A Trend Micro White Paper | **March 2021**

The State of Industrial Cybersecurity

Converging IT and OT with people, process, and technology

» 2020 industrial cybersecurity survey report for IT and OT teams in the United States, Germany, and Japan.

CONTENTS

1. Introduction
2. Methodology
3. Executive Summary
4. Survey Results
    1. Results of all three countries
        1. Cybersecurity incidents
        2. Challenges facing people, process, technology
        3. Cybersecurity measures implemented
        4. IT and OT collaboration
    2. Results by country: US, Germany, Japan
        1. Challenges facing people, process, technology
        2. Cybersecurity measures implemented
        3. Impetuses to institute collaboration
        4. Regulations and standards
        5. Organizational structures
        6. Human resource management
5. Conclusion and recommendations

INTRODUCTION

The purpose of this survey is to reveal the current state and challenges of industrial cybersecurity, especially in promoting secure smart factories. While manufacturing companies around the world are implementing digital transformation to survive and continue to grow, cybersecurity threats have become a top concern.

In industrial cybersecurity, the convergence of IT and OT has been an important issue for long time. There were inconsistencies not only in technology and environment, but also in people and processes. This survey provides insight into the importance of bridging IT and OT by comparing the benefits of each. Furthermore, as manufacturing companies play a part in the global supply chain, we focus on the differences found between three countries: The United States, Germany, and Japan. Our survey will provide you with tips and best practices on how to further advance the state of industrial cybersecurity.

METHODOLOGY

Objective

This report takes a look at the current state and challenges facing smart factories and shines a light on the importance of cybersecurity within these institutions. This is achieved by conducting a comparative analysis among the countries with the world's top manufacturing industries, The United States, Germany, and Japan, based on three criteria:

1. Challenges from the perspective of people, process, and technology
2. Implementation rate of cybersecurity technical measures
3. Status of collaboration within organizations, namely IT and OT

Our survey was conducted in collaboration with Vanson Bourne; an England-based global technology research company. The following criteria was met:

Method

Online survey. Anonymous answers.

Period

November 3, 2020 to December 1, 2020

Respondents

- Total of 500 respondents
- Countries: US (200), Germany (150), Japan (150)
- Company profile: Manufacturing with 1,000+ employees
- Role of respondents: IT (250), OT (250)

Decision makers determining cybersecurity measures in ICS environments

IT Department: Information Technology, IT Security

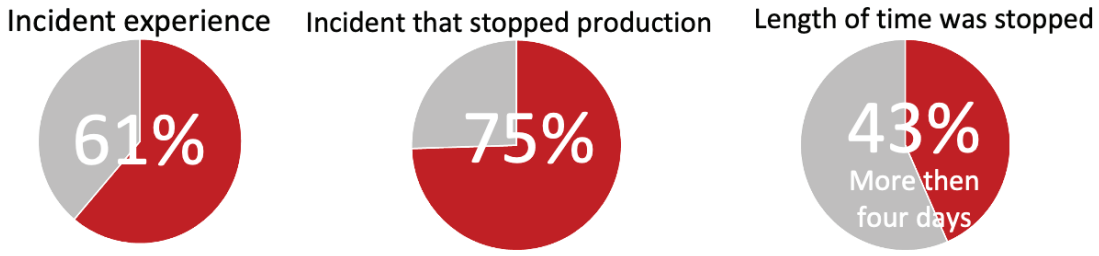
OT Department: Production Management, Production Engineering, Maintenance Management/Equipment Maintenance, Operations

1. EXECUTIVE SUMMARY – RESULTS OF ALL THREE COUNTRIES

CYBERSECURITY INCIDENTS

The majority of factories have experienced a critical incident.

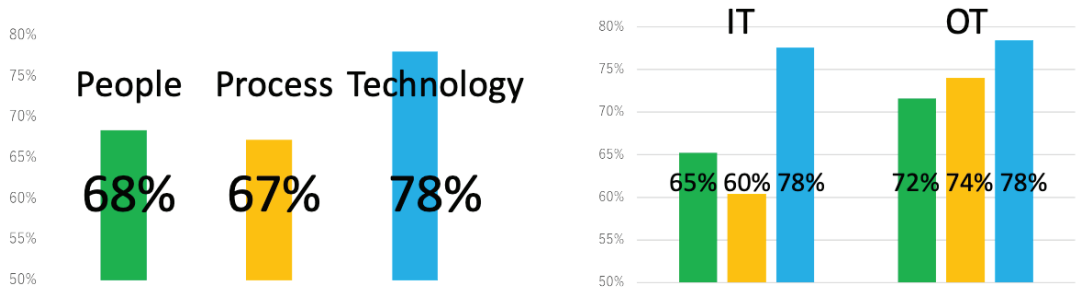
- 61% experienced incidents, of which 75% had system outages and 43% had more than four days of outages



CHALLENGES FACING PEOPLE, PROCESS, TECHNOLOGY

Technology remains the biggest challenge, but people and process are also facing issues.

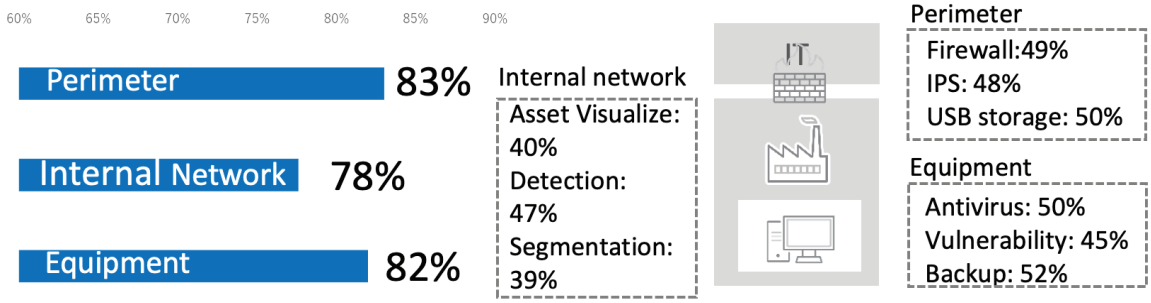
- OT recognizes people and processes as issues rather than IT



CYBERSECURITY MEASURES IMPLEMENTED

Most factories have already implemented technical measures.

