TOKYO ELECTRON

Information Security Report 2026

Editorial Policy

Issuance of an Information Security Report

Tokyo Electron issues an information security report to inform stakeholders about our security activities. This report outlines our comprehensive security measures. We remain committed to monitoring security threats, enhancing our security continuously and ensuring appropriate and transparent information disclosure.

Scope

This report and related data cover the entire Tokyo Electron Group (26 consolidated companies), with the exception of some domestic (Japan-exclusive) content.

Issued Date

August 2026

Period Covered

Fiscal 2026 (April 1, 2025 to March 31, 2026).

Contents

Message

Kimihiro Higuchi
Chair of Information Security Committee
Tokyo Electron Limited

Under our Corporate Philosophy—"We strive to contribute to the development of a dream-inspiring society through our leading-edge technologies and reliable service and support"—we are committed to advancing the semiconductor industry. By seriously pursuing technological innovation and continuously delivering high-value-added, state-of-the-art equipment and technical services for semiconductors, which support sustainable development in society, we aim for the medium- to long-term expansion of profit and sustainable improvement in corporate value.

At the same time, ensuring information security is a critical challenge as we carry out these efforts. With changes in the geopolitical landscape surrounding Japan, the strengthening of regulations related to information security, an expanding global supply chain, DX progress and rapid AI advancements in the business environment and increasing cyber threats, the risks surrounding information security are becoming more complex. To ensure business continuity, we must establish a secure and reliable data environment.

As an industry leader supporting the semiconductor market, we regard information security as an important managerial issue. Strong security measures are essential not only for business continuity but also as a competitive advantage in an increasingly challenging market. Alongside quality and compliance, information security is the source of our business competitiveness.

With this in mind, the Tokyo Electron Group Information Security Committee leads Group-wide efforts to strengthen security. We have established specialized departments with advanced expertise to protect confidential information, including customer and business partner data as well as proprietary advanced technologies, and to address a wide range of risks such as cyberattacks, internal fraud, product security and plant security. We continue to expand resources and enhance our measures while also educating employees about information security to prevent security incidents.

We remain committed to further advancing these initiatives for enhanced security to meet the expectations of our shareholders, customers, business partners and society as a whole. This report highlights our security efforts across the Tokyo Electron Group, and we appreciate your time in reading it.

Position of Information Security in Our Company

As digitalization advances across industries, the importance of the semiconductor and semiconductor production equipment industry continues to grow. However, with this increased significance comes heightened information security threats surrounding the business. We recognize that information security is an important managerial issue and actively implement measures to enhance it to protect customers and business partner information as well as confidential information on leading-edge technology.

Leading technology companies consistently face threats, including unauthorized access from external networks and internal data leaks. With over 60 years of experience in the semiconductor production equipment industry, our company has a wealth of leading-edge technological knowledge surpassing that of other companies and is attracting attention for its research and development with an eye for the future. We ensure the confidentiality, integrity and availability of all business-critical information and environments (hereafter, "information assets") to achieve the following security objectives.

- Protect and manage confidential information to prevent leaks and enhance customer satisfaction
- Prevent data tampering and ensure an environment for conducting business based on accurate information
- Strengthen resilience against incidents to ensure business continuity
- Comply with information security laws, regulations, social norms and the TEL's Code of Ethics to fulfill our social responsibilities
- Balance digital transformation (DX) with security using security solutions

To achieve these initiatives, we are strengthening our Group-wide information security systems and cybersecurity measures to protect information assets entrusted to us by our customers and business partners, as well as our own information assets, from threats while ensuring the secure delivery of our products. By continuously analyzing evolving security risks and refining our strategies, we aim to maintain proper risk control, support semiconductor advancements, and contribute to a prosperous society.

Main Activities

Information Security Governance

Building on the growing demand for semiconductors, our business and organization continue to expand. At the same time, in the area of information security, the weakest link can become a vulnerability, posing a risk of developing into a major security incident.

The Tokyo Electron Group, with its presence in various countries, must consider the different languages and legal regulations of each country to ensure information security across both the headquarters and the entire Group. Under the slogan "ONE TEL," we are building a governance system to ensure high information security across the entire Group.

1 Information Security Promotion Systems

The Board of Directors, which oversees our corporate governance, receives timely reports on information security activities from the Information Security Department. Based on the latest information security risks, the Board carries out daily corporate governance activities.

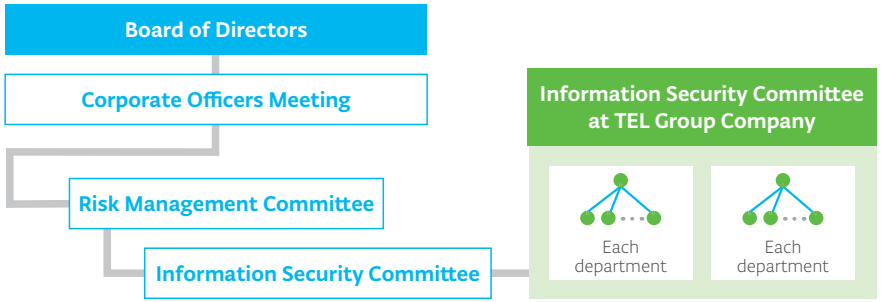
Additionally, under the Board of Directors and the Corporate Officers Meeting, we have established the "Tokyo Electron Group Information Security Committee," which is chaired by the Vice President and General Manager of Information Security at our headquarters. This committee promotes information security governance across the entire Group, determines information security policies for the entire Group and manages the progress of the security measures of each Group company.

At the headquarters, under the direction of the Vice President and General Manager of Information Security, the Information Security Department manages information security across the entire Group, executes security measures and conducts security operations across the entire Group.

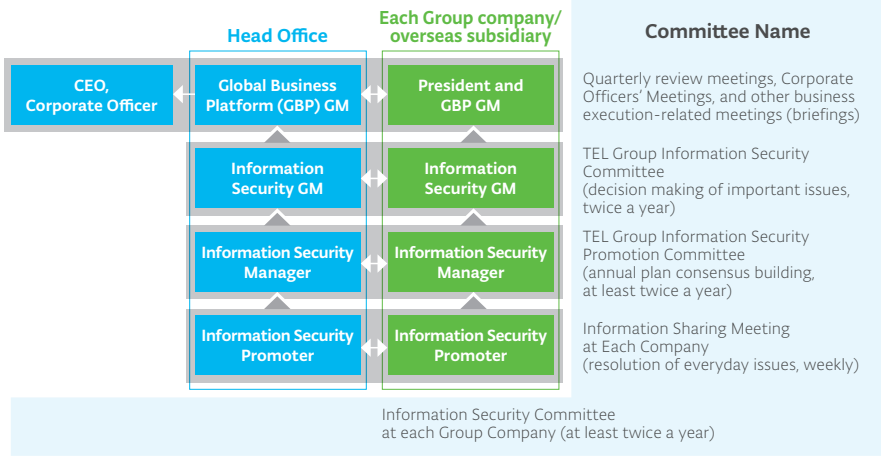
Furthermore, within each Group company, the General Manager (GM) in charge of information security leads the appointed information security managers and promoters, who form internal information security committees within their respective companies to establish effective governance for information security. We are working to strengthen security, while maintaining a shared recognition across the entire Group by seeking Group-wide collaboration following repeated discussions in each company.

Through these systems, we ensure a unified level of information security across the Group and, under the oversight of the headquarters, maintain a framework that allows us to quickly deploy various security measures while monitoring the overall security management situation across the entire Group.

Information Security Management System Diagram



Each Company's Information Security Systems



Information Security Governance

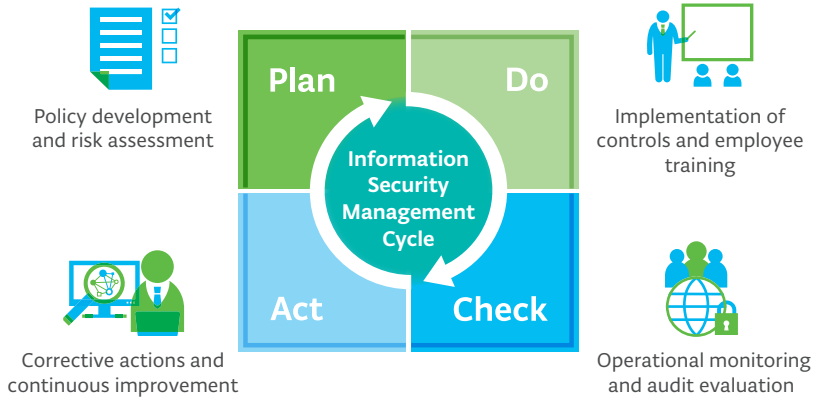
2 Information Security Activity Framework

Information security risks are constantly evolving, and it is essential for the entire organization to engage in continuous efforts that reflect the latest trends. At our company, we implement information security activities systematically, following the PDCA cycle based on information security management.

