# Cyber security in the digitalising factory

pwc

www.pwc.com/jp/en

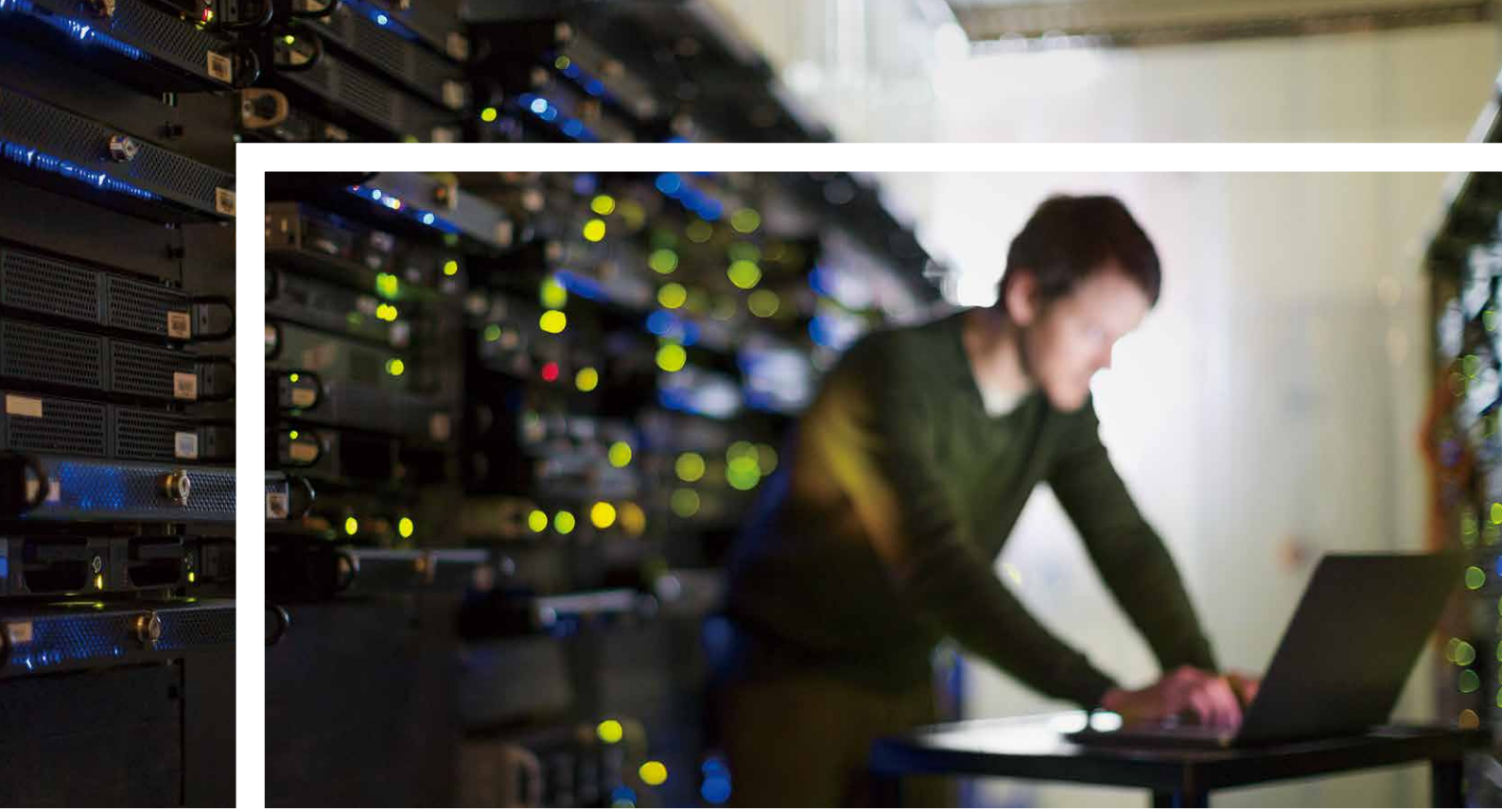
# Table of contents



# 1 Introduction

As digitalisation is accelerating continuously, the threat of cyber attacks has spread to the operational technology (OT; control and operation technology for production lines and systems) environment, which is the foundation of business activities. It is well known that cyber security incidents in factories and other OT environments have been occurring in Japan as well. PwC views OT security incidents that will threaten the very existence of companies and cyber security measures in the OT environment that prevent such incidents (‘OT security’) as important management issues.

Generally, knowledge of OT security is insufficient and companies with supply chains and manufacturing bases are struggling to promote it. This report explains important points and perspectives that companies need to consider in promoting OT security to help advance safe and secure business operations.



# 2 Categorisation and OT security in Factory (OT) environments

## Categorisation of OT environments

### (A) Major categories of OT environments

As industrial control systems (ICS) are used in factories and laboratories, which are OT environments, cyber security in OT is generally considered to be an effort that is different from traditional information security and IT security. The main reasons for this are that cyber attacks on information systems have been mainly conducted by exploiting vulnerabilities in the transmission control protocol/internet protocol (TCP/IP), and that, in many companies, the division responsible for information management and IT environment is different from that of the OT environment.

The OT environments are largely divided into (i) the factory automation (FA) environment and (ii) the process automation (PA) environment. The former consists of systems primarily designed to automate physical assembly and engineering processes; the latter consists of systems mainly designed to automate chemical synthesis and purification processes.

There are many other service systems using ICS, such as building automation (BA), and power grid and communication networks, but these will not be discussed in this report because such environments are used to provide services directly to users and have different characteristics from those used for in-house activities (factories and laboratories).

As this report mainly focuses on categorisation of the overall environment relating to OT security, PwC assumes a general situation while recognizing that there are many exceptions.

### (B) Characteristics of FA/PA environments and main differences

When considering OT security on a broader basis, there may be the misconception that availability is the top priority in all environments, or the misapprehension that no technical measures can be taken due to the difficulty in changing configurations. In fact, however, each OT environment is different in nature and discussing them as a whole is difficult, unlike the office automation (OA) environment. Just by categorising OT environments into FA and PA environments many differences are apparent, as shown in the table below (Diagram 1).

**Diagram 1: Categorisation of OT environments**

| Category | Indicator | (Reference) OA environment | FA environment | PA environment |
|---|---|---|---|---|
| Functions and actual conditions | Ease of configuration change | Easy | Comparatively easy | Difficult |
| | Output quality accuracy requirements | Low (Best effort) | High | Medium |
| | Standard | TCP/IP | TCP/IP + specific protocol | TCP/IP + specific protocols |
| | Operational system | Centralised across the company by IT division | Decentralised by manufacturing division | Centralised to a certain extent by operating vendor |
| Security | Subjects to be protected. | Information asset | Processes and equipment for processes | Processes and equipment for processes |
| | Prioritised security elements | Confidentiality | Availability | Integrity |
| | Impact in the case of security infringements | Data loss | Environmental, safety, product and equipment infringements | Environmental, safety, product and equipment infringements |

Source: PwC

## Points to note in OT security

Many Japanese companies will consider the optimal nature of their OT security management (structure, processes and technical measures) and planning measures (systems and mechanisms, and introduction of countermeasure products) to realise the optimal management. In doing so, it is important to appropriately understand the functions that individual OT environments within the organisation aim to achieve and the actual situation, as well as recognise the differences between the conventional approach to information security and IT security, and the approach to OT security.

For example, consider incident response activities. Given the characteristics of the OT environment, maintaining or restoring utilisation of facilities should be prioritised, so the incident response process should not be based on isolating damaged facilities, but on their continued utilisation. Next, unlike IT, the system and management of the OT environment is not centralised, so it is necessary for the organisation and personnel at the site where the incident is occurring to ascertain the situation, take initial responses, isolate and possibly triage the incident.

However, since the organisation and personnel at the sites are not originally designed for security management, they lack security expertise in terms of experience and skills. In order to ensure the processes that require security knowledge and skills function effectively, processes such as triage and incident isolation, it is also necessary to consider the use of third-party services to support the organisation and personnel at the sites, and the development of simple decision-making criteria (Diagram 2).

