case event is within business risk tolerances. While backing up the files is a core component of a successful backup solution, testing those backups is an equally important and often overlooked requirement. It is imperative that all backups are regularly tested for validity and the restoration process is tested and rehearsed so that required data can be reliably restored in the event of an incident.

Implementation Examples

Example 1: Ensure that you backup all your important data regularly. Make sure that you understand your tolerance for data loss and set your backup schedule accordingly.

Example 2: Configure automated cloud backup solutions.

Example 3: Store an offline copy of your daily backup in a secure, offsite location such as a safety deposit box or cloud storage vault.

Example 4: Regularly test that you can restore your files from all backup solutions.

Mappings to External Control Standards

- NIST PR.DS-11: Backups of data are created, protected, maintained, and tested.
- CIS 18 v8.1 Safeguard 11.2: Perform Automated Backups.
- CIS 18 v8.1 Safeguard 11.3: Protect Recovery Data.
- CIS 18 v8.1 Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data.
- CIS 18 v8.1 Safeguard 11.5: Test Data Recovery.

MSF.01.3 – Use Strong, Unique Passwords

Using strong, unique passwords and changing all default credentials is essential for securing your accounts and devices. Aim to create passwords that are at least 12 characters long and include a mix of letters, numbers and symbols—this complexity makes them much harder for threat actors to guess or crack using brute-force attacks. Default passwords, often set by manufacturers, are well-known and easily exploitable, so replacing them with secure, personalized passwords is critical. Longer and more complex passwords (particularly when used in combination with multi-factor authentication (MFA)[2] add an extra layer of security, significantly reducing the risk of a successful account compromise.

Implementation Examples

Example 1: Change default credentials on all devices and hardware before using them.

Example 2: Do not use names, important dates, favorite teams, brands, or any other personal information in your passwords. This type of information is commonly used by threat actors to seed brute-force attacks.

Example 3: Use a password management app to automatically generate and securely store all passwords.

Example 4: Do not share passwords between employees. Use a unique password for every user.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- CIS 18 v8.1 Safeguard 5.2: Use Unique Passwords.

2 See Also IO.01.5 Require Multifactor Authentication (MFA)

MSF.01.4 – Require Passwords on All Devices

Requiring a password on all devices—like computers, tablets, mobile phones, and network hardware is a simple, effective step toward keeping your data and accounts secure. Password protection acts as the first line of defense, preventing unauthorized access if a device is lost, stolen, or left unattended. Passwords help protect sensitive information and prevent unauthorized changes to security settings. This safeguard reduces the risk of breaches, identity theft, unauthorized access to personal or work networks, helping to ensure that only trusted users can access your device's data and settings.

Implementation Examples

Example 1: Require pin (minimum) or biometric (preferred) authentication for mobile devices.

Example 2: Enforce minimum complexity and/or length requirements for pins and passwords.

Example 3: Disable guest access and require password-protected accounts on all computers.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- CIS 18 v8.1 Safeguard 5.2: Use Unique Passwords.

MSF.01.5 – Require Multi-Factor Authentication

Implementing MFA is a highly effective way to add an extra layer of security to your accounts and devices. MFA requires users to verify their identity in two or more ways, typically combining something you know (like a password) with something you have (like a phone or security token) or something you are (biometric markers like a fingerprint or facial scan). This makes it much harder for attackers to gain access, even if they compromise your username and password. By enabling MFA, you significantly reduce the risk of unauthorized access, helping to protect your company data and accounts from cyberthreats.

Implementation Examples

Example 1: Set up an authenticator app for use as an MFA token for online accounts.

Example 2: Configure SMS or text alerts for account access verification. While not the most secure MFA method available, even SMS codes transmitted to your mobile number to verify access provide a significant increase in the difficulty of compromising an account.

Example 3: Configure facial ID or fingerprint authentication for access to mobile devices.

Example 4: Require MFA for all administrative accounts.

Mappings to External Control Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- CIS 18 v8.1 Safeguard 6.3: Require MFA for Externally Exposed Applications.
- CIS 18 v8.1 Safeguard 6.4: Require MFA for Remote Network Access.
- CIS 18 v8.1 Safeguard 6.5 Require MFA for Administrative Access.

MSF.01.6 – Basic Cybersecurity User Awareness Training Program

Implementing a basic cybersecurity user awareness training program is an affordable and effective way to empower users to recognize and avoid common security threats. This type of program educates employees on key topics like phishing scams, safe internet usage practices, secure password management, and how to identify suspicious emails or attachments. It can also cover policies on handling sensitive data and guidelines for reporting potential security incidents. By providing this training, businesses can help to ensure that every employee understands the role that they play in protecting sensitive information. This will reduce the likelihood of human errors that could lead to breaches or successful attacks.

Implementation Examples

Example 1: Provide mandatory basic cybersecurity awareness training to all employees and any other third parties that interact with internal company systems or assets.

Example 2: Provide training to personnel to help them recognize phishing and other social engineering attempts. Include information on how to properly report suspicious activity and on basic cyber hygiene requirements.

Example 3: Ensure that all employees and contractors understand the immediate and potential consequences of cybersecurity policy violations to both the individual and the company.

Example 4: Periodically test employees on their cybersecurity awareness and compliance with required cybersecurity policies.

Mappings to External Control Standards

- NIST PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.
- CIS 18 v8.1 Safeguard 14.1: Establish and Maintain a Security Awareness Program.

MSF.01.7 – Deploy Endpoint Detection and Response Software

Deploying Endpoint Detection and Response (EDR) software is a crucial step in enhancing cybersecurity by providing continuous monitoring and real-time analysis of potential threats across all devices in a network. EDR software helps detect, investigate, and respond to suspicious activities on computers, mobile devices, and servers. It offers advanced features like threat hunting, automated responses to block malicious actions, and detailed reporting to help security teams understand and mitigate risks. By implementing EDR, organizations can quickly identify and address potential threats before they lead to data breaches, strengthening overall security and improving incident response times.

Implementation Examples

Example 1: Monitor failed authentication attempts. These can be a sign of unauthorized credential use or a brute-force attack.

Example 2: Monitor endpoints for configuration changes that deviate from security baselines.

Example 3: Monitor both hardware and software for signs of tampering or unauthorized access.

Example 4: Proactively monitor endpoints for general cybersecurity health (e.g. missing patches, malware, unauthorized installations) and automate responses to prevent incidents and breaches.

Mappings to External Control Standards

- NIST DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 10.1: Deploy and Maintain Anti-Malware Software.
- CIS 18 v8.1 Safeguard 10.5: Enable Anti-Exploitation Features.
- CIS 18 v8.1 Safeguard 10.6: Centrally Manage Anti-Malware Software.

MSF.01.8 – Documented Hardware and Software Inventory Management

Maintaining a documented hardware and software inventory is vital for managing and securing your business's technology assets. By keeping a detailed record of all devices, applications, and systems in use, you gain better visibility over your network, making it easier to identify outdated or unauthorized items. A well-organized inventory helps track software licenses, monitor hardware for updates, and quickly identify devices that may need security patches. This practice also supports efficient troubleshooting and compliance with industry standards, ensuring that your technology environment is secure, up-to-date, and aligned with cybersecurity best practices.

Implementation Examples

Example 1: Create a centralized inventory document. Use a spreadsheet or inventory management tool to track all hardware devices and software applications in use, noting details like serial numbers, model, and license information.

Example 2: Assign responsibility for inventory updates. Designate someone to regularly updated the inventory list, adding new devices and removing retired or decommissioned items.3

Example 3: Perform routine inventory audits. Schedule periodic checks to verify that the inventory matches what's currently in use and to identify any unauthorized or unapproved devices or software.

Example 4: Monitor software license expirations. Track software license renewal dates in your inventory to prevent lapses that could lead to compliance issues or security vulnerabilities.

Mappings to External Control Standards

- NIST ID.AM-01: Inventories of hardware managed by the organization are maintained.
- NIST ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.
- CIS 18 v8.1 Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory.
- CIS 18 v8.2 Safeguard 2.1 Establish and Maintain a Software Inventory.

3 See also MSF.02.6 – Designate Cybersecurity Roles and Responsibilities

MSF.01.9 – Secure Wireless Networks

Encrypting all wireless networks with Wi-Fi Protected Access 2 (WPA2) or greater is crucial for protecting the confidentiality and integrity of data transmitted over Wi-Fi. WPA2 encryption helps prevent unauthorized access by ensuring that only authorized users can connect to the network. Securing wireless routers is equally important —by changing default login credentials[4] and disabling remote management, you reduce the risk of outsiders gaining control over your network settings. These steps protect against cyberthreats like eavesdropping and unauthorized network changes, safeguarding your data from attackers who might exploit weak or unsecured networks.

Implementation Examples

Example 1: Ensure that all wireless networks are configured with WPA2 encryption or stronger.

Example 2: Disable Wi-Fi protected setup (WPS) and all other insecure or automated authentication methods for wireless networks.

Example 3: Change all default credentials and configure strong, unique passwords for wireless network access.

Mappings to External Control Standards

- NIST PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.
- NIST PR.PS-01: Configuration management practices are established and applied.
- CIS 18 v8.1 Safeguard 3.10: Encrypt Sensitive Data in Transit.
- CIS 18 v8.1 Safeguard 4.1: Establish and Maintain a Secure Configuration Process.
- CIS 18 v8.1 Safeguard 4.2: Establish and Maintain a Secure Configuration for Network Infrastructure.
- CIS 18 v8.1 Safeguard 12.6: Use of Secure Network Management and Communication Protocols.

4 See also IO.01.3 Use Strong, Unique Passwords

MSF.01.10 – Implement a Least Privilege Account Access Policy

Implementing a least privilege account access policy is a fundamental security practice that limits user access to only the information and resources necessary for their job functions. By granting the minimum required permissions, businesses reduce the risk of accidental or intentional misuse of or access to sensitive data and systems. This approach helps prevent unauthorized access to critical files, reduces the attack surface in the event of a potential breach, and limits the damage that could occur if an account is compromised. A least privilege policy also ensures better control over access management, making it easier to audit, monitor, and enforce security protocols, ultimately strengthening overall organizational security.

Implementation Examples

Example 1: Ensure that employees only have access to the systems and data required for their assigned job duties. Careful attention should be given to the distribution of admin privileges, roles that do not explicitly require admin privileges must not be granted admin privileges.

Example 2: Take all attributes of the requested resource into account during each authorization decision: location, time and day of the week, cyber health of the requesting endpoint.

Example 3: Revoke access rights immediately when employees change roles or leave the organization.

Example 4: Do not grant access to any systems or data beyond the minimal access needed for the role.

Mappings to External Control Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 5.1: Establish and Maintain an Inventory of Accounts.
- CIS 18 v8.1 Safeguard 6.8: Define and Maintain Role-Based Access Control.

