txOne networks
Keep the Operation Running

Q2 2023 EDITION

A Comprehensive Perspective of JAMA/JAPIA Automotive Cybersecurity Guidelines

Contents

Introduction

In 2017, operations of multiple automotive manufacturers, such as Nissan's factory in the UK, were halted due to the WannaCry ransomware attack.[1] To this day, the automotive industry has been experiencing an increasing number of attacks. Based on the track record of automotive industry-focused attacks in 2022, we found that the targets are not just vehicle systems, but rather IT/OT systems. These systems impact operations and production and tend to be more susceptible to attacks which lead to real-world consequences for car manufacturers and their suppliers. One such example is when Honda suffered a cybersecurity attack in June 2020 that temporarily halted the company's operations in Italy, Japan, North America, Turkey, and the UK for car manufacturers and their suppliers.[2] In February 2022, Kojima Industries Corporation (a supplier of internal and external automotive parts) had its file server attacked by ransomware, forcing the world's largest automotive manufacturer to temporarily shut down all 14 factories and 28 production lines in Japan.[3] Fortunately, the Japanese automotive industry has begun to make serious efforts to improve cybersecurity in response to these incidents.

Automotive cybersecurity is particularly complex due to its dependence on three different levels working smoothly with each other: car manufacturers, suppliers (including electronic devices and software), and service providers (such as car dealers and car-sharing services).[4]

1. **Automotive Manufacturers:**

   a. **The Vehicle Itself:** The cybersecurity of the car largely depends on the security of each part of the vehicle. This includes the security mechanisms of computer control systems, connected car services, and manufacturing systems.

   b. **Automotive OA and OT System Daily Operations:** Internally, they use a large amount of information technology (IT)/OT systems, computers, and servers for daily business operations. These systems also require cybersecurity to ensure the safety of vehicle components at each stage of production and to write secure computer programs for cars. In addition, car companies and technology suppliers must share some of their intellectual property with each other to ensure the correct design and production of cars. This means that data security depends on everyone playing their part.

2. **Risk Management in the Automotive Supply Chain:** Cars are typically composed of tens of thousands of parts and powerful software. As more and more vehicles are equipped with software, electronic components, and connected services, car manufacturers have had to further expand their supply chains, including partnerships with software technology providers, autonomous driving module manufacturers, automotive LiDAR and camera module manufacturers, and telecommunications services among other new suppliers.

3. **Automotive Service Providers & Car-Sharing Services:** Both car dealerships and automotive transportation network service companies (such as Uber) handle a tremendous amount of personal information for customers, including names, home addresses, and GPS records, as well as bank accounts and transaction records.

In April 2019, the Japan Automobile Manufacturers Association (JAMA) launched a cybersecurity working group under its Electronic Information Exchange Committee. The Japan Automobile Manufacturers Association (JAMA) is a non-profit industry organization representing the interests of major Japanese car manufacturers. Established in 1967, JAMA aims to promote the development and growth of the Japanese automotive industry both domestically and internationally. JAMA's members include 14 leading Japanese car manufacturers, such as Toyota, Nissan, Honda, Mazda, Subaru, Mitsubishi, and Suzuki. These companies are at the forefront of automotive technology, innovation, and manufacturing, making Japan one of the largest and most influential automotive markets in the world.[5] JAMA focuses on various aspects of the automotive industry, including environmental protection, safety and cybersecurity, international trade, and regulatory affairs. JAMA also actively participates in international organizations, such as the International Organization of Motor Vehicle Manufacturers (OICA) and the World Forum for the Harmonization of Vehicle Regulations (WP.29). The association plays a crucial role in setting industry standards, guidelines, and best practices while advocating for fair and open global trade policies.

With this in mind, JAMA's cybersecurity working group held several meetings with stakeholders to discuss the "Guidelines for Cybersecurity in Supply Chain Risk Management". A few months after JAMA established the cybersecurity working group, the Japan Auto Parts Industries Association (JAPIA) also formed a cybersecurity working group. The Japan Auto Parts Industries Association (JAPIA) is a renowned non-profit trade organization representing the interests of Japanese automotive parts manufacturers and suppliers. JAPIA was founded in 1967 with the aim of strengthening the Japanese automotive parts industry, promoting technological advancement, and enhancing international competitiveness. JAPIA's members include various companies engaged in the production and supply of automotive parts, systems, and materials. JAPIA member companies range from large multinational corporations to small and medium-sized enterprises (SMEs), focusing on various aspects of the automotive supply chain. The two working groups from JAMA and JAPIA began collaborating in the summer of 2019 to develop the JAMA/JAPIA Cybersecurity Guidelines, with the first release of V1.0 guidelines on March 31, 2020.

