Securing Legacy Maintenance Software Project

Author

Jaime Lightfoot with Lightfoot Labs
On behalf of the NMFTA

Legacy maintenance software is characterized by its inability to be updated, outdated status, or requirement of an older operating system. It's linked to the equipment utilized by a truck or fleet, often posing challenges in transitioning to newer alternatives. Moreover, maintenance software holds considerable power, being trusted by the vehicle network and connected devices to alter any configurable settings on a truck. These attributes collectively contribute to significant cybersecurity risks. The report delves into these risks and offers strategies for managing them.

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

Intro

It takes a team to get goods delivered on time– everyone from the drivers, logistics, warehouses, telematics and regulatory tracking, sales, high-level business strategy, and mechanics. Each of these areas, much like the rest of our world, has become increasingly dependent on software, and with software comes cybersecurity risk.

While many transportation companies have leveled up their cybersecurity practices in the past few years, the focus has been on back office tools, since that's where real-world attacks have occurred. Ransomware stories are in the news every week, and in the transportation business, that poses a huge threat to uptime and the company's bottom line.

Nowhere is the truck more exposed than in a maintenance facility, where maintenance laptops running diagnostic software can connect to the vehicle, and after proving authorization (e.g. correct seed/key or ECU password), can change parameters or even rewrite firmware.

Due to the need to support older model years, or wanting software that "just works", legacy maintenance software remains widely in use. This legacy software can present a cybersecurity risk, because it performs important functions such as determining diagnostic issues, logging information for maintenance or legal reasons, and tuning or updating truck settings. Maintenance software is authorized by-design to perform those actions with a cyber-physical impact (and more). If any of these activities can be falsified or replaced with malicious messages, it can be costly or dangerous to the carrier. Additionally, the maintenance laptops and facilities themselves may be left out of standard corporate policies.

The advice to "just update" is not helpful, as mechanics must support older model year trucks, or due to cost/compatibility issues with the rest of the organization. However, the cybersecurity threat still remains in the form of the trusted connections with trucks, and connections to the rest of the company's business functionality. What's a transportation company to do?

There is no one-size-fits-all fix for security issues, but the process of threat modeling can supercharge your organization's cybersecurity defenses. Threat modeling allows you to create a strategy specific to your situation, assess and prioritize risks, and take action. Better yet, the process can be used elsewhere in your business to evaluate corporate, telematics, and third-party systems.

This report provides a guide to threat modeling maintenance software, and provides practical mitigations in the areas for maintenance software, devices, networks, and people/processes.

Threat Modeling

Why do threat modeling?

Threat modeling is a way to systematically identify potential attacks against a system, and to prioritize issues based on business risk. There are various frameworks and methodologies for conducting a threat modeling exercise, but all of them can be adapted to be useful for your organization and use case. Threat modeling helps you develop and use a cohesive strategy, rather than just a handful of tactics.

NMFTA considers threat modeling a "security culture accelerator that helps organizations proactively prepare for security challenges, build defenses, and constructively prioritize security needs." Threat modeling is recommended by CISA, used by large corporations, and is the industry standard for cybersecurity professionals as they approach attacking or defending a new system.

Threat modeling can be done anywhere in your organization, though this report will focus on maintenance facilities and the legacy software often in use there.

Who is involved in threat modeling?

The threat modeling process should involve stakeholders from many different parts of the business.

While many of the changes may be implemented by IT, management and business decision makers must be involved to represent business risks and concerns.

Additionally, the end-users of the software (in this case, technicians and maintenance facility management) should be included so as to develop solutions that don't hamper their ability to fix trucks.

Legal should also be involved to evaluate contract details with third-parties, and to assess legal risk and compliance concerns.

Threats to Legacy Maintenance Software

This report is about legacy maintenance software. Maintenance software includes any diagnostic software used to troubleshoot, tune or update settings or functionality on heavy trucks. Maintenance software can be "original supplier" (from an OEM or Tier 1) or "aftermarket"/third-party.

Legacy maintenance software refers to maintenance software that cannot be updated, has reached end-of-life status, and/or that requires an older operating system. The software corresponds to the equipment in use for a given truck or fleet, which means shopping around for competing products is often out of the question. Additionally, some trucks require legacy maintenance software due to older model year ECUs.

Why be concerned about maintenance software?

Maintenance software itself is very powerful: it is trusted by the vehicle network and devices it is connected to, and can alter any configurable settings on a truck. With enough reverse engineering, it may also be used to update truck component firmware in a malicious or dangerous way. Vehicle tampering can waste driver and mechanic time, damage components, and could evolve into a new ransomware vector of "bricking" the trucks themselves.

Maintenance software and facilities may also suffer from less cybersecurity attention compared to other parts of corporate technology. It may be partially left out of an organization's broader IT security discussions because it is considered part of "OT".

Lack of security protections and updates within the software itself, coupled with older operating systems, poses an additional threat. CISA considers end-of-life software in service of critical infrastructure–of which transportation

is a part–to be the "number one bad practice"[1], especially if the software is accessible from the internet.

Types of attackers and their motivations

There are many different types of cybersecurity attackers (often called "threat actors"), and as such, their methods, skill levels, and motivations vary.

- **Financially-motivated** attackers use ransomware to extort the high-dollar (even if not necessarily high-margin) organizations into paying. Ransomware gangs are moderately skilled and target companies at scale.
- **Ideologically-motivated** hackers are called "hacktivists" and target companies who are on the "wrong" side of an issue. Skill ranges can vary from tech-savvy "script kiddies" with too much time on their hands to more sophisticated attacks.
- **Nation state attackers** are the most highly-skilled and well-funded group. Transportation is part of our nation's critical infrastructure, which is why CISA, DHS, and TSA have worked to provide resources to find and address vulnerabilities. Nation state groups or APTs may target the trucking sector as a way to enact terrorism, disrupt the supply chain, or generally sow chaos and distrust.
- As with most industries, there's always the possibility of an **insider threat** via disgruntled employees.

Known Attacks and Threats

Currently, there are no publicly known examples of the trucks themselves being hacked. However, there are plenty of examples of trucking companies' enterprise and backend systems being targeted with ransomware, as well as many examples of truck- and automotive-hacking research that demonstrate the possible effects of what an attacker could do with unfettered diagnostic access.

Truck Hacking

Existing research shows what can be done with diagnostic and/or vehicle bus access:

- CANBusHack research[2] showing triggering of engine derate (vehicle disable or limp mode) via J1939 messages and NMFTA research showing similar effects by DEF message manipulation.
- A 2016 DEFCON presentation[3] demonstrates how a maintenance computer with a malicious RP1210 shim could change engine settings without the technician's awareness, with a small amount of reverse engineering effort.
- Another 2016 research effort[4] from University of Michigan shows that reverse engineering J1939 or diagnostic messages were easily reverse engineerable, and that diagnostic software settings could cut off engine cylinders, or cycle ABS pressure valves. This research also demonstrated that J1708/J1587 diagnostics require no authorizations and the vehicle diagnostic adapters (VDAs) connect to these diagnostics buses as well, on older trucks.
- A 2023 DEFCON presentation[5] showed how easy it is to tamper with vehicle diagnostic adapters, another tool in the chain of vehicle maintenance.

The same attack vector of infecting maintenance laptops to affect trucks at scale was also shown on passenger vehicles (Volkswagen), where researchers in 2015 tampered with a diagnostic application library to silently disable airbags.[6] Plenty more research has been done in passenger vehicles on other remote and/or trusted CAN bus access, including connected insurance dongles[7], dealership diagnostic tools[8], and in vehicle immobilizers[9].

1 https://www.cisa.gov/stopransomware/bad-practices
2 https://ioactive.com/guest-blog-urban-jonson-nmfta/
3 https://www.youtube.com/watch?v=PDIkcKtkeOE
4 https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf
5 https://www.youtube.com/watch?v=yX0_e4Szn5s
6 https://blog.crysys.hu/2015/10/hacking-cars-in-the-style-of-stuxnet/
7 https://www.securityweek.com/researchers-hack-car-insurance-dongle/
8 https://www.wired.com/2015/10/car-hacking-tool-turns-repair-shops-malware-brothels/
9 https://www.engadget.com/2015-08-14-car-immobilizer-easily-hacked.html

These research efforts show the extent of what can be done with vehicle bus access, such as through a maintenance laptop. Tampering with settings can cause longer downtime for trucks being repaired, or further waste driver and mechanic time by changing settings (such as governing speeds), causing the vehicle to limp back for repair. Coupled with remote access through laptops or always-connected diagnostic units, vehicle tampering could theoretically be done at scale and become a new form of ransomware.

Ransomware

Protecting maintenance software, devices, and facilities can help protect against vehicle tampering attacks. It also helps protect against ransomware, which is a top concern for many trucking companies.

In Sophos' 2023 report[10] 63% of respondents in transportation said they had been hit by ransomware, and 45% of that group said they lost "a lot" of revenue to the attack.

Ransomware in the realm of maintenance facilities can lock up computers, slowing down repair time. Infected maintenance devices can also be a vector into other areas of the company.

