

# FY 2024 Senior Management Briefing Session

## Request for Self-Evaluation and Implementation of Automotive Industry Cybersecurity Guidelines

Japan Automobile Manufacturers Association, Inc.

ICT Subcommittee  
General Policy Committee

Procurement Subcommittee  
Supply Chain Committee

Japan Auto Parts Industries Association

Cyber Security Subcommittee  
DX Management Committee

Supply-Chain Subcommittee  
Organizational Affairs Committee

August, September, October 2024

# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

## 1-1. Today's Briefing Session

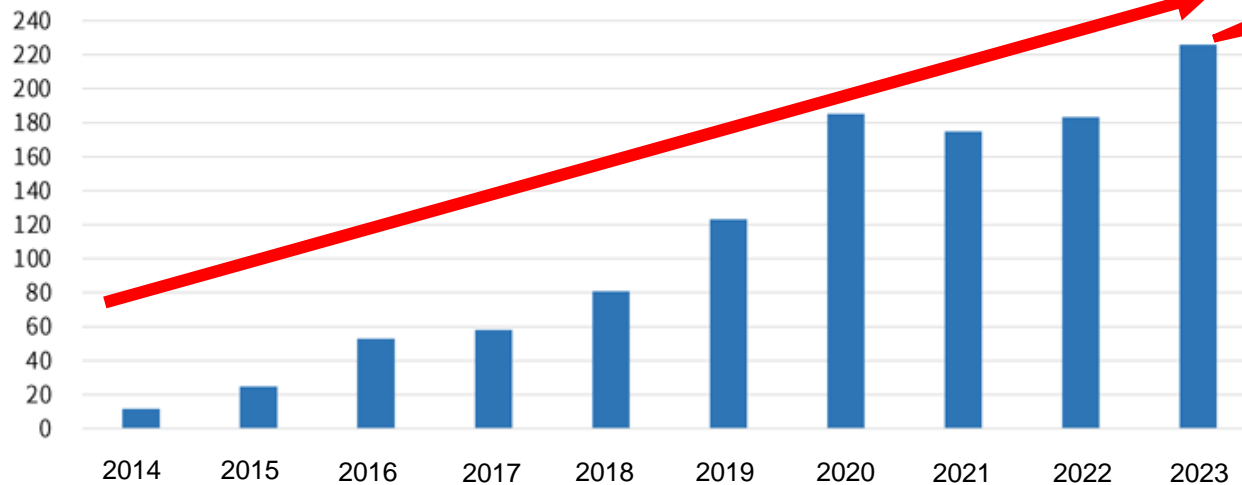
- ✓ Today, we invite you to confirm our observations regarding the rising global trends in information security incidents in recent years and request you to:
  - (1) **understand and enhance your organization's information security posture by applying the Automotive Industry Cyber Security Guidelines and**
  - (2) **collaborate with your business partners to elevate security standards across the supply chain.**
  
- ✓ Additionally, we will present a **video message from the Ministry of Economy, Trade and Industry pertaining to this initiative.**
  
- ✓ We sincerely hope this briefing will provide valuable insights for all participating organizations.

# 1-2. Global situation

Every device connected to the internet faces about **6,000 cyber-attacks daily**. These **attacks are becoming increasingly complex and sophisticated each year, with further escalation expected**. **By sector, the manufacturing sector experiences the highest volume of attacks**, accounting for 34% of all recorded incidents. **Cybersecurity is a critical issue for all organizations**, making it **essential to adopt a proactive approach to threats, viewing them as urgent and personal**.

Annual number of cyber-attack-related communications received per IP address (last 10 years)

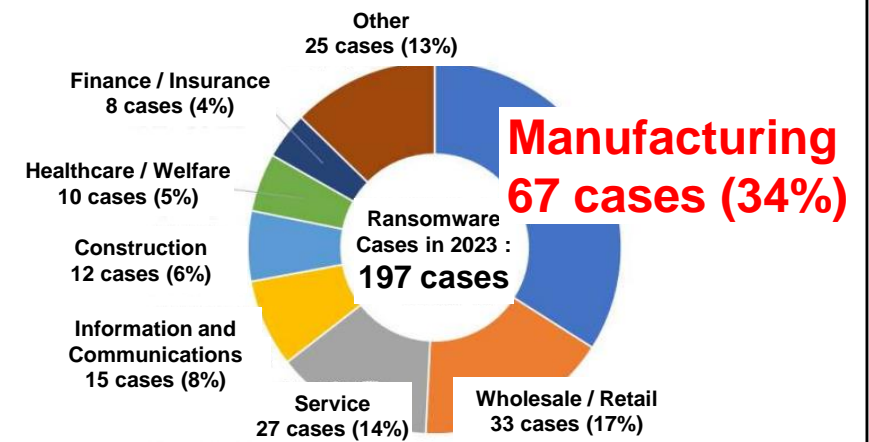
(Number of packets, Unit: 10,000)



Source: National Institute of Information and Communications Technology (NICTER) Observation Report 2023

Approx. 2.26 million cases/year (approx. 6,000 cases/day)

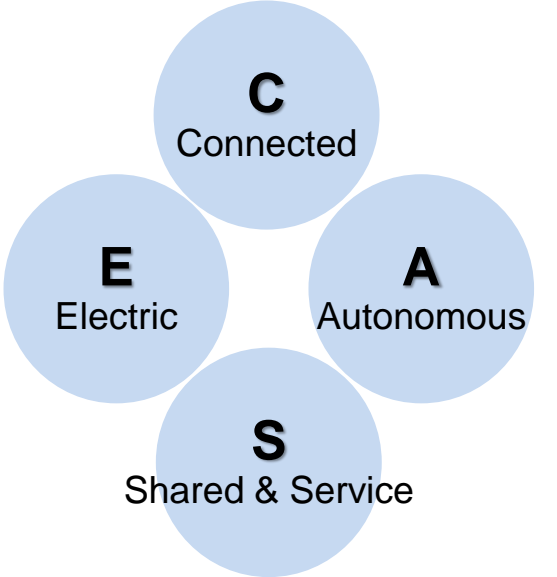
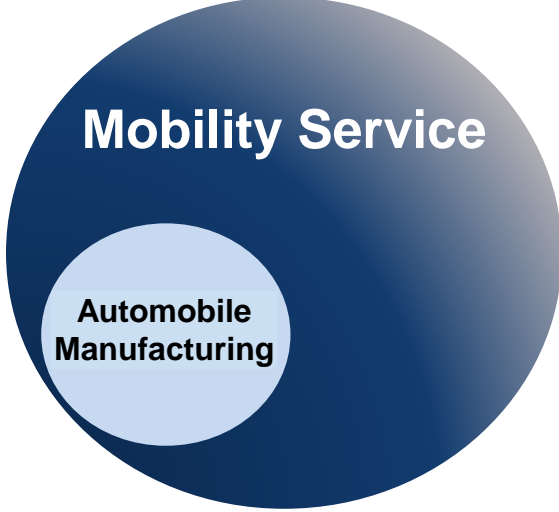
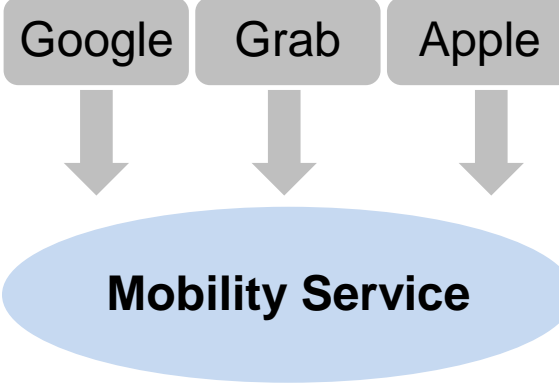
By sector (2023)



Source: "Trends in the Number of Reported Ransomware Cases" <National Police Agency>