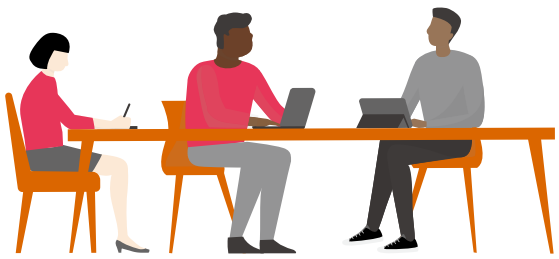
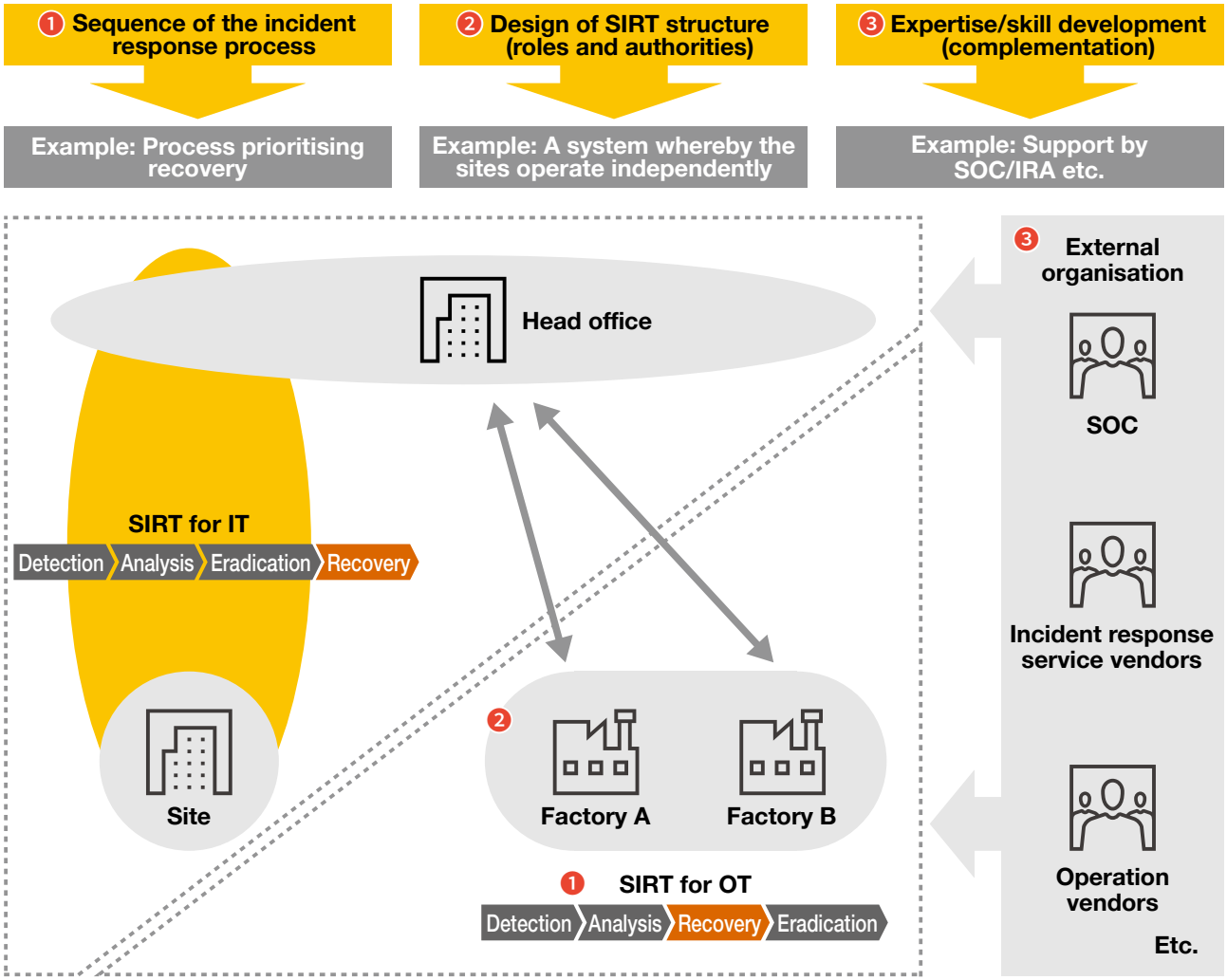


**Diagram 2: Points to note and examples of considerations in the incident response system**




SOC: Security Operation Centre
IRA: Incident Response Advisory

Source: PwC

# 3 Security governance at factories (OT) – Building a security management system emphasising the on-site capability

## Importance of OT security governance

An organisation that aims to manage the security of OT (Operational Technology: control and operation technology for production lines and systems) environments will be faced with the need to control the employees at the divisions responsible for the construction, operation, maintenance and business use of OT systems in the OT environment, and to manage the physical environment of factories and laboratories.

However, conventional IT security management has been designed and operated primarily to control office workers and IT divisions. In addition, IT security has also been able to partially manage organisations and employees by controlling the configuration of IT systems and installing security products. As for OT systems, however, there are many niche systems for each product and business, making it more difficult to standardise configurations and control organisations and employees with security products.

In order to manage OT security, it is necessary to ensure that company policies and rules regarding OT security are communicated in a practicable manner to employees who are engaged in the construction, operation, maintenance and business use of OT systems, and periodically review the management activities and encourage corrective actions if needed. Due to the differences in the nature and scope of OT security management and existing management methods, it has to be said that operating such a series of processes using existing management mechanisms is difficult.

In light of this reality, it is necessary to design and implement unique OT security governance apart from the IT security management system. The following sections will explain the important points in designing and implementing OT security governance (phase 1) and in achieving maturity (phase 2).

## Important points in OT security governance

Governance is generally achieved through three approaches: (i) policies and rules, (ii) systems and mechanisms and (iii) organisations and personnel. The same applies to OT security governance, and these approaches need to be adopted for proper security management. However, in design and implementation, the nature of OT security must be given due consideration.

### (A) Building systems-focused governance

OT security governance in the enterprise is facing a difficult situation. OT environments exist in every business and site, but a company needs to control them as a whole through a single governance system. Therefore, based on the standard rules set as a whole, each business unit or site is expected to develop operational rules, procedures and management mechanisms to achieve compliance with the rules through their own efforts.

On the other hand, as mentioned above, there are many niche systems in OT systems for each product and business. In light of the uniqueness and novelty of OT security, it is obviously difficult for each business or site to correctly understand the purpose and appropriate methods of OT security on their own, and to realise and implement security management in line with the company-wide rules.

Given these situations, the focus in OT security governance should be on systems and mechanisms, not rules. Standardised, company-wide rules are of course necessary, but it is not sufficient for the OT security governing organisation leading OT security governance to build a one-way, formal governance structure that just sets rules and encourages compliance. They must incorporate such rules into concrete systems and mechanisms, and aim to build realistic governance in which overall policies and rules are interactively coordinated in light of the reality of the systems and mechanisms at each site.

### (B) Focusing on site capability

Although standardisation of OT environments is progressing along with the advancement of digitalisation and openness, there are still many environments where each business or site has its own protocols and unique conditions that must be maintained. Against this background, it is desirable for corporate OT security governance to be based on a common company-wide policy, while at the same time appropriately taking into account the unique conditions of each site, integrating them into a security management system and implementing it. Therefore, when designing the OT security governing organisation, which plays a central role in OT security governance, it is important to ensure that each business unit and site can act on their own initiative and have the capability to properly enforce such authority. To achieve this it is necessary to ensure the effectiveness of in-site security management by, for example, increasing the proportion of personnel who are knowledgeable about the site-specific OT environment and are responsible for management and operation within the site, rather than an all-governing central body of personnel. Clarifying policies and standards to make it easier for each site to exercise its discretion under a certain level of control, and providing extensive education to support their start-up phase are also effective.

### (C) Adopting a maturity-based governance model

Security personnel who have already experienced the security governance process from building to maturity may try to apply mature models of security governance to their OT security as well. However, it is expected that such mature models will not work as envisaged. Security governance is strongly dependent on the level of understanding of security among personnel, the development state of the security management mechanisms, the degree of systemisation and the diversity of the environment to be protected. In OT security, personnel who understand the purpose and need for security and an environment where technical measures are in place are few. This is because OT security is very different from IT security, where personnel have basic knowledge and where systems and mechanisms for various security management purposes are incorporated within day-to-day operations and technical measures. Applying only a mature design of governance, despite the immaturity of the various real-world factors that affect the company's governance, will not dovetail well, nor function.

Therefore, in the development of OT security governance, the appropriate state of governance should be sought at the time, in line with the actual situation in each company. It generally takes a long time for governance to mature. For example, at the initial phase of an OT security initiative, the minimum rules need to be standardised, overall management mechanism and structure be set up and improve the security awareness and knowledge level of personnel, thereby expanding and deepening the system and structure through activities. Then, as the organisation's OT security management matures, the state of governance structure should be considered. By taking this approach, the state of OT security governance can be continuously maintained in an optimal state.