Ransomware can have downstream effects on other areas of concern for fleets and carriers, such as **regulatory compliance**. One ELD provider (Orbcomm) was hit with a ransomware attack in September of 2023[11]. With their cloud systems unavailable, Orbcomm customers had to use paper records, and eventually had to seek an FMCSA waiver as the outage dragged on. In another industry, a ransomware gang further extorted their victim by filing a cyber incident report to the SEC against an organization who refused to pay up.[12]

Ransomware attacks do not just affect big players. It's not a matter of being "too small to matter", because ransomware gangs often operate by volume, targeting as many companies with exposed, vulnerable software as possible. The mitigations in this report will help organizations defend against ransomware and vehicle tampering threats, as well as develop plans to more quickly recover.

Threat Modeling Maintenance Software

They say you don't know what you've got until it's gone, but in the world of software, you don't know what you've got until it's hacked. Threat modeling aims to prevent that by enumerating all the assets in scope, and the connections and dependencies between them. After enumeration, threats are ranked by business impact, and mitigations are enacted.

Within the world of maintenance software, enumeration means taking stock of all software and hardware in use. These assets include:

- The maintenance tools themselves (OEM and aftermarket)
- Supporting libraries, drivers, and DLLs including RP1210 DLLs
- Other supporting software tools on the laptop like business or security software;
- Licenses
- User accounts and credentials
- The operating system
- The physical hardware (laptops and VDAs)

In short, this covers anything that must be managed or updated, and any valuable information or access that must be protected.

10 https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
11 https://www.ttnews.com/articles/orbcomm-ransomware-attack
12 https://darkreading.com/cyber-risk/hackers-weaponize-sec-disclosure-rules-against-corporate-targets

Connections between all of the parts are mapped out in terms of data and workflows. What data is entering or leaving a laptop or tool via the internet, wired connections, or local networks? What workflows exist to protect access to a given resource? Specific to maintenance environments, this includes:

- Data flow to/from maintenance software to the internet, including licensing servers, update checks, analytics, and firmware downloads
- Data flow to/from maintenance software through RP1210 DLLs and other device drivers to the VDAs and eventually to the trucks
- Data flow to/from other laptop software to the local network (for example, file shares or printers) or externally (email, online portals, general internet browsing, etc).
- Physical access like the availability of USB ports and access to the laptop itself by maintenance technicians, and anyone else in the maintenance area.

When mapping data flow, consider that it can extend outside the maintenance part of the organization, into other IT-managed areas. Something not specific to maintenance laptops, but still relevant to the threat model discussion, is the domain registration of the laptop. Because ransomware is an extant threat, it's reasonable to assume that attacks on maintenance laptops and software could originate in the typical IT-managed domain. The attackers will have motivations to pivot from IT over to the maintenance laptops because of the increased impact. The maintenance laptops have frequent connections to high-impact operational technology (OT) and largely unpatchable systems (trucks); making this area much higher-risk. As such, our threat model–and later mitigations–will cover data flow in all areas, including IT management and segmentation.

Here is the result of such enumeration in an example maintenance scenario:

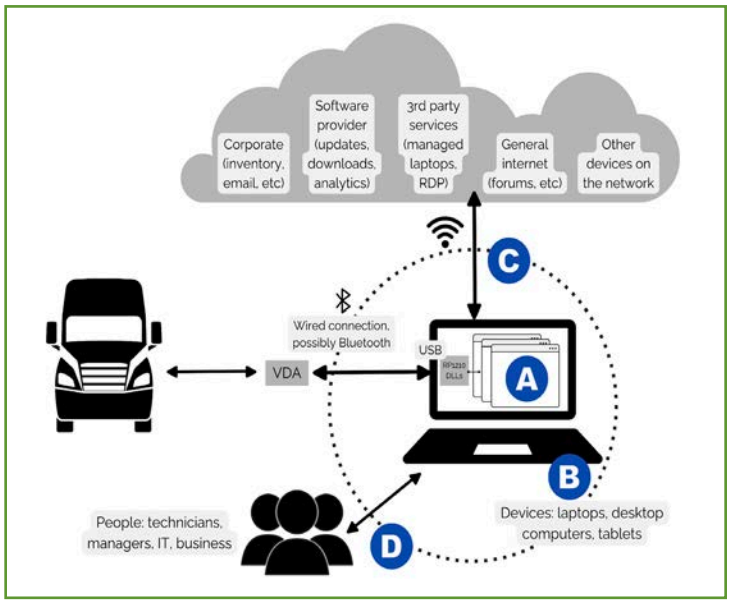

Figure 1

Each software program and data flow path in the threat model serves a business purpose. A computer system that allowed no access would be useless. But at the same time, each connection into or out of the threat model represents a method for attackers to gain access, leak information, or otherwise negatively influence the behavior of the maintenance environment. These exposed parts are what must be protected and monitored.

With an understanding of what is potentially exposed (the "attack surface"), the next step is to rank security risks by business impact. Everything is a tradeoff, and in the world of cybersecurity, businesses must balance security, productivity (of technicians), and cost.

Finally, organizations must enact mitigations. This is not a one-time event but instead a continuing effort that helps them better prevent, respond to, and recover from cybersecurity threats.

Mitigations

Enough about the threats and problems, how do we fix them? This section will be split into four sections, reflecting each of the four labeled areas in Figure 1:

These buckets are:

A. **Software:** The legacy maintenance software itself, and accompanying RP1210 DLLs.

B. **Devices:** Primarily laptops and desktop computers. This includes the operating systems, configurations, supporting software tools, and physical security

C. **Network:** This includes both the security of the wifi network that devices are connected to, firewall settings, and external connections to or from the computer or LMS.

D. **People and processes:** Including training, incident response plans, and other business tasks to support maintenance security at a high level.

Software

This section covers security controls within the legacy maintenance software (LMS) itself. LMS refers to maintenance software that has reached end-of-life status, or does not receive regular updates for other reasons. This software includes both original supplier (OEM and Tier 1) products, and aftermarket/third-party products, that support heavy vehicle maintenance, tuning, and other troubleshooting.

It's likely that maintenance devices will run many maintenance software products to support the trucks being serviced, including a mix of legacy maintenance software and more up-to-date software.

This report is focused on the risks of legacy maintenance software, but not all suggestions in this section may be feasible for all tools. Apply what you can and layer on other mitigations from the Device, Network, and People/Process sections.

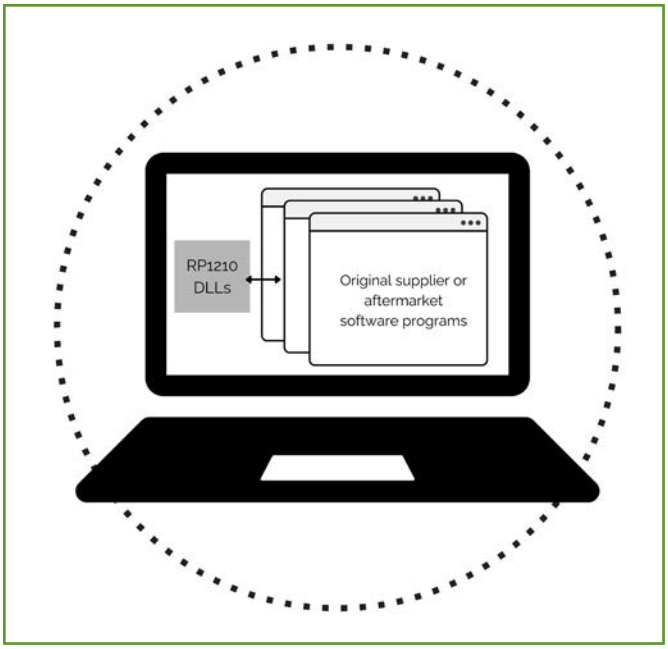

Figure 2

Regularly Update Maintenance Software

Why: Regularly updating any software gives end users new features, fixes bugs, and patches security issues within the tool itself or in the supporting libraries. In the case of LMS, updating software may also allow for more up-to-date operating systems to be used.

Updates are not always possible (such as for end-of-like products) but regularly updating and patching helps protect against exploits, including those developed from patch diffing the days and weeks after an update is released.

Who is involved: IT personnel should be responsible for tracking available updates, prioritizing them based on security concerns, and getting the updates in place. IT personnel will need to work with maintenance technicians to make sure updates are rolled out in a way that doesn't disrupt maintenance schedules.

How to implement: IT and maintenance can work together to collect a list of software in use, and current versions. Sourcing may also need to be involved, to help IT find vendor contacts. Once downloads have been identified from a known-good source and verified, save copies for future installations and backups. Prioritize any release notes that mention "security updates".

Test the updated software on a single laptop, with a mechanic, to make sure that it works as expected (and does not require rolling back to the previous version for usability reasons) before updating the rest of the laptops. Update the asset management system with the new version. If possible, work the update process into the overall IT patching schedule.

Run LMS as a Low-Privilege User

Why: If software is compromised (such as through an arbitrary file read or RCE), the attacker is granted the privileges of the user originally running the software. If the original user is an admin user, then the attackers are not restricted in any actions they want to take. They can add users, modify the system, disable endpoint protection, and so on. On the other hand, if software is compromised but runs as a low-privilege user, the attacker must continue working to find a way to elevate their privileges.

In other words, running software as admin lowers the required skill level of an attacker to successfully compromise your system. By itself, running as admin is not exploitable. But coupled with another vulnerability, it significantly raised the impact of a hack, because the attacker can modify the environment to their choosing.

Who is involved: IT personnel should implement these fixes. If software is not able to be run as a lower privilege user, business decision makers may need to work with the software vendor, or discuss other options with IT.