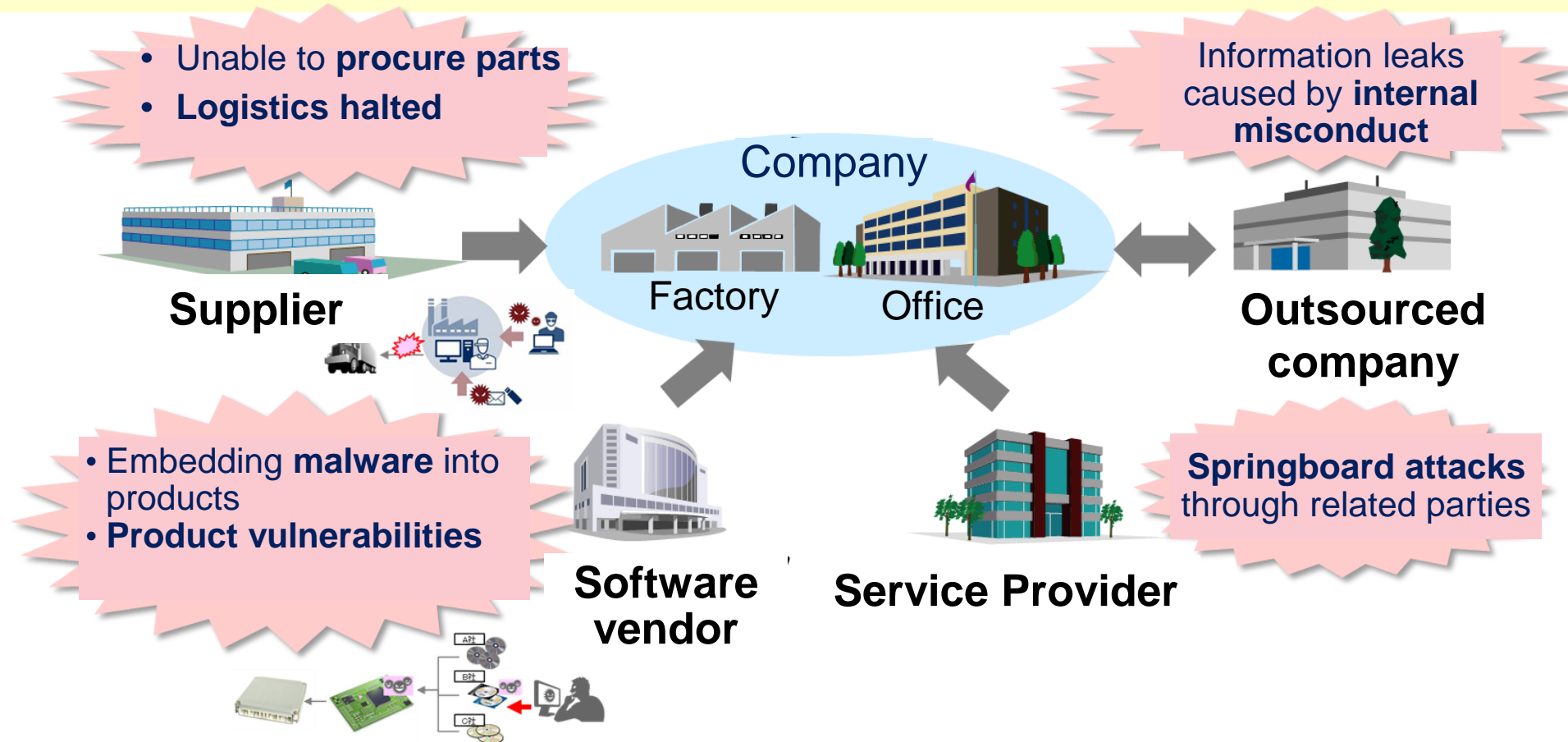
# 1-3. Changes in the automotive industry landscape: Changes in data management

The automobile industry is currently experiencing a transformative change that is unprecedented in the last century, fueled by advancements in CASE technologies. The **industry is collectively advocating for the integration of information technology (IT) to facilitate the development of a mobility society**. As these technologies are adopted, there is a **simultaneous increase in the volume of information and data being managed**.

Rapid technological innovations	Expansion of competitive domain	Changes in competing companies	Increase in the amount of data handled	
			Information owned	Details
<p>Simultaneous occurrence of <b>CASE Innovations</b> (Connected, Autonomous, Shared &amp; Service, and Electrification)</p>	<p><b>A transition from automobile manufacturing to mobility services</b> The domain is undergoing a significant change</p>	<p>The importance of hardware has decreased due to electrification, while <b>companies focusing on software</b>, such as autonomous driving, connectivity, and shared services, <b>are emerging as players</b>.</p>	<p><b>Vehicle information</b></p>	<ul style="list-style-type: none"> <li>• Location info</li> <li>• Speed info</li> <li>• Engine info</li> <li>• Control system info</li> </ul>
			<p><b>Technical information</b></p>	<ul style="list-style-type: none"> <li>• Drawings</li> <li>• CAD data</li> <li>• Development info</li> <li>• Design, etc.</li> </ul>
			<p><b>Privacy information</b></p>	<ul style="list-style-type: none"> <li>• Personal info</li> <li>• Financial info</li> <li>• Vehicle ownership info</li> </ul>
			<p>Alongside traditional information, <b>information</b> about electrification and smart technology <b>has risen considerably</b>.</p>	

# 1-4. Security Risks in the Supply Chain

As the industry continues to evolve and the amount of data grows, **protecting just one's own organization is no longer enough**. Attackers consistently exploit weaknesses within the supply chain, highlighting the need for **thorough risk management across all entities involved**.



# 1-5. Security Promotion Activities in the Automotive Industry Supply Chain

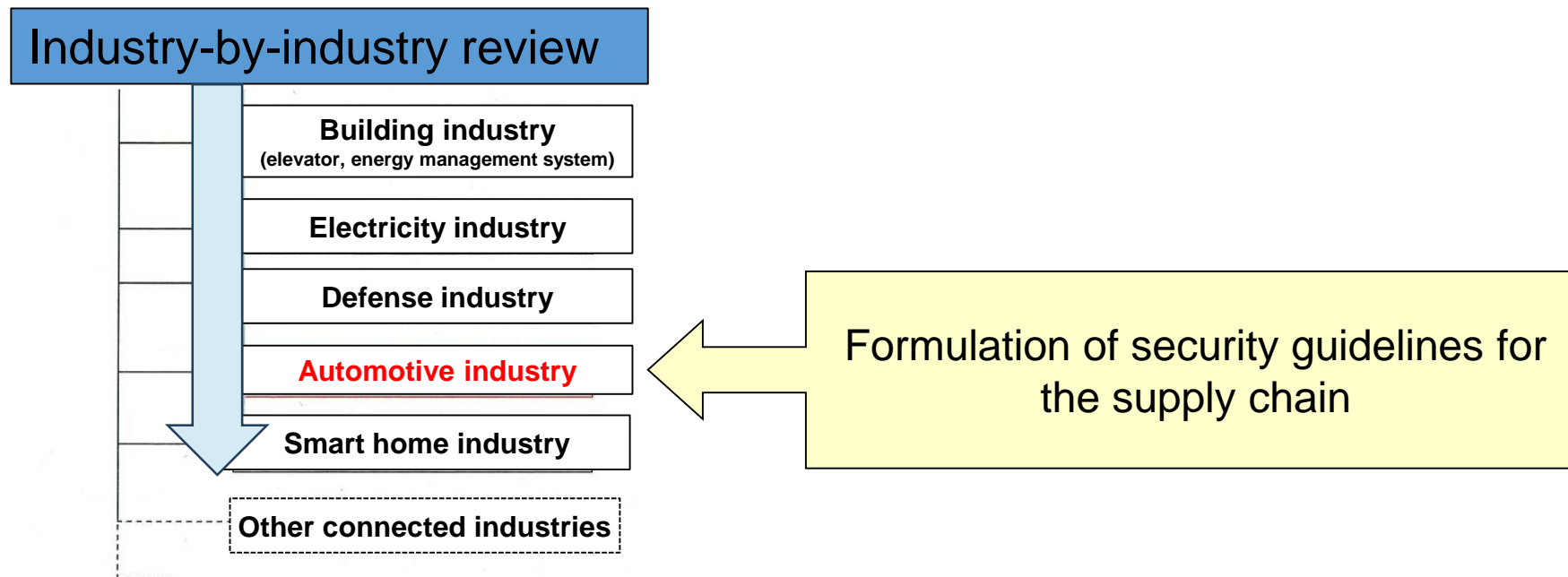
Activities undertaken by the automobile industry are guided by the country's overall policy.