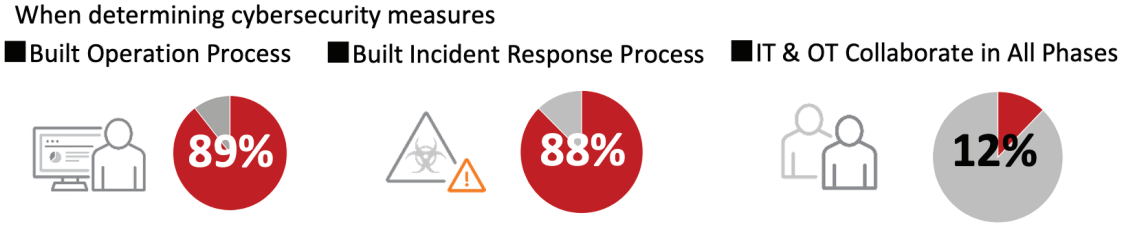
- Measures on the perimeter and on equipment are more frequently implemented than on the internal network



IT AND OT COLLABORATION

More organizations consider operations an extension of technology, but few organizations are involved in both IT and OT.

- Organizational collaboration allows for more advanced cybersecurity processes

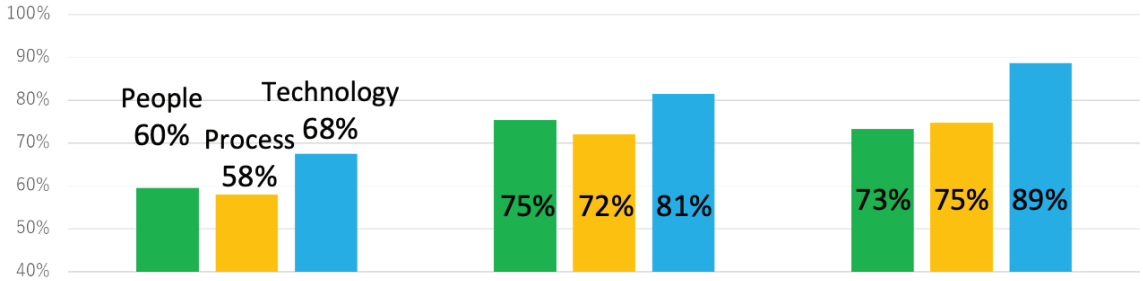


2. EXECUTIVE SUMMARY – RESULTS BY COUNTRY: US, GERMANY, JAPAN



CHALLENGES FACING PEOPLE, PROCESS, TECHNOLOGY

- Technology remains the biggest challenge in each country



CYBERSECURITY MEASURES IMPLEMENTED

- Perimeter and equipment measures have higher implementation rates

Perimeter: **85%**
Equipment: 82%

Equipment: **87%**
Perimeter: 85%

Perimeter: **79%**
Equipment: 77%

IMPETUSES TO INSTITUTE COLLABORATION

- Standards/guidelines are the leading methods to institute collaboration

Standard/Guideline:**64%**
Parent company instruction: 44%

Standard/Guideline:**58%**
Boards instruction: 55%

Standard/Guideline:**57%**
Partner/Customer request: 57%

REGULATIONS AND STANDARDS

- NIST CSF and ISO 27001 are the most common guidelines

NIST CSF: **67%**
ISO 27001: 53%

NIST CSF: **51%**
CIS controls: 43%

ISO 27001: **65%**
NIST CSF: 57%

ORGANIZATIONAL STRUCTURES

- Defining the CSO of a factory is the most important first step

Identify a leader: **60%**
Dedicated committee: 56%

Expand existing team: **49%**
Identify a leader: 48%

Identify a leader: **44%**
Expand existing team : 43%

HUMAN RESOURCE MANAGEMENT

- Providing internal training to employees involved in cybersecurity remains paramount

Internal training: **57%**
Hire new specialists: 56%

Hire new specialists: **48%**
Internal training: 45%

Internal training: **50%**
External training: 49%

Survey Results - All Three Countries

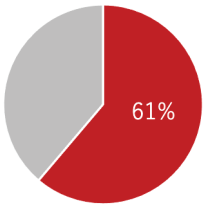
1-1. CYBERSECURITY INCIDENTS

The majority of factories have experienced a critical incident.

- 61% experienced incidents, of which 75% had system outages and 43% had more than four days of outages

The emergency cybersecurity incidents at factories is just the tip of the iceberg. In our survey, 61% of manufacturers said they experienced cybersecurity incident in their factory, while 75% of companies that have experienced an incident that caused a production outage. In addition, 43% of companies said that production activities had been suspended for more than four days as a result. These incidents are not uncommon and have a direct impact on production activities, leading to the importance of manufacturers to properly recognize the risks of cybersecurity in factories.

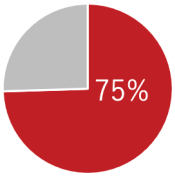
Figure 1. Incident experience



N=500

Q13:
Has your organization ever experienced a cybersecurity incident in your smart factories (e.g. a computer virus infection, unauthorized operation that exploits system vulnerabilities, or unauthorized access to the system)?