How to implement: Install the software as a non-admin user, likely under the account of a mechanic or technician who is not a local admin (which can be determined with Powershell command "Get-LocalGroupMember administrators").

Most software reviewed by NMFTA during this project did not need admin privileges. If a program does require admin privileges, you can use `procmon` to determine what specific privileged actions a program is trying to do, and potentially make modifications so that the program runs. Microsoft's Standard User Analyzer[13] tool can be used to troubleshoot UAC issues on Windows 7 and Vista operating systems. There are also tools available to handle admin privilege requirements at scale, such as PowerBroker and Beyond Trust.

Use Unique, Complex Passwords and MFA Where Applicable

Why: If maintenance software allows for the setup of different user accounts, and/or uses a portal for updates or other information, then a unique account should be set up for each user, along with a non-guessable password. Having individual accounts let you better determine attribution if something were to be breached.

Likewise, implement multi-factor authentication (MFA) for any login that is publicly accessible such as an online portal. MFA can significantly reduce the threat of brute-forcing attacks, where an attacker can repeatedly attempt to login based on publicly scraped user data (from sources such as LinkedIn) and password dumps. Deloitte reports that 80% of breaches[14] involved weak or bad passwords that could be guessed or brute-forced. Assume that attackers will be able to find or guess username data from LinkedIn or other publicly available sources.

Uptime is of crucial importance within the world of trucking, and security controls such as complex, unique passwords and MFA can

13 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/cc838047(v=ws.10)
14 https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

undermine that. Use a password manager so that passwords can be stored securely and accessed easily, requiring employees to only remember the master password in use.

Who is involved: IT, in coordination with maintenance to weigh uptime vs security concerns.
How to implement: With a list of software in use (through Asset Management), identify which tools allow for individual logins. Identify which accounts, if any, correspond to an online portal login and prioritize these as having complex passwords, and MFA.

To determine if an email username or password has been found in a previous breach–meaning that it will likely be used in brute-force attacks–check haveibeenpwned.com. Also consider using password managers to allow for easy usage of complex passwords while only requiring users to remember one master password. This can help prevent the use of guessable passwords and/or passwords stored in plaintext.

Have Known Good Copies of Software Tools

Why: Downloading and installing software under schedule pressure is an opportunity for accidentally downloading malicious maintenance software. If maintenance software is downloaded and vetted from the original vendor, this can be saved as a known-good or "gold" copy and reduce the risk of a future malicious download. It will also help commission new devices faster.

Who is involved: IT is responsible for finding the reputable source of the software and downloading and vetting it. IT will need to work with the maintenance technicians to determine the full list of software in use, as well as communicate with contracts/sales for any new software. IT must also make this software easily and safely accessible within corporate rules if maintenance technicians are allowed to install or update software.

How to implement: After determining the software in use and the current versions, IT can work with maintenance and sourcing/contracts to find the software vendor information. After downloading the software from the official source, they can validate it through checksums and signing details, and then store it on a network drive and/or offline backup.

Ideally, IT is responsible for software installation and updates on computers. But if maintenance technicians are able to install software, they should be given documentation on where to find the known-good copies. This mitigation should be coupled with the mitigations about restricting downloads and installations onto maintenance devices, such that all software installations follow this practice and use the known-good software.

Given the cost of maintenance software licenses, it's likely that the software copies will only be used in rare events such as emergency re-provisioning of devices. These software copies should be included in the incident response plan (likely as an offline copy) and also as part of the asset management system.

Ensure that LMS Has Not Been Tampered With

Why: Once a software tool is installed from a known-good, reputable source, you want to make sure that it has not unknowingly changed or been switched out beneath you. Such changes could jeopardize vehicle security.

Who is involved: IT

How to implement: This can be done with built-in Windows Tools such as AppLocker or its successor, Windows Defender Application Control (WDAC). Other software products may also include allowlisting capabilities. These tools allow an administrator to make a list of what applications may be run, and all other programs (including malware and viruses) will be denied execution. This is often called allowlisting or whitelisting.

Programs may be added to the list by signing or publisher details, hashes, or other information. If an application is not signed and must be added to the allowlist via a less secure AppLocker method (like file path), make sure that the regular

user accounts do not have write access to the applications or DLLs. This will likely require a separate account for updates. WDAC also allows for allowlisting based on the parent process or its managed installer[15]. Allowlisting should also include the RP1210 DLLs, which will be covered in the next section.

Application allowlisting is not always a great option for IT network environments, because end-users may need a variety of programs unique to their role in the company, and may need new programs to be installed from time to time. However, if the maintenance facilities in your organization have a fairly stable list of required programs, this can be a good way to only allow pre-approved programs to run. Ideally, this list of pre-approved programs should be limited to maintenance software programs only. If possible, maintenance laptops should not be used for day-to-day business functions. This is a part of separating IT systems from OT systems (trucks, docks, etc) – see later mitigations for more details.

These controls must be done without giving end-users local admin accounts, as these privileges allow a user to delete the WDAC/etc rules, effectively bypassing any protection.

Windows also offers protections against memory corruption exploits through EMET[16] (Enhanced Mitigation Experience Toolkit) in Windows 7, and now Windows Defender Exploit Guard[17] (WDEG) in Windows 10 and 11. This gives Enterprise Windows builds the ability to enable memory corruption mitigations like DEP or ASLR "underneath" the program without vendor involvement. This can potentially make them a good tool for legacy software, but it may cause stability issues in some cases and should be tested with the help of maintenance. Several of these tools may also require applications and DLLs to be signed, which is not always the case with maintenance software. Finally, ASLR is a far less effective mitigation on 32-bit binaries when compared to 64-bit binaries, as only 8 bits of the address can be randomized (compared to 17-19 bits of a 64-bit address)[18]. As such these protections should be approached with caution on older maintenance software, and combined with other mitigations.

Enable Application Allowlisting for RP1210 DLLs

Why: RP1210 is a recommended practice ("RP") developed by TMC to standardize communication through vehicle diagnostic adapters to maintenance software. This standardization allows any software program that implements the RP1210 API to work with any RP1210-compliant VDA.

All diagnostic traffic is handled by RP1210 DLLs, so if they are tampered with, then the diagnostic messages can be falsified, and/or malicious commands can be sent. All of this can happen without any technician interaction after the malicious, replacement DLL ("shim DLL") is placed in the correct directory.

How would this happen? Via a common malware attack method known as "DLL shimming". DLL shimming including a demo attack and code samples will be included in an RP1210 demo, but in short, a DLL can be written and placed ahead of the correct DLL in the search order, sometimes without admin privileges. This DLL can machine-in-the-middle (MitM) the traffic going to or returning from the vehicle diagnostic adapter, while otherwise allowing normal operation of the maintenance programs. DLL shimming can be mitigated by a combination of restricting user permissions, and application allowlisting.

15 https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/wdac-and-applocker-overview#windows-defender-application-control

16 For mitigations available from each Windows version, see page 10-11 of https://www.marcelosincic.com.br/blog/file.axd?file=2010%2F9%2FUsers+Guide.pdf

17 https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exploit-protection?view=o365-worldwide#mitigation-comparison

18 https://mandiant.com/resources/blog/six-facts-about-address-space-layout-randomization-on-windows

Who is involved: IT

How to implement: Full mitigation steps, including a walkthrough of configuring AppLocker, can be found in the RP1210 demo guide.

DLL shimming makes use of search order hijacking, which is a misuse of Microsoft's backwards compatibility feature to look in several locations for a DLL. This is a predetermined list of locations[19]. If a user-writable location is ahead of the real location of the DLL, a malicious shim DLL can be placed there. This will most likely be the application directory of a given maintenance software program, so lock down permissions in all maintenance software directories. DLL lookup order can be determined with SysInternals tools like Process Monitor ("`Procmon`") or Process Explorer.

However, maintenance applications could be copied elsewhere that a user has write access to (with the desktop shortcut updated to the new location). Therefore a complete mitigation of DLL shimming threats must include application allowlisting, which makes use of AppLocker, WDAC, or another software product to only allow execution of predetermined, known-good applications and DLLs. These applications and DLLs can be specified in a number of ways. The most convenient and secure is through a Publisher rule, which checks a file's signature information. If the file is updated (but is still signed), the rules do not need to be updated, which is not the case for allowlisting rules based on file hash. Application allowlisting should be done first in audit mode, to allow IT to monitor events over time and modify rules before having strict enforcement. This will help protect uptime and reduce rollout headaches.

As mentioned previously, a full walkthrough of a DLL shimming attack and mitigation can be found in the RP1210 demo guide.

Implement Asset Management for Which Tools, Versions, and Licenses Are In Use

Why: It's hard to know what to protect if you don't know what you have. Taking stock of what software programs (LMS and otherwise) are in use can help you respond faster to news of a vulnerability or breach. The practice of tracking assets in use is the basis of many other mitigations as well.
Who is involved: IT, with help from maintenance

How to implement: Track which maintenance software is in use on each laptop. This includes the product name itself, version number, licenses, any corresponding logins, and vendor emails and contact information if applicable. If a vendor email is known, see if vendor alert emails are available, and if so, signup with an email group that includes relevant IT personnel, maintenance managers, etc.

The usefulness of software asset management depends on how well understood the organization's threat model is. For example, knowing which products have internet connectivity can help IT prioritize security advisories when there is more work than available time to do it in.