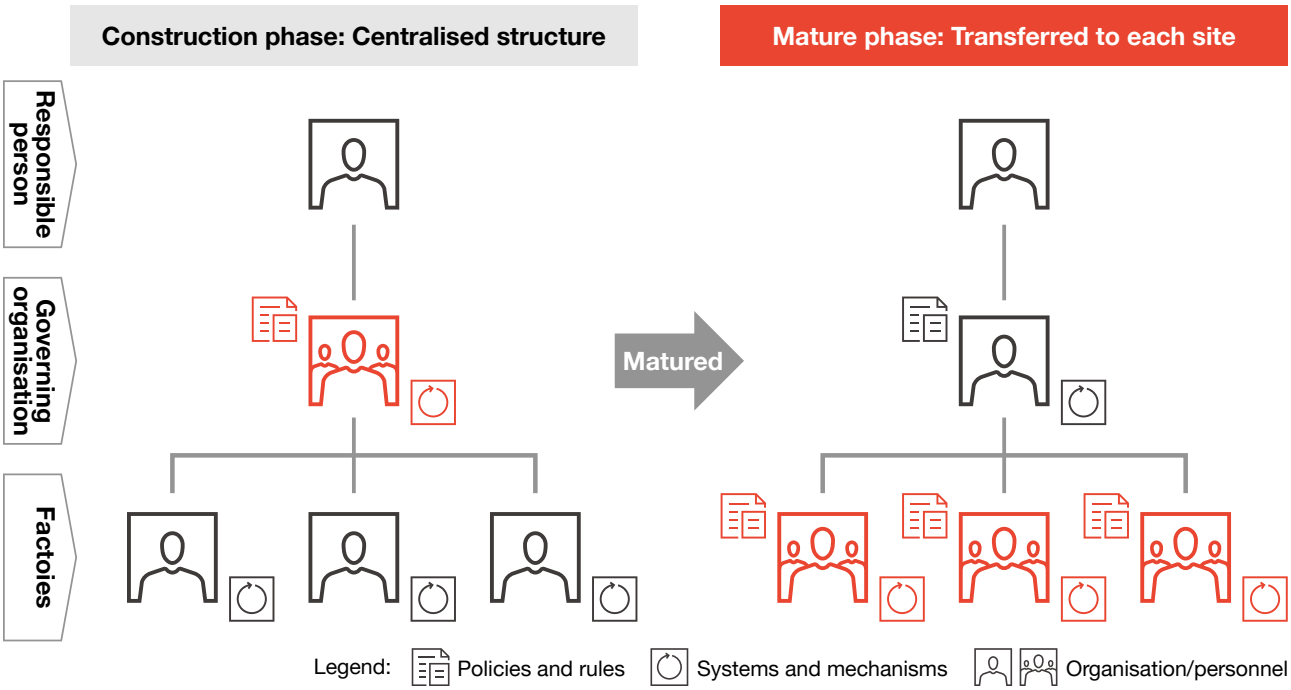
## Roles that OT security governing organisation should play

As mentioned above, the OT security governing organisation plays an important role in leading organisational OT security management initiatives. The organisation is expected to correctly recognise the need for OT security, advocate the importance of OT security as a new function for the organisation, and promote it by acquiring the necessary resources.

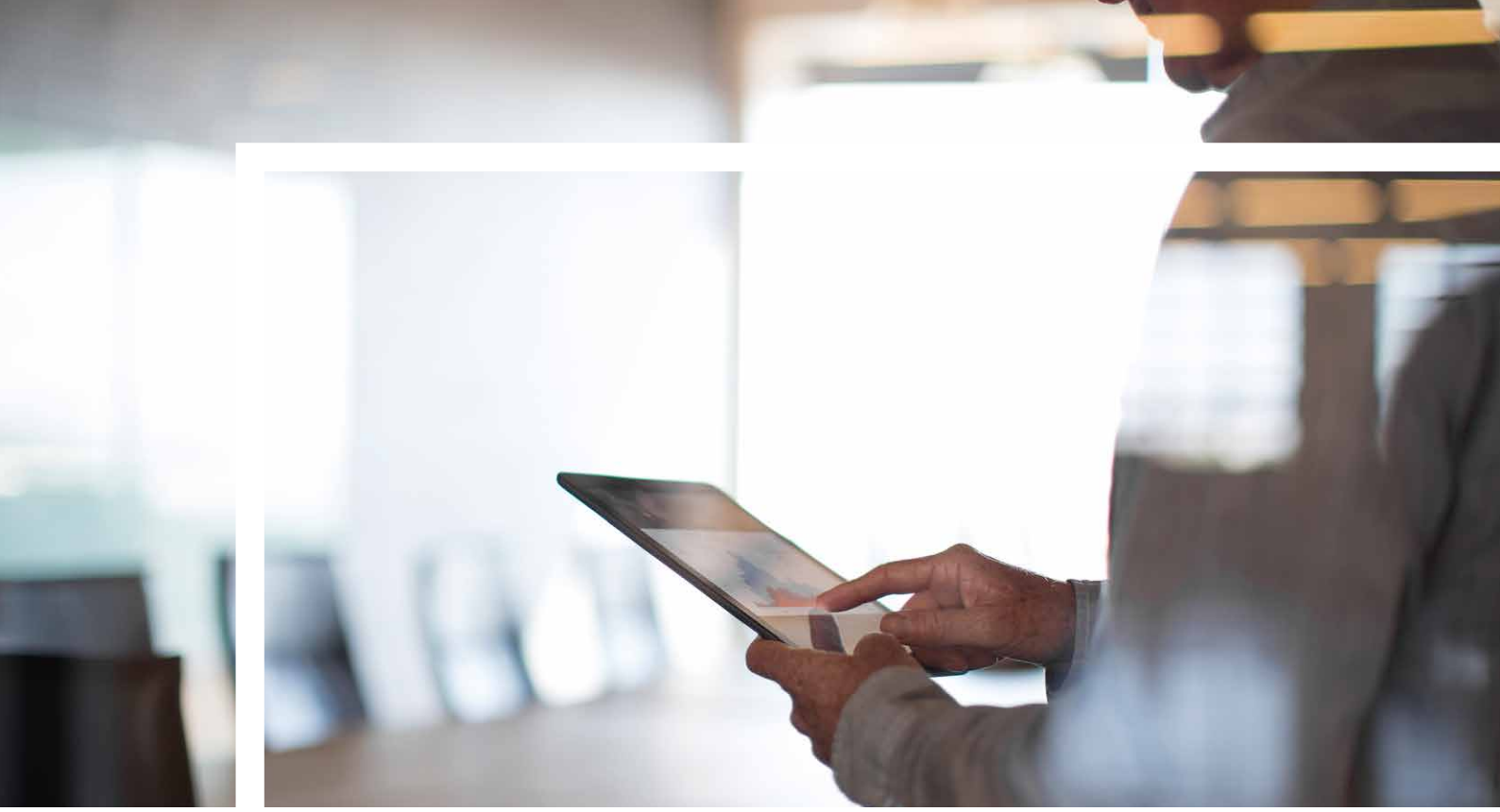
It is also an important activity for the OT governing organisation to go around the factories, the frontline of OT security, and explain the importance and business benefits of security to personnel on site, who tend to concentrate solely on their core business. At the same time, fostering understanding of the investment required for OT security among management and the head office departments of each business, and securing support for cooperation at each site, are also important. Furthermore, it is necessary to streamline the roles and cooperation methods with the existing IT security systems, and to efficiently achieve security management, including OT, throughout the entire organisation and without omissions.

Going forward, OT security governance will be a key management issue. The OT security management organisation is expected to play a significant role and is required to have the right resources to work on it.

**Diagram 3: Examples of OT security governance transitions**




Source: PwC



# 4 OT security assessment from an attacker's perspective using ATT&CK for ICS

## Necessity of OT security assessment from an attacker's perspective

Why is it necessary to assess OT security from an attacker's perspective? There are three reasons as below.

### Acquisition of perspectives that are free from OT environmental constraints

OT environments have more constraints than Office Automation (OA) environments and security measures are restricted. For example, measures that may affect the operation of equipment cannot be implemented, or the sophisticated security measures cannot be applied because legacy OS is still in use. However, attackers do not of course take into account such circumstances; if there are holes in the countermeasures, they will actively use such holes in their attacks.

By setting aside the constraints of the OT environment and assessing OT security from the attacker's perspective, vulnerable areas that need to be addressed can be identified. Then, if effective measures can be taken within the scope of constraints, such as adding measures to vulnerable areas or taking measures on the attack path if direct countermeasures cannot be taken, defensive capabilities can increase.

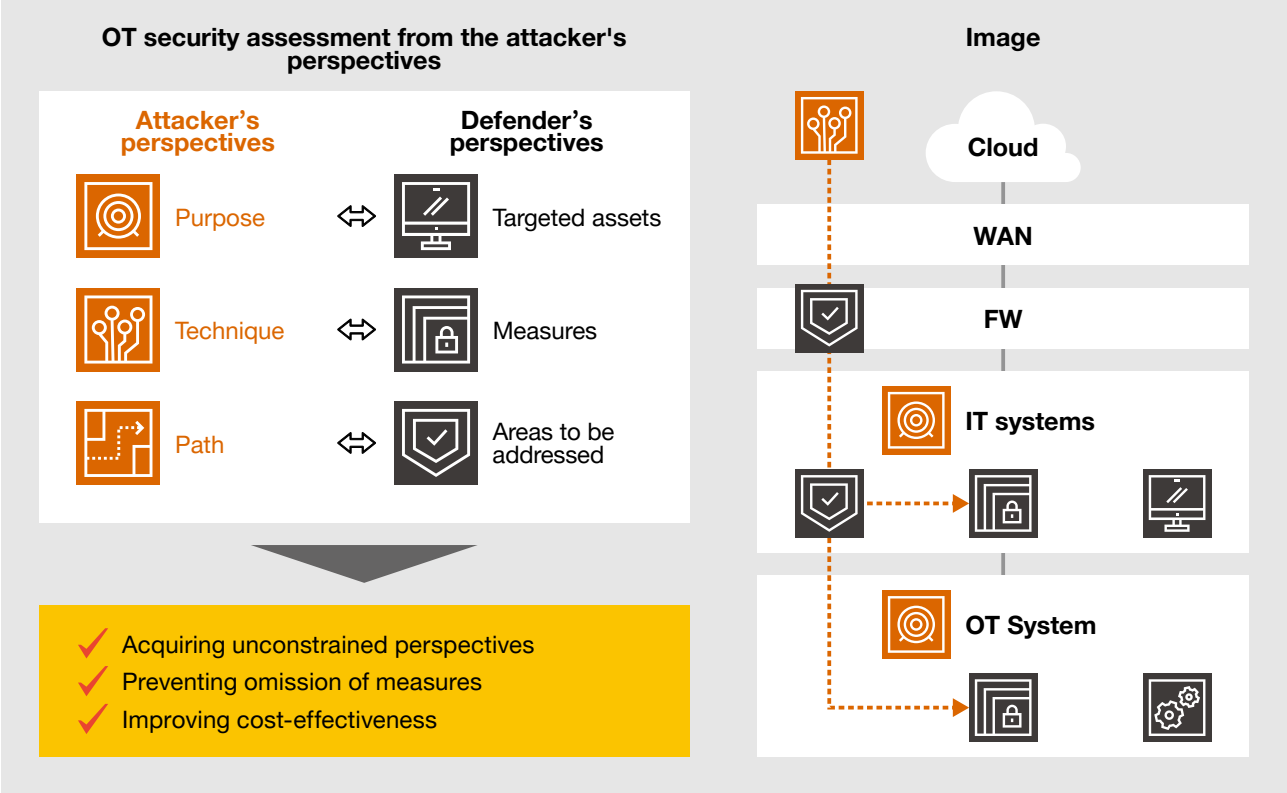
### Preventing omission of measures

If there are omissions in the cyber attacks envisaged when developing security measures, then appropriate measures are not possible. Assessing OT security based on comprehensive assumptions of cyber attacks that may occur in an organisation's OT environment will prevent omissions in an organisation's measures and ensure effective results.

### Improving cost effectiveness

Security measures are implemented by combining several measures with different scopes and effects. If an organisation wants to take a high level of measures against all cyber attacks, it becomes necessary to implement a large number of security measures for all the targets to be protected, which is not realistic due to cost and time constraints. Therefore, by assessing measures from the attacker's perspective and taking into account the ease of attack and its consequences, it can be understood which measures should be prioritised and which attack paths to focus on, thereby improving cost-effectiveness.

**Diagram 4: Need for OT security assessment from the attacker's perspectives**




Source: PwC

## Points to note in the assessment

Below are some points to consider when carrying out OT security assessments from an attacker's perspective.

### Ensuring comprehensiveness of attack scenarios

First of all, it is necessary to have a comprehensive overview of possible cyber-attacks in OT environments. Trustworthy cyber security organisations and institutions have published lists of cyber attacks in OT environments. This will help to ensure comprehensiveness at no cost ('ATT&CK for ICS', a prime example, is discussed below).

### Ensuring accuracy of assessments

As each OT environment is different in nature, the potential cyber attacks and their impact also vary depending on the environment. Therefore, in order to obtain an accurate assessment, it is necessary to understand the details of the OT environment. This enables a correct estimation of the actual likelihood of a cyber attack occurring in the OT environment under assessment and its impact.

The details of the OT environment that should be understood include the network configuration, the state of usage of USB flash drives, the roles and relationships of each system, the ease of recovery and the prioritisation of what should be protected based on these details.

### Carrying out ongoing assessments and improving measures

Since cyber attack tactics are constantly evolving, regular assessments must be carried out to understand whether security measures in place are sufficient against the latest attack tactics. In addition, changes in the OT environment may change the potential cyber attacks, and as a result, the security measures may also change. Therefore, before changing the network configuration or adopting new technology, a security assessment should be carried out and considerations made on whether or not there is a need to change existing security measures. Ongoing assessment and improvement of measures based on the assessment results will enable the ability to maintain and improve the effectiveness of the measures.

## ATT&CK for ICS to help assess OT security

Finally, the following reference material may be useful for OT security assessments. The Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a knowledge base on attackers' tactics and techniques prepared by a non-profit organisation in the US. The first edition was published in 2013 and has been continuously updated since then. In January 2020, ATT&CK for Industrial Control System (ICS) was released. ATT&CK for ICS provides a comprehensive and systematic overview of cyber attacks against OT environments, which can be used to carry out OT security assessment without any omissions. Its features are briefly described below.

### Functional levels and associated assets

ATT&CK for ICS has two additional elements specific to the OT environment that differ from the already existing ATT&CK for Mobile and ATT&CK for Enterprise.

#### Functional levels

The ATT&CK for ICS domain is indicated by the functional level of the Purdue model*[1]. Basically, functional levels 0-2 are the scope of ATT&CK for ICS (levels 3 and 4 are the scope of ATT&CK for Enterprise). By understanding the OT environment according to the Purdue model, one can understand the scope of ATT&CK for ICS.

#### Assets

There are a wide variety of assets in OT environments. ATT&CK for ICS generalises and lists these assets. Understanding the content of assets and which ones in an organisation'sr environment are affected by individual techniques can help the organisation take measures.

### Tactics and techniques

Another feature of ATT&CK for ICS is the visualisation of attackers' tactics and techniques in the form of a matrix.

The horizontal axis of the matrix shows the tactics, while the vertical axis lists the techniques used in each tactic. Attacks will be launched from the left to the right of the tactics. This matrix can be very useful as it provides a comprehensive, step-by-step overview of possible attacks, but it should be noted that not all steps are necessarily followed, as some steps may be skipped or the attacker's objective may be achieved before the impact (at the right end of the tactics column) is reached.

These reference materials will help to devise effective measures. ATT&CK for ICS is also practical enough to help understand specific examples of techniques and mitigation measures, so they should be read through in order to gain a better understanding.

---

*1: Standard model of enterprise architecture for Computer Integrated Manufacturing (CIM).

## Diagram 5: Examples of OT security governance transitions

**Tactical objectives of attackers (proceeding from left to right)**

**Tactics**

**Techniques used by each tactic**

**Technique**

| Initial Access | Access Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 techniques | 9 techniques | 6 techniques | 2 techniques | 6 techniques | 5 techniques | 7 techniques | 11 techniques | 3 techniques | 14 techniques | 5 techniques | 12 techniques |
| Drive-by Compromise | Change Operating Mode | Hardcoded Credentials | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Adversary-in-the-Middle | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Exploit Public-Facing Application | Command-Line Interface | Modify Program | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Automated Collection | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Exploitation of Remote Services | Execution through API | Module Firmware | | Indicator Removal on Host | Remote System Discovery | Hardcoded Credentials | Data from Information Repositories | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| External Remote Services | Graphical User Interface | Project File Infection | | Masquerading | Remote System Information Discovery | Lateral Tool Transfer | Data from Local System | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Internet Accessible Device | Hooking | System Firmware | | Rootkit | Wireless Sniffing | Program Download | Detect Operating Mode | | Block Serial COM | Unauthorized Command Message | Loss of Control |
| Remote Services | Modify Controller Tasking | Valid Accounts | | Spoof Reporting Message | | Remote Services | I/O Image | | Change Credential | | Loss of Productivity and Revenue |
| Replication Through Removable Media | Native API | | | | | Valid Accounts | Monitor Process State | | Data Destruction | | Loss of Protection |
| Rogue Master | Scripting | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Safety |
| Spearphishing Attachment | User Execution | | | | | | Program Upload | | Device Restart/ Shutdown | | Loss of View |
| Supply Chain Compromise | | | | | | | Screen Capture | | Manipulate I/O Image | | Manipulation of Control |
| Transient Cyber Asset | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Rootkit | | Theft of Operational Information |
| | | | | | | | | | Service Stop | | |
| | | | | | | | | | System Firmware | | |

Source: Prepared by PwC based on MITRE ATT&CK for ICS Matrix

# 5 The importance of reference modelling of security architecture in factory (OT) environments

## What is required for OT security

When implementing security architecture in OT environments, it is important to first recognise the constraints that exist within an organisation. Typical examples are listed below.

### Constraints

#### 1. It is necessary to prioritise functional requirements in the factory

Factories may continue to use software that only runs on legacy OS used for embedded systems. In some cases, for operational reasons, the use of that software has to be prioritised and an OS upgrade is not possible. In addition, the emphasis on productivity makes it difficult to have dedicated security personnel stationed at each factory from a cost-effectiveness perspective, which also contributes to these constraints.

#### 2. Production must not be disrupted

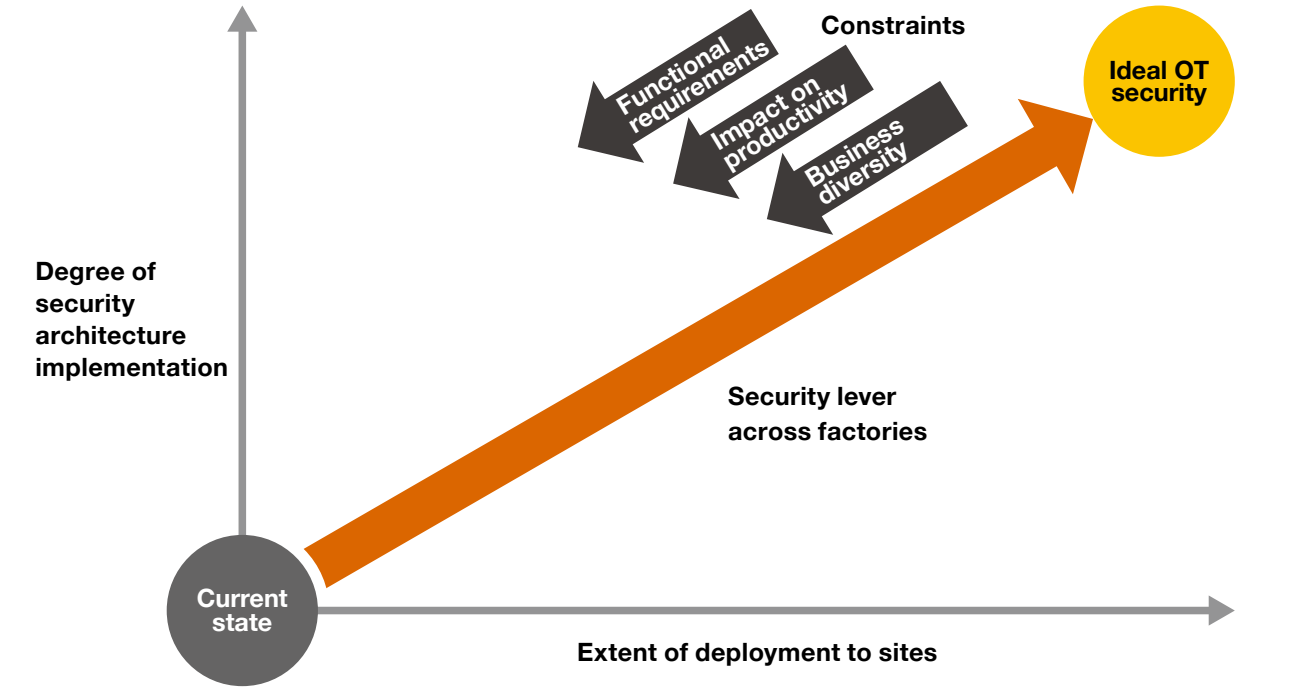
Many companies operate factories to produce and process their products. This means that the implementation of a security architecture must avoid delaying or disrupting the operation of the factory.

#### 3. Different factories have different operations and sizes

Many companies have several factories, both in Japan and abroad, due to production efficiency and labour cost reduction reasons. Each of them differs in size, nature of business and location. This means that it is not enough to simply implement security architecture in a particular factory, but it must be designed and implemented with all factories in mind.

Taking into account the constraints that these factories have, a combined effort is required to improve the OT security level for multiple factories both in Japan and abroad, while meeting functional requirements. A comprehensive and prompt response in the event of a security incident is also a key requirement.

**Diagram 6: Relationship between ideal OT security and constraints**




Source: PwC

## Benefits of reference modelling

Under the specific constraints of OT environments, it is expected to take an enormous amount of time, cost and operational load to implement a security architecture. Therefore, reference modelling of the design and implementation of the security architecture enables flexible design and implementation according to the characteristics of each factory. The main benefits of reference modelling are described below.

### Consistent security quality

Because the use of reference models ensures a certain standardised level of design and implementation, consistent security quality can be achieved, regardless of the size of the factory or the characteristics of the business.

### Cost reduction

As there is no need for individual design and implementation each time, the costs spent on individual design and implementation for each factory can be reduced.

### Time saving

As mentioned above, there is no need for individual design and implementation, which allows for faster implementation of security architecture.

### Prompter responses

By standardising the design and implementation, the operation after the implementation of the security architecture can also be standardised across factories. Furthermore, even if incidents occur in more than one factory, communication between factories is possible with a common understanding based on a reference model, making it easier to identify similar terminals based on information on the terminal that is causing damage and take necessary response.

## Requirements for reference modelling

Finally, we will consider the requirements for a reference modelling of the security architecture.

### Design and implementation policies not bound by scale or nature of work

If the design and implementation policies change according to the scale and nature of work at each factory, work duplication will occur at each plant and the quality of the security architecture will not be stable. Therefore, design and implementation policies not bound by scale or nature of work are needed.

### Distinction between basic and detailed design

On the other hand, if everything is standardised in the reference model, there may be cases where implementation does not proceed well in some factories. It is therefore desirable to standardise as far as the basic design, but enable the detailed design to be carried out taking into account the factory characteristics. This will enable cost and time reductions, while keeping the consistent quality of design and implementation across factories.

### Clarifying decision-making criteria to prioritise implementation

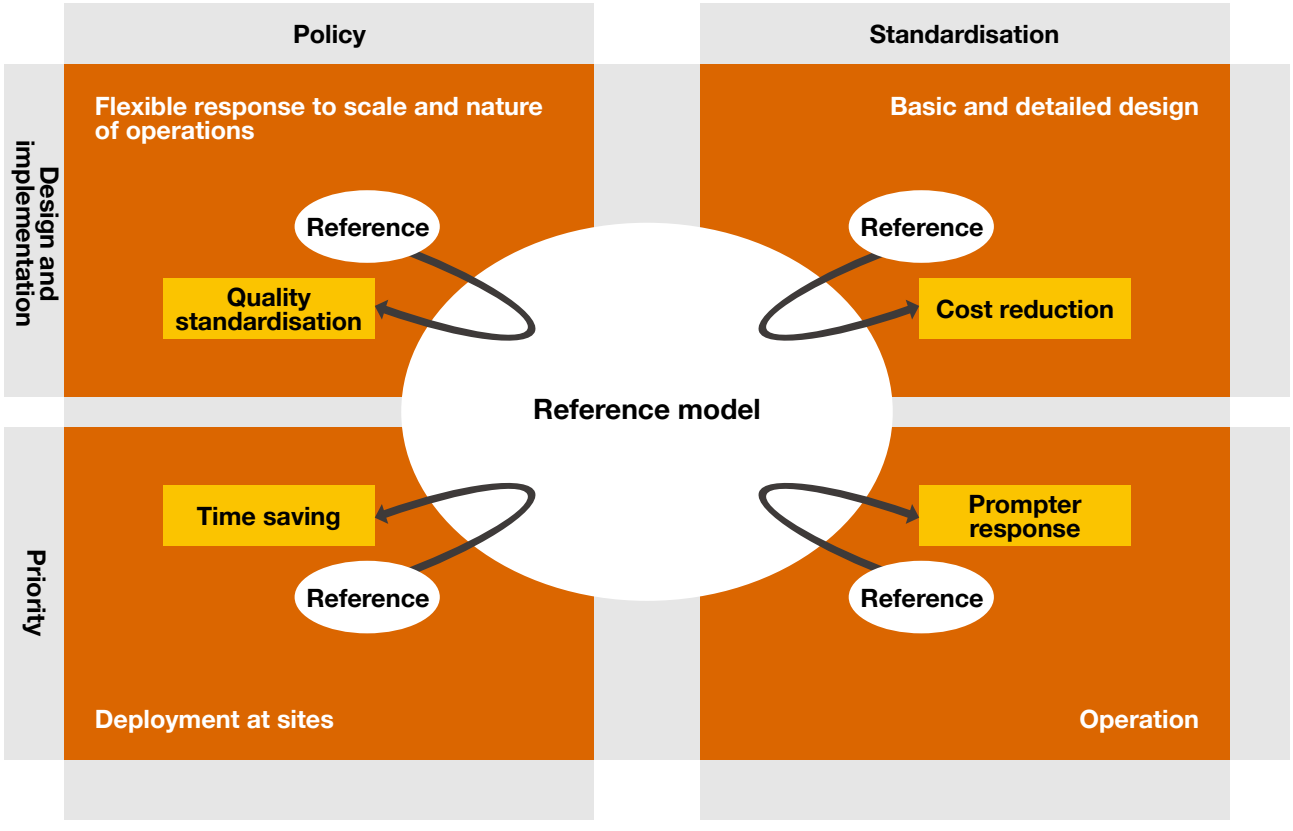
The more factories there are, the more effective the reference model will be. However, it would be inefficient to proceed with implementation across all factories without due consideration. In order to leverage the deployment to factories from a long-term perspective, it is necessary to have decision-making criteria to prioritise at which factories it is to be implemented, using the size of the factory and the nature of its operations as decision-making factors.

### Standardising fundamental operations

When considering operations after implementation, detailed operations may vary from factory to factory, but the fundamental operations need to be standardised. In order to prevent the spread of damage of an incident, it is necessary to be able to separate the network in the event of an emergency, so that production is not disrupted and the critical assets can be protected. This means that, when designing and implementing security architecture, it is important to take into account the ability to conduct a priority-based incident response.

While many companies have factories in Japan and abroad, the resources available to deploy security personnel and design and implement security architecture in factories are limited. In this context, reference modelling of security architecture is useful to ensure that security permeates all factories.

**Diagram 7: Requirements and benefits to be achieved by the reference model**




Source: PwC

# 6 Security personnel in the factory (OT) areas

## Security personnel required for OT environment

When hearing the words ‘security personnel,’ one may imagine ‘security specialists’ who have advanced expertise and execution capabilities. In the OT security field, however, security specialists play only a small part of the role of the initiative and are not the main role.

Regardless of IT and OT, a company’s approach to security requires both an administrative role to develop and oversee rules and mechanisms, and a role to implement and operate technical measures to realise the rules. The difference between IT and OT is the knowledge and skills, especially when implementing technical measures. In the case of IT, standardised technologies are used in the systems that implement security. On the other hand, in the case of OT, equipment and systems specific to the production of the organisation’s own products are usually used. Therefore, in order to implement and operate security measures, it is necessary to understand the technology of the organisation’s own equipment and systems, optimise security measures and implement them.

Based on the above assumptions, the following three types of security personnel in OT environments are defined and their respective requirements are explained as below.

### Management personnel

Personnel who are responsible for developing security rules and mechanisms, checking their implementation status and promoting improvements.

Management personnel are required to optimise general security management requirements as rules, by taking into account the characteristics of their own organisation’s business and equipment and then supervising and promoting them. They therefore need a basic knowledge of security management as well as a deep understanding of their own business and organisation.

### Technical personnel (OT systems specialist)

Personnel who are responsible for implementing and carrying out security measures in the design and development, operation and maintenance of OT systems.

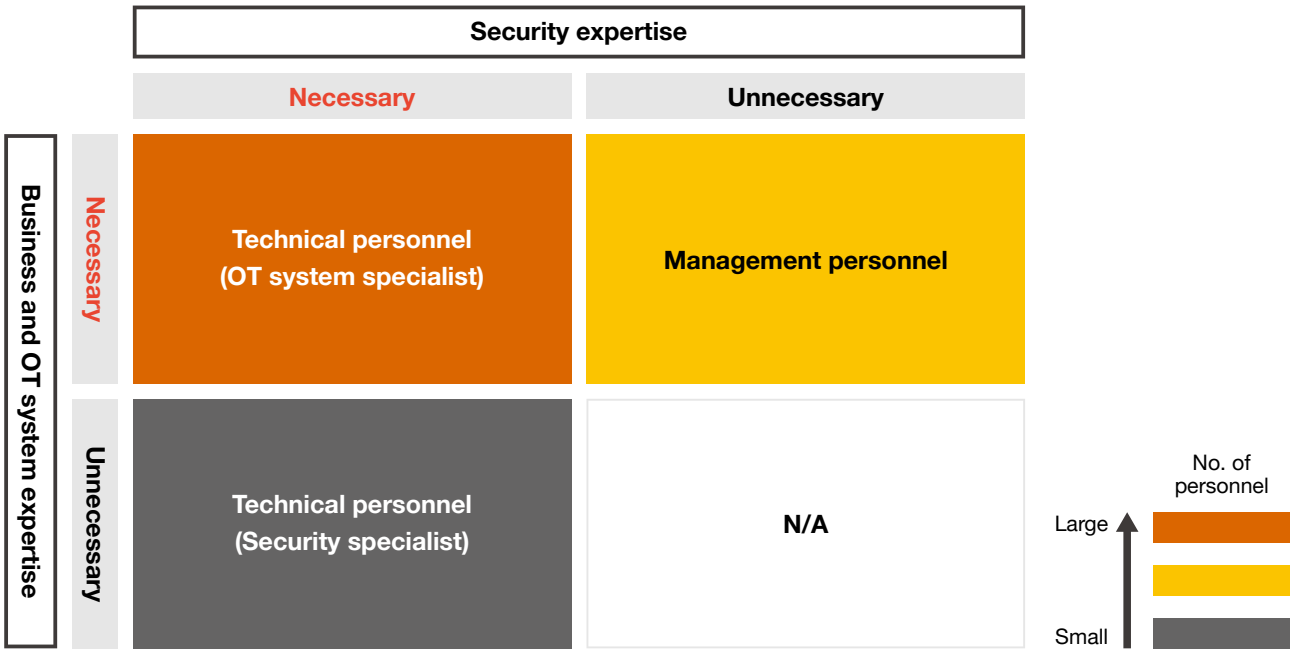
As technical personnel are required to integrate security requirements into the design and development, operation and maintenance of OT systems, they must have technical expertise in the same systems and their operation and maintenance, as well as security expertise. In addition, as many companies and organisations have different systems at different locations and often carry out the operational work on-site, the technical personnel will be located at each location and the number of the personnel will be the largest.

### Technical personnel (security specialist)

Personnel who are responsible for carrying out technical security tasks, such as security monitoring (security operation centre) and advanced analysis.

While a high level of security expertise is required, they do not need to have much expertise in business or equipment.

**Diagram 8: OT security personnel classification by knowledge and skills**




Source: PwC

## OT security personnel acquisition strategy

As mentioned above, many of the OT security personnel are required to have expertise in their own company's business, organisation or OT systems and their operation and maintenance. In order to acquire such personnel, it is desirable as a personnel strategy to increase security knowledge by utilising internal personnel who already have expertise in the company's business, organisation or OT systems and their operation and maintenance, rather than recruiting security personnel from outside. In addition, generally speaking the higher the level of specialisation required and the more standardised the knowledge/skills, the easier it is to effectively use external resources. In areas where there is no need for company-specific knowledge, it is advisable to consider outsourcing or appointing external personnel.

Based on the above, the strategies for acquiring each type of personnel can be described as follows.

### Management personnel

It is effective to educate personnel who understand the business characteristics of their own organisation and are positioned to promote OT-related measures (e.g. personnel with relationships with internal OT stakeholders) about basic security management knowledge.

It is desirable to consider what organisational units management personnel should be deployed in based on the organisation's governance strategy.

### Technical personnel (OT systems specialist)

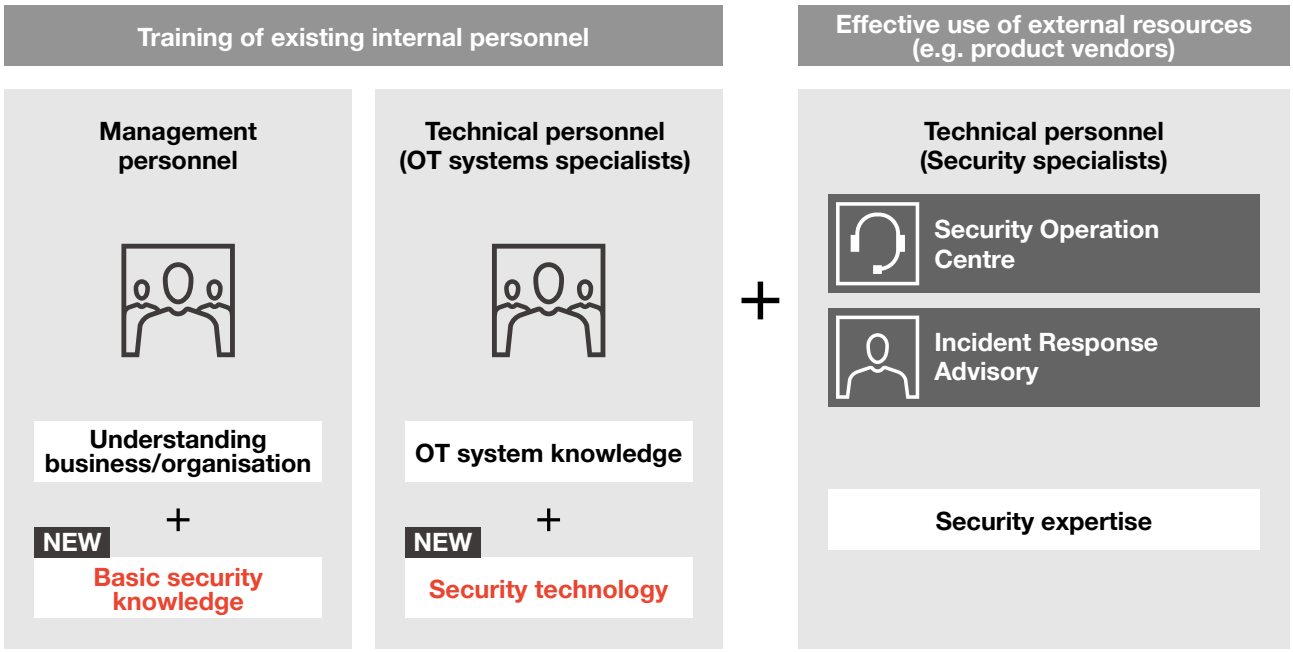
It is necessary to educate internal personnel with technical expertise in OT systems and their operation and maintenance on security expertise, including not only knowledge but also operational skills. As mentioned above, many companies implement and operate OT systems independently in each business and at each site, and these personnel need to be fostered at each site.

### Technical personnel (security specialist)

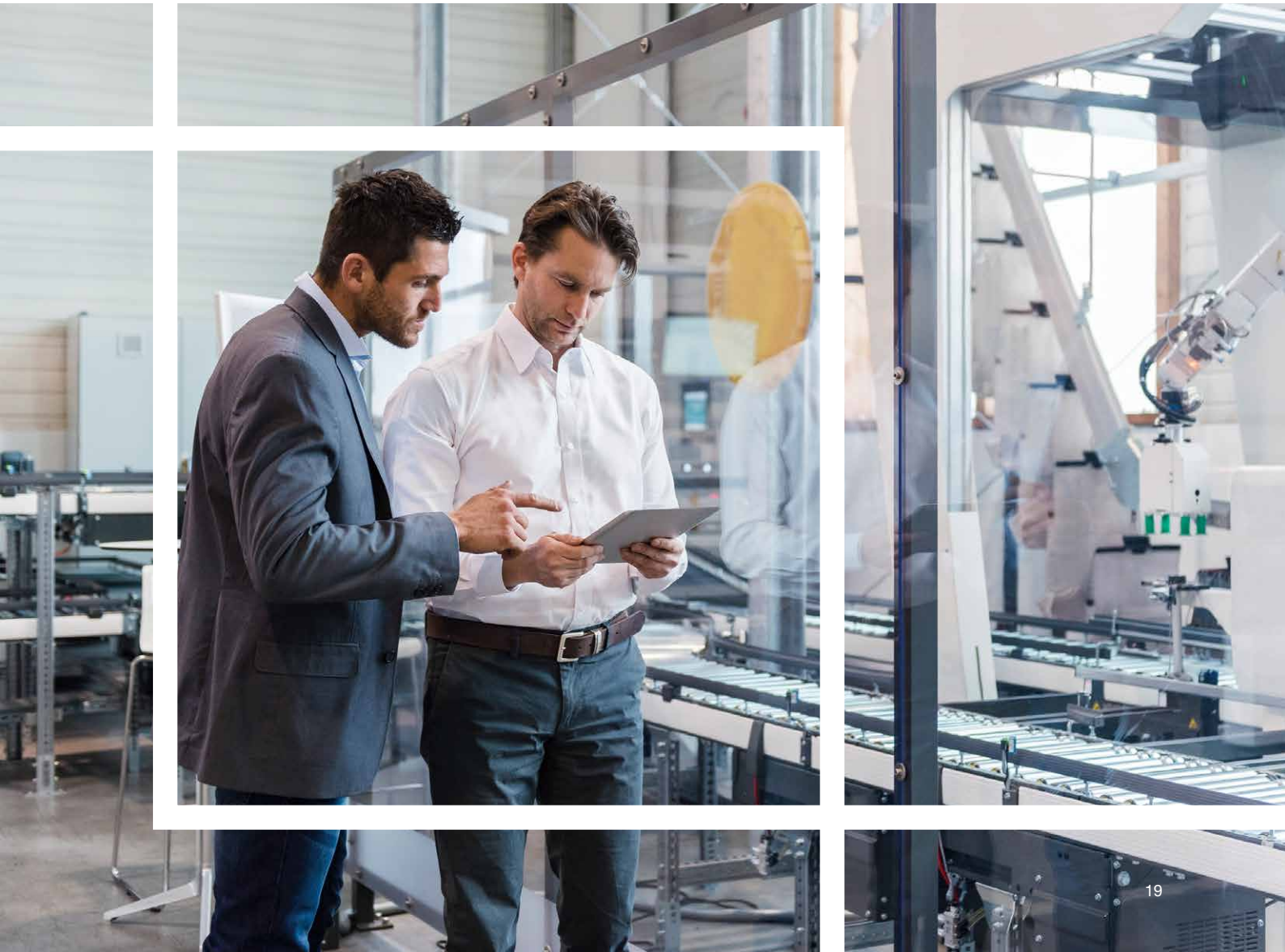
Technical personnel are required to have advanced security expertise, but they do not need to have much knowledge specific to their own organisation. For this position, therefore, external appointments and outsourcing can be used effectively. Considering the sharing of personnel in the IT division of within an organisation is also an efficient and effective strategy for acquiring security personnel.

We hope that Diagram 9 will also be referred to, and consider and implement education and outsourcing plans in line with respective personnel acquisition strategies to ensure the security of OT environments.

**Diagram 9: Strategies for acquiring each type of personnel**




Source: Prepared by PwC



# 7 Advanced cyber attacks targeting OT environments and countermeasures

## Alerts by US government agency

In April 2022, the US National Security Agency (NSA) issued a joint statement with the Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) warning against advanced persistent threat (APT) tools that target industrial control systems (ICS) and cause destruction or disruption.

Since the year 2010, the number of security incidents in critical infrastructure such as power plants and water supply facilities, ironworks and chemical factories has been increasing, particularly in Europe, the US and the Middle East. Attacks by APT tools are seen as comparable to these particularly strong attacks in the Middle East and Ukraine.

**Diagram 10: Cyber attacks that caused extremely serious damage to OT environments**

| | |
|---|---|
| 2010 | PLC settings were altered at an Iranian nuclear fuel facility and operations at the facility were disrupted. |
| 2015-2016 | Power transmission interruptions and system breakdowns caused massive blackouts at power facilities in Ukraine. |
| 2017 | The emergency shutdown function of a safety instrumentation system was activated incorrectly at a critical infrastructure in the Middle East. |

Source: Prepared by PwC

## What kind of attack is it? What aspects are advanced?

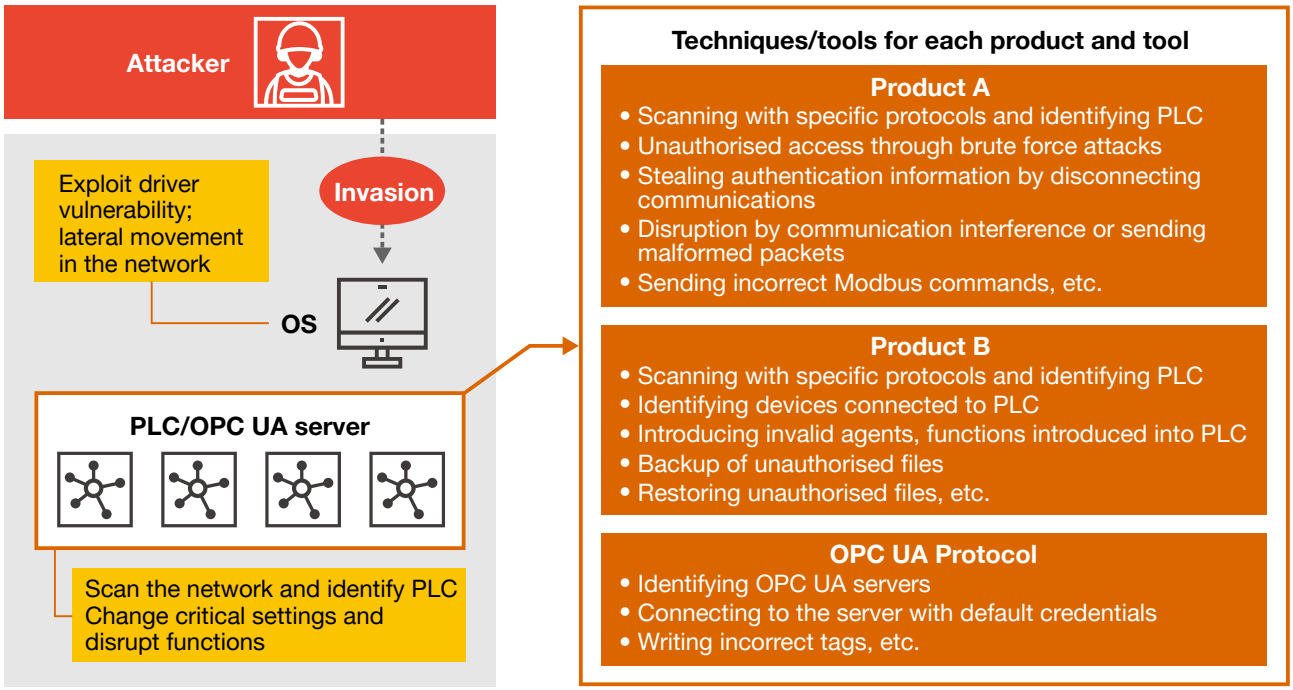
One of the reasons these attacks caused significant damage is that the attackers were familiar with industrial processes and manufacturing equipment – these attacks were not an accidental incident, such as malware targeting the IT environment accidentally entering the OT environment, but directly targeted the OT environment.

Attacks by APT tools are similarly targeted at specific products and protocols in OT environments and require special attention.

### Characteristics of attack techniques

- Exploiting a vulnerability (CVE-2020-15368) of the motherboard driver of an OS device to extend access on networks within the OT environment.
- Using tools developed in line with the specifications of a specific product or protocol (OPC UA) of a programmable logic controller (PLC) and causing destruction or disruption.

**Diagram 11: Exploitation of vulnerabilities - attacks against PLCs, etc.**




Source: PwC

## How to defend against attacks

In preparing for these attacks, 'defence through authentication' and 'detection of malicious communication and behaviour' are of particular importance.

In addition to these, the joint statement by NSA and others showed a wide range of other recommended measures for prevention, detection, response and recovery, indicating the importance of 'cyber resilience' in the event of a cyber attack.

**Diagram 12: Key recommendations (items in bold are of particular importance)**

| | |
|---|---|
| Defence | • **Implement multi-factor authentication on remote access devices**<br>• **Prohibit default passwords and change to stronger ones**<br>• Separate between OT and IT/internet; prohibit all but the minimum necessary communication<br>• Install minimum required applications and drivers<br>• Grant only the minimum necessary authorisation<br>• Make devices more robust with OS security features and EDR |
| Detection | • **Detect malicious communications (e.g. exploitation of vulnerabilities, lateral infection of malware)**<br>• **Detect malicious behaviour (e.g. installation of applications and drivers not used for business purposes) and events that may lead to service disruption (e.g. communication and processing delays, reboots), etc.** |
| Response | • Develop incident response plans<br>• Conduct regular incident response training with stakeholders (e.g. IT/OT divisions)<br>• Collect and store device logs, etc. |
| Recovery | • Obtain offline backups<br>• Ensure integrity through hash checking of firmware and controller configuration files |

Source: Prepared by PwC based on NSA information

## References


*1 Press release by the US National Security Agency (NSA) “APT Cyber Tools Targeting ICS/SCADA devices” April 13, 2022 (accessed May 13, 2022)

*2 US National Security Agency (NSA) , U.S. Department of Energy (DOE), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) Joint Advisory “APT Cyber Tools Targeting ICS/SCADA Devices” April 13, 2022 (May 13, 2022) (accessed on May 13, 2022)

*3 IPA’s attack case study material “Cyber incident case related to control system 1 - Large-scale power outage in Ukraine in 2015 -” September 2019 (accessed on May 13, 2022)

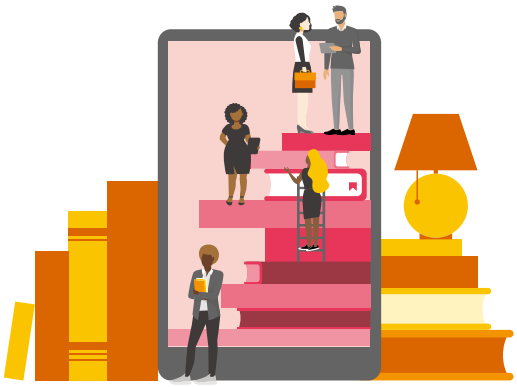
*4 IPA’s attack case study material “Control System-related Cyber Incident Case 2 - 2016 Ukraine Power Outage Due to Malware” July 2019 (accessed May 13, 2022)

*5 IPA’s attack case study material ``Control System-Related Cyber Incident Case 3 - 2017 Safety Monitor “Malware that targets control systems” July 2019 (accessed May 13, 2022)

*6 IPA’s attack case study material “Cyber incident case study related to control systems 4 - Stuxnet: The first malware that targets control systems ~” March 2020 (accessed May 13, 2022)

*7 MANDIANT BLOG “INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems” April 14, 2022 (accessed May 13, 2022)

*8 DRAGOS Whitepaper “PIPEDREAM: CHERNOVITE’S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS” April 2022 (accessed May 13, 2022)

# 8 In conclusion

In developing an organisation’s OT security management, responses that differ from traditional information and IT security are frequently required. The differences are obvious, for example, in the incident response system that many companies have developed. If systems, mechanisms or technical measures are designed for OT security management without taking into account the unique approach and environment of OT security, there is a strong concern that they will be ineffective and result in unnecessary investment and operational costs.

Meanwhile, cyber attacks have gone beyond the level of ‘crime’, such as targeting money, and have expanded to a means of ‘conflict’ between nations in cyberspace. It is expected that attackers will continue to deepen their understanding of the equipment and protocols used in factories and plants involved in critical infrastructure and businesses, develop sophisticated techniques and tools, and launch lethal attacks.

PwC provides comprehensive services for security risks in OT environments, including the assessment and the design and implementation of technical measures. In addition to directly supporting corporate OT security, PwC contributes to a better future based on safe and secure business activities and sustained growth of companies by sharing the knowledge and insights obtained through such support with society at large.

# Key members

**Yoshihisa Uemura**
PwC Consulting LLC
Partner

**Takahiro Moyama**
PwC Consulting LLC
Director

**Ryo Nunome**
PwC Consulting LLC
Senior Manager

**Keisuke Ohnuki**
PwC Consulting LLC
Manager

**Nao Kawai**
PwC Consulting LLC
Manager

**Kota Kisamori**
PwC Consulting LLC
Manager

**Yuya Kaneda**
PwC Consulting LLC
Manager

# Contact us

**PwC Japan Group**
https://www.pwc.com/jp/en/contact.html

**www.pwc.com/jp/en**

The PwC Japan Group is a collective name for the member firms of the PwC global network in Japan and their affiliates. Each firm within the PwC Japan Group conducts its business as a separate, independent business entity.
In response to our clients' increasingly complex and diverse corporate management issues, the PwC Japan Group has put in place a system that consolidates our knowledge in the fields of auditing and assurance, consulting, deal advisory, tax and legal services, and encourages organic collaboration among our professionals in each field. As a professional services network with approximately 11,500 certified public accountants, tax accountants, lawyers and other professional staff, we strive to provide services that more accurately address our clients' needs.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with nearly 364,000 people who are committed to delivering quality in assurance, advisory and tax services.

Published: December 2023 Control No: I202309-03

©2023 PwC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.