In the Plan phase, we identify information assets and conduct risk assessments within each organization, determining the necessary measures. In the subsequent Do phase, we execute educational and awareness activities for employees and deploy security measures. In the Check phase, we evaluate the execution of security measures through inspections and internal audits. In the Act phase, we analyze the results of the inspections and internal audits, taking corrective actions and reviewing rules and measures.

Through these continuous efforts, our company effectively maintains information security. Furthermore, from fiscal 2025, starting with the headquarters departments, we are gradually obtaining certification for ISO/IEC 27001:2022, the international standard for information security management systems, through assessments conducted by third-party certification bodies, with the aim of ensuring a common level of information security across the entire Group. We will continue to enhance our information security through ongoing improvements to meet the trust of our customers and business partners.

Information Security Management Activities



3 Management of Confidential Information and Response to Information Security Incidents

At our company, we handle many critical information assets, including important technical information that we possess, as well as information entrusted to us by our customers and business partners. We treat all information that is valuable to our business activities and needs to be kept confidential as confidential information, and we manage it strictly. As managers in charge of information management, heads of the departments handling the information designate the confidentiality classification for each piece of information, ensuring thorough labeling of each information asset to prevent misidentification or lapses in management. Based on these confidentiality classifications, we store data on servers for which strict access controls are implemented, monitor the transfer of information assets and take measures such as robust encryption. Additionally, when it is necessary to share information with external organizations, we utilize online storage services that ensure strong security.

In the event that an information security incident such as a leakage of confidential information occurs, the incident is immediately entered into the incident management system, ensuring that the situation is promptly shared with relevant departments, including the risk management department, allowing the entire organization to respond quickly. Furthermore, the Information Security Department analyzes the course leading up to the incident and the conditions of the occurrence, ensuring that the organization learns from it and takes steps to prevent recurrence.

If an information security incident occurs due to an employee's actions, regardless of whether intentional or accidental, it is dealt with strictly in accordance with the company's employment regulations.

Information Security Governance

Tokyo Electron's Governance and Information Security

Takashi Mineshima
General Manager, Information Security Unit, CISO (Chief Information Security Officer)
Tokyo Electron Limited

As mentioned in "Chapter 2: Position of Information Security in Our Company," the information security threats surrounding the semiconductor and semiconductor production equipment businesses have been rapidly increasing in recent years. When conversing during conferences and other occasions with Chief Digital Officers (CDOs) and Chief Information Officers (CIOs) from other companies in the same industry, including those from the U.S., the topic that comes up first and foremost is information security. In this field, there is a common understanding across companies that the industry should work together rather than competing, and there is a confirmed need to strengthen security as an industry as a whole. Our company, too, feels a sense of responsibility as a leader in the semiconductor industry in Japan, and each member of our team is committed to their work with a sense of duty.

The Tokyo Electron Group has set "Accelerate Global IS Orchestration!" as its IT activity guideline, including information security. This guideline expresses the idea that the members involved in IT and information security at both the headquarters and Group companies work together in harmony, much like an orchestra playing in unison. As information security and IT governance are positioned as top priorities, Group-wide initiatives are being promoted in a coordinated and aligned manner. Furthermore, to promote coordinated activities, the headquarters' Information Security Department sends personnel to overseas subsidiaries, strengthening collaboration as a bridge between the headquarters and local offices.

Accelerate Global IS Orchestration!

Orchestration of:
- Strategy
- Technology
- Security
- Governance (Process)
- Organization & People

4 Information Security Policy

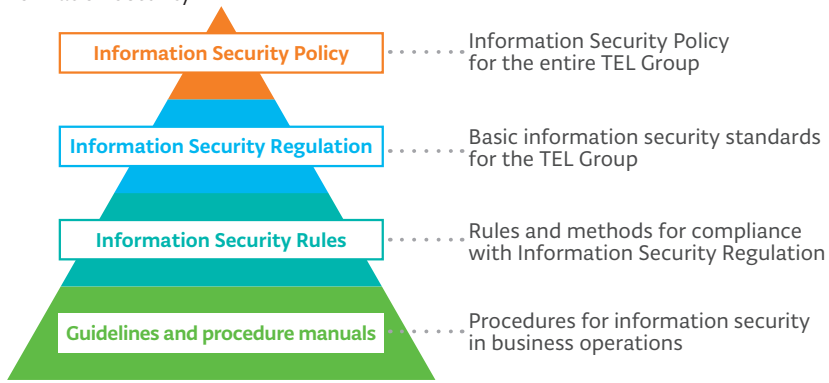
As a global company, it is crucial for the Tokyo Electron Group to implement the same level of security measures both at the headquarters and Group companies. To achieve this, we have established Group-wide information security documents as our security policy.

Our information security documents are structured as shown in the diagram on the right. At the first level, we have formulated the Information Security Policy, which defines the overall security principles for the Group. At the second level, we have the Information Security Regulation, which establishes the fundamental security standards for the company. At the third level, we have the Information Security Rules, which outline detailed rules and methods for complying with the Information Security Regulation. Additionally, at the fourth level, we have developed security guidelines and procedure manuals, which provide specific implementation procedures for information security in each business operation.

These information security documents have been formulated based on external security standards and international norms. We also review and update them regularly to reflect security threats and technological advancements, ensuring that we remain prepared for the latest security risks.

To maintain a unified security level across the Group, these information security documents are published in multiple languages on the company's internal portal site, allowing all employees to access them at any time.

Structure of Information Security Documents



Information Security Governance

5 Information Security Education and Awareness

To ensure information security, we have established an information security policy and implemented various measures, including physical and technical controls. However, people ultimately serve as the final line of defense. It is therefore essential that every employee understands the significance of the information they handle in daily operations and the responsibilities they bear, and acts with awareness of the measures defined in the information security regulations.

We provide annual training on information security regulations for all executives and employees. The content is standardized globally and provided in multiple languages to ensure accessibility for local employees. In addition, an information security handbook summarizing the regulation in a clear and user-friendly manner is made available on every employee's PC, enabling immediate access to the latest version. We also offer case-based training content covering scenarios such as misdirected emails and improper handling of information.

In parallel, we conduct role-based security training for specific groups, including managers and plant personnel, and incorporate information security as a key component of onboarding programs for new graduates and mid-career hires. Furthermore, to enhance employee awareness, we operate a portal site that consolidates information for internal use and distribute information security newsletters.

Additionally, at plants and overseas Group companies, we conduct site-specific security training tailored to their operational environments, and promote awareness activities such as displaying signage and posters and issuing alerts based on on-site risks, thereby supporting employees in correctly understanding key information security principles.

6 Information Security Exercises

As information security threats continue to grow, it is essential that employees promptly escalate any incidents to the relevant internal departments. In particular, phishing attacks targeting our employees and information assets occur on a daily basis, and there is a risk that actions such as opening malicious emails could lead to a large-scale information security incident affecting the entire company.

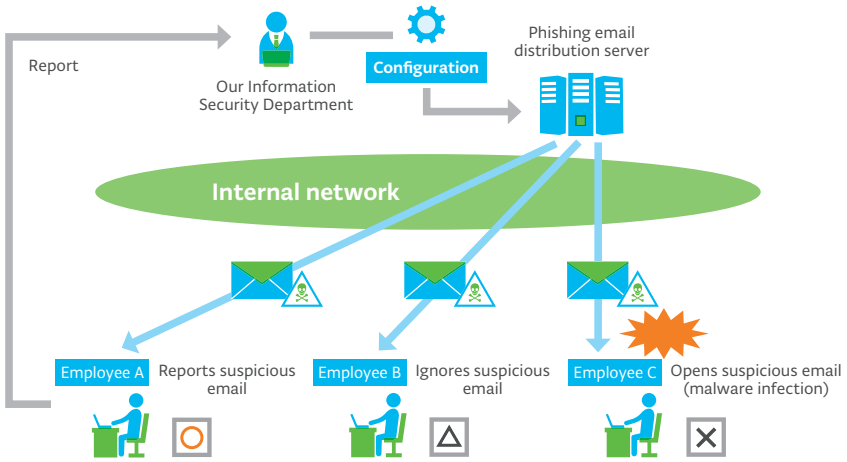
In response to these challenges, we continuously conduct phishing email exercises for all employees. By experiencing phishing emails simulating attacks, we deepen understanding of the risks and improve basic literacy in identifying suspicious emails. However, since humans cannot perfectly identify suspicious emails, it is essential to share information with the Information Security Department when a phishing attack occurs, enabling swift initial responses and actions to prevent similar attacks before they occur. Accordingly, we place greater emphasis on reporting rates rather than simply whether emails are opened, aiming to strengthen the organization's resilience to phishing attacks.