There are many solutions on the market for asset management systems, including many that are expensive and/or complex. One way of determining what information would be actually useful to store in a management system is to go through recent IT tasks, as well as any scenarios brought to mind by table-top exercises (see Incident Response), news stories, or this report, and then make a list of what documented information would either be crucial or helpful in addressing the problem, responding faster, etc. This can let you start simple and build out a list of needs before purchasing a solution.

Devices

Some legacy maintenance software programs cannot be updated or replaced with an alternative. This means that the next layer of mitigations start at the device level. Here, devices refers to laptops, desktops, tablets and

19 https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-security

smartphones. Legacy maintenance software will most likely be running on laptops and desktops, but tablets, smartphones and VDAs will be briefly covered here as well.

This section covers the security of these devices outside of the legacy maintenance software itself. Security of network connections will be discussed in the next section.

The goal is to have maintenance devices regularly updated and with permissions and tooling limited to only what is strictly required for maintenance. Extra tools and usage (such as email) should be done on a laptop without vehicle access.

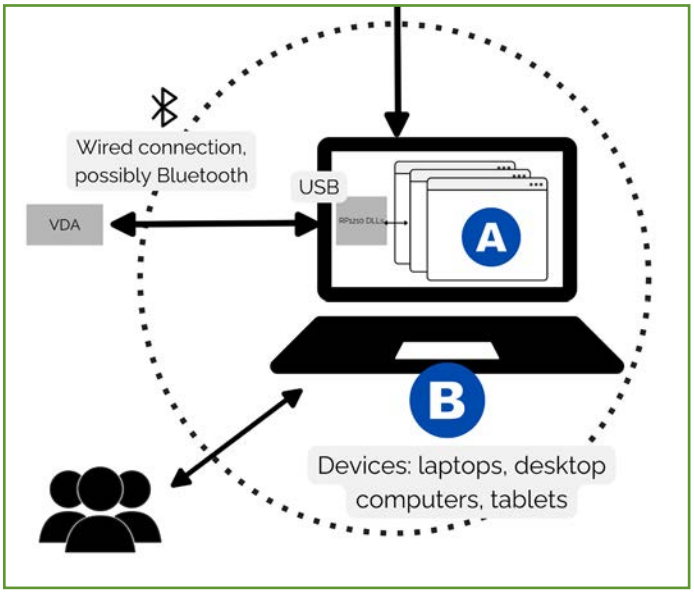

Figure 3

Update to the Latest Operating System and/or Latest Patches

Why: Some LMS products run on older versions of Windows, including those that have reached end-of-life status.

Lack of regular security updates from the original vendor makes outdated OSes a valuable target for attackers, who continually scan for legacy systems and software[20]. The FBI warned in mid-2020 about the usage of Windows 7[21] (which had been designated as end-of-life in early 2020), stating that it saw obsolete operating systems as a pattern in healthcare cyberattacks, which was of particular concern in 2020. Windows 8.1 also reached end-of-life status[22] and stopped receiving updates as of January 2023. Windows 10 will reach end-of-life status in October 2025, though the company has hinted at providing updates past that date, at an additional cost[23].

The security risk is not just in the operating system itself, but in the lack of security tooling updates. If your organization's maintenance laptops rely on built-in Windows tools, they will not receive updates if the operating system has reached end-of-life status[24]. Tools such as Microsoft Defender rely on signature-based detections, and lack of updates render the tool much less effective.

Who is involved: IT

How to implement: After identifying what software products are in use via the Asset Management mitigation, identify which products allow you to update to a newer operating system. The majority of tools evaluated by NMFTA during this project were able to run on Windows 10 or newer; in some cases with UAC virtualization enabled.

Patch management can be done at scale through mobile device management (MDM) remote monitoring and management (RMM) tools, allowing it to be included in corporate device patching schedules.

20 https://computerweekly.com/news/252501287/Legacy-vulnerabilities-may-be-biggest-enterprise-cyber-risk
21 https://s3.documentcloud.org/documents/7013778/FBI-PIN-alert-on-Windows-7-End-of-Life.pdf
22 https://support.microsoft.com/en-us/windows/windows-8-1-support-ended-on-january-10-2023-3cfd4cde-f611-496a-8057-923fba401e93
23 https://techcommunity.microsoft.com/t5/windows-it-pro-blog/plan-for-windows-10-eos-with-windows-11-windows-365-and-esu/ba-p/4000414
24 https://www.crowdstrike.com/blog/security-compromise-that-comes-with-windows-10-end-of-support/

If the software products in use do not allow you to update to a more modern operating system, severely limit internet connectivity via mitigations in the Network section of this report.

For software products that do allow a modern OS version (Windows 10 or newer), make sure you have a backup of the devices and/or known-good copies of all software in use, along with any modifications made. Test out an upgrade on a separate laptop in order to not affect technician uptime.

Do Not Give Users Unnecessary Admin Privileges

Why: Giving users admin privileges defeats many other security controls, as it can allow them to bypass security controls, install or run software, modify network or user settings, and more. One study claims that between 85-94% of critical exploited vulnerabilities could be avoided by removing local admin[25].

The earlier section on not running software as admin protects against a scenario where the LMS software or other software is exploited (such as through a memory corruption bug) and then used to escalate privileges, or compromise connected trucks or networks. Giving users admin privileges allows them to modify device settings to make the potential impact of LMS exploitation much bigger. It also allows for unattended laptops or laptops compromised remotely through other vulnerabilities to have LMS and supporting DLLs modified, or to spread malware into other areas of your business.

Who is involved: IT, in consultation with maintenance

How to implement: Work with maintenance to determine if administrative rights are required for any programs or tasks. Use tools like **`procmon`** or PowerBroker to investigate and resolve individual maintenance programs that need admin privileges. Then restrict any occasional admin capabilities to a trusted user (such as a shop manager). Ideally, no one has local admin privileges, and the ability of regular users to install and/or run software is limited through group policy and an application allowlist. Any admin privileges that have been granted should be regularly reviewed in an auditing process to prevent "privilege creep".

Remove or Restrict Tools That Are Not Needed for Maintenance

Why: Each tool that is running on a device is a potential vector for cybersecurity threats. This is especially true for software that has internet access and is in popular use, as more security research is focused on it.

Ideally, maintenance laptops should be used for maintenance functionality and nothing else, meaning that other business functionality (emails, portals, etc) and general internet browsing happens on another device that is not used for vehicle connections. This reduces the attack surface for these devices that have trusted vehicle access.

Who is involved: IT

How to implement: Review all installed software by using the Apps & Features view in Windows or with **`winget list`**[26]. Go through the list with maintenance personnel and determine which software is not used. Remove any old or unused software, along with any supporting software (updaters, drivers, databases, etc.).

If possible, move business functionality and other non-maintenance tools to a separate computer entirely, and reserve maintenance laptops for vehicle access purposes only.

25 https://computerworld.com/article/3173246/94-of-microsoft-vulnerabilities-can-be-easily-mitigated.html
26 https://learn.microsoft.com/en-us/windows/package-manager/winget/list

After removing any non-maintenance or other required software, restrict needed-but-risky tools such as Powershell. Any software left on the device must be regularly updated, preferably in an automated fashion through a mobile device management (MDM) or remote monitoring and management (RMM) tool.

Review scheduled tasks as well. Use Windows privilege escalation checklists[27] as a starting point for what tools or processes might be abused to gain SYSTEM privileges (for example, Powershell). Review open ports and interfaces and disable those not in use, such as IPv6.

Restrict physical interfaces, such as by disabling Bluetooth or restricting USB ports by device identifier (restricting to only approved VDAs). USB restrictions can be done with group policy. If USB functionality is occasionally needed, it can be restricted by user. USB port usage can also be covered by EDR or AV controls. In either case, USB restrictions need to be balanced with the needs of maintenance technicians.

Lastly, CISA provides hardening reference images[28] to compare your servers and devices against, and a list of vulnerabilities known to be exploited[29].

Have Separate User Accounts for Devices (With Strong Passwords and MFA)

Why: Have separate user accounts for each maintenance technician. This allows IT to manage permissions at an individual level (i.e. not give someone elevated privileges just because the login is shared with someone more senior). It also allows IT to better manage access if an employee leaves the company. Additionally, if a single login is shared across many devices, someone with physical or remote access can then easily compromise additional devices.

In the event of a stolen laptop or other unintended physical access, a strong password can help prevent an attacker from getting access (though this should be coupled with other mitigations like having an encrypted hard-drive, secure boot, and other hardware-level mitigations).

Who is involved: IT

How to implement: Make a list of all technicians and set up individual accounts for them. Enforce password complexity through group policy[30], and keep tabs on passwords that have been found in breaches through tools like haveibeenpwned.com.

Consider using a MFA option like Duo to further restrict logins.

Use Endpoint Detection and Response (EDR) and Anti-Virus Solutions

Why: there is no shortage of cybersecurity companies offering EDR products, sometimes marketed as a silver bullet. While there is no such thing in security, EDR products can serve as a first line of defense, and allow for device and file scanning, USB restrictions, malware prevention, monitoring, and firewall settings all in one.

Anti-virus often has simpler detection and response mechanisms, and functions largely on its own. EDR products are typically part of a larger system that allows for centralized monitoring, as well as forensics or after-the-fact reporting. Many of the mitigations discussed in this report, including filtering traffic, closing unneeded ports, and allowlisting applications can be done within an EDR system.