**Industry-standard guidelines are set** to enhance security across the industry.

We are collaborating with relevant companies in the industry to improve security levels.

[Standard Model]

**Ministry of Economy, Trade and Industry: Cyber Physical Security Framework (CPSF)**



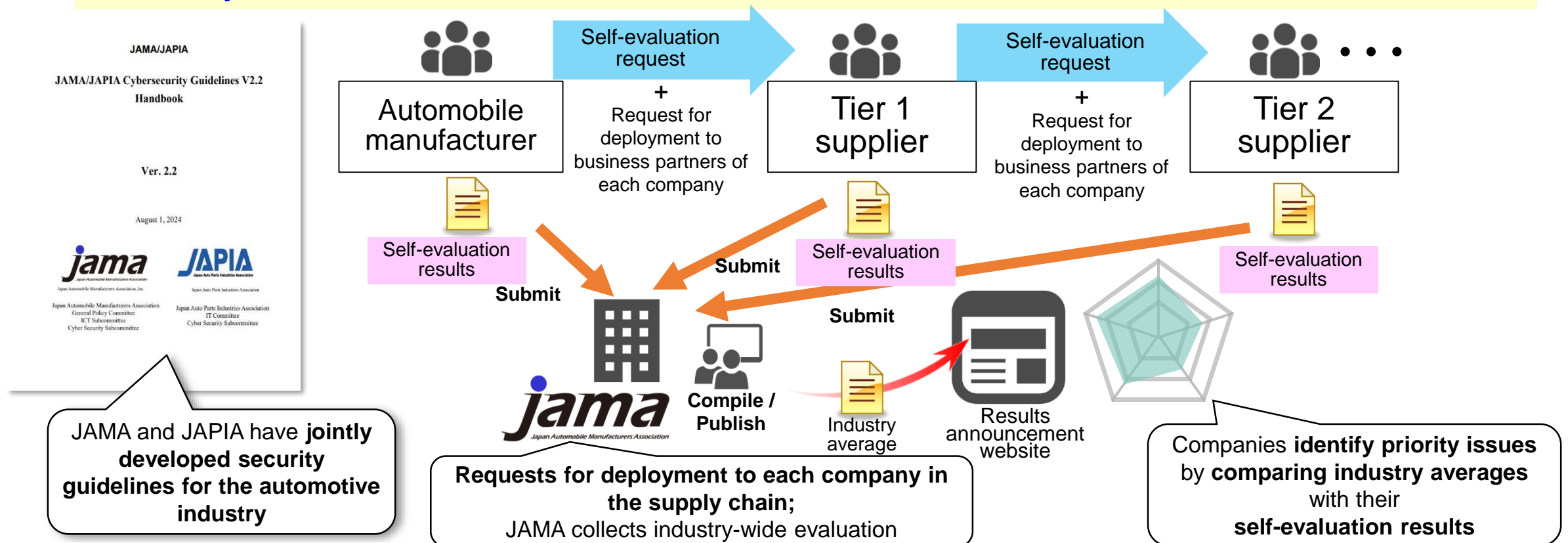


# 1-6. Specific Activities

In FY 2019, **JAMA and JAPIA collaboratively established industry-standard cybersecurity guidelines** in alignment with the METI's CPSF.

Beginning in March 2021, **the automotive industry has been requested to conduct self-evaluations and enhance its cybersecurity levels.**

→ Companies will use these self-evaluation results to **identify priority areas and take steps to enhance their security levels.**



# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

## 2-1. Introduction of Mr. Toshikazu OKUYA, Ministry of Economy, Trade and Industry



Toshikazu OKUYA

Deputy Director-General,  
Commerce and Information  
Policy Bureau

Mr. Okuya joined the Ministry of International Trade and Industry, now known as the Ministry of Economy, Trade and Industry (METI), in 1995. Over the years, he has undertaken various responsibilities, including macroeconomic analysis, the formulation of science and technology strategies, civil service system reform, and enhancing information system reliability. In 2010, he transitioned to the role of an industrial researcher at the Japan External Trade Organization (JETRO) New York Center. Since 2013, he has played a pivotal role in formulating Japan's 4th Strategic Energy Plan as the Director of the Supply and Demand Policy Office at the Agency for Natural Resources and Energy. He has been actively engaged in security trade control policy since 2015 and, in 2016, took on the position of Director of the Security Trade Control Policy Division, focusing on amending the Foreign Exchange Act to strengthen regulations concerning inward direct investment. **In July 2017, he was appointed Director of the Cybersecurity Division within the Commerce and Information Policy Bureau. Subsequently, in July 2021, he assumed the role of Director of the General Affairs Division of the Commerce and Information Policy Bureau and, in July 2022, transitioned to serve as the Director of the General Affairs Division of the Economic and Industrial Policy Bureau. As of July 2024, he continues to hold his current position.**

[Work history]

1995	Joined the Ministry of International Trade and Industry (METI)
August 2003	Researcher, Harvard University
August 2004	Pursued a Mid-career Master's at Harvard University's Kennedy School
July 2010	Seconded to the Japan External Trade Organization (JETRO) as an industrial researcher at the JETRO New York Center
June 2013	Director of the Supply and Demand Policy Office, Comprehensive Policy Division, Commissioner's Secretariat, Agency for Natural Resources and Energy (Additionally, Director of the Research and Public Relations Office starting June 2014)
June 2015	Director of the Security Trade Control Division, Trade Control Department, Trade and Economic Cooperation Bureau, METI
June 2016	Director of the Security Trade Control Policy Division, in the same department
July 2017	<b>Director of the Cybersecurity Division, Commerce and Information Policy Bureau, METI</b>
July 2021	<b>Director of the General Affairs Division, Commerce and Information Policy Bureau, METI</b>
July 2022	<b>Director of the General Affairs Division, Economic and Industrial Policy Bureau, METI</b>
July 2024	Current position

## 2-2. Video Contribution

\*This video has been removed due to issues related to video distribution rights management.

## 2-3. Appreciation for Video Contribution











- ✓ We sincerely appreciate Mr. Toshikazu Okuya from the Ministry of Economy, Trade and Industry for his valuable contribution to our discussion.
  - ✓ Moving forward, we will emphasize the senior management's mindset, using real-world case studies to deepen our understanding.
- Additionally, we will outline the request for self-evaluation in FY2024.

# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

# Actual Damage Incidents

# 3-1. Damage Cases Around the World

Major risks	Targeted organization	Damage outline	
Suspension of business	Auto parts manufacturing	<ul style="list-style-type: none"> <li>In February 2022, a <b>ransomware attack</b> on the company spread to its business partner, an automobile manufacturer, <b>suspending 28 production lines across 14 factories.</b></li> </ul>	 
	Nagoya Port	<ul style="list-style-type: none"> <li>In July 2023, a <b>ransomware attack caused a system failure</b> at the Nagoya Port Container Terminal, <b>halting operations for about 3 days.</b> Ultimately, the <b>loading and unloading of around 20,000 containers were impacted.</b></li> </ul>	
	General medical center in Kansai region	<ul style="list-style-type: none"> <li>In October 2022, a general medical center <b>suspended non-emergency surgeries and outpatient treatments</b> as a result of a <b>ransomware attack.</b></li> </ul>	
	Publishing	<ul style="list-style-type: none"> <li>In June 2024, a <b>cyber-attack</b> on a subsidiary's data center server caused system failures, <b>disrupting operations for the entire group.</b> The breach <b>leaked</b> employees' <b>personal information</b>, compromised contracts with business partners, and exposed student data from an educational institution.</li> </ul>	 
Confidential / personal information leakage	Communication services	<ul style="list-style-type: none"> <li>In November 2023, a server was targeted in a cyber-attack, leading to the <b>leak of about 440,000 pieces of personal information.</b> In February 2024, it is <b>possible that about 57,000 pieces of employee information may have been further compromised.</b></li> </ul>	 
	Electrical machinery manufacturing	<ul style="list-style-type: none"> <li>In January 2020, November 2020, and October 2021, there were <b>several information leaks resulting from unauthorized access to the company's subsidiary in China.</b> The leaked data included <b>20,000 pieces of defense-related information</b>, raising concerns about its <b>potential impact on national security.</b></li> </ul>	 



## 3-2. Cyber Attack on Nagoya Port: Overview

Nagoya Port, recognized as the leading port in Japan with an annual trade value of approximately 21 trillion yen, suffered a cyber-attack. **This incident has adversely impacted the operations of automobile manufacturers and caused delays in deliveries for apparel manufacturers.**

### Overview

- ✓ On the morning of July 4, 2023, a failure occurred in the Nagoya Port Unified Terminal System (NUTS), halting operations at all terminals in Nagoya Port.
- ✓ **The system was encrypted in a ransomware attack, leading to an operational failure.**
- ✓ **Recovery was prioritized, and the system was restored from a backup. Operations resumed at all terminals** on the evening of July 6, **roughly three days after the incident.**

### Impact

- ✓ Cargo handling schedules for 37 vessels were impacted.
- ✓ The loading and unloading of around 20,000 containers were disrupted.
- ✓ Operations were halted at several domestic bases of automakers.
- ✓ The delivery of clothing was delayed at apparel manufacturers, among others.
- ✓ **No information leaks were reported.**

### [Impact of terminal service outage]



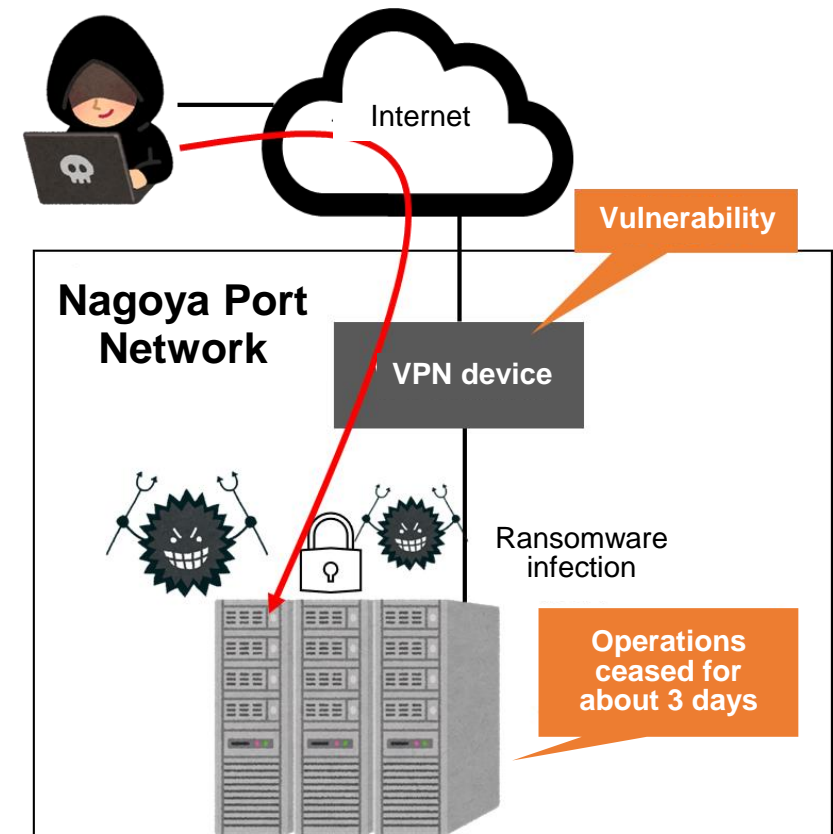
**This attack led to the suspension of operations at car manufacturers and delivery delays at apparel manufacturers.**

## 3-3. Cyber Attack on Nagoya Port: Status

There was a possibility that **unauthorized access occurred due to a vulnerability in a VPN device** used for maintenance. However, because recovery was prioritized and the response was carried out without proper investigation or analysis, the **route of infection could not be determined**. Additionally, **malware was found in the backups**, which delayed the recovery process as it needed to be removed.

### Status

- ✓ There was a possibility of **unauthorized access due to vulnerabilities in the maintenance VPN device**.  
\* Because recovery efforts were prioritized, the route of infection could not be determined.
- ✓ All physical and virtual servers in the data center were compromised.
- ✓ **Backups had only been maintained for three days, and malware was found in these backups**, which extended the recovery time needed for removal.
- ✓ Roughly 100 threatening documents were printed from the system's dedicated printer; however, these documents did not specify a ransom amount, so the attacker was not contacted.



## 3-4. Cyber Attack on Nagoya Port: Manager's Comments



I always believed that cyber-attacks primarily targeted large corporations.

**I could have never imagined** that an attack of the scale we experienced **would hit a small or medium-sized enterprise like ours.**

Source: NHK: <https://www3.nhk.or.jp/news/html/20230905/k10014183621000.html>

## 3-4. Cyber Attack on Nagoya Port: Problems and Learnings

### Problems

#### (1) Inadequate basic countermeasures

- Neglect of security measures for VPNs utilized in maintenance work
- Insufficient anti-virus protections
- Failure to maintain logs essential for incident investigations
- Inadequate duration for backups

#### (2) Lack of preparedness for incident response

- Response procedures for system failures were not established
- No opportunity to seek expert opinions during the initial response.
- Insufficient confirmation and evaluation of system reliability at the time of restoration

### Learnings

#### (1) Review the implementation status of essential countermeasures and consistently apply them based on the company's specific risks

⇒ Utilize the Automotive Industry Security Guidelines to evaluate the effectiveness of the company's countermeasures and make **ongoing improvements** through industry comparisons.

#### (2) In addition to preventative measures, develop a proactive plan for potential incidents.

⇒ **Create a plan** of response and recovery procedures for when an incident occurs, along with a detailed organizational structure and division of roles within the company.

⇒ **Conduct regular training** to help personnel anticipate and respond to incidents effectively.

**Cybersecurity measures should be viewed as a management issue, and strong leadership from senior management is essential for their effective promotion.**

Senior management should understand the associated risks, communicate their significance clearly and personally, establish a structured security response organization, make informed decisions regarding security investments, and take additional relevant actions.