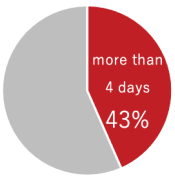
Figure 2. Incident that stopped production



N=306

Q15:
Did the cybersecurity incident/incidents stop the production systems in your organization's smart factories?

Figure 3. Length of time production was stopped



N=228

Q16:
How long were the production systems in your factories stopped by the cybersecurity incident/incidents?

1-2. CHALLENGES FACING PEOPLE, PROCESS, TECHNOLOGY

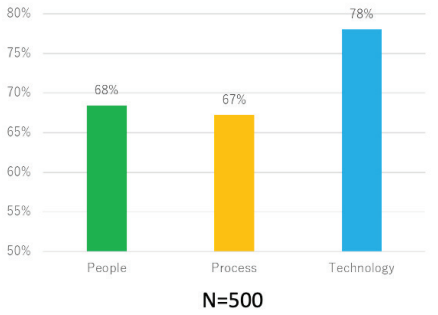
Technology remains the biggest challenge, but people and process are also facing issues.

- OT recognizes people and processes as issues rather than IT

Businesses require more than just the right technology in order to address cybersecurity risks. Organizational and process measures are also essential. In this survey, we investigated issues reported by respondents based on people, processes, and technology. Overall, the results uncover that companies have more technical challenges than issues with people or processes. Specifically, they are struggling to find effective ways to protect their factory, struggling to adapt to their own environment, and struggling to mitigate the negative impact on their regular operations.

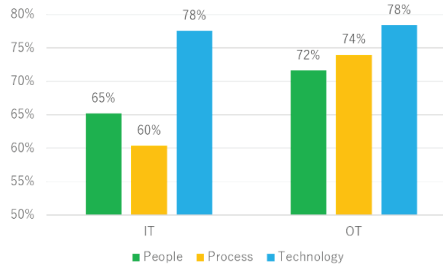
Also, when comparing IT respondents and OT respondents, the ratio of concern for technology ranks relatively the same, while OT are concerned about issues surrounding people and process more than IT. In particular, it can be said that the OT teams find it difficult to take inventory of their assets according to importance, identify threats and vulnerabilities in factories, and set security target levels.

Figure 4. Challenges to promote cybersecurity



N=500

Figure 5. Challenge to promote cybersecurity (IT - OT)

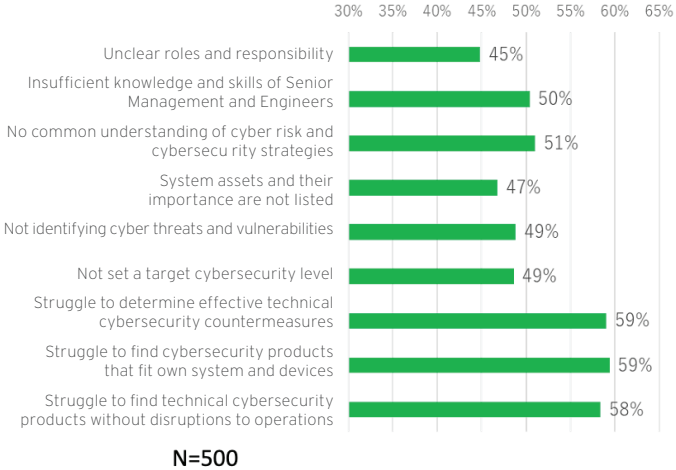


N=250 N=250

Challenges measuring the effectiveness, adaptability, and uniformity of technologies

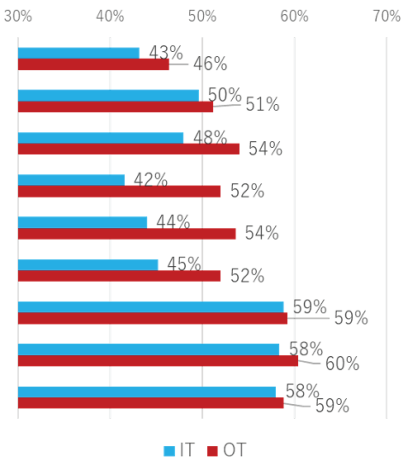
-OT found it difficult understanding and identifying risks, asset visibility, and setting target levels

Figure 6. Challenges to promote cybersecurity



N=500

Figure 7. Challenges to promote cybersecurity (IT - OT)



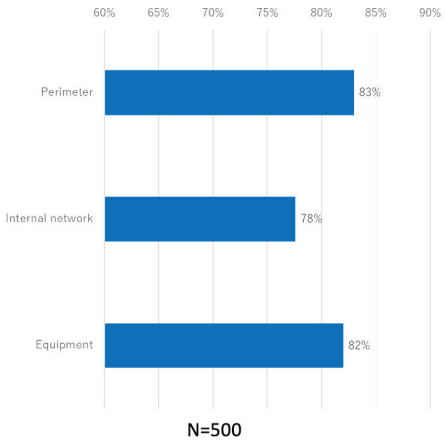
Q7:
To what extent do you agree or disagree with the following statements when it comes to promoting and improving the cybersecurity of your organization's smart factories? ("strongly agree"+ "somewhat agree")

1-3. CYBERSECURITY MEASURES IMPLEMENTED

Most factories have already implemented some technical measures.
-Countermeasures on perimeter and equipment are more often implemented than internal networks

Are IT and IOT teams currently following cybersecurity technical measures at factories? The survey found that most factories had some technical measures already implemented. When the countermeasure categories were grouped into perimeters, internal networks, and equipment, about 80% of the respondents in each category answered that some countermeasures had already been implemented. However, looking at each specific countermeasure, the implementation rate is ranges between 52% and 39%, showing that the countermeasure methods implemented differ depending on the factory.