Who is involved: IT and business leaders (for fund allocation)

27 https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation
28 https://www.cisecurity.org/cis-hardened-image-list
29 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
30 https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

How to implement: It's likely that most organizations reading this report already have an EDR system in their corporate IT space. This can be extended to cover maintenance laptops as well. If not, make a list of required functionality for an EDR (ability to scan files, USB port restrictions, firewall settings, etc) and the number of devices that need to be protected, in order to develop a budget. Compliance or audit requirements may necessitate a third party EDR or AV solution but Windows Defender can be used "for free" with the operating system otherwise. Make sure that the EDR receives regular updates for signature-based detection, and that any changes made to endpoint settings are checked through regular audits.

Ensure Physical Security of Devices

Why: Many corporate IT security policies focus on protection from remote threats that arrive via phishing, malicious downloads, and exploits. This is partially because there is a degree of physical security in most office settings. Employees must badge in, there may be double doors to prevent tailgating,[31] and so on.

Maintenance facility may not have the same level of physical security. In fact, bringing trucks in requires outside people to be allowed in the facility, and laptops may also need to be moved around for technician ease. Laptops may even be taken on the road for roadside repairs.

A physical security breach can allow an attacker to steal data, install malware or keyloggers, or access connected systems or networks. It may also just be simple theft, resulting in the loss of a laptop or other device.

Who is involved: IT, with consultation from maintenance.
How to implement: As with many of the other recommendations in this guide, physical security controls need to be balanced with technician needs. At a minimum, maintenance devices should not be taken home or to other non-work-related locations. Laptops should not be left unattended around guests, and should be locked or switched off when not in use. Use full disk encryption such as through BitLocker, and enable secure boot settings.

Lack of physical security controls may be partially compensated for with other mitigations, for example locking down USB port usage as part of removing unnecessary functionality or EDR. Consider physical security for smaller devices as well, such as VDAs and any mobile devices in use. Keep VDAs locked away when not in use, and use authentication for mobile devices).

Lastly, the physical security of the maintenance facility itself should be evaluated. including access keycards, limiting who is allowed in the maintenance areas (non-employees), restricting access to servers or network ports, using locks that are difficult to lockpick, and so on.

Only Use Known-Good VDAs

Why: While vehicle diagnostic adapters are somewhat outside of the scope of this report, their security should also be considered along that of the devices running LMS. If one of the goals of protecting legacy maintenance software is to prevent damage to trucks, VDAs are a crucial link in that process.

In 2023, Dr. Jeremy Daily and Red Balloon Security demonstrated how easy it was to modify the firmware of a VDA[32]. Their example showed how this could be used to patch VDAs to remove attack surface, but a more malicious scenario is also possible: modifying a VDA to tamper with information coming from or going to an ECU.

Who is involved: IT and maintenance

How to implement: While modifying VDA firmware to remove unnecessary functionality is likely outside of the interest of most maintenance facilities, the potential risk of leaving VDAs

31 https://www.mcafee.com/blogs/internet-security/what-are-tailgating-attacks/
32 https://www.engr.colostate.edu/~jdaily/presentations/2023%20WCX%20VDA%20Paperwith%20Red%20Balloon%20Security.pdf

unattended, or using outside VDAs should be understood. VDAs should be stored securely when not in use, and should be tracked so that only company-owned VDAs are in use by technicians.

Additionally, organizations should only purchase VDAs from the suppliers, rather than buying used equipment off of Ebay.

Take Regular Device Backups

Why: Known-good software copies were discussed earlier in this report. While these can be useful for installing or reinstalling individual programs, it is also useful to have a complete laptop copy in the case of device damage, theft, or a cybersecurity incident.

Backups are already a crucial part of IT security, so this report won't belabor the point further. However, be sure that all devices (including those that don't fall under the typical corporate IT umbrella) are included in backup plans.

Who is involved: IT

How to implement: Talk to maintenance and make a list of all devices (laptops, tablets, VDAs, etc) in use and include these devices in a regular backup schedule. As with all backups, testing the restoration process ahead of time is important. Also integrate the backups into the incident response plan discussed in the "People and Processes" section of the report to make sure that you have what you need available offline in the case of ransomware, etc.

Device Asset Management

Why: Asset management was discussed in the Software section to keep track of LMS software products and versions in use. It should be extended to include devices in use, along with their operating system version and patch status, login information, and any other relevant information.

Who is involved: IT

How to implement: Make a list of all devices in use, including laptops, tablets, mobile devices, and VDAs. Make note of related user accounts, operating system versions, patches, network information, and anything else that will help you quickly identify what devices need attention in the event of a critical vulnerability, network breach, or other incident response scenario.

Questionnaire for External Vendors

A questionnaire for evaluating external managed device vendors is included in the Appendix.

Network

A maintenance laptop, even with mitigations applied at the device and software level, may still be risky from a cybersecurity perspective. With the exception of malware introduced via USB, most dangers will enter (or exit) the maintenance laptops via the network. As such, network-related controls (even if the controls themselves happen at the device level) are of crucial importance.

As such, limiting its network connectivity and isolating it from other company functionality is the next layer of mitigations. The goal is to isolate a device's network connectivity to only that which is strictly required for maintenance functionality.

This section includes the security of the wifi network that devices are connected to, threats from the internet in the form of emails, downloads, etc, and what other devices or systems are accessible from the maintenance laptops.

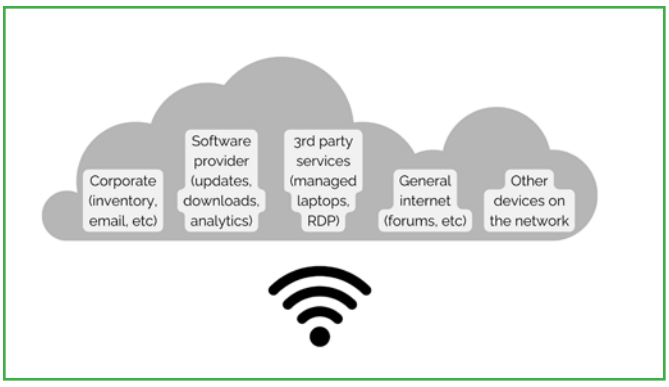

Figure 4

Segment Your Network to Isolate Maintenance Devices from Other Business Functions

Why: In the case of maintenance laptops with shared passwords and maintenance software that can't be updated, the safety of the endpoint can't be guaranteed. As such, these risky devices should be isolated on their own network segment (in addition to the earlier software- and device-level mitigations).

This is especially true for remotely managed or accessible devices, as was the case in the recent Target hack, where their payment network was breached through external access given to their HVAC contractors[33].

Who is involved: IT and maintenance managers.

How to implement: Because maintenance facilities are often a separate physical location than the rest of the organization, these devices may already be on a separate network. However, IT should work with maintenance to identify all laptops that need internet connectivity, and create a separate network for them. This network should be for these devices only, and not allow other devices such as personal smartphones, office printers, or non-maintenance computers. They should have limited access to network shares, especially those that are not necessary for maintenance work.

If possible, use your RMM, MDM, or other security tooling to prevent maintenance laptops from joining other, unauthorized networks. Also consider using access point isolation to prevent devices on this network from communicating with one another, if this does not cause maintenance functionality to break.

This, along with the rest of the network mitigation steps, will help limit access and connection to important networks. Treat traffic coming from this network with suspicion and use firewalls and other tools to detect and mitigate threats.

Ideally, the segmentation would be implemented in two ways. First is by the separation of In a Windows Active Directory (AD) environment, this means the maintenance laptops should have log-ins and all other credentials managed in their own Active Directory Tree, with no trust relationships between it and the usual IT tree. This is the best practice recommended by ISA/IEC/ISO 62443 [34]and also by SANS' ICS 410[35].

Enforce Wifi Security Practices and Limit Network to Maintenance-Related Devices

Why: Typically, IT security practices look at defending the perimeter of a network from outside threats. However, a compromised device on the network could attack a maintenance laptop laterally. One way to prevent this is by enforcing good Wi-Fi security practices.

Who is involved: IT

How to implement: The previous section discussed isolating risky devices on their own network segment, away from other business functionality. This network should be for maintenance devices only, meaning that the password should not be shared with employees for use on other laptops, computers, or personal devices.

Make sure that any wifi network available to truck drivers or guests is a separate network from the maintenance device network. Likewise, the devices should not connect to other networks besides the designated, secure network (this includes preventing hotspot usage unless specifically allowed for roadside maintenance). If possible, enforce these restrictions programmatically.

The maintenance wifi network should also have a strong password, use modern wireless encryption standards, and be configured to hide the SSID.

33 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
34 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
35 https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

Configure Firewall to Default-Deny Traffic and Allow Only Needed Connections

Why: the previous two sections discuss putting maintenance devices on a separate network, and then protecting that network through good Wi-Fi security practices, and preventing guest devices. This section is about limiting inbound and outbound connections further, through the use of firewall rules.

The goal is to have maintenance devices used for only maintenance functionality, as vehicle access is a potential attack vector. Keep regular browsing and business functions on a separate device.