Following this, the World Forum for the Harmonization of Vehicle Regulations (WP.29) released two critical cybersecurity regulations, R155 on Cyber Security and R156 on Wireless Software Updates (OTA), on June 24, 2020.

- UNECE WP.29 R155: Cyber Security Management System, CSMS
- UNECE WP.29 R156: Software Update Management System, SUMS

Passing these two cybersecurity regulations is mandatory for ensuring market access and vehicle type approval in UNECE WP.29 member countries, which also include binding requirements for car manufacturers (as well as tier 1 and tier 2 suppliers). Subsequently, on March 31, 2022, JAMA/JAPIA revised the Automotive Industry Cybersecurity Guidelines (v2.0) to improve cybersecurity measures throughout the automotive industry. These guidelines take into account the unique cybersecurity threats faced by car manufacturers and companies that make up the automotive supply chain, with the aim of promoting effective cybersecurity level inspections and helping to strengthen cybersecurity measures throughout the entire automotive industry.[6]

Overview of the JAMA/JAPIA Automotive Cybersecurity Guidelines

Since enhancing the security of the entire automotive industry supply chain is considered top priority, JAMA/JAPIA aims to develop guidelines that can be shared with domestic and international partners. Firstly, JAMA/JAPIA referred to the Cyber-Physical Security Framework by Japan's Ministry of Economy, Trade, and Industry in April 2019, which covers cybersecurity and supply chain risk management. In addition, the Cyber-Physical Security Framework cross-references cybersecurity guidelines and regulations from other countries, such as the NIST Cybersecurity Framework, ISO 27001, AIAG Cyber Security 3rd Party Information Security (Version 1), and the Small and Medium Enterprises Information Security Measures Guidelines (IPA) to achieve policy coordination.

Moreover, the guidelines are divided into three different cybersecurity levels to simplify and promote their application across the entire automotive industry (regardless of company size). This allows companies to prioritize essential items to build upon, making them accessible to all companies, including smaller ones. The latest version of the guidelines, Version 2, adds new items and adjusts the conditions under which implementation objectives should be achieved.

Framework of JAMA/JAPIA Automotive Industry Cybersecurity Guidelines

As mentioned earlier, the latest JAMA/JAPIA guidelines (revised V2.0 on March 31, 2022) serve as a first step, combining various existing cybersecurity standards and other benchmarks. By using these guidelines, organizations and individuals who are unsure where to start with security measures can take that initial step with confidence. Moreover, the guidelines define three levels, from the minimum implementation items to the ultimate goals to be achieved, with Level 1 being the minimum implementation items. The purpose of this is to demonstrate the minimum necessary countermeasures that must be used regardless of company size. The current guidelines primarily focus on the OA environment, but JAMA/JAPIA's future scope will expand to other areas, including equipment development, dealers, vehicles, and more.

The JAMA/JAPIA cybersecurity model framework divides best practices into 24 major areas, as follows: security policy, confidential information handling rules, compliance, system security, procedures under adverse conditions, access rights, daily education, inter-company information security requirements, information asset (information) management, risk response, understanding the details and methods of business transactions, internal connection rules, physical security, communication control, authentication/approval, deploying patches and updates, data protection, office tools related, malware countermeasures, detecting unauthorized access, backup/recovery, etc. By defining these 24 major cybersecurity areas, the goal is to achieve various security objectives and implement 153 control measures, with most discussions focusing on preventative measures. One such measure would be preventing confidential information leaks by defining rules for handling confidential information and communicating these rules within the organization. Another would be defining clear information security systems and roles, minimizing losses in the event of an incident/accident to restore normal operations as quickly as possible. Another measure would be dedicated to preventing information leaks, unauthorized modifications, and system stoppages caused by malware infections. However, these capabilities do not need to be implemented by all companies but rather are determined based on their requisite security level.

Table 1: Mapping NIST CSF with JAMA/JAPIA Cybersecurity Guidelines

NIST CSF Framework	Cybersecurity Domains	Condition(s) for Achievement	Percentage
Identify	Understanding details of business transactions and methods	4	10%
	Understanding the statuses of external connections	5	
	Applying patches and updates	6	
Protect	Policies	3	69%
	Compliance	4	
	Rules for handling confidential information	5	
	Information security requirements between companies	8	
	Management of information assets (information)	5	
	Management of information assets (equipment/devices)	1	
	In-house connection rules	5	
	Physical security	19	
	Daily education	13	

NIST CSF Framework	Cybersecurity Domains	Condition(s) for Achievement	Percentage
Protect	Access rights	5	69%
	Authentication/Approval	10	
	Communication control	10	
	Data protection	2	
	Malware countermeasures	6	
	System (Normal)	5	
	Office tool-related	5	
Detect	Detecting unauthorized access	6	4%
Respond	Risk response	10	13%
	Procedures in adverse situations	7	
	System (adverse situations)	3	
Recover	Backup/Restore	6	4%

JAMA/JAPIA Cybersecurity Levels

The latest JAMA/JAPIA guidelines aim to simplify and apply cybersecurity measures across the entire automotive industry, regardless of company size, by focusing on key items for prioritization so that all companies, including small ones, can use them. Level 1 specifies the minimum cybersecurity controls that organizations in the automotive industry should implement, involving 50 basic cybersecurity requirements. These requirements are intended to build a chain of security and trust between companies and their business partners and are also applicable to small and medium-sized enterprises.

Level 2 requires automotive industry organizations to strive for more advanced cybersecurity controls, covering 74 additional requirements. Companies should implement these controls, especially if they meet one of the following conditions:

1. Companies handling external confidential information (technical, customer information, etc.) within the supply chain.
2. Companies with significant internal technology/information relevant to the automotive industry.
3. Companies with a reasonable size/share that could have a significant impact on the industry supply chain due to unexpected disruptions.

It is worth noting that companies possessing these three characteristics must also simultaneously meet the Level 1 control measures.

Level 3 requirements primarily target companies representing the automotive industry for indexing or those with such goals, focusing on 29 advanced cybersecurity requirements. This is mainly considered from the perspective of company size and technical expertise. It is important to note that companies with these characteristics must simultaneously meet the control measures of both Level 1 and Level 2.

Table 2: JAMA/JAPIA Cybersecurity Levels

Cybersecurity Levels	Definition	Security Control Items
Level 3	From the perspective of company size and technical expertise, companies that are representative of or intricately tied to the automotive industry.	29
Level 2	Companies that a) handle external confidential information (such as technology and customer information) within the supply chain; b) possess significant internal technology or information relevant to the automotive industry; or c) are of reasonable size or have a reasonably large market share.	74
Level 1	Applicable to all companies (including small businesses).	50

The Focus of JAMA/JAPIA Automotive Cybersecurity Guidelines

The JAMA/JAPIA automotive cybersecurity framework consists of 24 domains, as shown in Figure 1, most of which originate from cyber-physical security frameworks and the NIST Cybersecurity Framework v1.1 control series. We will provide a brief explanation of each Cybersecurity Domain (not covering all details) for easier understanding of the core spirit of the guidelines.[7]

Identifying Automotive Cyber Supply Chain Risks

1. Understanding details of business transactions and methods

Companies need to prevent information leakage during business transactions by clearly defining methods for exchanging information assets and how they interact with business partners. JAMA/JAPIA requires companies to understand the information assets exchanged during business transactions with each partner and the methods used for such transactions.

Companies should, for example, establish and periodically review the information (i.e., receiving/sending orders) exchanged with each company and the methods used; or companies should establish IT equipment procurement security requirements and share them within the organization and among suppliers, diligently recording and storing evaluation results during procurement.

2. Understanding the statuses of external connections

Companies need to ensure safety and trust when using external information systems, while being able to respond quickly to information security incidents/accidents. JAMA/JAPIA believes that companies should clearly define external information systems (customers, subsidiaries, affiliates, contractors, cloud services, external information services, etc.) and properly manage their usage status regularly, or inspect network and data flow diagrams as needed to understand the organization's communication network structure, monitor cooperation with other organizations, and data flow directions.

3. Applying patches and updates

Patching vulnerabilities and security updates is an important method of protecting systems, helping to reduce the risk of unauthorized access and malware infection. The JAMA/JAPIA guidelines recommend that organizations should avoid using unsupported devices, operating systems, and software. At the same time, organizations should implement security measures to prevent unauthorized access from exploiting vulnerabilities. Organizations are advised to ensure that:

a. Unsupported devices, operating systems and software are avoided.

b. Security patches and updates are correctly applied to information systems, IT equipment/devices, and software.

c. Management systems and processes are established to address vulnerabilities.

d. Vulnerability diagnosis is performed on servers open to the external company before and after production, and measures are taken to defend discovered vulnerabilities.

e. Vulnerability diagnosis is performed on proprietary servers before and after production, and measures are taken against vulnerabilities.

f. Application software vulnerability diagnosis is conducted for web applications published on the Internet.

Protect Information and System Operations

1. Policies

JAMA/JAPIA recommends that as a member of the automotive industry, companies should have a basic understanding of cybersecurity concepts and policies as well as raise information security awareness within the organization. This can be achieved through two main measures:

a) Establishing an internal information security policy and communicating it within the organization.

b) Checking and reviewing detailed information about the company's internal information security policy as needed and widely communicating said policy within the organization.

2. Rules for Handling Confidential Information

JAMA/JAPIA recommends that companies should define rules for handling confidential information and communicate these rules within the organization to prevent the disclosure of confidential information. This would entail, for example, establishing and implementing a confidentiality system within the company, signing confidentiality agreements with temporary and transferred employees, collecting necessary confidential information and IT equipment when employees leave or contracts expire, and establishing rules for the use of IT equipment for business operations and communicating them within the organization.

3. Compliance

JAMA/JAPIA recommends that companies explicitly establish internal rules to guarantee compliance with information security laws. Companies can establish rules and provide education/communication within the organization. For companies that possess personal information, there is a need for internal rules specifically geared towards handling it safely. Companies also need to review their rules as needed to keep up with changes in the law.

4. System (Normal)

JAMA/JAPIA believes that companies should define a clear information security system and its attendant duties and improve and strengthen cybersecurity and data leakage prevention measures. Therefore, it is necessary for companies to establish a standardized information security risk management system, which includes defining the system, roles, and responsibilities under normal circumstances (including CISO) to achieve the collection and sharing of cybersecurity information. For example, companies could regularly review the normal system or establish a monitoring and analysis system for network attacks and trails and share the corresponding security measures with various departments of the company.

5. Daily Education

Companies should educate employees on the risks of malicious software and confidential information, as well as the correct approach to handling information, to prevent cybersecurity incidents/accidents. Therefore, JAMA/JAPIA's guidelines recommend that cybersecurity education and training must cover at least two bases.

First, companies should provide risk awareness education to employees, such as providing internal education on malware infections, educating personnel responsible for information security in each department about internal information security measures and management methods, and teaching company management how to understand their roles and responsibilities in cybersecurity.

Second, companies should provide education/training on information security incidents/accidents that have an impact within or across the organization and methods to minimize their impact. For example, providing education or training on responding to cybersecurity incidents/accidents, providing education or training on responding to cross-organizational information security incidents/accidents, and reviewing education or training content as needed.

6. Information Security Requirements Between Companies

JAMA/JAPIA also places great emphasis on information security in the supply chain, and companies should prevent the disclosure of confidential information in the supply chain and be able to respond promptly to incidents. Therefore, the automotive industry's supply chain is required to have clear information security requirements. For example, companies should be aware of the information security measures and status of business partners who handle important confidential information and understand how their own company handles important confidential information from other companies. In addition, they should collect or dispose of confidential information, access rights, etc. when contracts expire, clearly define how confidential information is handled between companies, regularly review the confidential information handling methods between companies for any issues and revise them as necessary. If a cybersecurity incident/accident occurs between a company and another company, roles and responsibilities of both parties should be clarified, and the roles and responsibilities documents with other companies should be regularly reviewed and revised as needed.

7. Access Rights

Companies should prevent unauthorized access to confidential areas or systems due to improper access rights settings, so proper access rights management becomes crucial (including physical and system access rights). For example, companies should define rules for managing access rights (room and system access rights) when personnel are transferred, and issue, change, disable, or revoke access rights according to management rules; they should also regularly, or as needed, take inventory of access rights. Ideally, all access logs should be securely stored and managed in a controlled access state.

8. Management of Information Assets

Companies should properly manage information assets to prevent the disclosure of confidential information. Therefore, companies need to set and understand the confidentiality level of information assets and manage information according to the confidentiality level. For example, defining management rules for confidential level information, creating a list of information assets with high confidentiality classification, or regularly or as needed reviewing the list of information assets created with high confidentiality.

9. Management of Information Devices and Equipment

Proper management of IT assets helps reduce the risks associated with information security incidents/ accidents and shortens response times in the event of a cybersecurity incident. Therefore, companies need to properly manage the information (version information, administrators, management departments, installation locations, etc.) of IT equipment, devices, and the OS and software that the company uses and owns. In essence, companies should develop relevant management rules based on the importance of IT equipment/devices, operating systems, and software.

10. In-House Connection Rules

Companies need to properly manage the use of internal networks to minimize the damage caused by information leakage and malware infections. Therefore, JAMA/JAPIA's cybersecurity guidelines require that when IT equipment/devices are connected to internal networks, restrictive access measures should be taken to minimize unauthorized device access to important systems. In addition, for remote working environments, JAMA/JAPIA's guidelines also recommend taking security measures to prevent security incidents (mainly information leakage and fraud).

11. Physical Security

JAMA/JAPIA places great emphasis on physical security measures, especially in preventing unauthorized access or modifications to critical equipment such as servers, which could lead to information leaks or system downtime. To this end, five information security requirements (19 control measures) have been established, including:

a. Implementation of physical security measures for areas where important assets such as servers are installed.

b. Implementation of security measures to prevent security incidents related to company access, such as unauthorized intrusion, unauthorized movement, information leaks, and suspicious behavior.

c. Control of items brought in/out of the organization.

d. Control of recording behavior within the company and adoption of preventive measures to prevent information leaks and security incidents.

e. Use of external storage media to prevent information leaks.

f. Implementation of information security measures for systems that store and use important information to minimize damage caused by human error.

12. Communication Control

In addition to deploying physical security measures to prevent unauthorized access to critical equipment such as servers, JAMA/JAPIA guidelines also require enhanced communication control to prevent network attacks and internal information leaks. This involves multiple technical control measures, including:

a. Enhanced network isolation: e.g., installing firewalls at the border between the Internet and the internal network to restrict communication; installing Web Application Firewalls (WAF) for web applications published on the Internet; ensuring that access to malicious websites is restricted.

b. Enhanced network configuration: Recording firewall filtering settings (communication permissions/ block settings) and regularly checking unnecessary settings; managing remote access IDs through regular checks for unnecessary IDs. In addition, the network should be isolated based on the importance of business and data.

c. Enhanced network resilience: Ensuring that network configuration does not affect the production environment during development or testing. In addition, enterprise systems should be able to continue providing services for Internet-facing websites and systems even while they are under DDoS attack.

d. Enhanced network confidentiality: Communication encryption to prevent eavesdropping and tampering of communication over the Internet; communication between terminals and Wireless LAN access points is encrypted.

13. Authentication/Approval

Enterprises need to prevent unauthorized use, operation, and modification of information systems to prevent information leaks/unauthorized modifications and ensure stable operation of the information system and IT equipment/devices. In addition, the organization must be able to investigate the causes of information leaks, unauthorized modifications, or system downtime when such incidents occur. JAMA/ JAPIA guidelines have formulated authentication and approval measures that information systems and IT equipment/devices should adopt to achieve the above objectives, including:

a. Assigning unique user IDs to each person.

b. Differentiating user IDs and system administrator ID permissions.

c. Defining and conveying password setting rules within the organization.

d. Setting password rules for external information systems and conveying them to personnel within the organization.

e. Regularly, or as needed, counting user IDs and system IDs and deleting unnecessary IDs.

f. Establishing procedures for the issuance, modification, and deletion of user IDs.

g. Approval is required for granting/changing/deleting management permissions and changing server and network equipment settings.

h. Implementing multi-factor authentication for systems used via the Internet.

i. Implementing connection timeout controls for important systems.

j. Implementing authentication log monitoring.

14. Data Protection

JAMA/JAPIA guidelines have formulated measures for data protection to reduce the risk of unauthorized access and malware infection, ensuring that data in the information system and IT equipment/devices is protected. Organizations are advised to ensure that the data on IT equipment/devices and information systems are properly encrypted. In addition, data received from external sources must be confirmed to be secure.

15. Office Tool-Related

JAMA/JAPIA guidelines focus specifically on information security management for office tools, with the most common risks coming from email, document sharing, and cloud services, among others, in order to reduce the risk of unauthorized access and malware infection. For example, organizations are advised to take information security measures to prevent information leakage caused by email transmission or to prevent incorrect email transmission. In addition, organizations should also establish prohibitions and restrictions on the use of websites and network applications and clarify and communicate these within the organization. If it is necessary to share documents with associated companies and business partners, usage rules for shared documents (including cloud services) must be established.

16. Malware Countermeasures

The threat of ransomware has become the most urgent issue in the manufacturing industry today in order to prevent information leakage, unauthorized modification, and system downtime caused by malware infection. JAMA/JAPIA guidelines recommend that companies implement control measures to prevent malicious software and quickly detect security anomalies. Specific measures include:

a. Using antivirus software on computers and servers to detect malicious software and provide notifications.

b. The virus code files for the antivirus software must be updated regularly.

c. Introducing a behavior tracking system that allows for detailed endpoint history records and remote responses after a malware infection.

d. Implement malware checks on email gateways to prevent malware infection through email.

e. The system enforces extension restrictions to prevent malware from infiltrating through email attachments.

f. Implement malware checks on web gateways to prevent malware infection through viewing unsafe websites.

Detect Unauthorized Access

1. Detecting Unauthorized Access

Due to unauthorized access, sensitive information may be leaked or assets may be damaged due to intentional or unintentional actions. Therefore, businesses need a mechanism to help detect unauthorized access in order to mitigate damage and ensure assets remain secure and operate normally. The JAMA/ JAPIA guidelines recommend that organizations take measures to promptly detect and block network attacks, and suppress the harm caused by targeted attacks and other network attacks. For example, establishing a monitoring system to continuously monitor unauthorized network access and obtain logs, in order to investigate intrusions and leakage routes in the event of a security incident or accident. In addition, organizations also need to take measures to promptly detect and block information security attacks, and suppress the harm caused by targeted attacks and other information security attacks.

Rapid Response to Risks, Incidents, and Accidents

1. System (Adverse Situations)

JAMA/JAPIA suggests that organizations should define their information security systems and roles, and minimize losses and restore normal operations as quickly as possible in the event of incidents or accidents. Therefore, it is necessary for organizations to establish clear incident/accident response systems and responsible personnel. For example, the organization should be capable of responding to information security incidents/accidents, recording incident summaries, their impact/response measures, and regularly reviewing the systems where incidents/accidents have occurred.

2. Procedures in Adverse Situations

In addition to defining information security systems and roles for prompt response to incidents and accidents, organizations must also clearly define information security incidents/accidents and execute them in business continuity plans or emergency response plans. For example, the organization's business continuity plan or emergency response plan should include information security incidents/accidents (such as malicious software infection procedures, initial procedures for responding to incidents, system recovery procedures, etc.), and regularly review the business continuity plan or emergency response plan for information security incidents/accidents and revise when necessary.

3. Risk Response

Organizations need to identify information asset security risks and take organizational measures to minimize the impact on business operations, including outsourcing operations. Therefore, JAMA/JAPIA requires internal information security risk control measures to be taken within the organization. For example, the organization can establish a list of IT equipment/devices and OS and software, including version information, administrators, management departments, installation locations, etc., or regularly review IT equipment/devices and information on operating systems and software. In addition, the organization can restrict the unauthorized installation of applications on smart devices and regularly check their installation status.

Minimize the Impact of System Stoppages and Data Loss

1. **Backup/Restore**

   Backup and recovery are important security measures for data protection and business continuity. Through data backups, organizations can ensure that they can recover data in the event of a network attack or natural disaster. Additionally, organizations can use backups to quickly restore critical systems and applications, minimizing downtime and ensuring that business operations can continue. For example, performing backups at appropriate intervals, establishing recovery procedures, and conducting backup and recovery tests for important data and systems are all important. Especially for systems that are critical to business continuity, data and procedures can be prepared to meet the recovery points and times for each system as needed.

How TXOne Solutions Meet JAMA/JAPIA Automotive Industry Cybersecurity Guidelines

Currently, the scope of the JAMA/JAPIA cybersecurity guidelines is limited to the company's basic OA environment, including areas related to corporate governance and areas related to actual security implementation. However, due to the increasing risks of attacks and information leakage targeting OT systems today, it is also ideal to include the OT environment in factories in the guidelines when considering automotive supply chain security. JAMA/JAPIA seems to have plans to expand the target area, including the factory area (OT environment), after 2023.[8]

In this chapter, we focused on the importance of security in the OT environment and the measures taken. We have added some guidelines from the JAMA/JAPIA cybersecurity guidelines to the description of OT to help OEMs and suppliers prepare for the future expansion of Japan's cybersecurity guidelines to the factory area (OT environment).

TXOne Networks' commitment to "keep the operations running" facilitates the process of risk assessment by providing visibility of the OT environment, defense capabilities, and expertise in advanced cyber threat detection.

- **Security Inspection:** Portable Inspector uses a removable approach to provide effective malware scanning with independent computer and physical isolation. It can detect and remove malicious software by bieng inserted into a USB port of any Windows and Linux device without the need for software installation or target system reboot.. In addition, Portable Inspector can collect asset information to generate an inventory list to increase IT/OT visibility and eliminate Shadow IT/OT. Equipped with an AES 256 hardware encryption engine, it also scans all files, confirming that it is free from malware before securely placing it into storage.

- **Endpoint Protection:** Stellar offers organizations an all-in-one OT solution for long-term endpoint security coverage, securing modernized assets with a library of ICS applications and certificates. For fixed-use and legacy systems, Stellar locks them down so that they can only conduct tasks related to their role, and StellarOne empowers smooth management throughout the asset lifecycle from a single pane of glass.

- **Network Defense:** Edge series employs auto-rule learning technology to assist organizations in automatically generating a network trust list, and allows organizations to create and edit L2-L3 network policies strictly based on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. Edge series also supports a wide range of industrial protocols and deeply analyzes network packets, enabling organizations to effectively block malicious behavior and errors without affecting production line operations. To protect legacy devices and production systems that are vulnerable to attack due to unpatched vulnerabilities, Edge series uses industry-leading signature-based virtual patching technology. In addition, Edge series minimizes the time required to configure and manage devices and can be easily deployed in an organization's existing OT environment.

We mapped our technical solutions and divided the functional areas in the JAMA/JAPIA cybersecurity guidelines into one of the three following categories:

- **Meets Requirement:** TXOne's solutions provide a direct way to meet the requirements mentioned in Japan's cybersecurity guidelines.

- **Supports Requirement:** TXOne Networks indirectly helps companies comply with the guidelines through the features of its solutions, mainly by streamlining processes or promoting value-added activities.

- **Not Applicable:** Some of the requirements are non-technical or not directly applicable to TXOne's technical solutions, but TXOne's solutions may help simplify written policies, procedures, and accelerate decision-making.

1. Identifying Automotive Cyber Supply Chain Risks

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Understanding details of business transactions and methods	Supports Requirement	• Portable Inspector automates malware scans, allows verification of vulnerability status, and provides instant assessment documentation to secure the procurement process.
Understanding the statuses of external connections	Meets Requirement	• Gaining better OT network visibility in terms of assets from specific vendors and all network topology, assets, software, and devices as well as applications traffic.

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Applying patches and updates	Meets Requirement	• Edge series virtual patching addresses even unpatchable asset vulnerabilities at a network level without requiring any re-configuration or changes to the asset being secured.

2. Protect Information and System Operations

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Policies	Supports Requirement	• The ODC (OT Defense Console) platform can centrally manage the network defense provided by the Edge series nodes, simplifying management even if the nodes are distributed across multiple locations. • Stellar can run on modern and legacy assets, and allows management from a single platform through StellarOne, strengthening management of modern assets and defense of legacy equipment. • ElementOne creates an inventory of OT asset information during routine scans, allowing verification of vulnerability status, OS (Operating System) updates, installed applications, and asset specifications.
Compliance	Supports Requirement	
Rules for handling confidential information	Supports Requirement	
Information security requirements between companies	Supports Requirement	
Management of information assets (information)	Supports Requirement	• Portable Inspector includes secure storage equipped with AES-256 encryption to completely safeguard all file transfers in your work site.
Management of information assets (equipment/ devices)	Supports Requirement	• Scan assets with Portable Inspector before onboarding, enabling stakeholders to confirm digital hygiene while also tracking asset security status through the entire asset lifecycle.
In-house connection rules	Meets Requirement	• Use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity.

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Physical security	Not Applicable	
Daily education	Supports Requirement	• OT zero trust-based solutions increase the efficiency of cybersecurity planning and execution, enabling more economical use of manpower while streamlining oversight and management concerns. • Portable Inspector is a user-friendly scanning device that requires no special training or education to use.
Access rights	Not Applicable	
Authentication/ Approval	Not Applicable	
Communication control	Meets Requirement	• Segment networks with the Edge series to make OT environments inherently more defensible, preventing lateral movement and other malicious actions by hackers. • Use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity.
Data protection	Supports Requirement	• Deploy EdgeIPS & EdgeFire to segment the network based on an understanding of regulations, data sensitivity requirements, and work group productivity – this prevents attackers from moving within your network or accessing any sensitive devices. • Define roles using trust list-based lockdown software Stellar to secure mission critical systems data against disruption. • Portable Inspector includes secure storage equipped with AES-256 encryption to completely safeguard all file transfers in your work site.

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Malware	Meets Requirement	• Conduct system hardening with the Stellar series lockdown software and trust lists to prevent all unapproved or suspicious applications and operations. • Edge series streamlines monitoring and inspection of OT traffic, even when specialized ICS protocols are in use. • Use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity.
System (Normal)	Meets Requirement	• Segment networks with the Edge series to make OT environments inherently more defensible, preventing lateral movement and other malicious actions by hackers. • Use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. • The Stellar series prevents unapproved USB device connectivity, script execution, and changes to configurations or data.
Office tool-related	Not Applicable	

3. Detect Unauthorized Access

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Detecting unauthorized access	Meets Requirement	• Network segmentation with the Edge series streamlines monitoring and inspection of OT traffic, even when specialized ICS protocols are in use. • Stellar disallows all activities that are not specifically trust listed while providing threat detection, including machine learning that identifies suspicious or malicious actions that are often part of unknown attacks.

4. Rapid Response to Risks, Incidents, and Accidents

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Risk response	Meets Requirement	• EdgeIPS comes equipped to make your IT and OT networks as integrated and coordinated with each other as possible, and to grant visibility of your shadow OT environment. • Portable Inspector collects a detailed snapshot of asset data including computer information, Windows Update status, and application lists. This information is collected automatically as the scan is being performed.
Procedures in adverse situations	Supports Requirement	• Use Portable Inspector's threat detection and quarantine functions for stakeholders to identify, analyze and initiate a strategic response to a cybersecurity incident. • Detailed scan logs and reports from TXOne solutions allow you to understand the target, nature, and potential impact of a threat. Determine the appropriate amount of time needed to retain logs. • Scan logs can also be exported to CSV files and then stored as evidence for nonrepudiation purposes or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server.
System (adverse situations)	Supports Requirement	• Conduct precise forensics with highly detailed scan logs and reports generated by the Edge series, the Stellar series, and Portable Inspector.

5. Minimize the Impact of System Stoppages and Data Loss on Business Operations

Key Subdomain	Practice Compliance Support	Application of TXOne Networks Solutions
Backup/Restore	Supports Requirement	• Portable Inspector is equipped with the AES 256 hardware encryption engine, which can assist ICS owners and operators in securely storing sensitive data in an air-gapped environment. At the same time, it conducts malware checks on stored files and securely saves them to a USB flash drive.

Conclusion

In the past, it has been a common concern in the field that implementing IT/OT security measures was untenable because they would only increase company costs. However, with the release of R155 Cybersecurity Regulations by the World Forum for the Harmonization of Vehicle Regulations (WP.29) and the new JAMA/JAPIA Cybersecurity Guidelines, the automotive industry will be strongly compelled to implement IT/OT security measures to defend against cyberattacks. As cyberattack methods rapidly evolve and since inadequate security measures can affect the entire supply chain, it is essential for automotive manufacturers to assess the cybersecurity maturity of their entire supply chain and require a level of cybersecurity in their contracts.

After the implementation of the JAMA/JAPIA cybersecurity guidelines, whether a company can continue to gain the trust of automotive industry clients will depend on whether the organization can achieve an acceptable level of cybersecurity. All automotive industry companies, regardless of size, should implement the requirements of the new JAMA/JAPIA cybersecurity guidelines. However, in the worst-case scenario, organizations that do not prioritize cybersecurity may be eliminated from the supply chain. This makes cybersecurity a crucial factor in the success or failure of suppliers.

In this article, we analyzed the background of the establishment of the JAMA/JAPIA cybersecurity guidelines, provided a brief explanation of cybersecurity control measures, and discussed how solutions can help organizations meet these guidelines. Enterprises can conduct self-assessments using a cybersecurity checklist, which can enumerate the current situation of the organization and the gap between its current cybersecurity status and cybersecurity goals, helping them understand the next steps to take. When an organization finds that many items have not been implemented and does not know where to start, they can rely on TXOne Network’s solutions to meet or simplify the requirements.

Although the guidelines currently prioritize OA security measures, we believe that IT should be evaluated together with the OT of smart factories. In the future, there is a high chance that Japan's cybersecurity guidelines will extend to factory areas (OT environments). For this reason, we believe that the best practice in the industry is to consider security measures in conjunction with important future actions such as smart factories and digital operations, rather than implementing IT security measures alone. TXOne Networks puts more emphasis on cybersecurity countermeasures in the OT environment. To help organizations strengthen OT defenses, our solutions are specifically designed for the OT environment and are based on the zero-trust principle to meet the organization's operational resilience requirements. We focus on the future of the automotive industry and will continue to provide security advice and share our insights to the sector.

References

[1] Naomi Tajitsu, David Evans, "Nissan resumes production at UK plant hit by cyber-attack", Reuters, May 2017.

[2] Joe Tidy, "Honda's global operations hit by cyber-attack", BBC News, June 2020.

[3] Satoshi Sugiyama, Tim Kelly and Maki Shiraki, "Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours", Reuters, February 2022.

[4] Mihoko Matsubara, "The Japanese Automobile Industry Is Taking Next Steps for Cybersecurity Collaboration", Lawfare, July 2020.

[5] JAMA, "Japan Automobile Manufacturers Association", JAMA, Accessed April 2023.

[6] ICT未来図, "自動車産業サイバーセキュリティガイドラインを読み解く～自動車産業サプライチェーンが実装すべき対策", ICT未来図, March 2023.

[7] JAMA/JAPIA, "JAMA/JAPIA Cybersecurity Guidelines: Further Development of Cybersecurity Measures in the Automobile Industry", JAMA/JAPIA, April 2022.

[8] 鎌田 浩一郎, "CASE時代にとるべき、自動車サプライヤーのサイバーセキュリティ対策", SoftBank, March 2023.

txone.com