Additional Reading

Once you have implemented the controls outlined in this section, you will be well on your way to creating a well-designed and effective cybersecurity program for your organization. For more information on the controls that make up this tier of cybersecurity maturity, consult the following sites:

https://www.nmfta.org/cybersecurity
https://www.nist.gov/cyberframework
https://www.cisecurity.org/controls/v8
https://www.cisa.gov/cyber-guidance-small-businesses

Initial: Mid-Sized Fleet Controls - Tier Two

An important step to take before beginning work on this next tier of controls is to define and document a set of Cybersecurity Performance Goals (CPGs) for the company. This will facilitate appropriate selection and scoping of all subsequent controls.

Tier two contains the next set of controls that Mid-Sized Fleets should implement after cybersecurity fundamentals are addressed. These controls represent a significant portion of a well-developed cybersecurity program for businesses at this scale. It is important to clearly define the business processes and strategic goals first and then design and implement the specific controls from this section in ways that align with both current processes and strategic goals. Ongoing evaluation of this alignment is strongly recommended to ensure that the security program continues to effectively protect and support the company without interfering with business requirements. There are additional controls available that fall in this tier and further study of the NIST CSF and CIS 18 v8.1 standards is recommended. The controls in this section represent the most cost effective, highest impact controls at this maturity level.[5]

5 This level of cybersecurity maturity maps to NIST maturity level: Risk Informed

MSF.02.1 – Documented Incident Response Plan

A defined and documented incident response plan (IRP) is essential for effectively managing cybersecurity incidents. This plan should outline the procedures that your business will follow to detect, respond to, and recover from security incidents. A well-designed IRP ensures a coordinated response, minimizes negative business impact and downtime, and helps to reduce the damage caused by breaches or attacks. With a clear plan in place, companies can reduce confusion during an incident, streamline communications, and ensure compliance with regulations and customer service-level agreements (SLAs). Maintaining and regularly testing an up-to-date IRP is critical to effective incident response.[6]

Implementation Examples

Example 1: Develop a written IRP document. Include key sections such as roles and responsibilities, incident detection and analysis, containment strategies, communication channels and policies, eradication steps, and recovery procedures. Ensure that the IRP is specifically tailored to the company's business operations and specific risks and requirements.

Example 2: Create and document an Incident Response Team (IRT). This team should consist of designated members responsible for executing the IRP, including IT staff, fleet managers, dispatch representatives, and legal or compliance personnel. Ensure that each member of the IRT receives adequate training on their responsibilities as defined in the IRP.

Example 3: Conduct regular IRP reviews and update the plan as needed to keep pace with changes in technology, personnel, and business requirements. Schedule IRP reviews immediately following any major system or personnel changes as these may render parts of the current plan obsolete.

Example 4: Periodically conduct simulated incident response exercises. Conduct tabletop exercises (TTX) or mock incidents to test your IRP, identify any gaps and confirm staff readiness to response effectively in the event of a real incident.

Mappings to External Controls Standards

- NIST ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.
- NIST PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.
- CIS 18 v8.1 Safeguard 17.1-9: Incident Response Management.

6 See Appendix A

MSF.02.2 – Document Contractual Requirements

Documenting contractual cybersecurity requirements ensures that the company and its vendors, partners, and service providers understand and adhere to consistent, agreed-upon security obligations and SLAs. Clear documentation helps to reduce the risks associated with third-party relationships and helps to ensure compliance with regulatory requirements. This documentation also helps to protect sensitive data shared across the organization's business ecosystems. This promotes accountability and reduces the likelihood of security breaches stemming from vendor or partner vulnerabilities by ensuring that all vendors are informed of and held to a set of security standards, defined in service contracts.

Implementation Examples

Example 1: Require vendor security assessments. Before entering into contracts with any vendor, evaluate vendor security practices through questionnaires and documentation review to ensure they meet your business's standards.

Example 2: Develop cybersecurity clauses in contracts. Include specific requirements such as data protection measures, incident reporting timelines, security certifications [e.g. System and Organization Control Type 2 (SOC 2), Payment Card Industry Data Security Standard (PCI-DSS))], and access control policies.7

Example 3: Establish incident notification terms. Define how and when vendors or partners must notify your business of security incidents, including details about the scope and impact thresholds that must trigger notification. Ensure that these terms are included in all contracts.8

Example 4: Review all contracts regularly. Periodically evaluate and renegotiate or update contractual agreements to reflect changes in technology, regulations or business requirements.

Mappings to External Controls Standards

- NIST GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.
- NIST GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.
- NIST GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.
- NIST GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.
- CIS 18 v8.1 Safeguard 15.1: Establish and Maintain an Inventory of Service Providers.
- CIS 18 v8.1 Safeguard 15.2: Establish and Maintain a Service Provider Management Policy.

---

7 Mid-sized fleets may have varied levels of success getting vendors to agree to cybersecurity-related clauses. If a clause is rejected, careful review of the vendor's existing contract terms and conditions as well as detailed discussions and documentation review is recommended to confirm that the vendor is meeting or exceeding all requirements and will continue to do so if the contract is signed.

8 Here as well, if vendors or partners refuse requested notification terms and conditions, careful review of the contract and business value of the relationship is warranted. Exceptions should be documented and approved by company leadership.

MSF.02.3 – Inventory and Classify All Business Data

Inventorying and classifying all business data is a critical step in ensuring data security and compliance with applicable privacy regulations and security standards. Once you define and categorize all data based on its sensitivity and value to your business, you can apply the appropriate security controls and prioritize protection efforts. This process helps ensure that sensitive data, such as personally identifiable information (PII) or financial records, are protected with stricter controls, while less critical data is managed accordingly. Completing this important step will help you to better control access to data, assist in detection of threats and inappropriate use of data, and more effectively protect your company's data.

Implementation Examples

Example 1: Maintain a list of the designated data types of interest (e.g. PII, protected health information, financial account numbers, organization intellectual property, operational technology data).

Example 2: Monitor all new data to identify new instances of designated data types.

Example 3: Assign data classifications to designated data types through tags or labels.

Example 4: Track the provenance, data owner, and geolocation of each instance of designated data types.

Mappings to External Control Standards

- NIST ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.
- CIS 18 v8.1 Safeguard 3.2: Establish and Maintain a Data Inventory.

MSF.02.4 – Document Service Inventory

Maintaining a documented service inventory is essential for identifying and managing all the services the company relies on to operate or provides to external partners. These services may include cloud platforms, managed IT services, telematics providers, and other third-party services essential to your fleet's operations, as well as any hosted services that the business provides to external parties (e.g. load tracking, invoice payment). A comprehensive inventory allows you to monitor services usage, track reliability and performance, identify potential vulnerabilities, and ensure alignment with your cybersecurity strategy. By understanding and tracking the services used or provided, a business can better assess risks, track compliance with contracts and regulations, and respond effectively to service-related incidents. This practice will also help to identify potential concentration risks where a company is overly dependent on a single vendor, creating a possible single point of failure.

Implementation Examples

Example 1: Create a centralized service inventory. Use a spreadsheet for a low-cost/low-complexity option or a service management tool to record details such as service names, providers, contract terms, renewal dates, and key contacts.

Example 2: Identify all critical services, create a prioritization structure based on their importance to the operation, such as transportation management system (TMS) and telematics services for dispatch, and assign each service an appropriate risk score based on the impact the loss of the service would have on the business.

Example 3: Assign specific responsibility for service inventory management to a designated team member or department. This responsibility must include the duty of regularly updating the inventory with new services, changes to existing contracts, or decommissioned services.

Example 4: Perform routine service audits. Periodically review the service inventory to confirm accuracy, verify compliance with security requirements, and identify unapproved or redundant services.

Mappings to External Controls Standards

- NIST ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.
- NIST ID.AM-04: Inventories of services provided by suppliers are maintained.
- CIS 18 v8.1 Safeguard 15.1: Establish and Maintain an Inventory of Service Providers.

MSF.02.5 – Software Version Controls

This control builds on the basic update control listed in tier 1.[9] Maintaining software version controls is essential for ensuring that all applications and systems within your organization operate on secure, supported versions. Outdated or unpatched software increases the risk of vulnerabilities that can be exploited by attackers. By implementing software version controls, businesses can standardize updates, reduce compatibility issues, and maintain compliance with security best practices.

Implementation Examples

Example 1: Create a software version tracking system. Use an inventory tool, or for a low cost/low complexity option a spreadsheet, to document the current versions of all software in use.

Example 2: Establish a patch management process. Regularly monitor for updates or patches released by software vendors and prioritize applying critical updates to address security vulnerabilities.

Example 3: Automate version controls where possible. Use endpoint management tools or centralized software management platforms to automatically detect, update, and enforce approved software versions.

Example 4: Schedule periodic version reviews. Perform routine checks to ensure all software remains updated, supported, and compliant with company policies. Remove all unsupported or end-of-life software from your systems.10

Mappings to External Controls Standards

- NIST ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.
- NIST PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.
- NIST ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycle.
- CIS 18 v8.1 Safeguard 7.3: Perform Automated Operating System Patch Management.
- CIS 18 v8.1 Safeguard 7.4 Perform Automated Patch Management.

9 MSF.01.1 - Keep Software and Operating Systems Updated

10 Be aware of operationally critical software that reaches end of support or requires operating systems that have reached end of support. Special attention must be paid to providing secure solutions for these types of situations while minimizing negative impact on the business. Further information about this situation regarding maintenance diagnostics software specifically can be found here: https://info.nmfta.org/securing-legacy-maintenance-software-research-whitepaper

MSF.02.6 – Designate Cybersecurity Roles and Responsibilities

Designating clear cybersecurity roles and responsibilities is essential for creating an accountable and structured security environment. By assigning specific duties to team members—such as monitoring threats, managing incident response, or overseeing compliance—businesses ensure that every aspect of cybersecurity is covered. This practice helps streamline communication, prevent gaps in security coverage, and clarifies who should take action in various scenarios, such as responding to incidents or conducting audits. Defining roles and responsibilities, as emphasized in NIST CSF and CIS 18 standards, not only strengthens the company's overall security posture but also enhances coordination, accountability, and responsiveness to evolving threats.

Implementation Examples

Example 1: Identify a security point person. Choose someone within the company to work with your service provider (or internal IT if applicable), ensuring that cybersecurity questions and tasks are addressed.

Example 2: Create a basic IRP and assign primary incident responder duties to someone on the team. Outline who to call and what steps to take if a security issue arises, such as a hacked email account or suspicious activity.

Example 3: Assign someone to oversee sensitive data. Have a trusted person monitor access to critical data like payroll and customer records, ensuring that only authorized people can access or modify this data.

Example 4: Designate a security awareness advocate. Pick a team member to promote safe practices, like using strong passwords, recognizing phishing emails, and to help organize regular security reminders or cybersecurity awareness training.

Mappings to External Control Standards

- NIST GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.