Who is involved: IT, and maintenance

How to implement: For this section to be done well, IT and maintenance need to work together to make sure that crucial services are not being left out of the allowlist rules (previously called "whitelist" rules). However, because the maintenance laptops should have a smaller set of software tools needed (compared to some other parts of the company), these needs can likely be determined with some investigation.

Network connections should have a default-deny policy, which means that anything not explicitly allowed is denied.

First, IT can review inbound and outbound traffic for each piece of LMS software, including what's needed for updates, license server checks, and analytics (if the company has opted into providing analytics). This traffic can be turned into a firewall allowlist. IT can then review traffic requirements for other required software on the device, as well as any system updates or services required, and IT security monitoring tools.

IT and maintenance should also discuss what online portals (such as vendor service portals, time tracking, warranty tracking, inventory, etc) are needed for maintenance. If this can't be moved to a non-vehicle maintenance laptop, these portals should be added to the firewall allowlist. If there are occasional or exceptional internet needs, such as being able to go on a technician forum to troubleshoot difficult issues (that cannot be done on a different device), IT may be able to allow these cases as an admin override from the maintenance technician manager, rather than adding them to the allowlist.

Organizations can also use a reverse proxy as an additional layer of protection between a potentially vulnerable maintenance device, and the external connections it must make for licensing, updates, etc. A reverse proxy would sit between the maintenance laptop and the server trying to send it requests. It would receive incoming traffic and forward it to the maintenance laptop, isolating it from a direct internet connection (and can also be combined with firewall usage (making the reverse proxy essentially a two-firewall DMZ setup).

For ideal segmentation, implement this as a pair of firewalls protecting a DMZ that sits between IT and OT. The IT-side firewall can be managed by the IT accounts, and the OT-side can be managed by OT accounts. The same personnel can operate the accounts, but the separate domain accounts help further segment the two areas of the organization. See the previous section on segmentation for more details. This is the best practice for "major boundaries" as taught in SANS ICS 410[36].

36 https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

Review Open Network Ports

Why: When exploits like CitrixBleed[37] or other critical vulnerabilities hit the news, journalists will sometimes include a number of vulnerable devices. One such way they gather this information is from tools that regularly scan the internet for exposed services, effectively creating a search engine for servers and IoT devices. A few examples are Shodan[38], Censys[39], GreyNoise[40], and Hunter[41].

While much of this same information could be individually collected via command line tools such as **`nmap`** or other port scanners, automated scanning tools collect and organize this information at scale. While port accessibility should be managed by your organization's firewall settings, it's still good to keep an eye on things. Tools like these allow red teamers, penetration testers, and other hackers to evaluate an organization's attack surface, so it makes sense for defense/IT to review it as well.

Who is involved: IT

How to implement: Evaluating your company's internet-connected services can be done with external services like the ones listed above. It can also be done internally through command line tools such as **`netstat`** to list open ports on an individual computer, or with **`nmap`** or other port scanners to scan a network. Review any open ports and any unexpected devices on the network, which has hopefully been limited to only necessary maintenance devices. An introductory guide for **`nmap`**[42] and Shodan[43] are included in the footnotes.

This is not just a matter of looking at the maintenance devices, though they are of course included. There may be other devices within a maintenance facility that should be reviewed, such as cameras, gateways, HVAC services, and other IoT devices.

Restrict Remote Access to Maintenance Devices

Why: In some cases, remote access is needed, and can even be a valuable maintenance feature (such as the 3rd party tools that give you on-demand remote technician help). On the other hand, remote access, especially RDP, has been the source of serious vulnerabilities, including Eternal Blue and BlueKeep.[44]

Who is involved: IT

How to implement: If you do not need remote access, disable it entirely (and make sure users do not have permissions to re-enable it). This can be done through group policy[45].

If you do need remote access, put controls around how it is used, such as requiring a manager to enter admin credentials and requiring MFA (such as with Duo). If possible, restrict the computers and/or users[46] who can use remote access. This might include requiring a maintenance manager to provide admin credentials in order for a technician to use remote access. If a program needs to be installed for remote support from an OEM, remove it once the remote support has finished.

IT can work with maintenance to support only the remote access scenarios that should be allowed. For example, a maintenance facility might send a technician out into the field to connect a laptop to equipment that needs to be diagnosed. A technician at the maintenance

37 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-exploits-citrix-bleed-in-attacks-10k-servers-exposed/
38 https://www.shodan.io/
39 https://search.censys.io/
40 https://www.greynoise.io/
41 https://hunter.how/
42 https://www.redhat.com/sysadmin/quick-nmap-inventory
43 https://danielmiessler.com/p/shodan/
44 https://en.wikipedia.org/wiki/EternalBlue and https://en.wikipedia.org/wiki/BlueKeep
45 https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/deny-user-permissions-to-logon-to-rd-session-host
46 https://learn.microsoft.com/en-us/answers/questions/235264/how-to-restrict-rdp-connection-to-specific-source

facility might then RDP into the first laptop. In this example, IT could restrict access to only domain-controlled laptops, and possibly only laptops coming from the maintenance network, or from specific devices. This would allow the on-highway case while also protecting against other outside RDP / remote access attempts either to laptops in the field, or attempts to laptops at the maintenance facility. If the on-highway or field cases are not needed at all, remote access can be restricted even further.

Use Company-Owned Devices for Roadside Laptop Usage

Why: Much of this report assumes the scenario of a laptop that never leaves a maintenance facility, or its intended network. But some devices may be needed in the field, such as for roadside maintenance work or other maintenance locations.

Who is involved: IT and maintenance, plus funding from business decision makers

How to implement: Organizations who have this need will need to evaluate how often it happens, and how maintenance technicians currently address needs for connectivity. Many maintenance software tools will not run without being able to connect to a license server, so some internet connectivity must be available.

Rather than using personal devices (which you cannot guarantee the security of) for connectivity, organizations should provide devices such as hotspots. They can then restrict the laptops from joining other networks through group policy. The hotspots or other roadside devices should be secured through strong passwords, filtering/blocking unnecessary connections, and other restrictions similar to the device- and network-level mitigations. IT and maintenance will have to work together to determine a trade-off between the ability to get their job done quickly versus security concerns.

Next, determine if there's any other use for personal devices within a work context. If your technicians use bluetooth connected VDAs, they might be connecting these VDA dongles to their smartphones. If this is the case, the company should provide designated smartphone or tablet devices to use that adhere to IT security policies.

Restrict and Scan File Downloads

Why: Downloads can obviously be dangerous, but it's not always an option to ban them entirely. Ideally, downloads of maintenance software have already been addressed in Have Known Good Copies of Software Tools, but maintenance technicians may need to download other files to help troubleshoot a truck equipment issue.

Who is involved: IT and maintenance

How to implement: Work with maintenance to determine what kinds of files are legitimate and needed for their work. Use a group policy and/or other tooling (like Microsoft Defender Smartscreen[47] or a third-party EDR) to block the downloads of other file types, and to scan the allowed file types. There may also be security tooling available at the application level to scan and/or restrict file downloads, such as within an email client.

Microsoft Sharepoint has built-in virus protection available[48], which can be configured to scan all uploads and then move verified uploads to a shared directory. This can be a good automated solution to ensure that all files are scanned before entering maintenance laptop domains. This may already be included in your organization's Microsoft licensing plan (e.g. as part of Microsoft 365).

47 https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

48 https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide

Backups and/or Updates for Connected Maintenance Services

Why: Backups and known good copies have already been discussed for the specific legacy maintenance software in use, and the devices that they run on.

Maintenance devices may have other software on them, such as fleet management tools or business-related tools (emails, time-tracking, etc.). These tools should be limited to only what is necessary for maintenance functionality (see "remove unnecessary tools") but the remaining tools must be included in updates and backup plans.

Who is involved: IT, with input from maintenance on what services are used.

How to implement: Work with maintenance to discuss all connected services and devices that are used, that the company has control over. This might include warranty information, time tracking, email clients, or regulatory paperwork, to name a few options. Consider both what could be an incoming source of a cybersecurity incident, and also what might be affected if a maintenance laptop was compromised.

Any software that relates to trucking uptime or regulatory compliance should be backed up if possible (for example, being able to take a database copy of maintenance logs that are stored in a cloud service). These services should be considered in your incident response plans as well and any workarounds should be discussed in advance.

More common tools related to business functionality (such as email clients, Zoom, etc) may have fewer regulatory consequences if they are outdated or unavailable, but are also likely to attract more security research. This means that you should keep up to date with critical vulnerabilities and update these tools regularly. If they are not needed on maintenance laptops, remove them.

Remember that in general, it's not the backups themselves that are important, but the ability to restore. Test your restoration procedures regularly. Furthermore, when a ransomware attack hits, you will not be able to access restoration procedure plans if they are stored in network shares or even on removable drives. Therefore, restoration procedures should be printed and stored as hard copies. Test this workflow as part of your incident response plans.

Review Other Devices on the Network and Apply Security Measures

Why: The WiFi security practices mitigation recommends having a separate network for only maintenance-related devices. This network should not include other areas of the business, including drives or devices not relevant to maintenance needs.

So far, the phrase "maintenance devices" has mostly meant maintenance laptops. But some organizations may need to have other maintenance-related devices on the network, such as a printer or security camera. These devices should be used for maintenance needs only, and not shared with other areas of business functionality. Common office equipment is often the target of security research and attacks, such as widespread printer hacks[49].