Figure 8. Cybersecurity measures implemented (3 groups)



Those with a high implementation rate of 50% or more feature countermeasures for device backup (52%), antivirus for equipment (50%), and ensuring USBs are free from malware before connecting to an OT network (50%). In addition, measures to protect the perimeters with IT (such as firewalls (49%) and IPS (48%)) also have a high implementation rate. Ranking lower are asset visualization (40%) and network segmentation (39%).
It seems that it is relatively easy to implement the measures that can be taken for the perimeter and each device. On the other hand, it is difficult to review or change whole environments, such as listing the all assets and modifying the network configuration.

Specific measures are implemented less than 50% of the time
- Asset visualization and segmentation rank the lowest

Figure 9. Cybersecurity measures implemented

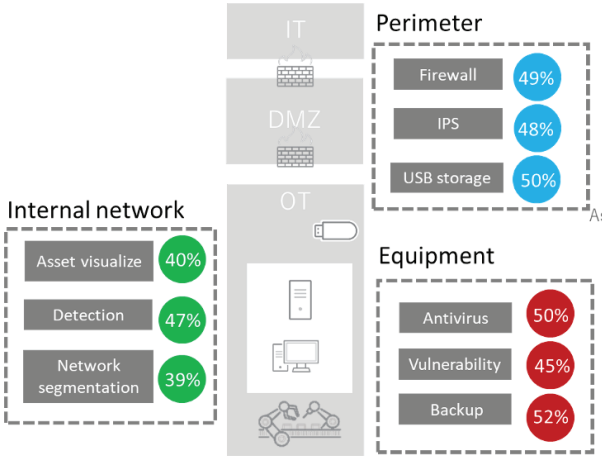
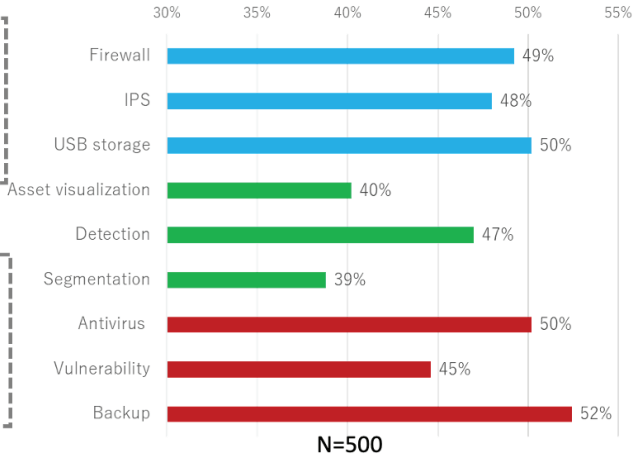


Figure 10. Cybersecurity measures implemented (Specific)



Q10: Which cybersecurity technical measures has your organization implemented or have plans to implement to protect your smart factories? ("already implemented")

1-4. IT AND OT COLLABORATION

Most organizations understand the importance of process alongside that of technology, but few are involved in both IT and OT.

- Nearly 90% have built operation and incident response processes, but only 12% collaborate in all phases

When selecting technical measures for cybersecurity, 89% of organizations also build operational processes while 88% also build incident response processes. Most manufacturing industries understand that cybersecurity is not just effective in introducing technical mechanisms and tools, but also effective in recognizing incidents during regular run-times. In order to use the technology effectively, it is important to properly set security tools and detect anomalies while monitoring it. In addition, a level of preparedness is necessary in order to respond to security incidents in an appropriate manner.

On the other hand, only 12% of manufacturers have both IT and OT teams involved in decision-making when selecting technical measures and building processes. It would be desirable for both IT and OT opinions to be reflected at all stages when selecting technology and building operational processes and incident response process.

Figure 11. Build operation process

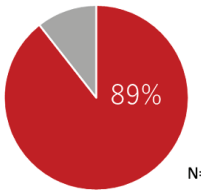


Figure 12. Build cyber incident response process

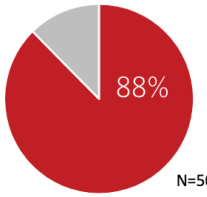


Figure 13. IT & OT collaboration

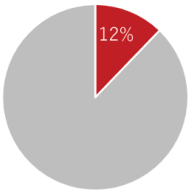


Fig 11: Q2"Yes", Fig 12: Q4"Yes", Fig13: Both IT and OT involved in all Q1, Q3 and Q5
Q1: When determining which cybersecurity technical measures to use for your organization's smart factories, which of the following departments were involved in decision making?
Q2: When determining your organization's smart factories' cybersecurity measures, did your organization build an operation process?
Q3: Which departments are involved in making decisions about your organization's smart factories' operation process?
Q4: When determining your organization's smart factories' cybersecurity measures, did your organization build a cyber incident response process?
Q5: Which departments are involved in your organization's smart factories' cyber incident response process?

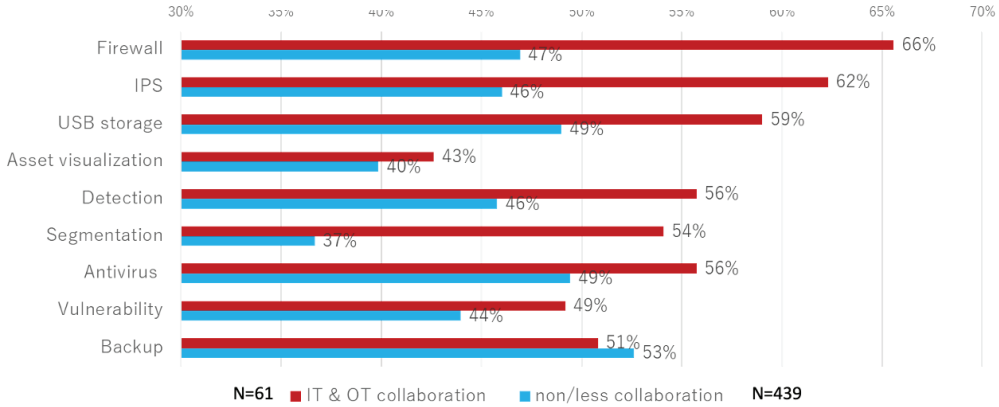
Organization collaboration takes cybersecurity one step forward.