MSF.02.7 – Replace MFA with Windows Hello or Similar

Implementing advanced authentication methods like Windows Hello or equivalent passwordless solutions can enhance user experience and strengthen security. These technologies leverage biometric authentication (e.g. fingerprint or facial recognition) or secure PINs that are tied to hardware. This provides a robust alternative to traditional MFA. By replacing MFA with modern passwordless systems, companies can reduce reliance on passwords, reduce the risk of phishing-based credential theft, and streamline access for users.

Implementation Examples

Example 1: Deploy Windows Hello for business. Configure Windows Hello for secure, passwordless authentication using facial recognition, fingerprints, or PINs, tied to the user's device.

Example 2: Evaluate compatible alternatives. Consider other passwordless authentication systems, such as Fast IDentity Online 2 (FIDO2)-compliant keys or mobile-based biometrics solutions, that integrate with your existing systems.

Example 3: Train users on passwordless authentication. Educate employees on the benefits of biometrics and hardware-tied authentication, including how to use these methods securely and effectively.

Example 4: Phase out traditional MFA gradually. Implement a phased rollout to replace MFA with passwordless authentication, focusing on high-risk or high-priority systems first. Monitor the entire transition carefully and modify the process as needed to ensure minimal business disruption.

Mappings to External Controls Standards

- NIST PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.
- NIST PR.AA-03: Users, services, and hardware are authenticated.
- NIST PR.AA-04: Identity assertions are protected, conveyed, and verified.
- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 6.3 Require MFA for Externally Exposed Applications.[11]
- CIS 18 v8.1 Safeguard 6.4 Require MFA for Remote Network Access.
- CIS 18 v8.1 Safeguard 6.5 Require for Administrative Access.

11 The CIS Safeguards referenced in this control all refer to MFA as a secure login option. Bear in mind that Windows Hello will only satisfy the requirements for these safeguards if properly configured to require biometric authentication.

MSF.02.8 – Prevent Remote Administrative Access to Systems

Restricting remote administrative access to systems is essential to reducing the attack surface and protecting critical resources. Unauthorized remote access is a common entry point for cybercriminals, including ransomware and credential theft operations. By preventing remote administrative access and implementing strict access controls, businesses can reduce the risk of exploitation, improve accountability, and help to maintain the integrity of their systems. For situations requiring remote access, secure alternatives such as virtual private networks (VPNs), zero-trust models, or jump servers should be employed.

Implementation Examples

Example 1: Disable remote administrative access by default. Configure systems to block administrative access over remote protocols such as Remote Desktop Protocol (RDP) or Secure Shell (SSH), unless explicitly required.

Example 2: Implement a jump server. For situations where remote administrative access is necessary, use a dedicated, hardened jump server with MFA and logging enabled to act as an intermediary.

Example 3: Enforce network-level access restrictions. Use firewalls or access control lists (ACLs) to restrict remote administrative access to specific IP ranges or authorized devices only.

Example 4: Monitor for unauthorized access attempts. Set up alerts and review logs to detect and respond to unauthorized or suspicious access attempts targeting administrative accounts or services.

Mappings to External Controls Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- NIST PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.
- NIST PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.
- NIST PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected.
- CIS 18 v8.1 Safeguard 6.4: Require MFA for Remote Network Access.

MSF.02.9 – Restrict Admins to Privileged Access Workstations

Privileged Access Workstations (PAWs) are dedicated systems used exclusively for performing sensitive administrative tasks. Restricting access to PAWs is critical to protecting privileged accounts from compromise, reducing exposure to malware, and ensuring secure management of critical systems. By limiting access to authorized personnel and enforcing strict security controls, businesses can safeguard administrative credentials and maintain the integrity of their environment.

Implementation Examples

Example 1: Configure PAWs for specific users and tasks. Assign PAWs to privileged users, such as system administrators. Restrict these workstations to only approved administrative activities, ensuring that no email, web browsing, or non-administrative tasks are performed.

Example 2: Enforce access controls. Use group policies or identity and access management (IAM) solutions to restrict logins on PAWs to only authorized administrative accounts. Ensure that MFA or other passwordless, hardware restricted alternatives are mandatory.

Example 3: Isolate PAWS from the regular network. Place PAWs on a segregated network segment with limited communication pathways to reduce their exposure to potential threats.

Example 4: Perform regular audits of PAW usage. Monitor and log activities on PAWs to detect anomalies, ensure compliance with policies, and identify any misuse or unauthorized access (attempted or successful).

Mappings to External Controls Standards

- NIST PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.
- NIST PR.AA-03: Users, services, and hardware are authenticated.
- CIS 18 v8.1 Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts.

MSF.02.10 – Proactive End-of-Life Management Policies

Proactively managing hardware and software end-of-life (EOL) helps to ensure that your organization remains secure, compliant, and operationally efficient. When technology reaches EOL, it no longer receives vendor support. This includes critical security updates, leaving your systems vulnerable to exploitation. A proactive EOL management policy involves identifying, planning for, and replacing EOL systems before they become a risk. Doing this minimizes the potential disruption to your operations and reduces potential security vulnerabilities.

Implementation Examples

Example 1: Create and maintain an EOL inventory. Track hardware and software lifecycles in your asset inventory, noting support expirations dates and planned replacement timelines.

Example 2: Establish EOL replacement policies. Define and implement policies to replace EOL systems at least 6–12 months before their support ends. Prioritize critical systems and applications.

Example 3: Communicate EOL replacement plans with stakeholders. Notify relevant stakeholders, including IT staff and fleet or maintenance managers as applicable, about upcoming EOL deadlines and replacement schedules.

Example 4: Budget for lifecycle management. Allocate funds in annual budgets for replacing or upgrading systems that are approaching EOL to ensure smooth transitions with minimal financial strain.

Mappings to External Controls Standards

- NIST PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.
- NIST PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.
- CIS 18 v8.1 Safeguard 2.1: Establish and Maintain a Software Inventory.
- CIS 18 v8.1 Safeguard 2.2: Ensure Authorized Coftware is Currently Supported.

MSF.02.11 – Configure Email Security

Configuring Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies, along with a Secure Email Gateway (SEG), is essential for protecting your business from email-based threats like phishing and spoofing. SPF helps verify that emails claiming to be from your domain are sent from authorized servers, while DMARC builds on this by allowing you to set policies on how to handle unauthenticated messages. A SEG further enhances protection by filtering incoming emails for malicious content. When used together, these tools help to prevent unauthorized email use, protect against spam and phishing, and safeguard sensitive communication.

Implementation Examples

Example 1: Set up SPF Records. Configure SPF by adding a Domain Name Service (DNS) record that specifies which mail servers are authorized to send emails on behalf of your domain.

Example 2: Implement DMARC policies. Configure DMARC policies in your DNS settings to dictate how to handle messages that fail SPF and DomainKeys Identified Mail (DKIM) checks, such as marking them as spam or rejecting them completely.

Example 3: Use a secure email gateway (SEG). Deploy a secure email gateway to filter out phishing attempts, malware, and spam before emails reach anyone's inbox, ensuring an added layer of email protection.

Example 4: Monitor DMARC reports regularly. Enable DMARC reporting to receive feedback on email authentication results, helping you identify unauthorized email activity and adjust your policies as needed.

Mappings to External Control Standards

- NIST DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 10.1: Deploy and Maintain Anti-Malware Software.

MSF.02.12 – Layered Network Access Controls

Implementing layered network access controls is a key strategy for protecting your business network by limiting access based on user roles and security levels. This approach creates multiple checkpoints, such as firewalls, VPNs, and segmented networks, that control who can access specific areas and systems. By layering these controls, you make it harder for unauthorized users to move through your network and reach sensitive information, even if they breach one layer. This practice reduces the risk of data breaches, supports regulatory compliance, and aligns with cybersecurity frameworks like NIST CSF and CIS 18, creating stronger, more resilient network defenses.

Implementation Examples

Example 1: Use a secure Wi-Fi network with a strong password. Set up a secure, password protected Wi-Fi network for business use and avoid sharing it with non-employees or using it for personal devices.

Example 2: Enable a firewall on your router. Ensure that the firewall feature on your router is active to block unwanted access to your network and monitor for unusual activity.

Example 3: Implement device-based access controls. Only allow approved devices, like company laptops or tablets, to connect to your main business network. This limits network access to known devices, adding another layer of security.

Mappings to External Control Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 3.12 Segment Data Processing and Storage Based on Sensitivity.

MSF.02.13 – Internal Network Segmentation

Implementing internal network segmentation involves dividing your business network into separate segments or sections, each with its own access controls. This practice prevents users from moving freely across the network, so if one part of the network is compromised, the threat remains contained to that segment. Network segmentation can help protect sensitive information, limit the impact of cyberattacks, and make it easier to monitor network activity for potential issues. For small companies, this approach strengthens security by ensuring that access to critical areas, such as financial records or fleet data, is limited to authorized users only.

Implementation Examples

Example 1: Separate financial systems from general operations. Isolate accounting and payroll systems from other parts of the network to protect sensitive financial data.

Example 2: Create a dedicated network segment for fleet management. Keep fleet management and maintenance systems on a separate network segment so that access is limited and closely monitored.

Example 3: Restrict internet access for certain segments. For sensitive areas like employee data, limit or block internet access to reduce direct exposure to online threats and browser-based attacks.

Example 4: Implement user-based access controls for each segment. Only allow access to specific segments for employees who need it, ensuring that data and systems are accessible only to relevant team members or departments.

Mappings to External Control Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 3.12 Segment Data Processing and Storage Based on Sensitivity.

MSF.02.14 – Operational Technology Segregated from Information Technology

Segregating operational technology (OT) from information technology (IT) networks is critical to protecting the integrity, availability, and safety of systems that control physical processes. OT environments, such as telematics systems and vehicle control systems, often have unique vulnerabilities and operational requirements that differ from those of traditional IT systems. Proper segregation reduces the risk of lateral movement by attackers, limiting the impact of malware or ransomware, and ensures that critical OT systems are not disrupted by IT-related incidents. It also reduces the possibility of any risks being introduced from the OT environment to the IT environment, or vice versa.

Implementation Examples

Example 1: Implement network segmentation. Prioritize the creation of a demilitarized zone (DMZ) between the OT and IT environments. Use firewalls, virtual local area networks (VLANs), or software-defined networking (SDN) to isolate OT systems from IT networks.

Example 2: Establish access controls for OT environments. Limit access to OT systems to authorized personnel only. Enforce multi-factor authentication (MFA) for remote and local access.

Example 3: Monitor traffic between IT and OT networks. Deploy intrusion detection and prevention systems to monitor and control communication between IT and OT environments for potential threats or anomalies.

Example 4: Use dedicated tools for OT systems. Avoid managing OT systems with IT tools or software that are not specifically designated for OT environments to prevent inadvertent risks or disruptions.