Much like the laptops and other devices running legacy maintenance software, other devices such as printers should be considered a possible threat vector, especially if there is any internet connectivity involved.

Who is involved: IT

How to implement: These devices should be included in the Asset Management and Incident Response plans. This includes regular updates, likely through a vendor-specific portal or management tool. They should also have their passwords changed to something that is not guessable or the default password. Their internet connectivity (open ports, firewall settings) should

49 https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/

be reviewed. Lastly, they should be considered in incident response plans as something that will need to be restored in order for the maintenance facility to resume normal operations after a cybersecurity incident.

Use Updates and AdBlockers for Browser Security

Why: Everyone knows that internet ads are annoying and obtrusive, but lately, they've also become a vector for malware. The FBI released a bulletin in late 2022[50] warning of cybercriminals using advertisements to impersonate legitimate brands to trick end-users into downloading and installing malware. Some so-called "drive-by download" attacks[51] can even infect computers without any user interaction.

Along with having known good copies of software tools, restricting downloads, and _, installing an ad blocker can help limit the chances of a malware infection for maintenance devices with internet accessibility.

Considering again that attackers may likely pivot from IT into the maintenance laptop domain, it would be prudent to run a separate Windows Server Update Services (WSUS) server inside the maintenance laptop network segment. This will help ensure that attackers cannot use an IT-managed update server as a means of pivoting (and is another best ICS best practice per SANS ICS 410).

Who is involved: IT

How to implement: On maintenance devices with internet connectivity, install an adblocker browser extension such as uBlock Origin. This can also be done through Group Policy, see Google's "Managing Extensions in your Enterprise" guide[52]. Also, regularly update the browser to apply security updates and restrict browsing to maintenance-related needs only, through network controls.

People/Processes

The last section of mitigations is all about people within an organization, and the processes that they follow. Cybersecurity can either be helped or hindered by this. Employee security awareness helps bake cybersecurity defenses into the organization, and processes make sure that individual security improvements are maintained over time.

As you can imagine, the lens of people and processes can apply to this entire report. In all of the mitigations in this report, organizations must find a compromise between the needs of IT security, and the needs of maintenance. IT can report on security needs, maintenance can report on operational needs, and business leaders will need to balance the two, accepting the risk involved for prioritizing operations over security.

Manage Separate Domains Separately

Why: The technical details of implementing ideal network separation have already been discussed in earlier sections. Proper segmentation also involves people and processes: notably, being able to leverage IT expertise between the IT and OT areas of the business, while still maintaining domain separation.

Who is involved: IT

How to implement: Earlier segmentation mitigations include having separate Active Directory trees for IT and OT domains. This does not necessarily mean that you need two separate administrators–it can be the same person. However, these administrative accounts (and any other high-privileged accounts) should be separate between the two domains. This prevents attackers from using IT domain persistence to move laterally (pivot) into the maintenance laptop domain.

Another recommended mitigation discussed earlier is the use of separate instances of

50 https://www.ic3.gov/Media/Y2022/PSA221221?=8324278624
51 https://usa.kaspersky.com/resource-center/definitions/drive-by-download
52 https://docs.google.com/document/d/1pT0ZSbGdrbGvuCsVD2jjxrw-GVz-80rMS2dgkkquhTY/edit

EDR and other security solutions. This was recommended for a similar reason–preventing an IT domain compromise from spilling over into the OT part of the organization. However, separate instances of security tooling does not mean that you need different product types between the domains. The same software products should be used in both the IT and OT domains to benefit from bulk licensing and to make the best use of the expertise of personnel within your organization. Separate instances and separate credentials should then be used to maintain segmentation.

Provide Security Awareness Training for Maintenance Techs

Why: Trucking industry surveys have shown that a very low percentage of carriers train their drivers or office staff in cybersecurity practices[53]. While cybersecurity is much more than just not clicking on phishing links, phishing does have a significant impact on a company's bottom line, and is a starting point for many attacks. The FBI's 2021 IC3 report stated that phishing scams are the cause for nearly 22% of breaches, and that ~83% of companies experience phishing attacks[54]. CISA states that phishing is the entry point for 90% of attacks[55] (though not all of them are successful).

That means that in addition to technical security changes through IT management, organizations should also consider raising the cybersecurity defense skills of their people.

Who is involved: maintenance technicians and their supervisors.

How to implement: One way to defend against phishing attacks, social engineering, and other cybersecurity attacks is to include all employees, including maintenance technicians, in security awareness programs. This includes phishing awareness, understanding of Business Email Compromise (BEC) attacks, and an understanding of what the cybersecurity risks are to trucks, specifically. Employees should be advised to seek out-of-band confirmation for important or sensitive requests (such as granting access or making financial transfers), especially given the rise of AI voice and video scams.

Organizations can also include general operational security ("opsec") best practices such as not sharing passwords over email, and not posting specifics of a maintenance facility's software or hardware on internet forums.

Additionally, corporate messaging should clearly communicate that cybersecurity is a priority for the company, and that doing tasks securely is worth the effort for overall business success.

Cybersecurity training should never be about shaming an employee for making a mistake. Instead, it should be focused on education and improvement. Technicians are crucial to the trucking industry and giving them the tools they need to do their job securely helps everyone with uptime.

NMFTA has written more about phishing attacks at https://nmfta.org/beware-of-look-alike-domain-threats-protecting-your-online-identity/ and also recommends the following CISA guidance on preventing phishing attacks: https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one.

Have a Process or Plan for When Employees Notice Suspicious Behavior

Why: It's one thing to be prepared for suspicious or malicious behavior, but it's another thing to actually react to it. If one employee in your company is being targeted with phishing attacks, it's likely that others may be as well. Spreading the news can help others thwart attempted attacks.

Likewise, no one knows the trucks and typical behavior better than the maintenance

53 https://www.truckinginfo.com/10170328/minimize-the-threat-of-cyber-attacks-at-your-fleet
54 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
55 https://www.cisa.gov/stopransomware/general-information

technicians. If they see unusual or suspicious behavior, there should be a process for them to follow to report it (such as with a manager) and get it remediated.

Who is involved: technicians, technician managers, IT, and possibly HR.

How to implement: Some categories of suspicious behavior can be predicted in advance, such as phishing. Education about phishing attacks (Provide Security Awareness Training for Maintenance Techs) or social engineering should include a way to report suspected attempts. IT, HR, or whoever is responsible for company-wide updates should send out an email to give other employees a heads up. Employees should also know how to report physical security issues, such as lost or stolen equipment.

For other suspicious behavior, such as computers or trucks acting "weird", the process is less clear. Is there another technician or manager that can be consulted if someone notices something suspicious? Have employees been encouraged to seek a second opinion on suspicious behavior?

Additionally, organizations that are big enough to have a SOC service can consider including maintenance laptops in that plan. This will allow them to proactively monitor and react to malicious behavior.

Have a Process for When a Maintenance Technician Leaves the Company

Why: Typically, IT will have a policy in place for when an employee leaves the company, especially when that employee corresponds to a specific Active Directory user.

In cases where there is no Active Directory account for a particular user, there still may be access in other forms that should be rejected. Palo Alto Networks reported in 2022 that, while insider threats are the cause of only 5% of total breaches, 75% of insider threats are from disgruntled ex-employees[56].

Who is involved: IT, technician managers, and HR.

How to implement: Make sure that if employees leave the company, all access is removed. This includes returning any company devices, building access keycards, online portal logins for tools especially those that store sensitive company data. If there are not separate logins for online portals, change the password.

Use asset management of software to make sure that all of the bases are covered and that the access revocation does not fall through the cracks just because they do not have a typical laptop user account.

HR likely already has a policy for when employees leave the company. They can work with IT and maintenance technician managers to develop a plan that is specific to technicians, and the three parties can work together to make sure the plan is enacted if or when an employee leaves.

Perform Regular Audits

Why: In addition to having a way of reporting if something goes wrong, it's also good to check that the security processes that have been put in place actually remain in place. This means regularly verifying that the implemented mitigations are still working as expected, via regular audits.

Who is involved: IT and maintenance technicians.

56 https://start.paloaltonetworks.com/2022-unit42-incident-response-report

How to implement: For each policy in place, whether pre-existing or inspired by this report, there needs to be a way to verify that it is still in place. Some of these policies may be enforced by group policy, but some may need manual checks, and/or in-person discussion with personnel.

For example:

- Have new tools been installed on maintenance laptops?
- Do all employees know the rules, where to find good copies of software?
- Have computers and applications been updated on schedule?
- Have firewall rules been modified, and are there any new, unexpected user accounts?
- Are there any outdated devices on the network that require manual updates, such as a printer?
- On the "people" side of things, are there security settings on the laptops that are onerous for the technicians? If so, is there an alternative that would work better, and still strike a healthy balance between operations and security?

Cybersecurity Should Be Considered in RFQs and Sourcing

Why: An ounce of prevention is worth a pound of cure. There are some IT security issues that create a lot of extra work for something that could have been avoided with more questioning or representation of cybersecurity concerns.

Who is involved: this is not just a task for IT, though IT should certainly be involved. Business leaders, sourcing, and legal can also help push the organization's cybersecurity posture forward by bringing cybersecurity into sales meetings, contracts, and budget discussions.

How to implement: Business leaders and sourcing personnel should be sure to involve IT in any discussion for new software services, including in maintenance facilities. This will allow them to ask vendors questions focused on security, and to either prevent or anticipate future workarounds needed to keep the organization secure.