- Especially implemented network security

The results show that if both IT and OT teams participate in the selection of technical measures and the decision-making process in factory cybersecurity, the implementation of technical measures will be easier. In particular, there are significant differences in measures such as firewalls, IPS, and network segmentation.

Looking at the results of recognizing challenges in people and processes, there are significant differences, especially between IT and OT. This includes inventory of assets and their importance, identification of threats and vulnerabilities, and setting of security target levels. The key would be to have a common understanding of the process.

Figure 14. Cybersecurity measures implemented (IT-OT)



Q10: Which cybersecurity technical measures has your organization implemented or have plans to implement to protect your smart factories? ("already implemented")

Survey Results
- Results by Country: US, Germany, Japan



2-1. CHALLENGES FACING PEOPLE, PROCESS, TECHNOLOGY

Technology is the biggest challenge in each country.

- US: Overall, awareness is relatively low compared to the other two countries
- Germany: Awareness on people and process are higher than the other two countries
- Japan: The difference between technology and people and process is larger

The trends and differences in people, processes, and technology challenges in factory cybersecurity are explored across the United States, Germany, and Japan.

The United States has a relatively low number of manufacturing industries that recognize these as challenges. It seems to be related to more advanced technical measures described later. Germany tends to be more invested in people and processes more than other countries. Since their organizational structure and human resource management are still developing at the same rate as other countries, it can be said that there is a greater emphasis is on the impact of non-technical aspects on cybersecurity.
In Japan, many manufacturing industries reported that they have experienced issues with technical measures. It can be said that there is a strong tendency to recognize that technology is a more effective cybersecurity tool than people and process.

Figure 15. Challenges to promote smart factory security

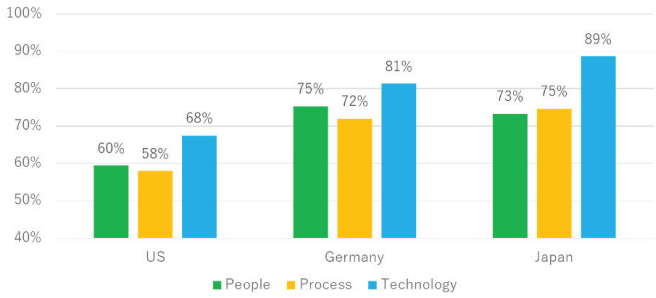
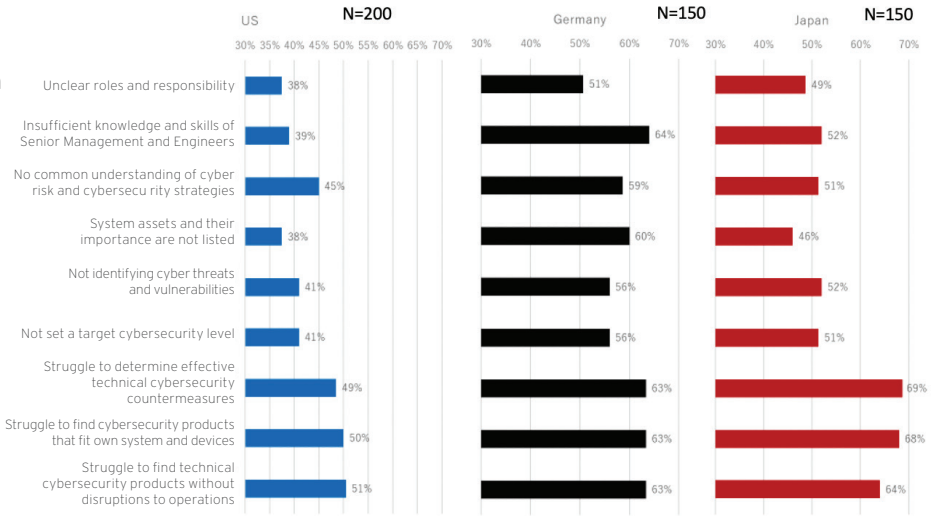


Figure 16. Challenges on people, process and technology



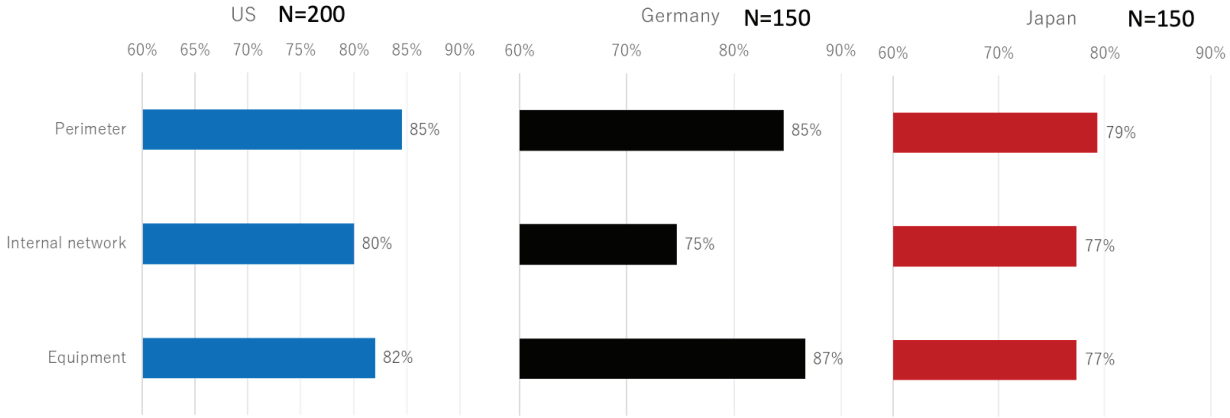
Q7:
To what extent do you agree or disagree with the following statements when it comes to promoting and improving the cybersecurity of your organization's smart factories?