Mappings to External Controls Standards

- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- NIST ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.
- CIS 18 v8.1 Safeguard 12.2: Establish and Maintain a Secure Network Architecture.
- CIS 18 v8.1 Safeguard 13.4: Perform Traffic Filtering between Network Segments.

MSF.02.15 – Encrypt All Devices

Encrypting all devices is a critical security measure that ensures data remains protected even if a device is lost or stolen. Encryption converts data into unreadable code that can only be unlocked with a decryption key, preventing unauthorized access to sensitive information. Encrypting devices, such as laptops, mobile phones, tablets, and storage devices, helps to secure customer information, financial data, and other sensitive records.

Implementation Examples

Example 1: Enable full disk encryption. Activate full disk encryption on all company laptops, desktops, and tablets (e.g. BitLocker for Windows, FileVault for macOS) to protect data stored on the device.

Example 2: Use mobile device encryption. For mobile phones and tablets, enable device encryption through the settings menu to secure data, especially for devices used for business communication.

Example 3: Encrypt removeable storage media. Encrypt all external drives, USBs, and other portable storage devices used for business purposes to protect data when transferring files or backing up information.

Example 4: Require strong passwords for encrypted devices. Ensure that all encrypted devices are protected with strong, unique passwords or PINs to prevent unauthorized access to the encrypted data.12

Mappings to External Control Standards

- NIST PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.
- CIS 18 v8.1 Safeguard 3.9: Encrypt Data on Removeable Media.
- CIS 18 v8.1 Safeguard 3.11: Encrypt Sensitive Data at Rest.

12 See also IO.01.3 – Use Strong, Unique Passwords

MSF.02.16 – Enable Detailed Security Logging

Enabling detailed security logging is essential for tracking and understanding activity across your network, systems, and devices. Security logs provide valuable insights into who accessed systems, what actions were taken, and any unusual behavior that may indicate a potential security threat. Detailed logging helps you detect and investigate incidents quickly, supports regulatory compliance, and provides critical evidence in the event of a security breach. By maintaining comprehensive logs, you strengthen your company's ability to monitor security and respond effectively to any suspicious activity.

Implementation Examples

Example 1: Enable logging on all key systems. Ensure that logging is activated for all essential systems, such as servers, network devices, and applications to capture critical security events.

Example 2: Configure centralized log storage. Use a centralized logging solution to collect and store logs in one location, making it easier to review and analyze events across multiple systems.

Example 3: Set up alerts for unusual activity. Configure alerts for specific security events, such as failed login attempts or unusual network activity.

Example 4: Retain and regularly review logs. Schedule routine log reviews to identify patterns or anomalies and retain logs for a designated period to comply with legal or regulatory requirements.

Mappings to External Control Standards

- NIST PR.PS-04: Log records are generated and made available for continuous monitoring.
- CIS 18 v8.1 Safeguard 8.2: Collect Audit Logs.

MSF.02.17 – Access to OT and Vehicle Systems Based on Role and Attribute-Based Access Control

Implementing role-based access control (RBAC) and/or attribute-based access control (ABAC) for operational technology (OT) and devices that interact with onboard vehicle systems helps to ensure that access to sensitive systems is granted only to authorized individuals based on their specific job roles. This reduces the risk of unauthorized access, human error, and potential security breaches. By enforcing RBAC, businesses can align access permissions with operational responsibilities, maintain audit trails and enhance the security of critical systems such as telematics, fleet management systems, and onboard vehicle control systems.

Implementation Examples

Example 1: Define roles and permissions. Establish clear roles for users interacting with OT and devices that interact with onboard vehicle systems (e.g. fleet managers, maintenance staff, IT administrators) and assign appropriate access levels for each role.

Example 2: Use centralized identity and access management (IAM) systems. Leverage IAM platforms to enforce RBAC policies consistently across OT and devices that interact with onboard vehicle systems, integrating with existing authentication systems.

Example 3: Restrict administrative access to OT systems and devices that interact with onboard vehicle systems. Limit access to a small group of trusted personnel and require MFA or other secure, passwordless solutions for all access.13

Example 4: Review access regularly. Conduct periodic audits of user's roles and permissions to ensure that they remain aligned with current responsibilities. Revoke access for users who no longer require it for completion of assigned duties. Immediately revoke access in the event of an employee termination.

Mappings to External Controls Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- NIST PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.
- CIS 18 v8.1 Safeguard 6.5: Require MFA for Administrative Access.
- CIS 18 v8.1 Safeguard 6.8 Define and Maintain Role-Based Access Control.

13 Further reading at https://www.microsoft.com/en-us/windows/tips/windows-hello

MSF.02.18 – Preventative Maintenance Cycles Include Checks for Tampering with Onboard Electronics on Power Units and Trailers

Incorporating tampering checks into preventative maintenance (PM) cycles is essential for ensuring the security and functionality of onboard electronics in power units and trailers. These systems, such as electronic logging devices (ELDs), telematics units, and sensors, are critical to fleet operations but may be at risk of being tampered with, either maliciously or inadvertently. By routinely inspecting these systems during PM cycles, businesses can detect unauthorized modifications, maintain compliance with regulations, and reduce the risk of operational disruptions caused by compromised systems.

Implementation Examples

Example 1: Develop a tampering inspection checklist, include specific steps to visually and digitally inspect onboard electronics for signs of tampering, such as broken seals, unauthorized devices, or altered configurations.

Example 2: Train maintenance staff. Provide training to maintenance teams on identifying potential tampering indicators and security handling onboard electronics.

Example 3: Monitor systems logs and alerts. During PM cycles, review logs from onboard systems to identify anomalies such as unexpected configurations changes or unexplained downtime, that may indicate tampering.

Example 4: Implement anti-tampering measures. Use tamper-evident seals, secure hardware enclosures and mounting hardware, and alarm systems to deter unauthorized access to onboard electronics.

Mappings to External Controls Standards

- NIST PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.
- NIST PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.
- NIST PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected.
- NIST PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.
- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.

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

MSF.02.19.A - Maintenance Facilities: Diagnostic Laptops

Maintenance diagnostics laptops pose unique cybersecurity challenges due to their role in interfacing with vehicles and often running legacy or specialized software. To protect enterprise networks from potential malware, unauthorized access, and system tampering, it is essential to isolate these laptops from the broader IT infrastructure while ensuring that they remain fully functional for their intended purpose. Proper isolation safeguards critical systems and minimizes the risk posed by the trusted connections these devices maintain with vehicles.[14]

MSF.02.19.B - Warehouse and Dock: Handheld Scanners and Portable Devices

Segregating handheld scanners and portable devices used in warehouse operations from enterprise infrastructure is critical for maintaining the security and integrity of both operations and corporate systems. Warehouse devices often interact with sensitive supply chain data and operational workflows while being exposed to unique threats, such as physical tampering or unauthorized access. Isolating these devices minimizes risks from malware, unauthorized access, and lateral movement within the network.

Implementation Examples

Example 1: Place diagnostic laptops on a separate, isolated network segment dedicated to operational technology (OT) systems. Implement strict access controls to prevent lateral movement into enterprise IT networks.
Example 2: Disable unnecessary internet connectivity on diagnostics laptops and warehouse mobile devices. Where connectivity is essential, use a tightly controlled allowlist for specific services such as license servers or firmware update sites.

Example 3: Use hardware-based firewalls and endpoint detection and response (EDR) tools on diagnostics laptops. Restrict admin privileges and ensure tamper-proof settings for both hardware and software.

Example 4: Deploy network monitoring tools to track the activity of maintenance and warehouse devices. Flag unauthorized communication attempts or unusual data transfer patterns.

Mappings to External Controls Standards

- NIST PR.AA-03: Users, services, and hardware are authenticated.
- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.

14 Further reading at https://info.nmfta.org/securing-legacy-maintenance-software-research-whitepaper

MSF.02.20 – Diagnostics Laptops are Physically Controlled to Prevent Unauthorized Access or Tampering

Physically controlling maintenance diagnostics laptops is critical to preventing unauthorized access, tampering, or theft, which could compromise sensitive systems and vehicle configurations. These laptops often store or interact with critical diagnostic software and hardware, making them a prime target for cyber and physical threats. By implementing robust physical security measures, businesses can safeguard the integrity of their maintenance processes and reduce potential risks to both OT and IT systems.

Implementation Examples

Example 1: Store diagnostics laptops in locked cabinets, safes, or other secure locations when not actively in use. Restrict access to authorized personnel only.
Example 2: Attach laptops to fixed workstations with locking cables or similar security devices to prevent theft. Consider using tamper-evident seals for additional security.

Example 3: Install surveillance systems in maintenance facilities to monitor access to diagnostic laptops and deter unauthorized activities.

Example 4: Use asset tracking software or physical tracking tags (e.g. RFID) to monitor the location of each diagnostic laptop within the facility or during transport.

Mappings to External Controls Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- NIST PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.
- CIS 18 v8.1 Safeguard 4.6: Securely Manage Enterprise Assets and Software.

Intermediate: Mid-Sized Fleet Controls – Tier Three

The controls in this section focus on fine tuning the core cybersecurity program laid out in the previous two sections. Some of the controls in this section will require a more significant investment of both time and resources. However, the return on investment will be worth the effort as these controls, when properly implemented and managed, will dramatically improve the overall security posture of the business.[15] Additional resources for the following two sections may be found at the end of this document. Intermediate and advanced cybersecurity programs require extensive tailoring and scoping of a wide range of controls to effectively address the specific security concerns of the business. Please refer to the *additional resources* appendix for a list of several documents and sites that will provide insights into these additional controls.

15 This level of cybersecurity maturity maps to NIST maturity level: Repeatable

MSF.03.1 – Bring Your Own Device Policies and Restrictions are Actively Managed

Actively managing the use of personal devices to access work systems or data is a critical step in reducing the risk of accidental or intentional data loss, corruption or introduction of malware. Bring your own device (BYOD) policies and restrictions can help to mitigate risks associated with personal devices accessing company networks, systems, accounts, or data. Personal devices may lack adequate security controls and can introduce vulnerabilities, such as malware, unauthorized data access, or accidental data leakage. A robust BYOD policy ensures that both network access and company accounts are adequately secured, minimizing potential threats to the enterprise environment.

Implementation Examples

Example 1: Develop and communicate clear policies outlining acceptable use, security requirements, and prohibited activities from personal devices. Include specific rules for accessing company accounts, cloud platforms, or sensitive data from BYOD devices.

Example 2: Require MFA for all access to company accounts, including email, cloud platforms, collaboration platforms, to ensure that only authorized users can gain entry, even if device security is compromised.

Example 3: Use identity access management (IAM) tools to enforce conditional access policies that restrict logins from personal devices unless they meet security requirements (e.g. up-to-date operating systems, encryption, and endpoint protection or mobile device management (MDM) client).

Example 4: Deploy data loss prevention (DLP) solutions to monitor, restrict, and log the transfer of sensitive data from company accounts to personal devices or unauthorized locations.