# Senior Management Attitude

## 3-6. Risks from Cyber-Attacks: Business Suspension

Cyber-attacks on supply chains resulted in the **suspension of vehicle production operations**  
 → **Cyber-attacks directly impact business continuity.**

### Case study of operational suspension due to supply chain attack

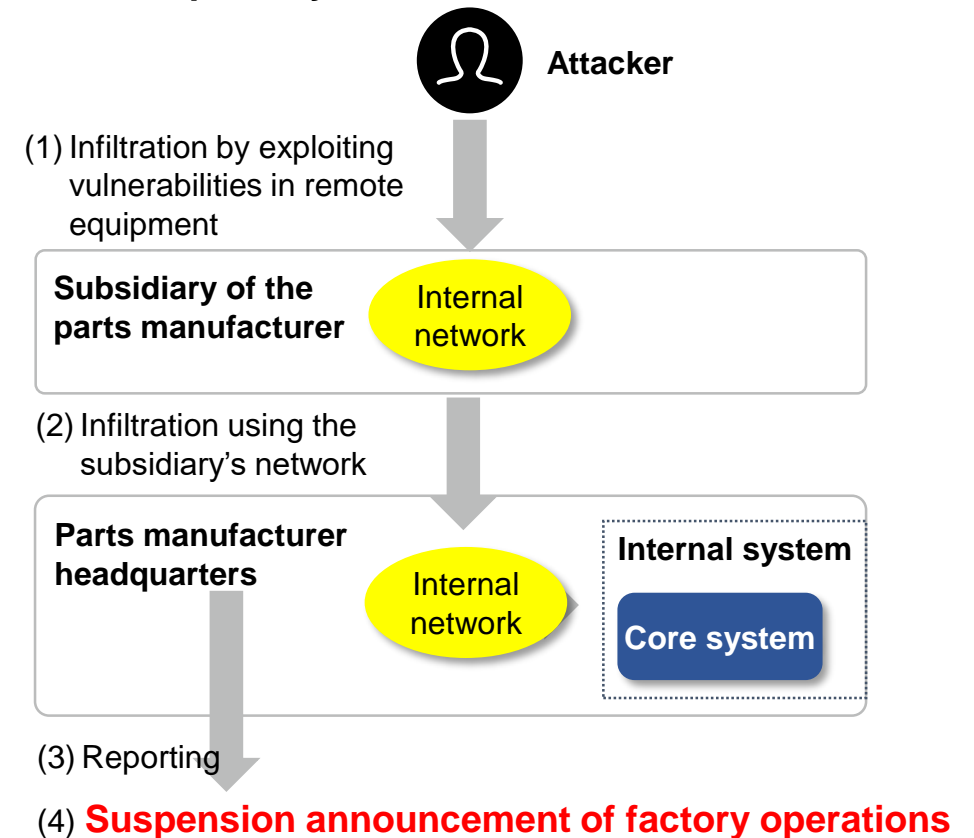
#### Outline

- In February 2022, the company suspended operations at all its domestic factories, which include 28 production lines at 14 locations, due to a system failure at one of its parts manufacturers.
- A vulnerability in a remote connection device used by a subsidiary of the parts manufacturer was exploited, leading to a breach of their network. Subsequently, the headquarters network of the parts manufacturer was also compromised.
- This incident rendered several internal systems, including email, inoperable and **shut down the core system** responsible for issuing and receiving part orders and managing delivery data.

#### Impact

- **The one-day shutdown of all domestic factories impacted the production of approximately 10,000 units**, estimated to represent 5% of the monthly production volume in January of that year.

#### Speculative overview of the case based on publicly available information



# 3-7. Risks from Cyber-Attacks: Litigation

Infiltration using a legitimate employee ID indicates that **employee information may have been compromised, raising concerns about potential litigation risks.**

→ **If measures are not implemented, the senior management could face liability.**

## Case Study of Litigation Risk

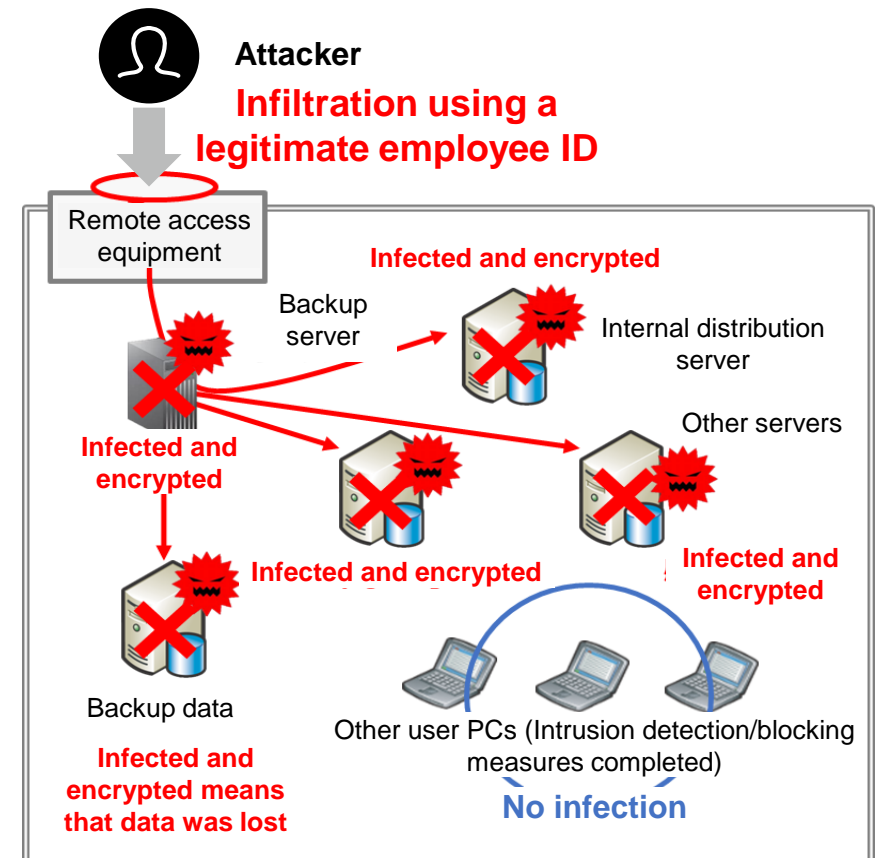
### Outline

- In June 2023, a cyber-attack targeted the North American base of a major automobile manufacturer.
- A remote connection device at this base was exploited using the ID of a legitimate employee, causing various servers on the network to be infected and encrypted, which led to a system shutdown.
- However, since the production and internal systems, such as email, operated through external systems, there was no business interruption.

### Impact

- All internal servers and networks were suspended.  
No impact on production.
- A lawyer was consulted **due to concerns about potential employee information leaks**  
This could lead to a lawsuit from the affected employee.

### Incident Overview



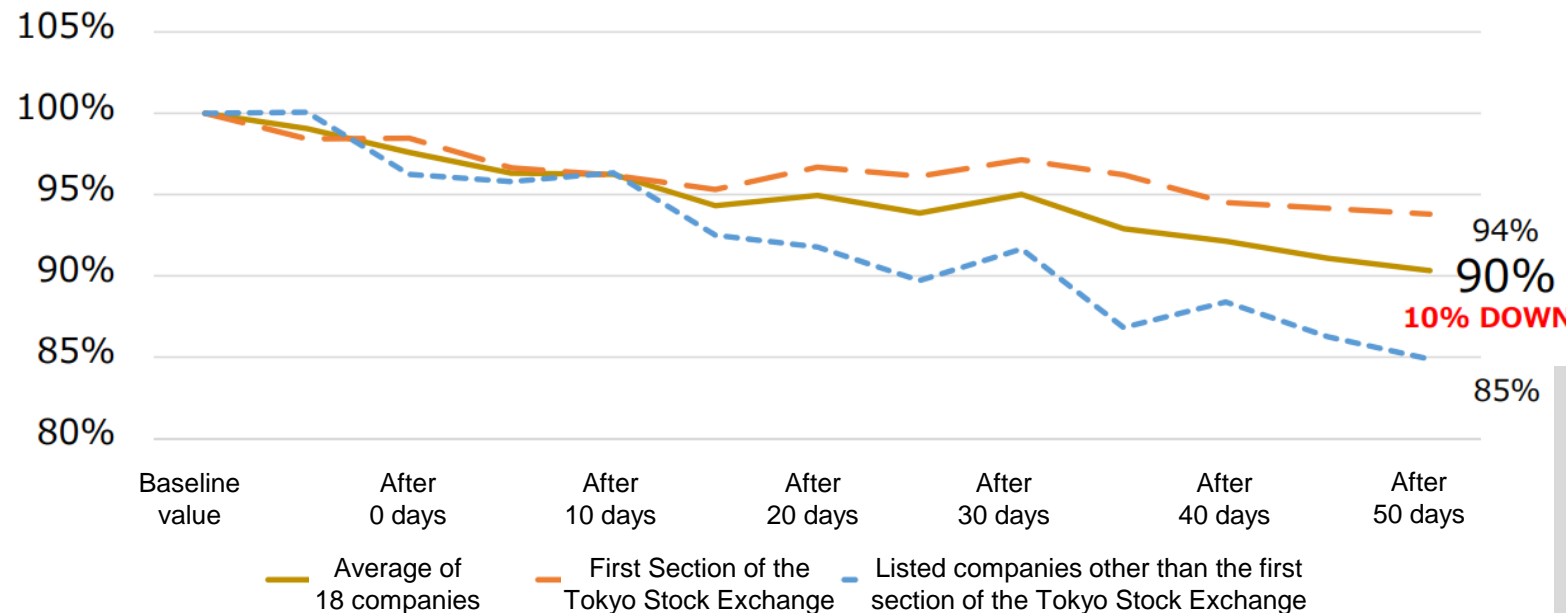
# 3-8. Risks from Cyber-Attacks: Stock Price Decline