Business leaders and sourcing can also include cybersecurity in the RFQ process. The appendix includes a handful of questions that can be added to any RFQ questionnaire.

Legal can also consider cybersecurity concerns (such as regular updates, best practices, communicating cybersecurity issues, etc) in the contracts process.

Business Leaders Should Exercise Their Personal Networks for Threat Intel

Why: Companies facing ransomware or other cyberattacks understandably do not want to go public about it. However, having this information can help other organizations be more proactive about current threats. In the absence of publicly available information, organizations can keep their finger on the pulse through other methods.

Who is involved: business leaders, and IT.

How to implement: Utilize your network to stay up-to-date on current threats, including attack vectors. As mentioned previously, a lot of ransomware gangs will go for volume of attack, which means their tactics may be used against a large number of companies. If your network is willing to share details of how they recovered, use this information to review the incident response plans and defenses you have in place, and shore up the weak areas.

There are also official organizations for threat sharing. This includes ATA's CyWatch program (https://www.trucking.org/fleet-cywatch), the Automotive ISAC (https://automotiveisac.com/) and FBI's IC3 (https://www.ic3.gov/). Additionally, CISA has a database of known exploited vulnerabilities (https://www.cisa.gov/known-exploited-vulnerabilities-catalog).

Create and Test an Incident Response Plan

Why: The best case scenario is that your company is never affected by a cyber attack. This is the outcome everyone hopes for: our defenses thwart all attacks, software remains updated, and employees never click bad links. But it's difficult to stay ahead of all threats while also running regular business operations. Rather than just hoping for the best, one should also plan for the worst. Incident response plans are crucial for getting back on the road as soon as possible after an attack.

Who is involved: everyone. IT, business leaders, HR, legal, maintenance technicians, and technician managers.

How to implement: Between management, IT, and maintenance personnel, make a list of what functionality needs to be restored after a cybersecurity breach. This includes software, devices, and network functionality as described in earlier sections. For example:

- Are there known-good backups of software or device images that are available, offline?
- Are there plans for what to do if a device has been infected?
- And what tools are in place to help detect that something has gone wrong (built-in Windows security tooling, a SOC, endpoint detection and response products, reporting by employees)?
- Do you have an offline copy of your incident response plan?

And of course, backups and incident response plans need to be tested. A backup that cannot be restored is no better than having no backup at all.

IT should also consider upstream breaches, and their effects on the maintenance facility. If a software vendor is breached and alerts the company, does the asset management system clearly show which laptops and logins would be affected? And are there contingency plans if an upstream system (such as a fleet management tool that includes regulatory reporting) goes offline?

Incident response plans are not just the responsibility of IT, however. Companies should consider what else is needed in the case of a breach, and this is largely the domain of business leaders, legal, and HR. For example:

- What will be communicated internally, if a breach occurs?
- What will be communicated to downstream customers?
- Are there any regulatory compliance functions that could be affected by a cybersecurity event, and if so, what is the workaround?
- Will your company report a cybercrime attempt to the FBI[57]?
- Will your company need to report to the SEC[58]?

One way to involve more employees in the incident response planning process is to use table-top exercises (TTX). This allows you to think up worse case scenarios, and roleplay how the company would respond. This way, you can identify gaps in your processes before they are a real issue. You can use this approach to come up with scenarios specific to maintenance software (such as infected or stolen maintenance laptops, insider threats, etc) or scenarios that include other areas of the organization, too.

The NMFTA has developed a set of resources to help facilitate TTX meetings, available in the form of a playbook[59],Participant Handbook[60] and Instructor Handbook[61] PDFs.

57 https://www.fbi.gov/investigate/cyber
58 https://www.sec.gov/news/press-release/2023-139
59 https://nmfta.org/wp-content/media/2022/11/Ransomware-Playbook-Template.pdf
60 https://nmfta.org/wp-content/media/2022/11/Participant-Handbook.pdf
61 https://nmfta.org/wp-content/media/2022/11/Facilitator-Handbook.pdf

Get External Security Help

Why: Finally, managing cybersecurity risk is a lot of work for an organization, especially given that it's not their primary function! Cybersecurity efforts can be outsourced to other companies to help lighten the load, shore up defenses, and continue improving.

Who is involved: IT personnel, business leaders, and possibly others.

How to implement: There are a variety of cybersecurity services available, with more available every single year.

The most common type of external security help is phishing training and general cybersecurity awareness, which was discussed earlier.

Companies can also hire security consultants for vulnerability assessments, penetration testing (often called "pen tests"), and/or red team assessments. Each of these test the cybersecurity posture of an organization by trying to breach their defenses as "white hat hackers". Then, a report is shared with IT and other stakeholders, along with mitigation steps to prevent the successful avenues of attack. These services range from more theoretical to more "real world" and can be adjusted to your organization based on needs and uptime concerns.

Organizations may want to consider putting a Vulnerability Disclosure Program (VDP) in place. This is a process by which organizations can accept help from security researchers who have found a vulnerability, and work to remediate it in an agreed-upon way. If these guidelines (typically described as "good faith effort") are followed, the organization will agree not to threaten or pursue legal action. While most organizations do not want to invite unwanted attention, the truth of the matter is that automated scanning of the internet for vulnerabilities is already happening. CISA has provided a sample legal template that organizations can use[62], and Bugcrowd has published information on what makes a VDP successful[63]. At a minimum, having a "security.txt" file on your website can make sure that emails from security researchers reach someone in IT[64].

Last but not least is participating in NMFTA's cybersecurity conferences, and using the ever-increasing number of resources available on its website. The NMFTA hosts a cybersecurity-focused trucking conference every fall called the Digital Solutions Conference, each year in a different location. Past information can be found here: https://nmfta.org/nmfta-event/digital-solutions-conference/.

NMFTA also has published cybersecurity resources on telematics, ELDs, avoiding ransomware, and more on its blog, research page and resources page.

The NMFTA wants to align its efforts with the needs of its partners. If you have a particular cybersecurity concern you'd like help with, please contact NMFTA at cyber@nmfta.org.

62 https://www.cisa.gov/vulnerability-disclosure-policy-template
63 https://www.bugcrowd.com/glossary/vulnerability-disclosure-program-vdp/
64 https://securitytxt.org/

Appendix

Appendix A: Questionnaire for Evaluating Externally Managed Device Vendors

Answers to these questions should be formalized into a service level agreement (SLA) with the external vendor.

1. What MDM/RMM is in place to administer policies and updates to maintenance devices?
2. What are patch timelines for critical vulnerabilities, such as those in the operating system? What are hours for emergency support?
3. What is the regular patching schedule? Are there processes in place to ensure that patching and backups happen even if there's a large amount of tickets?
4. What is support like for non-critical technical help? Is there a ticketing system, how quickly should a response be expected, are there excluded hours or services? What is the average time to resolution?
5. What EDR or anti-virus solution is in use?
6. What are the data retention policies? How often are backups taken, where are they stored, and how long are they kept?
7. How are passwords and credentials managed? Do they enforce MFA? How are passwords handled if an employee leaves the company?
8. What information is collected by monitoring systems in use?
9. How many years have they been in service, and what certifications/qualifications do they have?
10. What security training do they provide to their own staff? What security practices do they have in place to keep your data secure?
11. When was the last internal security testing performed, and what were the results?
12. How are incidents remediated and then reported to the customer?
13. How do you audit employee access of customer systems? How do you audit changes made to systems?

Appendix B: RFQ Questionnaire

This set of questions can be included in a RFQ for aftermarket or third-party maintenance software tools. These questions are a subset of NMFTA's Cybersecurity Requirements for Telematics Systems matrix[65].

1. **SAA-020** and **SAA-030**: Has the software undergone security testing, such as pen testing?
2. **SAA-030**, **SAA-040**, and **SII-170**: How do they monitor for CVEs in supporting libraries, and how soon will they push out an update in the event of a vulnerability in a supporting library?
3. **SII-021**, **SII-180**, and **SII-171**: What processes will they follow and/or support will they make offer in the event of a vulnerability in the product? How soon will they remediate, and report to end customers?
4. **SII-100**: What processes will they follow and/or what support will they offer in the event of a breach of their company and/or servers that support the maintenance tool(s)? How soon will they remediate, and report to end customers?
5. **SII-030, SII-130, SII-150** and **SII-070**: Are binaries signed? What secure coding practices are in place?
6. **SII-090** and **SII-120**: How are customers alerted to updates, especially security related updates? How quickly do they respond to security disclosures from researchers?
7. **CM-040** and **SCP-130**: Does the software support current Windows operating system versions? If it does not support Windows 11 are they on track to support it before Windows 10 reaches end-of-life in 2025?
8. **SCP-010, SCP-020, SCP-050**, and **CM-010**: What outbound connections does the software need to make? How are these servers/endpoints secured? Can the organization opt out of analytics, if applicable?
9. **AC-070** and **SCP-140**: If the maintenance software includes an online portal login and/or remote access as part of the product, what protections are in place to prevent brute-force login attempts?
10. **M-020**: If the software includes cloud storage of customer data, how is this data protected and backed up?

65 https://github.com/nmfta-repo/nmfta-telematics_security_requirements

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

1001 N Fairfax Street Suite 600
Alexandria, Virginia 22314-1798
(866) 411-6632
www.nmfta.org