Mappings to External Controls Standards

- NIST ID.AM-01: Inventories of hardware managed by the organization are maintained.
- NIST PR.AA-03: Users, services, and hardware are authenticated.
- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 3.6: Encrypt Data on End-User Devices.
- CIS 18 v8.1 Safeguard 4.10: Enforce Automatic Device Lockout on Portable End-User Devices.
- CIS 18 v8.1 Safeguard 4.11: Enforce Remote Wipe Capability on Portable End-User Devices.
- CIS 18 v8.1 Safeguard 4.12: Separate Enterprise Workspaces on Mobile End-User Devices.

MSF.03.2 – Security Incident and Event Management Solution

A security incident and event management (SIEM) solution is a powerful tool that helps businesses monitor, detect, and respond to security threats in real time. SIEM systems collect and analyze security data from across a business's IT infrastructure, including network devices, servers, and applications. By aggregating logs and correlating events, SIEM solutions can identify suspicious activities and provide alerts. This enables quicker responses to potential incidents. SIEMs also offer centralized visibility and reporting, which can help a business meet regulatory compliance requirements and improve their overall security posture.

Implementation Examples

Example 1: Choose a scalable SIEM tool. Select a SIEM that can grow with your business, ensuring that it can handle increasing data volume and complexity as your needs expand.

Example 2: Integrate all critical data sources. Connect key systems, like firewalls, endpoints, and cloud services to the SIEM to ensure a comprehensive view of the security landscape of the entire business.

Example 3: Customize alert settings. Set up specific alerts for high-risk activities relevant to your business to reduce noise and false positives. This will allow your security team to focus on critical security incidents.

Example 4: Establish regular log reviews. Develop a process for routinely analyzing SIEM logs and reports, allowing for early detection of anomalies and a proactive approach to security management.

Mappings to External Control Standards

- NIST DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.
- CIS 18 v8.1 Safeguard 8.9: Centralize Audit Logs.

MSF.03.3 – Secure Baseline Configurations or Device Images

Establishing secure baselines for devices is an essential practice to ensure that all devices in a business meet minimum security standards. A secure baseline includes configurations and settings that will harden a device against common vulnerabilities, such as disabling unnecessary services, enforcing strong password policies, and applying security patches. By creating these baselines for each type of device—whether computer, mobile phone, or network hardware—and using standardized device images, companies can maintain consistent security measures across their environment, reducing the risk of attacks and simplifying compliance with cybersecurity standards.

Implementation Examples

Example 1: Define baseline configurations and create device images. Develop standardized security configurations and create device images for each type of device, ensuring that secure settings are consistently applied when new devices are deployed.

Example 2: Use automated tools for baselines and images. Implement tools that automate the application of baseline configurations or device images to ensure that all devices have the exact same security settings across the business without relying on manual action.

Example 3: Regularly review and update baseline images. Schedule routine reviews to update baselines and recreate device images as new threats emerge or as compliance requirements change, keeping configurations current.

Example 4: Monitor for baseline deviations. Set up monitoring to detect when a device falls out of compliance with its baseline, allowing IT or cybersecurity personnel to quickly address the potential vulnerabilities and restore the device to its secure state.

Mappings to External Control Standards

- NIST PR.PS-01: Configuration management practices are established and applied.
- CIS 18 v8.1 Safeguard 4.1: Establish and Maintain a Secure Configuration Process.
- CIS 18 v8.1 Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure.

MSF.03.4 – Port Security Enabled on All Network Access Ports

Enabling port security on all network access ports is essential for preventing unauthorized devices from connecting to the wired network. This helps mitigate the risk of rogue devices, unauthorized access, and potential network-based attacks such as address resolution protocol (ARP) spoofing or media access control (MAC) flooding. By enforcing port security configurations, businesses can maintain greater control over network access and protect sensitive IT and OT environments from potential breaches.

Implementation Examples

Example 1: Configure port security to allow only authorized devices, identified by their MAC addresses, to connect to each network port. Maintain a documented list of approved devices for management and auditing purposes.

Example 2: Set limits on the number of MAC addresses that can be associated with each port to prevent unauthorized devices from connecting and overwhelming the port with traffic.

Example 3: Configure network switches to disable ports automatically if unauthorized access attempts are detected. Require administrative intervention to re-enable the port.

Example 4: Use network monitoring tools to regularly review port activity logs for unauthorized access attempts or anomalies. Investigate and remediate incidents promptly.

Mappings to External Controls Standards

- NIST PR.PS-01: Configuration management practices are established and applied.
- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- NIST DE.CM-01: Networks and network services are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 12.2: Establish and Maintain a Secure Network Architecture.
- CIS 18 v8.1 Safeguard 13.9: Deploy Port-Level Access Control.

MSF.03.5 – Policy and Technical Controls to Enforce Connection Medium (Wi-Fi/Wired)

Implementing policies and technical controls to enforce connection mediums (e.g. Wi-Fi or Wired) ensures that devices access the network through secure and approved channels. This reduces the risk of unauthorized access, network spoofing, and data leakage by ensuring connections are made via authenticated and protected mediums. Enforcing these controls also helps maintain a clear separation between trusted and untrusted networks.

Implementation Examples

Example 1: Establish and document policies that specify which connection mediums are approved for different use cases. For example, sensitive OT systems may require wired connections, while Wi-Fi may be limited to specific devices or areas.

Example 2: Use a Network Access Control (NAC) solution to enforce policies for connection mediums. Restrict devices to connect only through authorized mediums and ensure compliance with encryption and authentication protocols (e.g. WPA3 for Wi-Fi).

Example 3: Disable unused mediums on devices. Configure devices to disable unused network interfaces, such as Wi-Fi on devices that should only connect via wired ethernet, to prevent unauthorized connections or bridging between networks.

Example 4: Use network monitoring tools to track device connections and alert administrators if unauthorized mediums are used or if devices attempt to connect to both Wi-Fi and wired interfaces simultaneously.

Mappings to External Controls Standards

- NIST PR.PS-01: Configuration management practices are established and applied.
- NIST PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.
- CIS 18 v8.1 Safeguard 1.5: Use a Passive Asset Discovery Tool.
- CIS 18 v8.1 Safeguard 4.1: Establish and Maintain a Secure Configuration Process.
- CIS 18 v8.1 Safeguard 12.6: Use of Secure Network Management and Communication Protocols.

MSF.03.6 – Deploy Application Security Software

Deploying application security software increases the protection of endpoints and networks from threats such as malware, unauthorized software usage, and data breaches. Application security solutions provide visibility, control, and enforcement over the applications running on devices, ensuring that only authorized and safe applications can execute. These tools are particularly important for defending against evolving threats targeting applications and their specific vulnerabilities.

Implementation Examples

Example 1: Implement application allowlisting. Use application allowlisting tools to permit only pre-approved and vetted applications to run on company systems. Regularly review and update the allowlist as new applications are added or existing ones are retired.

Example 2: Deploy an endpoint protection platform (EPP). Use EPP solutions to detect, block, and remove malware, ransomware, or other malicious software. Ensure that the platform includes features such as real-time monitoring and behavioral analysis.

Example 3: Integrate Runtime Application Self-Protection (RASP). Deploy RASP solutions to monitor application behavior during execution and block malicious actions, such as unauthorized code execution or exploit attempts.

Example 4: Automate vulnerability scanning. Use application security tools to scan for known vulnerabilities in installed applications. Prioritize patching or replacing applications flagged as high risk.

Mappings to External Controls Standards

- NIST PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.
- NIST ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.
- CIS 18 v8.1 Safeguard 2.2 Ensure Authorized Software is Currently Supported.
- CIS 18 v8.1 Safeguard 2.3: Address Unauthorized Software.
- CIS 18 v8.1 Safeguard 2.4: Utilize Automated Software Inventory Tools.
- CIS 18 v8.1 Safeguard 2.5: Allowlist Authorized Software.

MSF.03.7 – Fully Implement Zero-Trust Architecture

Zero-trust architecture (ZTA) is a security model that operates under the principle of "never trust, always verify," assuming that threats could come from both outside and from within the organization's network. Rather than relying on perimeter defenses alone, ZTA enforces strict identity verification, access control, and continuous monitoring for every user and device attempting to access resources, regardless of their location. By segmenting access and verifying each request, ZTA minimizes the risk of unauthorized access and lateral movement inside a network.

Implementation Examples

Example 1: Enforce strong identity verification. Implement multi-factor authentication (MFA) and identity verification processes for every user and device to ensure that only verified individuals can access network resources.

Example 2: Apply least privilege access. Limit access permissions based on job role or function, granting users only the minimum access they need to perform their tasks.

Example 3: Continuously monitor and assess activity. Use tools like SIEM and network detection and response (NDR) to monitor network activity, looking for any anomalies that could signal a security threat.

Example 4: Segment the network with micro-segmentation. Break down the network into smaller zones or segments, controlling access to each part separately so that if one area is compromised, threats cannot move as easily into other areas of the network.

Mappings to External Control Standards

- NIST PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.
- CIS 18 v8.1 Safeguard 5.1: Establish and Maintain an Inventory of Accounts.

MSF.03.8 – Network Intrusion Detection System

A network intrusion detection system (NIDS) is a critical security tool that monitors network traffic for suspicious activities or potential threats. By analyzing data packets moving though the network, a NIDS can identify patterns that may indicate unauthorized access, malware or other security issues. When a threat is detected, the system generates alerts, allowing security teams to respond quickly to prevent further damage. NIDS solutions provide valuable visibility into network activity, helping organizations protect sensitive data, maintain compliance with security standards, and reduce the risk of a successful breach.

Implementation Examples

Example 1: Deploy NIDS at key network entry points. Position the NIDS at critical points within the network, such as near the firewall or in high traffic areas (network trunk links) to monitor all incoming and outgoing data effectively.

Example 2: Configure NIDS to detect specific threats. Tailor the NIDS settings to detect threats relevant to your environment, such as unauthorized logins, known indicators of compromise (IOCs) related to specific threats, malware activity, or abnormal bandwidth usage.

Example 3: Integrate NIDS with SIEM solutions. Connect the NIDS to a SIEM system to correlate alerts with other security events, providing a comprehensive view of potential incidents.16

Example 4: Regularly update NIDS signatures and rules. Keep the NIDS up-to-date with the latest threat signatures and detection rules to ensure that it can identify new attack patterns and signs of activity around new vulnerabilities.

Mappings to External Control Standards

- NIST DE.CM-01: Networks and network services are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 13.1: Centralize Security Event Alerting.
- CIS 18 v8.1 Safeguard 13.3: Deploy a Network Intrusion Detection Solution.