2-2. CYBERSECURITY MEASURES IMPLEMENTED

Perimeter and equipment measures have a higher implementation rate than internal network measures.

- US: Perimeter measures are high
- Germany: Equipment measures are high
- Japan: Overall low, but with all three at a similar rate

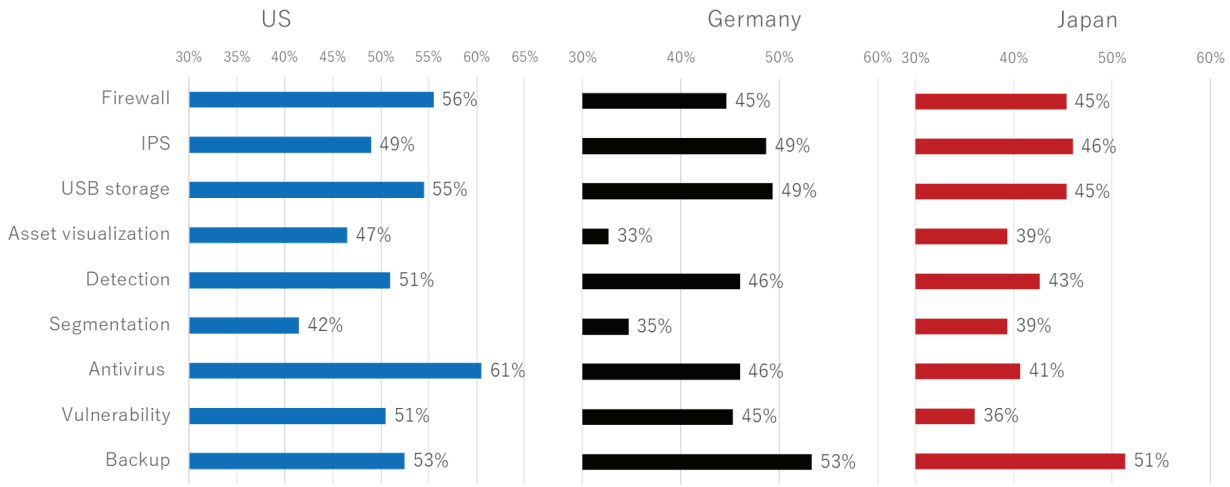
Figure 17. Averages of implemented rate



We compared the results of respondents who answered that some measures had been implemented in each of the three areas (perimeter, internal network, and equipment) by country. Perimeter measures are high in the US, while equipment measures rank high in Germany. Japan ranks each generally low, but there is little difference between the three.

Looking at the implementation rate by specific measures, firewall (56%) and equipment malware security (61%) are high in the US. They seems to be common as a basic measure, like IT. In Germany, high implemented measures include equipment backup (53%), IPS (49%), and USB storage (49%) as they do not easily affect running operations. In Japan, equipment backup (51%) is high, while nothing else is noticeably high.
The two items that ranked lowest as far as implementation rates overall are asset visualization and segmentation. Asset visualization, which is the first step in risk assessment, is low in Germany (33%) and Japan (39%), but relatively high in the US (47%). Segmentation is low in all countries (US: 42%, Germany: 35%, Japan: 39%), suggesting that it is a difficult measure to implement.

Figure 18. Implemented rate of technical measures



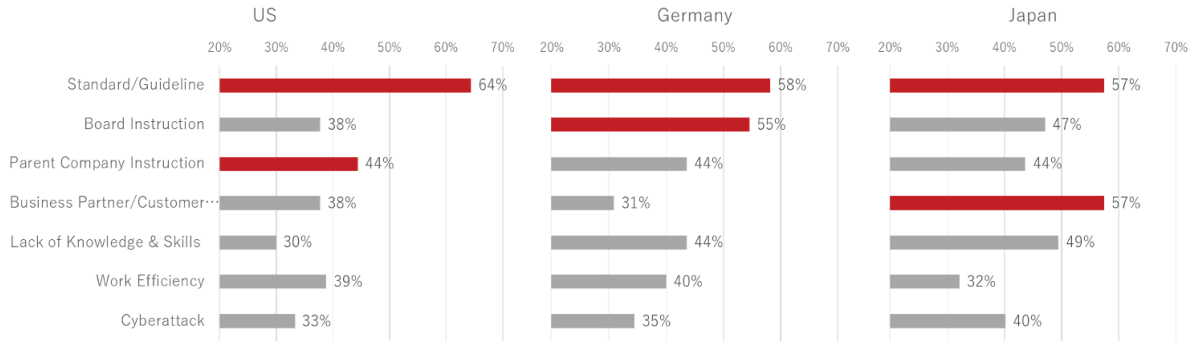
Q10: Which cybersecurity technical measures has your organization implemented or have plans to implement to protect your smart factories? : "already implemented"

2-3. IMPETUSES TO INSTITUTE COLLABORATION

Standard/guideline are the leading methods to institute collaboration.
Regulations and guidelines in all countries were the biggest cause for collaborating with other departments to improve factory cybersecurity. (US: 64%, Germany: 58%, Japan: 57%)
National regulations and industry guidelines for cybersecurity can be a great trigger for motivating an organization.