Additionally, the system personnel and security-related departments conduct cyber incident response exercises to ensure that proper information sharing and rapid initial responses can be taken when cyberattacks targeting our company occur. During the exercise, participants take actions, assuming that an incident has occurred, based on cyber attack scenarios prepared in advance. Any issues identified during the exercise are recorded and addressed for future improvements. Information sharing is conducted in a practical manner, such as through web meetings, chats, or face-to-face meetings, simulating actual incidents.

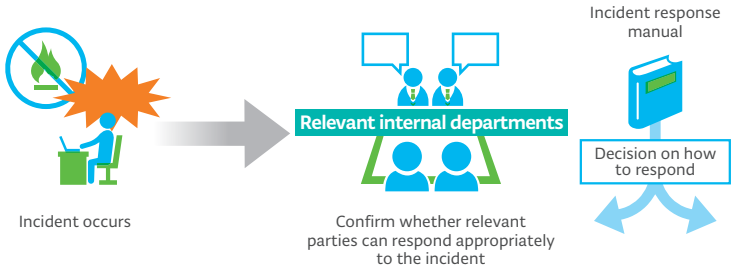
By continuously conducting these information security exercises, we enhance the organization's overall security resilience. This enables us to ensure swift recovery actions in the event of an incident.

Information Security Governance

Phishing Email Exercise



Cyber Incident Response Exercise



7 Information Security Audits and Inspections

Even with established information security regulations and training programs, there is a risk that the rules may become formalized and neglected in daily operations. To ensure compliance with the information security regulations, we conduct the audits and inspections below.

Internal audits on information security

At our company, a variety of information assets are handled by not only employees but also temporary and contracted staff across many departments. Therefore, to verify that information security regulations are being appropriately followed in each department, we conduct annual internal audits related to information security.

In these audits, we confirm whether information assets are being properly protected and whether information security activities are being appropriately conducted within each organization in accordance with the company's internal information security regulations. The audit results are reported to the responsible parties, and if deficiencies are identified, corrective actions and improvements are carried out.

Inspection of security measures for internal information systems and cloud services

We operate many internal information systems to execute business. For the information systems we build and operate, we verify that necessary security measures such as appropriate patching, authentication and access control, malware protection and backups are being implemented in accordance with information security regulations. If deficiencies are found, prompt corrective actions are taken.

Additionally, to quickly respond to the progress of digital transformation (DX) and changes in the business environment, the use of external cloud services is increasing. In such cases, we collaborate with external specialized companies to conduct security evaluations of the relevant cloud services. If deficiencies are identified during the evaluation, we request corrective actions from the cloud service provider. If it is difficult to address the issues, we switch to a more secure cloud service, ensuring strict management.

Information Security Governance

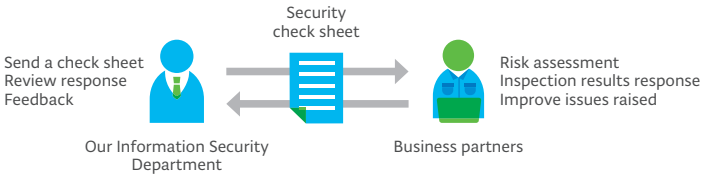
Information security inspections for business partners

Our semiconductor production equipment is produced with the cooperation of many business partners. To protect the entire supply chain from information security threats, we work together with our business partners to continuously improve security measures.

We request an annual information security assessment from our business partners and confirm whether appropriate information security measures are being implemented. Specifically, we conduct document-based (paper-based) checks using a security check sheet, and also have specialized auditors from our security department make visits to business partners for which on-site verification is required.

If deficiencies are identified during the inspection, we promptly provide feedback to the business partner and request corrective actions. Additionally, based on the trends in threats and incidents, we regularly review various inspection items.

Document-Based Inspection



Visiting Inspection

Information Security Governance

Global Information Security Governance Issues

Makoto Sasaki
Promotion Group Leader, Information Security Department
Tokyo Electron Limited

What are the challenges in advancing Tokyo Electron's information security governance?

In promoting information security governance, we strongly recognize the importance of communication.

Currently, we conduct security assessments for Group companies, including our own, and major business partners to understand the current state of security measures. While providing support for necessary corrective actions, we are working toward the establishment of unified governance. However, ensuring unified governance while collaborating with members from countries with different cultures, languages, time zones, regulations and technical differences is a significant challenge. To address these issues, we foster a common understanding through regular meetings with responsible parties and the deployment of educational programs, maintaining a flexible approach.

Additionally, active collaboration with external experts and various organizations is indispensable. By incorporating the latest information and trends, we can further improve the quality of security governance. I myself engage in ongoing discussions with responsible parties on how to reflect the insights gained through information exchange with external parties in our company.

To resolve these challenges, it is not enough to proceed with our own initiatives. We aim to further improve information security governance by collaborating across the entire Tokyo Electron Group and the entire supply chain.

Yudai Suzuki
Information Security Analyst
Tokyo Electron U.S. Holdings, Inc.

With generative AI becoming a major topic lately, how are you approaching governance?

Traditionally, various services such as CRM and training have been introduced for specific purposes; however, analytical and support functions leveraging generative AI and advanced machine learning technologies are increasingly being implemented in these services, thereby rapidly expanding the scope of AI utilization across entire business processes. While the advancement and widespread adoption of AI contribute to improved operational efficiency and added value, the periodic review of governance in response to technological progress and evolving usage patterns has become an important challenge.

At Tokyo Electron, with information security at its core, relevant departments, including IT governance, compliance, legal, and intellectual property, collaborate to continuously develop and enhance cross-functional governance rules for digital technologies, including the use of AI.

Furthermore, for generative AI used as a standard across the Tokyo Electron Group, the Information Security Department is involved from the trial phase under the management of the Information Systems Department, helping to reduce security risks from the early stages of planning and deployment.

By continuously advancing these initiatives, we aim to maintain and strengthen a secure generative AI usage foundation and contribute to the sustainable value creation of the Tokyo Electron Group.

Technical and Physical Measures

Reports of cyberattacks, such as targeted attacks and ransomware, continue unabated, posing a significant threat to business continuity. Additionally, amid rising geopolitical tensions, cyberattacks by state-sponsored hacker groups and the activity of cybercriminal organizations operating as established business models are increasing and becoming more and more sophisticated. There are also concerns about the leakage of confidential information due to internal fraud by employees, as well as risks posed by malicious individuals infiltrating company facilities to steal or destroy information assets.

To address these threats, our company is continuously strengthening both technical and physical security measures.

1 Security Monitoring

Unauthorized communications and suspicious emails targeting our company's information assets and employees are detected daily. Our Security Operation Center (SOC) operates 24 hours a day, 365 days a year, with specialized security experts monitoring cyber incidents.

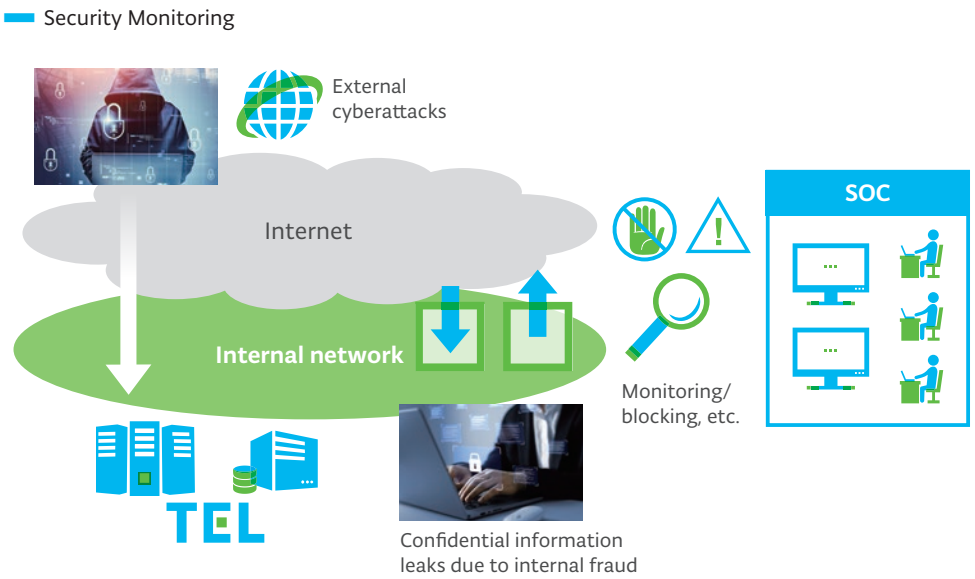
Security monitoring devices, such as Endpoint Detection and Response (EDR) installed on employee PCs and servers, generate logs, which are aggregated using Security Information and Event Management (SIEM) systems. When suspicious events are detected, swift investigation and analysis are conducted. Additionally, attacks targeting employee accounts pose a major threat. The SOC continuously monitors for suspicious activities such as unauthorized external login attempts and account misuse.

In addition to external cyberattacks, internal fraud and employee negligence can also lead to serious incidents. We need to provide thorough security education, while being required to address risks that include employees intentionally violating company policies by taking confidential information outside the company or introducing personal devices that could cause malware infections due to poor security awareness.

To prevent such inappropriate employee actions, we enforce strict access controls and continuous monitoring. If misconduct is discovered, strict disciplinary measures are taken against the individual concerned.

Through these security monitoring efforts, we protect our critical information assets from a wide range of security threats.

Security Monitoring



Technical and Physical Measures

2 SIRT Initiatives

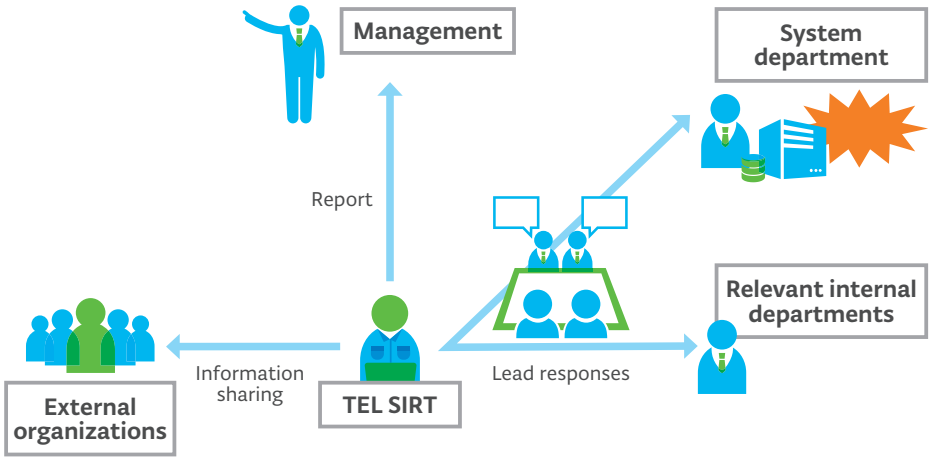
Our company possesses confidential information on various high-value technologies and products, making it an attractive target for attackers. At the same time, given the large scale and diverse business domains of our organization, the attack surface is extremely broad. From a strategic perspective, cybersecurity presents an asymmetric battle between attackers and defenders. Attackers need only exploit a single vulnerability at any given time, while defenders must continuously protect all potential attack points. As a result, preventing 100% of cyberattacks is highly challenging. Therefore, we recognize the importance of assuming that cyber incidents will occur and securing a resilient system that allows rapid incident detection, containment and recovery.

The Security Incident Response Team (SIRT) collaborates with the SOC to respond to security incidents. In 2020, we established TEL SIRT as the center of excellence for the entire Group.

TEL SIRT receives notifications from the SOC and takes the lead in taking a series of actions for addressing incidents for which responses are determined to be necessary, including blocking communications, preventing the expansion of damage, preserving evidence, investigating and analyzing the causes. In the event of a cyber incident, collaboration with relevant internal departments and external organizations is essential for resolving the situation. Therefore, the specialized organization TEL SIRT ensures overall control, enabling rapid incident response.

TEL SIRT regularly collects intelligence information, such as profiles of cyberattack groups and attack methods, as well as the latest vulnerability information that may be exploited in cyberattacks, from various sources including security information sites and the dark web. The collected threat information is analyzed by security researchers and is used to enhance daily security monitoring and security measures, as well as to support company-wide alerts and corrective actions.

TEL SIRT Incident Response

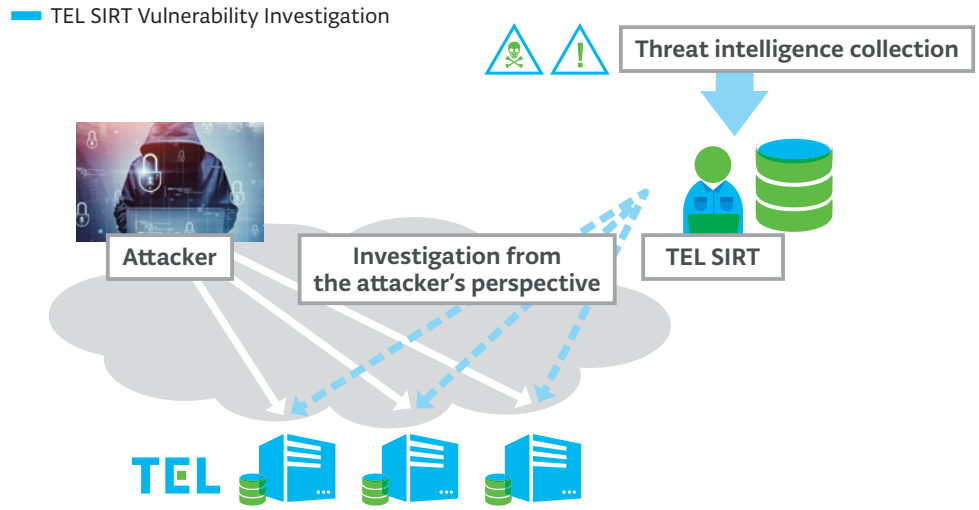


Technical and Physical Measures

TEL SIRT considers it crucial to adopt an attacker's perspective and proactively assess the risk of cyberattacks before an attacker acts. For the systems operated and managed by the company, TEL SIRT conducts preemptive vulnerability assessments. Since new vulnerabilities are discovered daily, regular vulnerability checks are performed, along with patrol investigations to ensure that no systems have been unintentionally exposed.

Additionally, TEL SIRT checks for potential vulnerabilities and misconfigurations related to the company, leveraging information available on the internet through Open Source Intelligence (OSINT) activities, which are often used by attackers. Furthermore, for critical systems, we conduct penetration testing—simulated unauthorized intrusion tests—to check for the presence of vulnerabilities that could lead to security breaches.

TEL SIRT plays a crucial role in protecting our information security as a cybersecurity specialist with both defensive and offensive perspectives.



TEL SIRT's Initiatives for Strengthening Cybersecurity

Teruo Fujikawa
TEL SIRT/Internal Security Group Leader, Information Security Department
Tokyo Electron Limited

Cybersecurity incidents are widely reported today, making your job quite challenging. What motivates you the most?

Cyberattacks can occur 24 hours a day, 7 days a week, 365 days a year, so there is never a time to completely let our guard down. However, I feel a strong sense of responsibility and purpose knowing that TEL SIRT acts as a defensive barrier protecting our company from increasingly sophisticated cyber threats. Additionally, since our company supports the growth of the semiconductor market, safeguarding it from cyberattacks means contributing to a prosperous society built on semiconductor technology—a mission I find extremely fulfilling.

What do you focus on as a TEL SIRT member?

To counter the ever-evolving cyberattack techniques, improving the skills of our SIRT members is essential. All members maintain a high level of awareness and actively gather security-related information on a daily basis while participating in external security training programs. These efforts help enhance TEL SIRT's monitoring technique and incident response capability. We plan not only to make efforts within the company, but we also actively engage in external events and collaborate with outside security teams to further hone our advanced skills.

Technical and Physical Measures

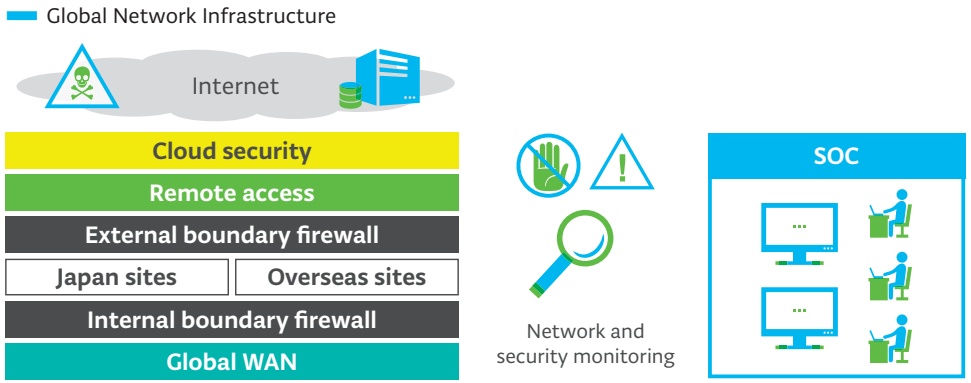
3 Network Security Measures

Our company utilizes many cloud services to promote DX, and ensuring the secure use of data stored in cloud environments on the internet is a key challenge. Additionally, our employees operate in a global environment and adopt a hybrid work style, regardless of whether they are working remotely or from the office.

In light of these circumstances, we are building a secure global network infrastructure based on a unified network security policy to achieve consistent operations across global locations.

We have deployed next-generation firewalls at each location to filter and monitor high-risk communications, and introduced cloud security services across all locations to ensure seamless operations between network and security while strengthening security in cloud environments. In addition, we have established a remote access environment using multi-factor authentication, enabling all employees worldwide to work securely and efficiently.

Similar to the previously mentioned EDR, these networks and devices are centrally monitored by our SOC, and in the event of suspicious activity, immediate actions such as communication blocking are taken. Additionally, in case of network failures due to equipment malfunctions, we have established a system that allows us to quickly provide support in collaboration with various sites.



4 Physical Security Measures

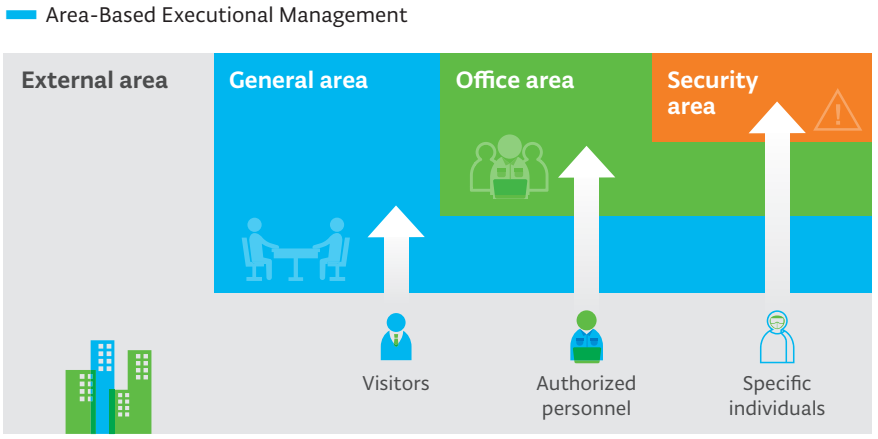
To prevent unauthorized individuals from accessing our plants and offices, and coming into contact with our information assets, we have divided our plants and offices into zones and implemented access control measures according to the level of each area.

The general area includes outdoor walkways, parking lots, entrances, meeting rooms for visitors and cafeterias located away from the plants and offices within the company's premises. This area is fenced and monitored by security personnel.

The office area is restricted to employees and pre-authorized personnel only, with strict access management through a physical authentication system.

The security area is where we handle highly confidential information, such as technical data. Access to this area is restricted to specific individuals who have been authorized by the area manager, even if they are employees. The use of devices such as smartphones with cameras is prohibited. In addition, continuous surveillance is conducted using security cameras, and some specific areas also employ biometric authentication systems as an additional measure.

By implementing a strict physical authentication system with a focus on information security, we ensure that access to our information assets is tightly controlled to prevent unauthorized access.



Security Measures for Manufacturing Sites and Products

For Tokyo Electron, which develops semiconductor production equipment, strengthening security at its production and development sites is an urgent issue. We are working to enhance plant security to ensure that each plant operates safely and stably.

Furthermore, for products delivered to customers, we implement security measures based on industry standards such as SEMI E187/E188[1], and the laws and regulations of each country, such as the EU Cyber Resilience Act[2]. Through these efforts, we also strive to ensure product security, contributing to the stable operation of our customers' semiconductor production plants.

1 SEMI E187/E188: SEMI E188 is a standard for equipment designed to prevent malware infections in plant systems through patch applications and maintenance. SEMI E187 is a cybersecurity standard for Fab equipment (semiconductor production equipment) aimed at protecting data related to semiconductor manufacturing.
2 The EU Cyber Resilience Act (EU CRA) is a law in the European Union (EU) that mandates security measures for digital products by manufacturers.

1 Strengthening Plant Security

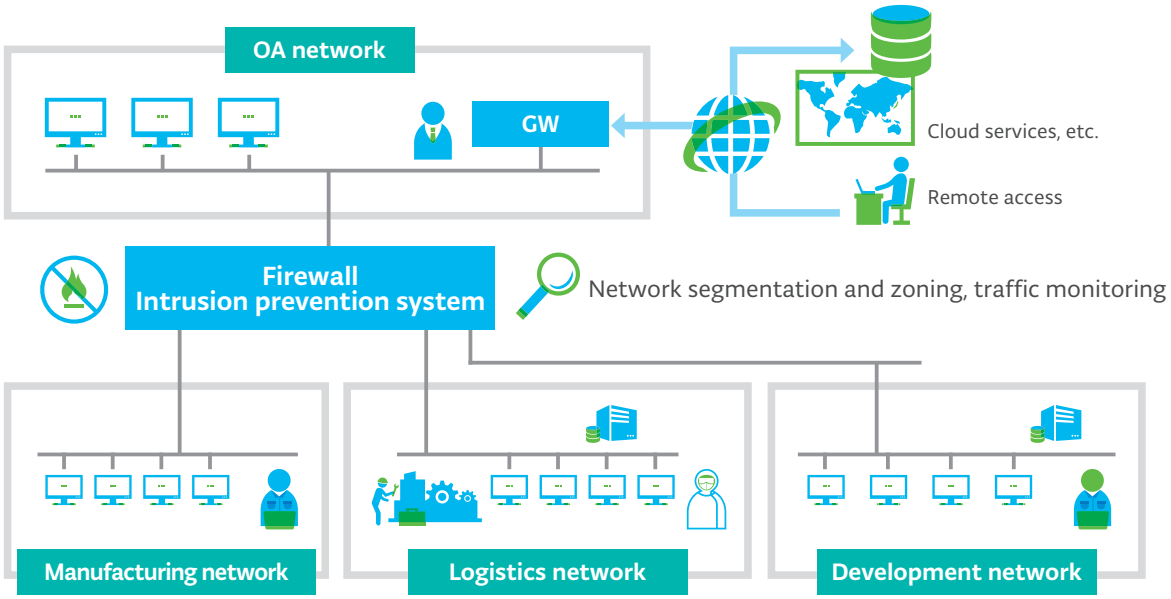
Plant networks, which were previously in closed environments, are becoming more open and digitally transformed, increasing the risk of information security incidents such as cyberattacks and ransomware infections.

In plants, it can be difficult to apply information security measures designed for standard office environments or OA networks as they are. For this reason, we have formed a dedicated team led by members with expertise in plant security to strengthen security measures. Additionally, we have established plant security guidelines based on international standards. Following these guidelines, we implement solutions across the Group and monitor them to ensure each plant operates safely and stably.

Manufacturing, logistics, and development networks in plants are clearly separated from OA networks by firewalls and intrusion prevention systems, with traffic monitoring in place. Furthermore, each network is segmented into smaller units using VLANs, minimizing potential damage in the event of an incident. All devices connected to these networks are managed through an inventory system, ensuring that if an incident occurs, the SOC/SIRT team works closely with on-site plant personnel for a swift response.

Through these initiatives, we maintain stable business operations without halting production and development activities at each plant.

Strengthening the Security of Plant Networks



Security Measures for Manufacturing Sites and Products

2 Strengthening Product Security

Product security landscape and our basic policy

Product security is becoming increasingly important in today's digital society, making its assurance an essential challenge for companies.

The product security landscape is evolving, with the EU Cyber Resilience Act (EU CRA) enacted and set to take effect in December 2027. In the U.S., legislative efforts are also advancing, with the National Cybersecurity Strategy announced in March 2023 explicitly outlining regulatory measures. Against this backdrop, customer inquiries and demands regarding SEMI standards have been increasing. Furthermore, as semiconductor plants continue to advance their smart manufacturing capabilities, cybersecurity is becoming even more critical. Cybersecurity risks in semiconductor plants include a wide range of threats, such as production disruptions due to malware infections, financial extortion and data leaks from ransomware attacks, theft of confidential information and production interference through tampered procedures or unauthorized control.

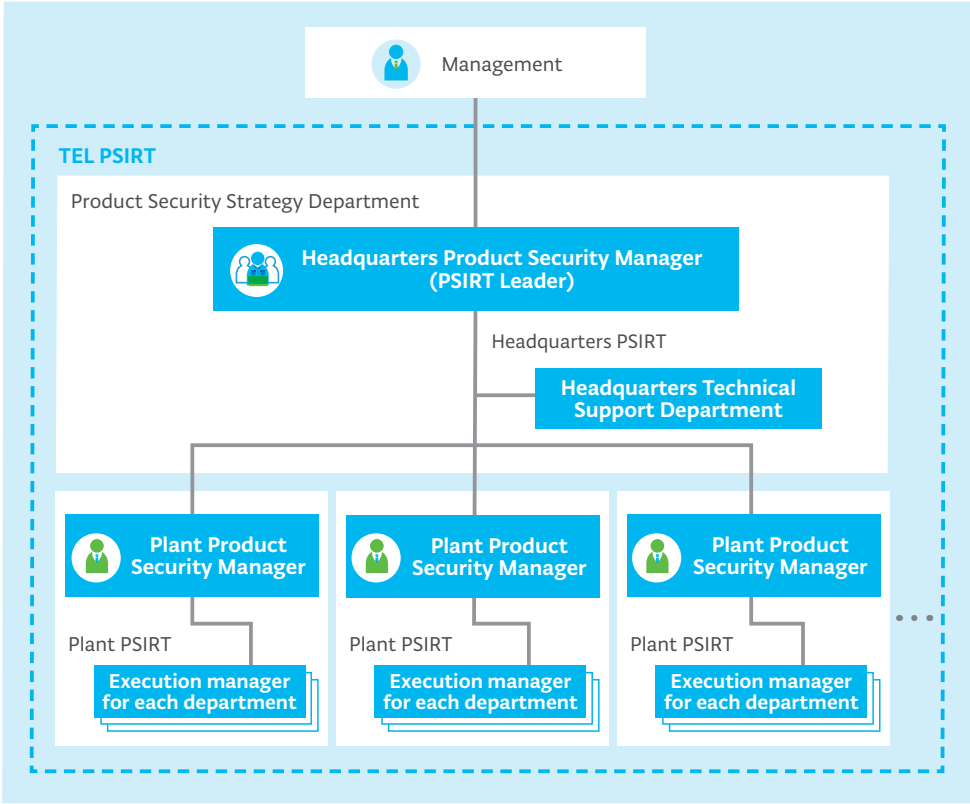
To ensure customers can use our products and services with confidence, we have established the following Basic Product Security Policy. We implement robust security measures in our products, and in manufacturing and field support.

Basic Product Security Policy

- Prevent disruptions to semiconductor device manufacturing caused by attacks on our products
- Prevent attacks that use our products as entry points
- Protect customers' information assets and our own information assets

Product security promotion system

To oversee and ensure security across all our products, we have established the Product Security Strategy Department. This department serves as the command center, coordinating various internal and external stakeholders while consolidating the latest information, technologies and expertise related to product security. Through this approach, the department establishes standardized rules and processes across the company. Additionally, to solve issues promptly at the time of emergencies, such as detecting vulnerabilities and the occurrence of incidents, we are reinforcing our structure by setting up Product Security Incident Response Team (PSIRT) units not only at our headquarters but also at all domestic and international plants, allowing flexible collaboration.

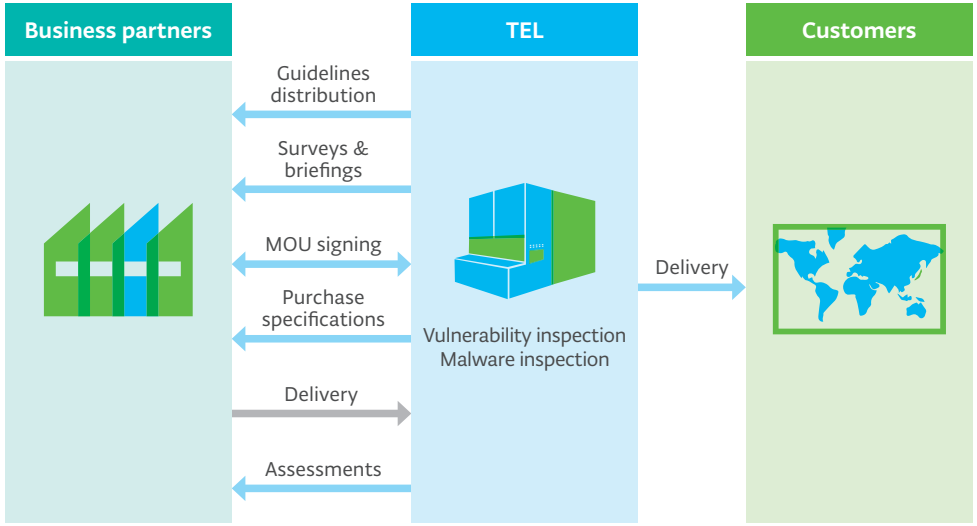


Security Measures for Manufacturing Sites and Products

Business partner engagement

To prevent any compromise to our product security due to components procured from business partners—including both hardware and software—we conduct regular security assessments of our business partners. These assessments help address issues and drive improvements in product security measures.

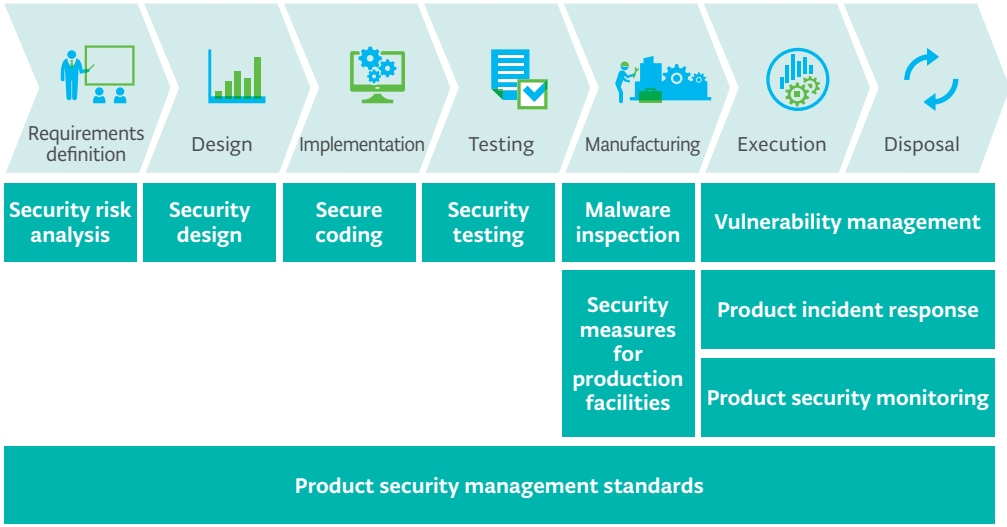
Specifically, we issue product security guidelines for business partners summarizing our collaboration requirements. We check and enhance the understanding of our business partners by holding briefings and conducting surveys, while concluding memorandums of understanding (MOUs) that stipulate product security requirements, including compliance with the product security guidelines. Additionally, purchase specifications explicitly outline security requirements in accordance with the guideline, and we conduct periodic on-site assessments. If any issues are identified, corrective actions are taken as necessary.



Development of secure products and services

We have established a product development process that ensures that product security is appropriately considered at each stage of the product development lifecycle, resulting in secure products.

Security-related regulations, such as the EU Cyber Resilience Act (EU CRA), not only require the implementation of secure features but also demand the establishment of a product development process that incorporates security. To comply with this, it is necessary to integrate a secure product development process into the workflow of each department. Specifically, we refer to international standards concerning the product development lifecycle and create documentation on development processes tailored to our products. By incorporating this documentation into the existing documents of each department, we drive the practice of the new processes. These efforts aim to improve product security and ensure reliability.

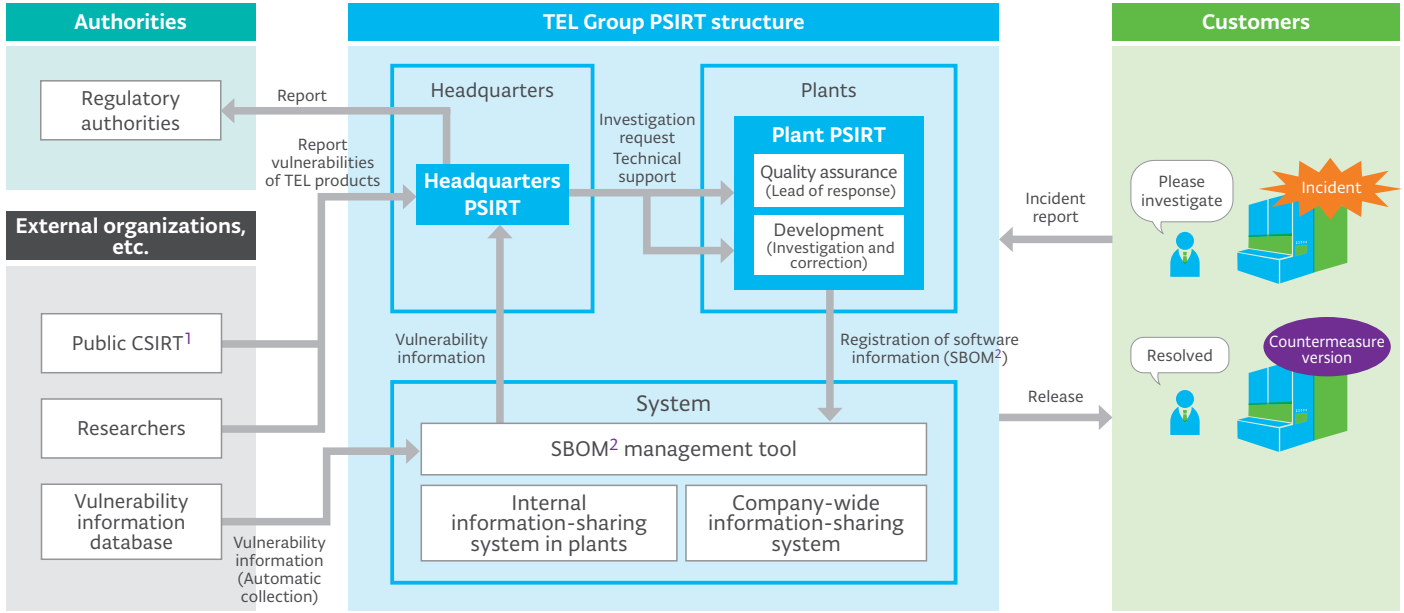


Security Measures for Manufacturing Sites and Products

Response to vulnerabilities and incidents

To maintain product security, it is essential to continuously gather the latest vulnerability information, assess its potential impact on products and prevent the exploitation of vulnerabilities by cyberattacks. We have established a vulnerability response flow in which the PSIRT at both our headquarters and plants collaborate. This flow involves collecting and detecting vulnerabilities, analyzing impacts and implementing countermeasures based on priority.

In addition, to prepare for incidents caused by cyberattacks, we conduct regular incident response training to verify and continuously improve our response flow. Through these efforts, we will build a structure that enables us to smoothly respond to incidents in the event that they occur under the leadership of the PSIRT, such as by minimizing damage, quickly restoring operations, providing information to stakeholders, investigating the root cause and considering measures to prevent reoccurrence.



1 Public CSIRT: A public specialized organization in each country that responds to cyberattacks and vulnerabilities, and conducts the collection, sharing, and coordination of information
2 SBOM (Software Bill of Materials): A bill of materials for software

Aiming to Establish a Collaborative Model as an Industry Standard

Hideo Mori
Expert, Product Security Strategy Department
Tokyo Electron Limited

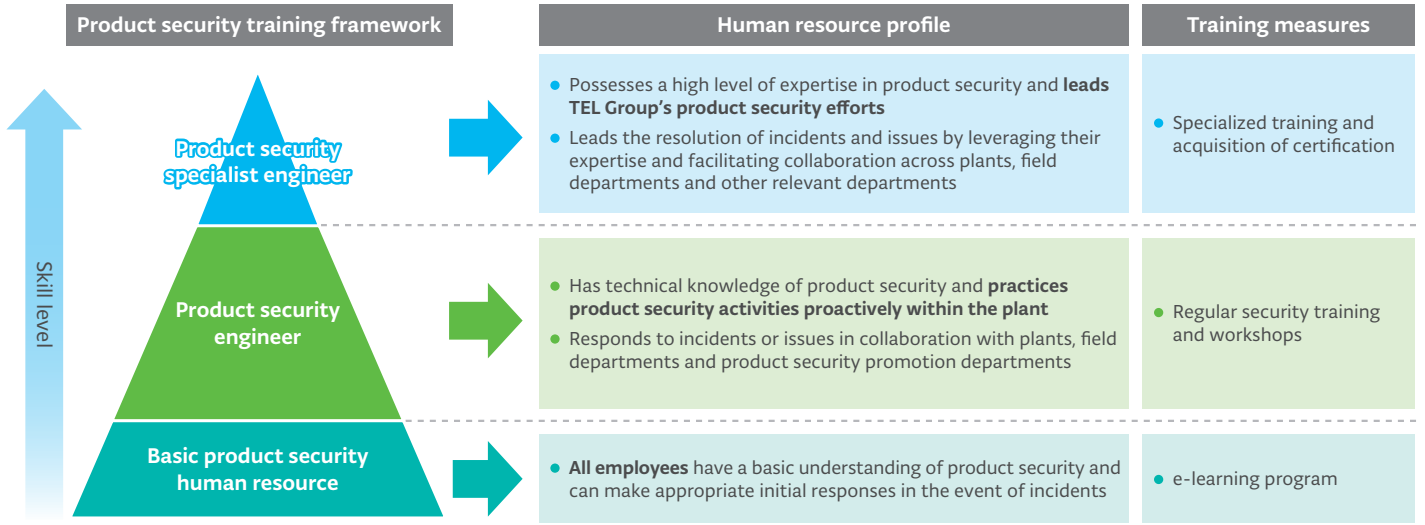
Semiconductor production equipment is composed of various devices, each of which is equipped with various software. It is extremely difficult for us to independently track all software, including open-source software (OSS), and address vulnerabilities. Therefore, we collaborate with our business partners and enhance the reliability of the entire supply chain by sharing vulnerability information, as well as by establishing frameworks for collaboration, thereby aiming to reduce security risks. This collaboration involves many technical and operational challenges, but through trials with our business partners toward collaboration and discussions and co-creation with external security experts, we aim to establish a collaborative model that becomes a standard for the industry, contributing to the further development of the semiconductor industry.

Security Measures for Manufacturing Sites and Products

Product security human resource development

To ensure the security of our products, it is essential that each employee reliably implement product security measures. To achieve this, we have set up human resource categories related to product security and the desired attributes for the individuals in these roles, and we conduct educational programs based on these. We provide foundational training for all employees, as well as specialized training for engineers involved in product security development and operations and dedicated teams responsible for product security incident response.

In addition, we are working to develop professionals with advanced knowledge and skills who can lead product security initiatives. We will continue to strengthen our training initiatives and further enhance the overall product security level across the company.



"Offensive" Product Security Enhancement Activities

Oriyuki Iijima
Vice President, Product Security Strategy Department
Tokyo Electron Limited

As semiconductors are critical strategic resources, the importance of cybersecurity measures in semiconductor plants is expected to increase further in the future. We carry out production security activities, aiming to make robust security and response systems become a part of the product value for our customers. Our Product Security Strategy Department plays a central role in these activities. We are responsible for formulating and executing the Group's overall product security policies. While cybersecurity measures are often associated with "defensive" actions, the work we do is much more challenging as it involves engaging deeply and broadly in product security. In fact, we view it as an "offensive" activity. We are committed to working together as one company to provide our customers with secure products and high-value-added services.

External Activities and Strengthening Information Security Human Resources

We strive to be an industry leader not only in terms of technological capabilities and business scale in the semiconductor production equipment business, but also in the information security field. To counter increasingly sophisticated cyberattacks worldwide, we are committed to building an advanced defense framework and setting industry standards, contributing to the sustainable growth of the semiconductor industry. As part of this effort, we are actively engaged in standardizing security measures within the semiconductor industry and external collaboration.

At the core of information security is people. As the shortage of security professionals becomes a serious societal issue, we will strengthen our security organization, positioning information security as one of our top priorities.

1 Security Activities Outside the Company

We lead the activities of the Semiconductor Manufacturing Cybersecurity Consortium (SMCC), a business entity considering the strengthening of cybersecurity at SEMI, in which companies and groups belonging to the global semiconductor industry participate. In December 2023, we were selected as a member of the Governing Council of this newly established entity, where we play a role in decision-making and oversight of its operations. In addition, we actively participate in all working groups as either a chair or a member, playing a central role in discussions.

Additionally, we take the lead in promoting SMCC's initiatives at SEMI-hosted conferences worldwide, delivering presentations on SMCC activities and the company's cybersecurity efforts. At the Cybersecurity Forum held annually of SEMICON Japan, we have co-organized the program as an executive committee member alongside SEMI from 2023 to 2025, delivering the Opening Remarks and a presentation on our initiatives. Furthermore, at the first-ever Global Standards Summit, which was organized to discuss technological standardization strategies for the semiconductor industry's future, we represented SMCC by speaking on cybersecurity standardization strategies and joining a panel discussion with representatives from other standardization organizations, contributing to the overall security enhancement of the semiconductor industry.

In addition, recent cyberattacks have been occurring in companies of all industries and sizes, with attack methods often being reused across different organizations. To respond to these threats promptly, a single-company approach is insufficient. Instead, it is crucial to build trust and strengthen collaboration among organizations facing similar challenges.

Our TEL SIRT supports the strengthening of security collaboration and actively participates in external security organizations that bring together a diverse range of entities, including industry, government and academia. Through these activities, we promote the collection of threat intelligence and the sharing of various security-related information.

Security organizations we belong to

- Nippon CSIRT Association (NCA): An organization that fosters close collaboration among Computer Security Incident Response Teams (CSIRTs) in Japan and contributes to solving CSIRT-related challenges.
- FIRST (Forum of Incident Response and Security Teams): The world's largest organization of CSIRTs, established to foster close collaboration among CSIRTs worldwide and to contribute to solving challenges faced by these teams. It comprises a wide range of members, including corporations, government agencies, and academic institutions.
- Japan Network Security Association (JNSA): A nonprofit organization engaged in awareness-raising, education, research and information dissemination related to network security.
- Security Transparency Consortium: A voluntary organization dedicated to fostering knowledge-sharing for the utilization of visibility data (such as SBOM) to mitigate supply chain security risks.

External Activities and Strengthening Information Security Human Resources

2 Strengthening Information Security Human Resources

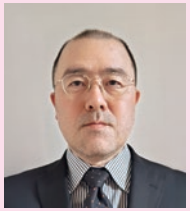
With the recent growth in threats to information security, the demand for security professionals continues to expand. Security work spans a wide range of areas, making it difficult to define it under a single category.

For instance, security analysts monitor threats daily, while engineers strengthen security measures for products and plants. In addition to technical roles, professionals handling security management and audits must have knowledge of security-related laws and standards. While more specialized areas may require collaboration with external experts, the areas that serve as foundations for a business company must be supported internally by employees. Aiming to build a top-tier security framework, we are strengthening the recruitment and development of security human resources.

The information security field evolves rapidly, making continuous skill development a critical challenge. In addition to daily on-the-job training, our security department has established structured learning programs on information security. Specifically, employees are encouraged to obtain security certifications such as Certified Information Systems Security Professional (CISSP) and participate in corporate employee training courses on information security offered by universities. Furthermore, through internship programs, we provide opportunities for students to engage with leading-edge security technologies and experience the excitement of learning about security, while also promoting initiatives to communicate the company's commitment to security to top talent interested in security.

We are actively strengthening the recruitment and development of security professionals who support both our business and overall security, driving forward our efforts in security talent development.

Activities in External Organizations and Strengthening Information Security Human Resources



Eiji Hagio
Vice President, Information Security Department
Tokyo Electron Limited

With the recent worldwide increase in semiconductor demand and growing geopolitical concerns, security risks in the semiconductor industry and semiconductor companies have gained significant attention. How is the Tokyo Electron Group addressing these challenges?

SEMI, an international organization in the semiconductor industry, has recognized the increasing importance of security and established SMCC, a cybersecurity consortium, to enhance security across the industry. SMCC currently has eight working groups, and I serve as the chair of one of the groups that is responsible for developing security evaluation methods for the supply chain. Through regular meetings, we have collaborated with industry members to draft a checklist, which has been officially published as a SEMI document. Additionally, at the Cybersecurity Session of SEMICON West in July 2024, we were the only Japanese company delivering a lecture. We are advancing our activities, aiming to contribute to the semiconductor industry and strengthen the company's presence, as well as to promote the value of cybersecurity in Japan's semiconductor industry globally as an industry leader.

Given this situation, how does the Tokyo Electron Group plan to strengthen its security organization?

We have a critical mission to lead the enhancement of information security across the entire Tokyo Electron Group. We are formulating a security roadmap for future reinforcement and based on the roadmap, we will strengthen our measures and advance the recruitment and development of security professionals. Our commitment to human resource acquisition and development is clearly stated in our recruitment website and interviews with hiring agencies. We seek individuals who share our vision to collaboratively shape the next phase of the Tokyo Electron Group's security. Our approach is built on three pillars: strengthening security measures, securing and developing talent and enhancing our presence. By achieving industry-leading cybersecurity in both name and substance, we aim to contribute to the security of the semiconductor supply chain.

Tokyo Electron Overview

1 Company Overview (As of March 31, 2026)

Corporate Name	Tokyo Electron Limited
Head Office	Akasaka Biz Tower, 3-1 Akasaka 5-chome, Minato-ku, Tokyo 107-6325, Japan
Established	November 11, 1963
Number of employees	20,236 (Entire Group)

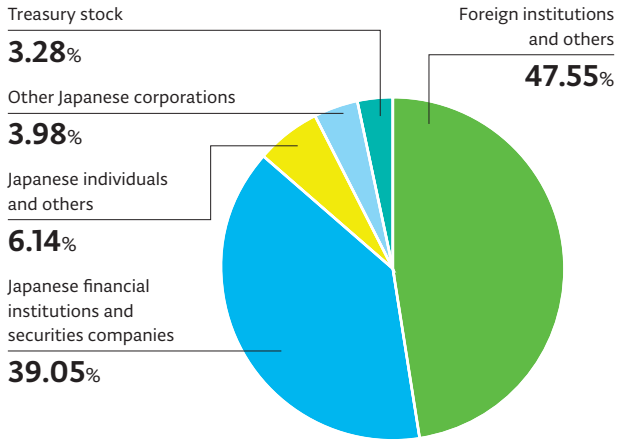
2 Stock Information

Common Stock Listed on	Tokyo Stock Exchange Prime Market
Authorized	900,000,000 shares
Issued	471,632,733 shares
Number of shareholders	114,525

Major Shareholders

Shareholders	Number of shares held (thousand)	Voting share ratio (%)
The Master Trust Bank of Japan, Ltd. (trust account)	111,481	24.43
Custody Bank of Japan, Ltd. (trust account)	46,224	10.13
TBS HOLDINGS, INC.	15,112	3.31
THE CHASE MANHATTAN BANK, N.A. LONDONSECS LENDING OMNIBUS ACCOUNT	14,891	3.26
STATE STREET BANK AND TRUST COMPANY 505001	11,569	2.53
HSBC HONG KONG-TREASURY SERVICES A/C ASIAN EQUITIES DERIVATIVES	7,408	1.62
GOVERNMENT OF NORWAY	6,738	1.47
JP MORGAN CHASE BANK 385781	6,644	1.45
BNYM AS AGT/CLTS NON TREATY JASDEC	6,418	1.40
JP MORGAN CHASE BANK 385642	5,678	1.24

Distribution of Ownership among Shareholders



TOKYO ELECTRON LIMITED

Akasaka Biz Tower, 3-1 Akasaka 5-chome,
Minato-ku, Tokyo 107-6325, Japan
Tel: +81-3-5561-7000
www.tel.com