16 See also IO.04.1 – Security Incident and Event Management (SIEM) Solution

MSF.03.9 – Network Intrusion Prevention System

Network intrusion prevention systems (NIPS) are security tools designed to monitor network traffic for suspicious or malicious activity and actively block or mitigate potential threats in real time. Unlike intrusion detection systems (IDS) which only alert on detected threats, NIPS can automatically take action, such as dropping malicious packets or isolating affected devices to prevent attacks from compromising the network. This proactive defense helps businesses protect sensitive data, minimize disruption, and reduce the risk of unauthorized access or malware spreading across the network.

Implementation Examples

Example 1: Deploy NIPS at key network points. Position NIPS at strategic locations, such as entry points to critical networks or near sensitive data storage to effectively monitor and protect essential assets.

Example 2: Configure NIPS with specific detection rules. Customize NIPS rules to detect and respond to common threats specific to your environment.

Example 3: Regularly update NIPS signatures and rules. Keep the system's detection signatures up-to-date to protect against new threats, ensuring that it can recognize the latest attack methods.

Example 4: Integrate NIPS with security monitoring tools. Connect NIPS to a SIEM system to correlate intrusion data with other security events, gaining deeper insight into potential threats and network activity.

Mappings to External Control Standards

- NIST DE.CM-01: Networks and network services are monitored to find potentially adverse events.
- CIS 18 v8.1 Safeguard 13.8: Deploy a Network Intrusion Prevention Solution.

MSF.03.10 – Secure Communication Between Telematics Systems and Telematics System Providers

While the carrier themselves will likely not be able to modify the communication channels utilized by their telematics devices, careful selection and vetting of telematics devices and vendors is key to ensuring that this control is satisfied. Ensuring secure communications between telematics systems and Telematics System Providers (TSPs) is critical for protecting sensitive vehicle and fleet data from interception, tampering, and unauthorized access. Telematics systems often transmit operational, regulatory, and location data, which, if compromised, could result in significant operation disruptions, data breaches, or safety risks. Implementing secure communication practices safeguards this data and ensures compliance with cybersecurity and privacy standards.

Implementation Examples

Example 1: Strong encryption protocols (e.g. TLS 1.3) are used to secure data in transit between telematics systems and TSPs. Ensure that encryption is applied consistently across all communication channels

Example 2: Implement mutual authentication (e.g. certificate-based) between telematics systems and TSPs to prevent unauthorized devices or servers from accessing sensitive data.

Example 3: Configure systems where possible to disable legacy communications protocols to protect against downgrade attacks.

Example 4: Configure access control policies to allow only pre-approved IP addresses or endpoint to communicate with telematics systems. Block unauthorized devices or systems attempting to connect.

Mappings to External Controls Standards

- NIST PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.
- CIS v8.1 Safeguard 3.8: Document Data Flows.
- CIS v8.1 Safeguard 3.10: Encrypt Sensitive Data in Transit.

Additional Resources

- NMFTA Telematics Security Requirements Matrix (TSRM) Documentation https://nmfta-repo.github.io/nmfta-telematics_security_requirements/nmfta-telematics_security_requirements/Telematics_Security_Requirements_Matrix.html

Advanced: Mid-Sized Fleet Controls – Tier Four

Advanced cybersecurity controls require additional investment both in time and in resources. However, they will pay dividends when it comes to the security and resiliency of your operation. One of the best ways to avoid being a victim of cybercrime is to be the least appealing target.[17] For mid-sized fleets, this level of cybersecurity maturity focuses heavily on governance, risk management, compliance, and the documentation and policies required to consistently support a robust and sophisticated cybersecurity program. The goal of the guidance in this section is to bring a business from one with consistent, and comprehensive security to one with an industry leading and adaptive culture of security.

MSF.04.1 – Legal and Regulatory Compliance is Actively Managed

Actively managing legal and regulatory compliance ensures that businesses adhere to applicable laws, industry standards, and contractual obligations related to cybersecurity and data protection. This practice minimizes the risk of fines, legal actions, or reputational damage while fostering trust with stakeholders, partners, and customers. By staying up-to-date with regulatory requirements and incorporating them into cybersecurity polices, businesses can ensure long-term operational and legal integrity.

Implementation Examples

Example 1: Maintain a compliance register. Create and regularly update a compliance register documenting all applicable laws, regulations, and standards (e.g. Federal Motor Carrier Safety Administration (FMCSA), PCI-DSS, Cybersecurity and Infrastructure Security Agency (CISA) guidance, NMFTA guidance, California Consumer Privacy Act (CCPA), etc.) relevant to cybersecurity and data protection in your organization.

Example 2: Assign specific responsibility for ensuring compliance. Designate a compliance officer (or team) responsible for monitoring regulatory changes, implementing necessary adjustments and maintaining evidence of compliance.

Example 3: Perform routine internal and external compliance audits to verify adherence to legal and regulatory requirements. Address identified gaps promptly with documented corrective action plans.

Example 4: Integrate compliance into policies and training. Compliance should not be expected to operate in a vacuum. Align cybersecurity policies, procedures, and employee training programs with relevant legal and regulatory frameworks to ensure company-wide adherence.

Mappings to External Controls Standards

- NIST GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed.

17 This level of cybersecurity maturity maps to NIST maturity level: Adaptive

MSF.04.2 – Regular Assessments and Exercises

Conducting regular risk assessments, vulnerability assessments, penetration tests, and tabletop exercises is crucial for proactively identifying and mitigating cybersecurity risk within abusiness. **Risk assessments** evaluate potential threats, vulnerabilities, and impacts on key assets, providing insights into areas needing improved security. **Vulnerability assessments** involve scanning systems and networks for known vulnerabilities, allowing for proactive patching and updates to reduce the risk of exploitation**. Penetration tests** simulate real-world attacks to identify weak points in defenses, offering a practical view of where systems may be vulnerable. CISA offers free network testing for critical infrastructure organizations[18] and can serve as a solid starting point for trucking operations seeking to harden their public-facing digital assets. **Tabletop exercises,** which involve running through hypothetical incident scenarios, enable teams to practice their response strategies, enhancing readiness for actual incidents. Together, these practices improve your business's ability to detect, respond to, and recover from cyberthreats and attacks.

Implementation Examples

Example 1: Schedule regular risk and vulnerability assessments. Conduct assessments periodically to evaluate evolving threats and scan for known vulnerabilities, prioritizing areas needing immediate attention and timely patching.

Example 2: Engage qualified professionals for penetration tests. Hire cybersecurity experts or third-party services to perform penetration tests, ensuring an objective review of potential security gaps in systems and applications. Ensure that penetration tests are conducted within a clearly defined scope and with documented, mutually agreed upon rules of engagement.

Example 3: Conduct tabletop exercises with key stakeholders. Organize tabletop exercises with staff involved in incident response to simulate different cyberattack scenarios, helping everyone understand roles and improve response coordination. Ensure that any third-party cybersecurity or IT service providers are included in tabletop exercises and are aware of the business's service level agreement (SLA) expectations.

Example 4: Document findings and actions plans. After each assessment, test or exercise, document the results, identify areas for improvement, and create prioritized action plans to address any identified vulnerabilities or gaps in the business's cybersecurity defenses.19

Mappings to External Control Standards

- NIST ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.
- NIST ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.
- CIS 18 v8.1 Safeguard 7.1: Establish and Maintain a Vulnerability Management Process.
- CIS 18 v8.1 Safeguard 7.2: Establish and Maintain a Remediation Process.

18 https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
19 See also IO.04.08 Prioritized Risk Register

MSF.04.3 – Mobile Device Management Solution

A mobile device management (MDM) solution is an important tool for securing and managing mobile devices used within an organization, particularly when employees use smartphones, tablets, or laptops to access company data remotely. MDM solutions enable IT administrators to monitor, manage, and secure mobile devices from a central console, enforcing security policies such as device encryption, app controls, and remote wipe capabilities. By implementing an MDM solution, businesses can reduce the risk of data leaks, protect sensitive information on mobile devices, and maintain compliance with cybersecurity standards even when employees work from outside the office.

Implementation Examples

Example 1: Establish device enrollment and inventory tracking. Use MDM to register all devices accessing company data and keep an updated inventory of devices and their configurations.

Example 2: Enforce security policies on all devices. Set and apply policies for password requirements, device encryption, and screen lock settings to ensure that mobile devices meet the business's security standards.

Example 3: Enable remote wiping capabilities. Configure MDM to allow remote wiping of devices in case they are lost or stolen, further protecting sensitive information from unauthorized access.

Example 4: Restrict and manage app usage. Use MDM to limit which applications can be installed or accessed on devices, helping control data exposure and prevent the use of risky or unauthorized apps.

Mappings to External Control Standards

- NIST ID.AM-01: Inventories of hardware managed by the organization are maintained.
- CIS 18 v8.1 Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory.

MSF.04.4 – Prioritized Risk Register

A prioritized risk register is a structured document that helps organizations identify, assess, and rank cybersecurity risks based on their potential impact and likelihood of occurrence. By listing risks in order of priority, businesses can focus on addressing the most critical threats first, ensuring that resources are directed to areas that pose the greatest danger to operations and data security. A well-maintained risk register is essential for informed decision-making, enabling proactive risk management and supporting compliance with cybersecurity standards. This approach improves resilience by ensuring that the business is prepared to mitigate high-priority risks before they materialize

Implementation Examples

Example 1: Identify and categorize risks. Document potential cybersecurity risks, categorizing them based on the type of threat (e.g., phishing, ransomware, insider threats) to gain a comprehensive view.

Example 2: Assess impact and likelihood. Rate each risk according to its potential impact on the business and the likelihood of it occurring, helping to prioritize high-risk threats.

Example 3: Assign mitigation strategies. Develop specific actions or controls to address each risk, focusing first on the most critical risks that need immediate attention.

Example 4: Regularly review and update the register. Schedule periodic reviews of the risk register to adjust priorities, add new risks, and update mitigation plans as the cybersecurity landscape changes.

Mappings to External Control Standards

- NIST ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.
- CIS 18 v8.1 Safeguard 7.2: Establish and Maintain a Remediation Process.

MSF.04.5 – Documented Vendor Management Program

A documented vendor management program ensures that third-party vendors, suppliers, and service providers adhere to the business's cybersecurity policies and meet regulatory compliance requirements. This practice reduces the risk of supply chain vulnerabilities, unauthorized access, and data breaches caused by third-party relationships. By establishing and maintaining a comprehensive vendor management program, the business can monitor vendor performance, enforce contractual obligations, and strengthen overall cybersecurity posture.

Implementation Examples

Example 1: Develop and document vendor evaluation criteria. Establish a standardized process for evaluating vendors before onboarding, including cybersecurity assessments, compliance checks, and contractual requirements for data protection and incident response and reporting.

Example 2: Maintain a vendor inventory. Create and regularly update an inventory of all vendors, including the services they provide, the data they access, and the associated cybersecurity risks.

Example 3: Implement risk-based vendor tiers. Categorize vendors into risk-based tiers based on their access to sensitive data or systems, as well as their criticality to business continuity. Apply stricter security requirements and monitoring for high-risk vendors.