In addition, there is a characteristic difference between countries. In Japan, the request from business partners and customers (57%) is top the cause along with regulation. In Germany, instructions from the management (55%) is in second place. In the US, instructions from the parent company (44%) is ranked second, and in Germany, instructions from the management (55%) is ranked second.

Figure 19. Impetuses to institute collaboration



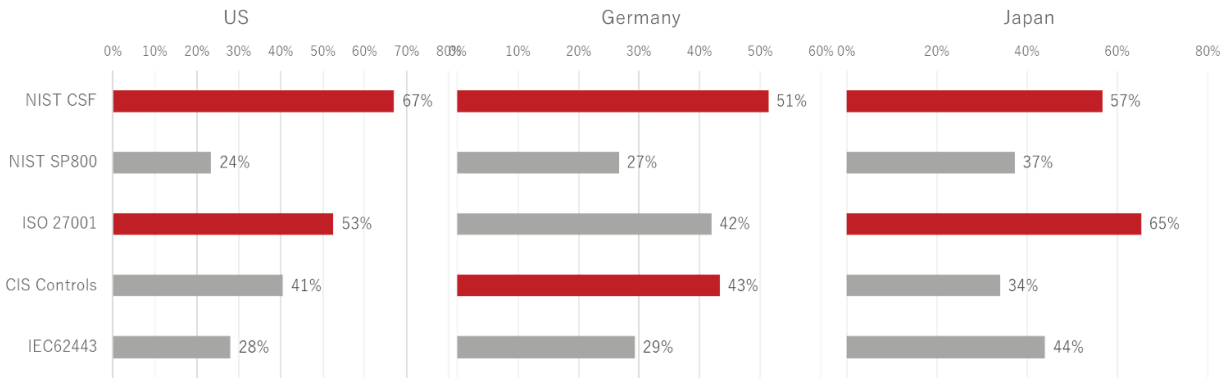
Q9: What caused your organization to decide to collaborate with other departments to improve your smart factories' cybersecurity capabilities?

2-4. REGULATIONS AND STANDARDS

NIST CSF and ISO 27001 are the most common guidelines.
What are the regulations or guidelines that manufacturers in each country need to comply with? Overall, NIST's CSF (Cyber Security Framework) and ISO2 7001 (ISMS) are most common. NIST CSF is a framework (not a regulation) that every company should comply with, but it seems to be popular because it is easy to use for security planning in many companies. ISO 27001 is an ISMS standard that belongs to the IT world, but it also seems to be useful for information management in factories.

In the US, NIST CSF (67%) is overwhelmingly high, followed by ISO 27001 (53%).
In Germany NIST CSF (51%) ranks highest with CIS Controls (43%) ranking second.
Japan is the only country among the three with ISO 27001 (65%) at the top, which is higher than NIST CSF (57%).

Figure 20. **Regulations & standards**



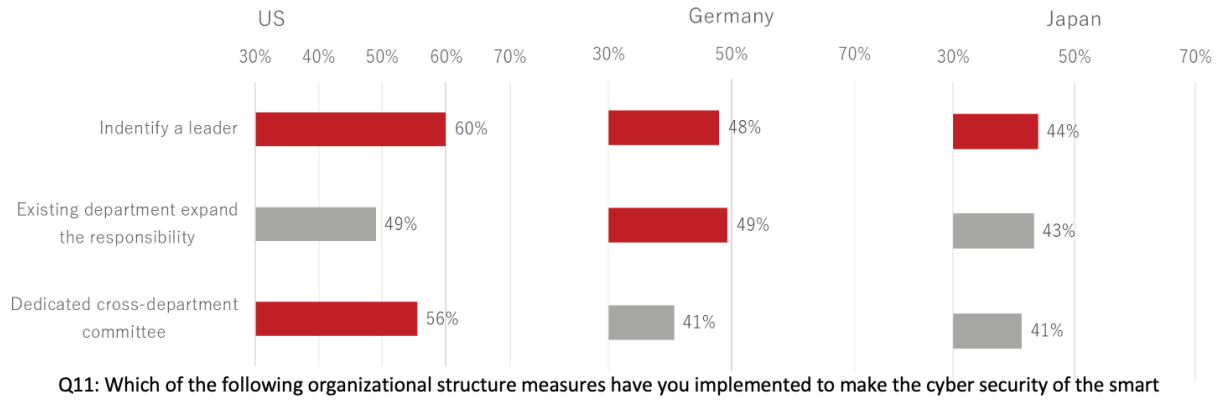
Q19: What regulations or industry standards do your organization's control systems need to comply with?

5. ORGANIZATIONAL STRUCTURES

Defining the CSO of a factory is the most important first step.

The most common organizational structure measure for effective factory cybersecurity has been to appoint a factory cybersecurity officer. The US has the highest rate of implementing organizational changes to support cybersecurity, with identifying a leader (60%) and dedicated cross-department committees (56%). Germany is improving cybersecurity by expanding the responsibilities of existing organizations (49%). Compared to other countries, there are few companies in Japan that have modified their organizational structure.