If information leaks, **stock prices typically decline by 10%**  
 → Cyber-attacks **directly affect corporate value.**

## Impact of cyber-attacks on stock prices

- When information leaks occur in Japan, stock prices **drop by an average of 10%.**
- In particular, stock prices of companies not listed on the First Section of the Tokyo Stock Exchange **decline by 15%.**

Analysis of Stock Price Trends After Timely Disclosure of Cyber Incidents (n=18)



**Survey Method**

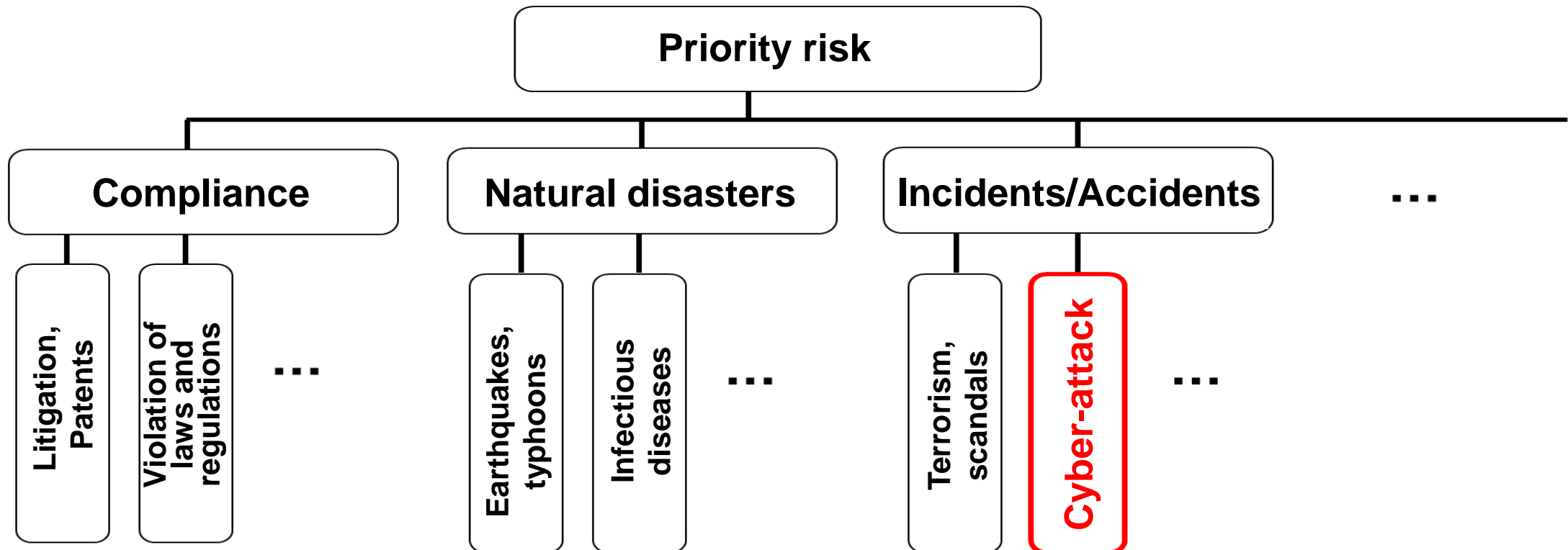
- The study focused on 18 companies that promptly disclosed incidents to the stock exchange.
- These companies were selected based on their timely disclosures made after July 2014.
- A period of 10 days prior to each disclosure date was established as the baseline value (100%).
- Adjustments were made for fluctuations in the Nikkei Stock Average.

Source: "Cyber Risk Quantification Model" by Japan Cybersecurity Innovation Committee (JCIC)



### 3-9. Leadership Actions Required from Senior Management

**Cyber-attacks represent a high-priority risk for companies to address. Senior management should exemplify strong leadership in cybersecurity initiatives, fostering awareness among employees and throughout the organization.**



## 3-10. Senior Management Attitude

- The “Cybersecurity Management Guidelines” issued by the Ministry of Economy, Trade and Industry outline **essential considerations for senior management to safeguard their businesses against cyber-attacks effectively**.
- In an increasingly complex risk environment where cyber threats are both frequent and sophisticated, management **executives should determine the appropriate security measures and investments to integrate into their corporate strategies**.

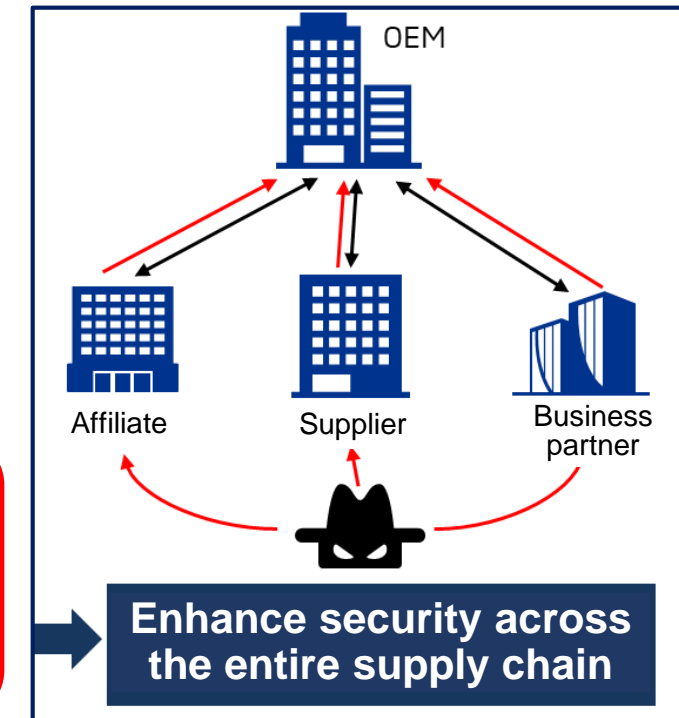
◆ Three essential principles for senior management to consider, as outlined in the Guidelines:

- (1) Acknowledge cybersecurity risks and **demonstrate leadership in addressing them**.
- (2) **Implement security measures across the entire supply chain**, including all business partners and subcontractors.
- (3) **Actively communicate** about security risks and mitigation strategies with relevant parties, both regularly and in emergencies.

 **Point !**

Security measures should be viewed not as a “cost” but as a vital “investment” essential for supporting future business activities and fostering growth.

Investing in security is the responsibility of senior management, and their decisions are crucial to its effectiveness.



“No chain is stronger than its weakest link.”  
Refer to: “The Valley of Fear,” Arthur Conan Doyle, 1914.