Example 4: Enforce regular vendor assessments. Conduct periodic reviews of vendor cybersecurity practices, including compliance audit results, penetration test findings, and confirmation of security certifications (e.g., SOC 2, ISO 27001).

Mappings to External Controls Standards

- NIST GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.
- NIST GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.
- NIST GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.
- CIS 18 v8.1 Safeguard 15.2: Establish And Maintain a Service Provider Management Policy.
- CIS 18 v8.1 Safeguard 15.4: Ensure Service Provider Contacts Include Security Requirements.
- CIS 18 v8.1 Safeguard 15.6: Monitor Service Providers.

MSF.04.6 – Formalized, Documented Cybersecurity Policies

Formalized, documented cybersecurity policies are essential for setting clear guidelines on how your business protects information, manages risks, and maintains regulatory compliance. These policies establish the foundation for acceptable behavior, defining standards for everything from password management and data handling to device usage and incident response. Well-defined policies help employees understand their responsibilities, support a unified approach to security, and demonstrate a commitment to cybersecurity. Documented policies also make it easier to manage and enforce security practices, minimizing the potential for vulnerabilities due to inconsistent or unclear expectations.

Implementation Examples

Example 1: Develop comprehensive policy documents. Create clear, accessible policies that cover key areas like data protection, access control, acceptable use, and incident response. Ensure that these policies are tailored to the specific needs of your business.

Example 2: Store cybersecurity policies in a secure, easily accessible location, such as a protected shared drive or internal website so that all employees can reference them as needed but only authorized parties can modify the policy documents.

Example 3: Schedule regular policy reviews. Set up regular review intervals to update policies as new risks, technologies, and compliance requirements arise, ensuring that policies remain current and relevant.

Example 4: Incorporate policies into employee training and employee manuals. Make cybersecurity policies a part of regular employee training to reinforce their importance and ensure that all employees understand that adhering to established standards for cybersecurity is their responsibility.

Mappings to External Control Standards

- NIST GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.

MSF.04.7 – Documented Change Control Process

A documented change control process is essential for managing modifications to a business's IT systems and network infrastructure in a controlled and secure manner. This process involves formally evaluating, approving, and recording changes to ensure they are necessary, tested, and implemented with minimal disruption to operations. By documenting each step – from request to implementation and review – businesses can reduce the risk of introducing new vulnerabilities, improve system stability, and maintain compliance with cybersecurity standards. A well-structured change control process promotes consistency, accountability, and transparency in how changes are managed.

Implementation Examples

Example 1: Establish a change request system. Set up a formal system for submitting change requests that includes details such as the reason for the change, potential impact, and affected systems.

Example 2: Create a change approval process. Develop a procedure to review and approve changes, involving key stakeholders and designated security personnel or security service provider to assess risks and ensure alignment with security policies.

Example 3: Test changes before implementation in live environments. Require testing in a controlled environment to identify potential issues and minimize disruption before deploying changes in a live environment.

Example 4: Document and review all changes. Record details of each change, including outcomes and lessons learned, and conduct periodic reviews to refine the change control process and address any recurring issues.

Mappings to External Control Standards

- NIST ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.

MSF.04.8 – Documented Access Control Lists

Maintaining documented Access Controls Lists (ACLs) is critical for defining and enforcing access permissions to systems, networks, and data. ACLs ensure that only authorized users, devices, or services can access specific resources, reducing the risk of unauthorized access, data breaches, and insider threats. By documenting and regularly reviewing ACLs, businesses can maintain a clear understanding of their access control configurations, ensuring that they remain aligned with the security policy and business requirements.

Implementation Examples

Example 1: Define ACLs based on the principle of least privilege, ensuring that users and systems only have access to the resources necessary for their roles. Document these permissions and align them with business policies.

Example 2: Store ACLs in a centralized, accessible location, such as a configuration management database (CMDB) or version controls system, to ensure consistency and easy auditing.

Example 3: Schedule periodic audits of documented ACLs to verify they are up-to-date and accurately reflect current access requirements. Remove unnecessary or outdated permissions.

Example 4: Use monitoring tools to detect unauthorized changes to ACLs. Configure alerts to notify IT staff of suspicious modifications or attempts to bypass access controls.

- Mappings to External Controls Standards
- NIST PR.AA-05: Access Permissions, Entitlements, and Authorizations are Defined in a Policy, Managed, Enforced, And Reviewed, And Incorporate The Principles of Least Privilege and Separation Of Duties.
- CIS 18 v8.1 Safeguard 6.8: Define and Maintain Role-Based Access Control.

MSF.04.9 – Formalized, Documented Disaster Recovery Plan

A formalized and documented Disaster Recovery Plan (DRP) is essential for ensuring business continuity in the event of a cybersecurity incident, natural disaster, or other disruptive event. A well-designed DRP outlines the processes, resources, and personnel necessary to restore critical systems, data, and operations efficiently. By proactively preparing for potential disruptions, businesses can minimize downtime, mitigate financial losses, and protect their reputation.

Implementation Examples

Example 1: Develop a comprehensive DRP that includes detailed recovery objectives, such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), for critical systems and data. Specify roles, responsibilities, communication plans, and escalation paths for disaster recovery teams.

Example 2: Maintain secure, offline backups of critical systems and data and ensure that they are available and regularly tested for integrity. Store these backups in geographically diverse locations to protect against regional disruptions.

Example 3: Conduct regular disaster recovery drills to test the DRP and verify that it is up-to-date. Drills such as tabletop exercises or full-scale simulations can identify gaps in the DRP or training of team members and serve to improve recovery procedures when lessons learned are incorporated into DRP updates and future training.

Example 4: Integrate the DRP with the business's IRPs. Ensure that the DRP aligns with the business's IR strategies to provide a smooth transition from incident containment to system recovery activities.

Mappings to External Controls Standards[20]

- NIST RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.
- NIST RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.
- NIST RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.
    - CIS 18 v8.1 Control 17.x – Incident Response Management
    - CIS 18 v8.1 Safeguards 17.1 through 17.9 all provide guidance that is relevant in whole or in part to this control.

20 External mappings for both control MSF.04.09 and control MSF.04.10 are the same. While these controls are unique and reference different nuances in the incident response, business continuity section of this guidance, they both closely map to the same portions of the NIST CSF and CIS 18 controls frameworks

MSF.04.10 – Formalized, Documented Business Continuity Plan

A formalized documented Business Continuity Plan (BCP), while similar in nature to a DRP, focuses more heavily on the restoration of the essential *business functions* required to ensure continuity of operations whereas the DRP focuses primarily on restoring critical systems and data required to *support* these business functions. A comprehensive BCP identifies potential risks, establishes contingency measures, and outlines recovery priorities to minimize downtime and maintain critical operations. Proactive business continuity planning enhances business resilience, safeguards customer trust, and helps to maintain compliance with legal and contractual obligations.

Implementation Examples

Example 1: Perform a Business Impact Analysis (BIA) to identify and prioritize critical business functions and determine the impact of downtime. Use this analysis to guide BCP development and resource allocation.

Example 2: Develop a comprehensive BCP document that outlines key business processes, critical systems, and dependencies. Include recovery priorities, personnel roles, and step-by-step procedures to restore the essential operations during various disruption scenarios.

Example 3: Identify and prepare backup facilities or remote work solutions to ensure operational continuity if primary locations are unavailable.

Example 4: Conduct regular BCP drills and simulations to evaluate the effectiveness of the plan. Update the BCP to reflect changes in business operations, personnel, or technology.

Mappings to External Controls Standards[21]

- NIST RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.
- NIST RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.
- NIST RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.
- CIS 18 v8.1 Control 17.x – Incident Response Management
    - CIS 18 v8.1 Safeguards 17.1 through 17.9 all provide guidance that is relevant in whole or in part to this control.

21 External mappings for both control MSF.04.09 and control MSF.04.10 are the same. While these controls are unique and reference different nuances in the incident response, business continuity section of this guidance, they both closely map to the same portions of the NIST CSF and CIS 18 controls frameworks

Goal – Security-Minded and Empowered Culture is Universally Accepted

A universally accepted security-minded and empowered culture serves as the backbone of a robust cybersecurity program. When every individual – leaders, employees, and partners – embrace cybersecurity as a shared responsibility, the business becomes more resilient, adaptable and capable of addressing evolving threats while taking advantage of new technology. By embedding cybersecurity into the company's core values and daily operations, a security-focused culture fosters collaboration, accountability, and proactive engagement at every level. There are several core principles underpinning this organizational culture:

Leadership Commitment

Leaders must prioritize cybersecurity as an organizational value, visibly supporting initiatives, allocating resources, and setting clear expectations for secure practices throughout the organization.

Collaboration and Inclusion

Cross-functional collaboration ensures that cybersecurity is not siloed within IT but becomes a shared goal across all departments. Every team and individual have a role in maintaining security, from operations to maintenance to fleet management.

Education and Empowerment

Regular training and awareness programs provide employees with practical tools to identify, report, and address cyberthreats confidently. Empowered employees are an essential line of defense against security incidents.

Continuous Adaptation

A security-focused culture evolves to face new challenges. Businesses should regularly evaluate risks, update processes, and incorporate lessons learned from past incidents to stay ahead of emerging threats.

A security-focused culture is more than just a collection of principles. It's a dynamic and integral part of a mature cybersecurity program. This culture enhances risk management by ensuring that employees and leaders actively identify and mitigate risks. This culture improves incident readiness by fostering an environment where cybersecurity drills and proactive planning enable the company to respond effectively to threats and incidents. This culture ensures continuous improvement through feedback loops and regular reviews of security policies. This ensures that these policies stay relevant as threats evolve. This culture boosts business resilience. The shared ownership of cybersecurity enables quicker recovery from incidents and builds long-term trust within and outside the company in the larger business ecosystem.

This culture transforms cybersecurity from an operational necessity into a shared vision, concluding this guidebook with the following goal:

A resilient, adaptive, and empowered business where security is everyone's responsibility.

Implementation Examples

Example 1: Incorporate security metrics and initiatives into performance reviews, strategic objectives, and operational plans to align individual and departmental efforts with cybersecurity priorities.

Example 2: Celebrate employees who demonstrate a commitment to security to foster engagement and reinforce positive behavior.

Example 3: Establish safe, transparent channels for reporting security concerns or incidents.

Example 4: Designate “security champions” in each department and among the driver pool to bridge the gap between cybersecurity teams and other functions, promoting best practices and addressing questions at a local level.

Additional Resources

The guidance found in this document is drawn from several cybersecurity standards, frameworks, and best practice publications. Further reading on the controls outlined herein may be found in the resources listed below.