Figure 21. **Organization structure**



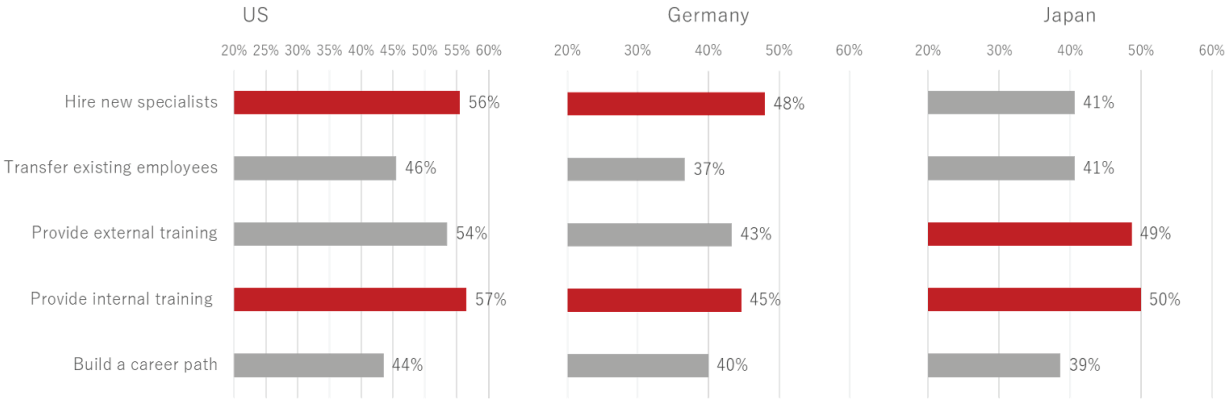
Q11: Which of the following organizational structure measures have you implemented to make the cyber security of the smart factory work effectively?

6. HUMAN RESOURCE MANAGEMENT

Providing internal training to employees involved in cybersecurity remains paramount.

The most common human resource management measure for factory cybersecurity has been internal training on factory cybersecurity. In the US, internal training (57%) is followed by hiring specialists (56%). Germany ranks hiring specialists (48%) and internal training (45%) highest. The US and Germany value sharing knowledge and skills through internal training while welcoming new specialists from the outside. Japan concentrates on internal training (50%) and external training (49%) and attempts to gain cybersecurity expertise by training existing human resources.

Figure 22. **Human resource management**



Q12: Which of the following human resource management measures have you implemented to make the cyber security of the smart factory work effectively?

Conclusion and Recommendations

Manufacturers are rushing to introduce technical cybersecurity measures in the factory, but are still in the development process. The key to moving forward is involving both IT and OT in the decision-making process.

The next steps are asset visibility, identifying the risks, and setting the goals

Factory cybersecurity is in the developing phase. Cyber incidents have not been rare, and many companies are making progress in both organizational and technical approaches and most of them aware the risks attached. As factory cybersecurity evolves in the next few years, this survey shows that it is difficult to select appropriate technical measures. This means that the manufacturing industry requires urgent and effective action to address cybersecurity risks. They are aware that cybersecurity should be implemented in and they are actively working towards it. As shown in Fig. 7, there is little difference in awareness of technology issues between IT and OT, but in terms of processes, more OT teams have issues with asset visualization, risk identification, and goal setting. After assessing the current situation and setting appropriate goals for their own factory, we will be able to implement technical measures in the right place at the right time.

Understanding the differences and involving both IT and OT in the process

Organizational silos are one of the obstacles to promoting cybersecurity together with DX in the manufacturing industry, this means cooperation between departments is required. This survey reveals the current state of factory cybersecurity in terms of people, processes, and technology, focusing on the differences and similarities between IT and OT, and across countries.

In order for organizations with different backgrounds to work together effectively, we must first recognize that there are differences. It's not necessary to have the same opinion, but sharing goals and involving the opinions of both IT and OT in the decision-making process would push industrial cybersecurity forward. IT and OT recognizing the differing methods that each play their respective roles is a big step towards keeping operations running in the factory.

Recommendations

Best practice to keep operations running:
In order to overcome cyber risks, certain security issues need to be addressed. In order to "keep operations running", Trend Micro proposes a three-step approach that consists of prevention, detection, and persistence.

First step: Prevention:
In this step, we aim at reducing threat intrusion risks at data exchange points like the network and DMZ.
These risks may come from IT and OT, USB storage used in a factory, laptops/outside machines brought into a factory by third parties at maintenance, and from an IoT gateway. We offer solutions to ensure this data exchange remains safe.

Second step: Detection:
Secondly, we detect cyberattack activities in OT environment on the premise that there is no such thing as 100% prevention. Anomaly network behaviors such as command and control (C&C) communication and multiple log-in failures should be detected as soon as possible to prevent massive damage. We offer passive detection solutions connected to L2 SWITCH/L3 SWITCH mirror ports in DMZ or on shop floor so asset owners can detect anomalous situations during the early stages of a cyberattack without impacting system availability.

Third step: Persistence:
In the last step, we look at protecting the most critical environments on a shop floor while minimizing the affected area. On a shop floor, there are many critical assets which link directly to production and its control.
To protect those environment from cyberattacks, which manage to sneak by the prevention and detection layers, we offer a solution for industrial network security and industrial endpoint security. These solutions are purpose-built to adapt to OT environment characteristics like high temperature, ease-to-use, and minimal performance impact

How can Trend Micro help cybersecurity in factories?

Based on threat intelligence that combines IT and OT, Trend Micro helps customers solve their problems in terms of people, processes, and technology in factory cybersecurity.

Integrated threat intelligence: The Trend Micro Research team delivers 24/7 threat investigation from around the globe, including vulnerability intelligence from our Trend Micro™ Zero Day Initiative™ (ZDI) program. And combined with research on finding vulnerabilities, predicting future threats and our OT expertise brought by TXOne Networks, a company formed by a joint venture of Trend Micro and Moxa, makes our solutions more effective.

People: The threat research results we publish will help increase awareness within the organization. The training and certifications we provide based on our intelligence and experience can enhance your cybersecurity expertise.

Process: Our professional and management services can help customer's process during each phase of risk assessment, planning, implementation, operations, and incident response.

T**echnology:** Our connected solutions and XDR capabilities, via our Trend Micro Vision One™ platform, empower CISO and security operation teams with more precise alert detection and automatic response, reducing monitoring complexity and operating costs.

For more details on our solutions and practices, visit our Smart Factory Solution page

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003