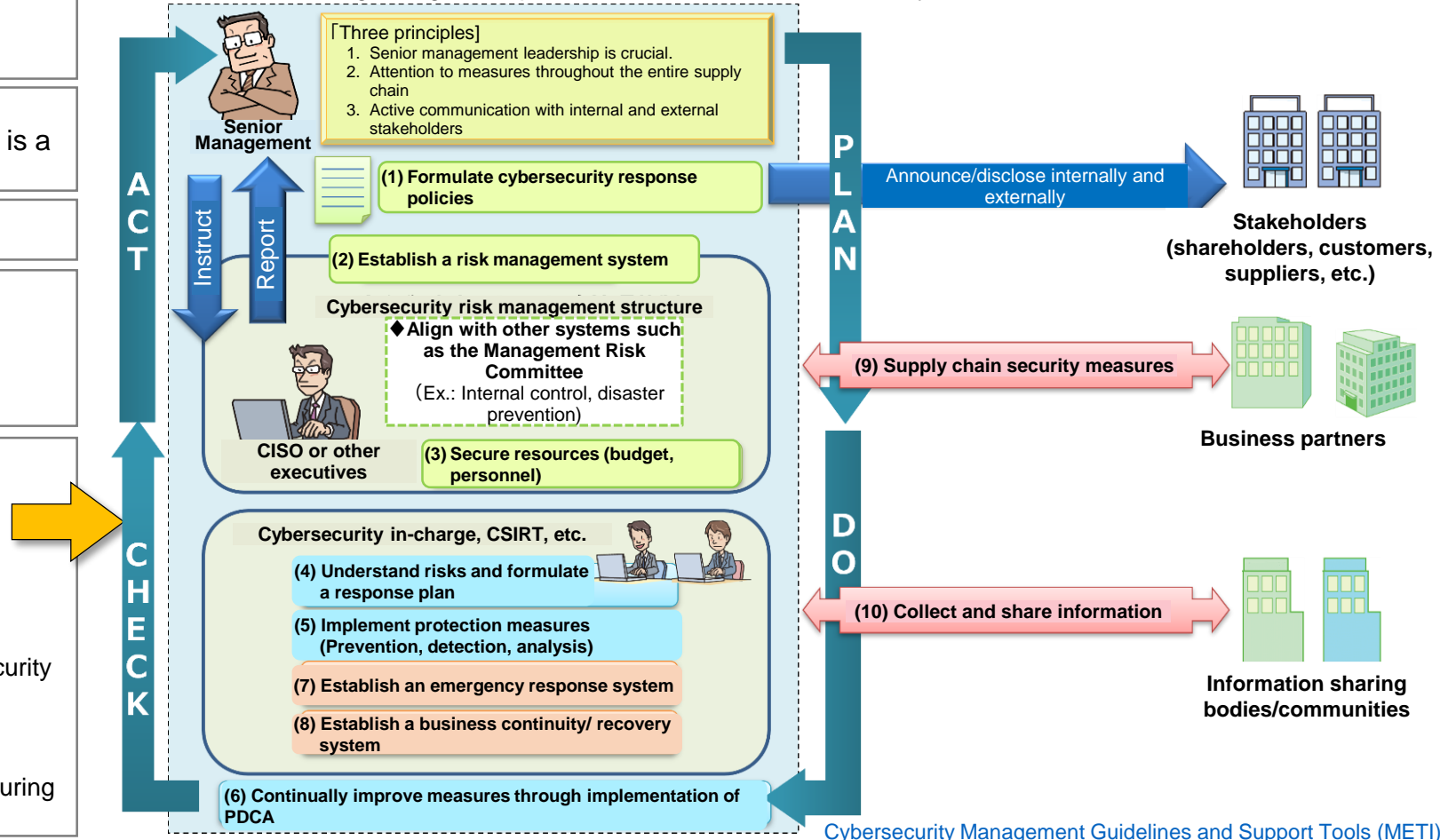
# 3-11. Reference: Cybersecurity Management Guidelines

**Cybersecurity Management Guidelines offer a framework for senior management to execute cybersecurity measures as part of a corporate strategy.**

## Overview of Cybersecurity Management Guidelines

Three principles that senior management needs to recognize to protect their companies from cyber-attacks, and ten important items that senior management should ensure their managers (CISO, etc.) are informed about regarding the implementation of information security measures.

<b>Purpose</b>	To promote cybersecurity measures under the leadership of senior management
<b>Target</b>	Senior management of companies that deliver IT systems and services, as well as those for which IT is a critical component of their business strategies
<b>Issuer</b>	Ministry of Economy, Trade and Industry
<b>Revision</b>	Ver1.0 : December 2015 Ver1.1 : December 8, 2016 Ver2.0 : November 16, 2017 Ver3.0 : March 24, 2023
<b>Contents</b>	<ol style="list-style-type: none"> <li>1. Introduction</li> <li>2. <b>Three principles which the senior management need to recognize</b></li> <li>3. <b>Ten important items of cybersecurity management</b></li> </ol> Appendices <ol style="list-style-type: none"> <li>A) Check sheet of cybersecurity management</li> <li>B) Reference information on cybersecurity measures</li> <li>C) Information to reference when preparing for a cybersecurity incident</li> <li>D) Relationship with relevant standards and frameworks</li> <li>E) Definitions of Terms</li> <li>F) Guidelines for building a cybersecurity system and securing human resources</li> </ol>



# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

## 4-1. Analysis of Self-Evaluation Results for FY 2023

- ✓ In FY2023, a total of 3,240 companies completed self-evaluations (see 1-6. Specific Activities for details).
- ✓ Average scores for all security level items showed improvement compared to FY 2022.
- ✓ About 20% of companies are still at Level 1, indicating a need to improve security to at least Level 2.

Year	Total responses	Total number of valid responses	Average score
2023	3,240 companies	3,240 companies	Level 1 items: 81.84/100 points (81.8%) Level 2 items: 120.00/148 points (81.1%) Level 3 items: 42.91/58 points (74.0%)
2022	4,026 companies	3,961 companies	Level 1 items: 76.95/100 points (77.0%) Level 2 items: 110.49/148 points (74.7%) Level 3 items: 37.35/58 points (64.4%)
2021	2,300 companies	2,296 companies	Level 1 items: 70.97/100 points (71.0%)

(In 2021, only level 1 items were included because the version was V1.0.)  
Systemization reduced duplication of the same company.

### FY 2023 Average Score Details

Target level	No. of companies	Average score			
		Level 1 items	Level 2 items	Level 3 items	Total
Level 1	659 companies	62.05/100 points (62.1%)	-	-	62.05/100 points (62.1%)
Level 2	1,830 companies	85.42/100 points (85.4%)	116.84/148 points (78.9%)	-	197.08/248 points (79.5%)
Level 3	751 companies	94.46/100 points (94.5%)	136.34/148 points (92.1%)	42.91/58 points (74.0%)	258.03/306 points (84.3%)
Total		81.84/100 points (81.8%)	120.00/148 points (81.1%)	42.91/58 points (74.0%)	-

## 4-2. Requests for FY 2024

- ✓ In order to consistently monitor your progress, we request that you conduct a self-evaluation similar to the one completed in FY2011.

**Submission deadline: December 31, 2024**

- ✓ We are hopeful that this initiative will extend to a broader range of suppliers, thereby fostering its growth throughout the automotive industry.

### 1) Self-evaluation by companies and results submission to JAMA



### 2) Request to business partners

\* Self-evaluation and results submission to JAMA



## 4-3. JAMA/JAPIA-expected Achievement Level and Timeline

✓ Maintain the same level of achievement and timeline as last year.

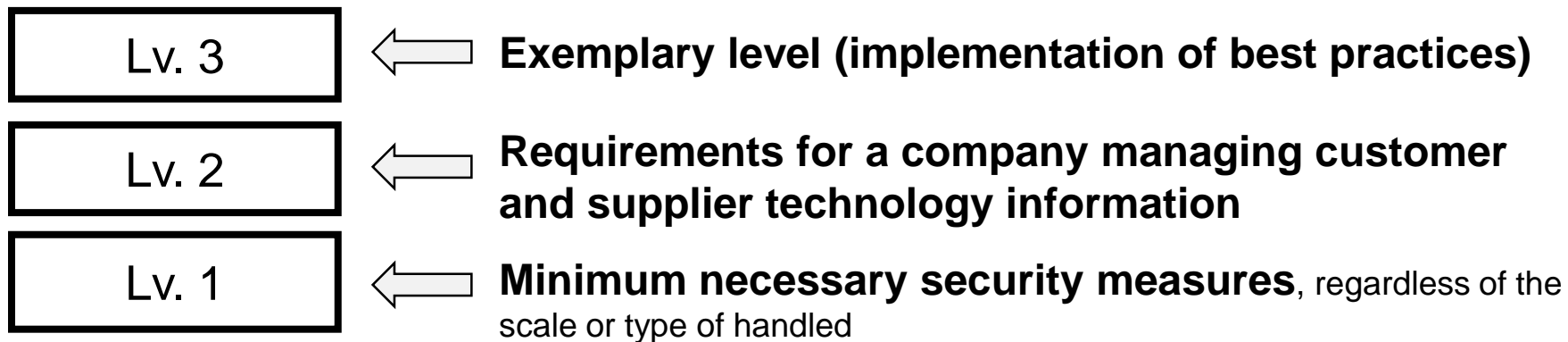
⇒ **Please strive to meet this target within this FY 2024.**

- Level: We request **all companies** in the automobile industry **to comply with the requirements in Levels 1 and 2.**
- Timeline: We request that you plan for systematic improvements by the **end of fiscal year 2024.**

\* Automobile manufacturers, leading Tier 1 companies, and organizations with advanced technology and expertise are encouraged to strive for Level 3.

\* While this may pose some challenges, we kindly ask that you meet all Level 1 requirements by the end of FY2012 and work to fulfill Level 2 requirements to the best of your ability.

### < Security Level Definitions in the Automotive Industry Cybersecurity Guidelines >



## 4-4. Self-Evaluation and Report Submission Guidelines

Please assess your security posture according to the FY 2024 Automotive Industry Cybersecurity Guidelines and submit your report based on the following guidelines.

Items		Description
1	JAMA check sheet used for self-evaluation	<ul style="list-style-type: none"> <li>The check items remain the same as those for fiscal year 2023; however, the checklist has been updated due to minor revisions. <b>Please ensure you obtain and use Checklist V2.2 from the following site on the JAMA website:</b>  <a href="#">Automotive Industry Cybersecurity Guidelines   JAMA - Japan Automobile Manufacturers Association</a></li> </ul>
2	Submission deadline	<ul style="list-style-type: none"> <li><b>Please submit by the end of December 2024.</b></li> </ul>
3	Submission methods (JAMA/requester)	<ul style="list-style-type: none"> <li>Before proceeding, please confirm the submission method outlined in the site referenced in section 1 above.</li> <li>The submission method outlined in the guidelines has partially changed.               <ol style="list-style-type: none"> <li><b>Apply through the "Application for Information on Automotive Industry Security Activities" link at the site specified in section 1.</b></li> <li><b>Alternatively, submit using the destination URL provided via email.</b></li> </ol> </li> </ul>
4	Supplementary information	<ul style="list-style-type: none"> <li>Companies that receive a request for self-evaluation are requested to <a href="#">ask their tier-1 suppliers to perform self-evaluations</a>. Additionally, they should request that these suppliers extend this self-evaluation request to their tier-1 suppliers.</li> </ul>



# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

## 5-1. Schedule for Upcoming Seminars

- ✓ **To enhance the cybersecurity robustness across the entire automotive industry supply chain**, the following initiatives will be implemented:
  - Provision of information aimed at **enhancing the skills of security promotion personnel**
  - Consultation sessions to **resolve issues related to security promotion**, with 12 sessions planned.
- ✓ **Event details** will be available on the JAMA website. Please visit for more information.

Event	Description	Schedule
Sharing information for promotion personnel	<b>Enhancing the skills of security promotion personnel</b> (provide an explanation of priority items in the guidelines)	October 2024 onwards
Various consultation sessions	<b>Consultation on security promotion issues</b> (12 sessions planned)	October 2024 to March 2025

Notification method: Announcements will be made in the “Updates” section of the JAMA homepage.

[<https://www.jama.or.jp/release/latest\\_update/>](https://www.jama.or.jp/release/latest_update/)

## 5-2. Application for Information on Automotive Industry Security Activities

- ✓ Beginning this fiscal year, **to improve cybersecurity measures within the automotive industry**, JAMA and JAPIA will share information about our information security activities and related initiatives as needed.
- ✓ Updates will be sent via email to individuals who select **“I would like to receive more information”** in the **“URL for Application for Information on Automotive Industry Security Activities”** section on page 32.

English

**FY2024**

**Application for information on automotive industry security activities**

Purpose

This form serves as an application site for receiving information regarding various security activities provided by the Japan Automobile Manufacturers Association (JAMA) and the Japan Auto Parts Industries Association (JAPIA).  
Before submitting your application, please confirm your understanding of the intended use of the information below and proceed only if you agree to these terms.

\* Required

1. About the use of various information entered in this form  
The personal information and company name entered in this form will be utilized for group activities, including enhancing various security measures in accordance with the personal information protection policies of the Japan Automobile Manufacturers Association (JAMA) and the Japan Auto Parts Industries Association (JAPIA).

If you agree to this use, please check the box below and proceed with your application.  
If you do not agree, please close this form.

### << Upcoming information release >>

- ✓ Details regarding the self-evaluation of the Automotive Industry Cybersecurity Guidelines.
- ✓ Information about the briefing session on the self-evaluation request.
- ✓ Information about various consultation sessions and more.

6. Would you like to receive information from the Japan Automobile Manufacturers Association (JAMA) and the Japan Auto Parts Industries Association (JAPIA) secretariat? \*



**I would like to receive more information.**



I do not wish to receive information.

# Today's Agenda

1	Introduction
2	Video courtesy of the Ministry of Economy, Trade, and Industry
3	The importance of cybersecurity measures (Nagoya Port Incident Case Study)
4	Request for self-evaluation for FY 2024
5	Forthcoming events and the application process for information on automotive industry security activities
6	Summary
7	Q&A

## 6-1. Request to Participating Senior Management

- 1. Information security is a key management concern that demands effective risk response strategies from senior management.**
- 2. Senior management should demonstrate leadership in fostering information security initiatives within the organization and among employees.**

## 6-2. Today's Requests

- 1. Understand and enhance your company's information security level** using the “Automotive Industry Cybersecurity Guidelines”
- 2. Engage your business partners** to elevate security throughout the supply chain  
\*Assess the security capabilities of your business partners and **enhance the level across the supply chain.**

# In Conclusion - Reference

Begin by focusing on the fundamental concepts.  
 Following this, explore services that can assist you in preparing for potential security incidents.

Clearly communicate these “three essential points”:

- Avoid opening email attachments carelessly.
- Refrain from visiting suspicious websites unnecessarily.
- Do not fall for “support scams,” such as claims, “You’re infected; you need support.”

Additionally, what steps can small and medium-sized enterprises with limited human resources and budgets take to prepare for security incidents?



**Act decisively, before it's too late.**  
 Address cybersecurity issues before they occur!

**OTASUKETAI Cybersecurity Rescue Team**

<p><b>Monitoring</b> (Constant monitoring)</p> <p>24/7 monitoring          Detects behavioral and problematic attacks to safeguard your PC and network.</p>	<p><b>Emergency response</b></p> <p>Local IT service providers will promptly address issues as they appear.          (Remote support might be available)</p>	<p><b>Insurance</b></p> <p>Simple cyber insurance covers various unforeseen costs incurred when responding to an incident, such as on-site support.</p>
---	--	---

**A complete package at an affordable price!**

## Cyber Security Rescue Team Service

<https://www.ipa.go.jp/security/otasuketai-pr/>

A service that provides a comprehensive package at an affordable price, which includes the following features:

1. Monitoring: 24/7 surveillance to detect unusual behavior and problematic attacks.
2. Emergency response: Local IT service providers rush to address issues when they arise.
3. Insurance: Basic cyber insurance covers various unexpected costs incurred while responding to damages caused by a cyber attack, including on-site support.

Thank you for your attention.