1. Center for Internet Security. (2021). *CIS Controls v8.1* Retrieved from https://www.cisecurity.org/controls/cis-controls-list
2. Cybersecurity and Infrastructure Security Agency. (2020). *Domain-Based Message Authentication, Reporting, and Conformance (DMARC)*. Retrieved from https://www.cisa.gov/resources-tools/resources/domain-based-message-authentication-reporting-and-conformance-dmarc
3. Cybersecurity and Infrastructure Security Agency. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
4. Cybersecurity and Infrastructure Security Agency. (2020). *Incident Response Plan (IRP) Basics*. Retrieved from https://www.cisa.gov/resources-tools/resources/incident-response-plan-irp-basics
5. Cybersecurity and Infrastructure Security Agency. (2021). *Multi-Factor Authentication (MFA)*. Retrieved from https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa
6. Cybersecurity and Infrastructure Security Agency. (2021). *Enterprise VPN Security*. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a
7. *Protect your personal information and data*. (2024, July 29). Consumer Advice. https://consumer.ftc.gov/articles/protect-your-personal-information-and-data
8. Federal Trade Commission. (2016). *Protecting Personal Information: A Guide for Business*. Retrieved from https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
9. National Cybersecurity Center of Excellence. (2019). *Data Integrity: Recovering from Ransomware and Other Destructive Events*. Retrieved from https://www.nccoe.nist.gov/data-integrity-recovering-ransomware-and-other-destructive-events
10. National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
11. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
12. National Institute of Standards and Technology. (2016). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (SP 800-46 Rev. 2)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
13. National Institute of Standards and Technology. (2024). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (SP 800-171 Rev. 3)*. Retrieved from https://csrc.nist.gov/pubs/sp/800/171/r3/final
14. National Institute of Standards and Technology. (2016). *Security Considerations for Network Segmentation (SP 800-125B)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-125b/final
15. National Institute of Standards and Technology. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B)*. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

16. National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
17. National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
18. Federal Trade Commission. (2018). *Cybersecurity for Small Business*. Retrieved from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
19. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 20*. U.S. Department of Commerce. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Acronyms

ABAC – Attribute-Based Access Control

ACL – Access Control List

ARP – Address Resolution Protocol

BCP – Business Continuity Plan

BIA – Business Impact Analysis

BYOD – Bring Your Own Device

CCPA – California Consumer Privacy Act

CIS – Center for Internet Security

CISA – Cybersecurity and Infrastructure Security Agency

CMDB – Configuration Management Database

CPG – Cybersecurity Performance Goals

CSF – Cybersecurity Framework

DKIM – Domain Keys Identified Mail

DLP – Data Loss Prevention

DMARC – Domain-Based Message Authentication, Reporting, and Conformance

DMZ – Demilitarized Zone

DNS – Domain Name Service

DRP – Disaster Recovery Plan

EDR – Endpoint Detection and Response

ELD – Electronic Logging Device

EOL – End of Life

FIDO2 – Fast IDentity Online 2

FMCSA – Federal Motor Carrier Safety Administration

IAM – Identity and Access Management

IOC – Indicator of Compromise

IRP – Incident Response Plan

IRT – Incident Response Team

IT – Information Technology

MAC – Media Access Control

MDM – Mobile Device Management

MFA – Multifactor Authentication

MSP – Managed Services Provider

MSSP – Managed Security Services Provider

NIDS – Network Intrusion Detection System

NIPS – Network Intrusion Prevention System

NIST – National Institute of Standards and Technology

NMFTA – National Motor Freight Traffic Association

OS – Operating System

OT – Operational Technology

PCI-DDS – Payment Card Industry Data Security Standard

PII – Personally Identifiable Information

PKI – Public Key Infrastructure

PM – Preventative Maintenance

RBAC – Role-Based Access Control

SaaS – Software as a Service

SDN – Software-Defined Networking

SEG – Secure Email Gateway

SIEM – Security Incident and Event Management

SMB – Small to Medium Business

SOC 2 – System and Organization Controls Type 2

SPF – Sender Policy Framework

SSL – Secure Sockets Layer

TLS – Transport Layer Security

TSP – Telematics System Provider

TSRM – Telematics Security Requirements Matrix

TTX – Tabletop Exercise

VLANs – Virtual Local Area Network

VPN – Virtual Private Network

ZTA – Zero-Trust Architecture

Appendix A

Incident Response – Initial Steps

Effectively responding to a cybersecurity incident requires swift, organized action to limit lateral movement, minimize damage, and secure systems. Let's look at the first stages of an incident, from detection, through declaration of an official incident, and the implementation of an Incident Response Plan (IRP).

Establish Incident Indicators

This is a fancy way of saying that your business should have a standardized process in place for proactively monitoring logs, systems, and networks for anomalies. Ensure that you have a baseline of normal activity patterns identified. Use threat intelligence feeds and automated detection tools to identify unusual activity quickly. Educate your team to recognize phishing attempts or other suspicious activity. Early detection is the foundation of incident response, enabling faster action and limiting escalation.

Analyze and Verify Potential Threats

Assess alerts to determine their validity and severity. Correlate indicators across tools to confirm if a genuine incident is occurring. Prioritize suspected incidents based on impact, scope, and urgency. Accurate analysis ensures focus is placed on real events, avoiding wasted effort on false positives. It is important to ensure that an anomaly represents a true incident or threat to the business, prior to initiating formal incident response plans. Don't get in the habit of "crying wolf" over every alert or it will undermine the credibility of the security team in the event of a true emergency.

Contain the Incident Quickly

Isolate any affected systems to prevent lateral movement. Apply network segmentation, or disconnect compromised devices as needed and coordinate containment actions with stakeholders to minimize disruption. Containing the threat will help to halt its spread and limit further damage. However, it is critical to understand the operational impact of quarantine actions and to work to minimize operational impact wherever possible. Don't make the cure worse than the cause!

Initiate an Incident Declaration

Inform key stakeholders of the *validated* incident. Activate the incident response team and designate roles (ideally these will be clearly defined in your IRP). Record details about the attack for documentation and further investigation. A formal incident declaration ensures that the response process is fully engaged and that all key stakeholders are aware of the incident and apprised of actions to be taken.

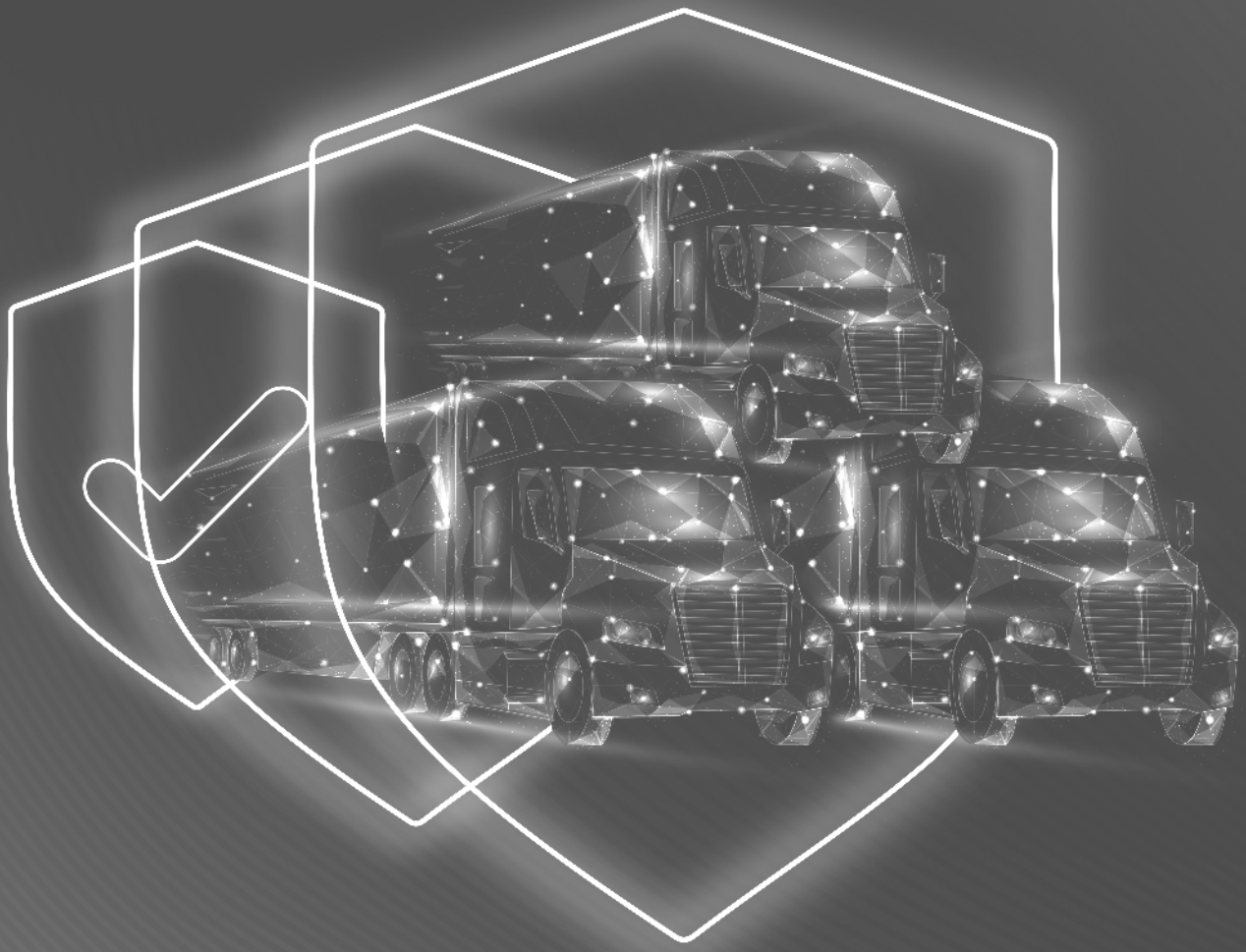
Implement Remediation Steps

Disable compromised accounts, apply patches, and remove malicious files or scripts from affected systems. The specifics of this step will depend on the nature of the incident, but the focus must be on prompt, informed actions that directly address the verified threats related to the current incident. It is important that at this stage, communication is initiated with relevant external parties (e.g., law enforcement, external vendors, etc.). Taking swift remediation action protects critical assets and reduces attacker dwell time. This is crucial to lowering the overall impact of the incident.

Document and Communicate Progress

Keep stakeholders informed about containment and remediation progress. This does not mean providing a play-by-play of every action taken but rather ensuring that all relevant parties are kept up-to-date on the status of the incident and the progress of the incident response team in a meaningful way that is relevant to their stake in the incident response process. Maintain detailed records for post-incident review and any legal requirements (evidence, legal action, etc.). Begin planning recovery actions to restore normal operations. Clear documentation will also prove invaluable in a post-incident review and supports accountability and lessons learned.

A well-executed initial response can significantly reduce the impact of a cybersecurity incident. By focusing on early detection, rapid containment, and structured communication, businesses can position themselves to mitigate risk and recover effectively. Preparation and adherence to a defined incident response process are critical to success.



NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER