The State of Industrial Cybersecurity

Prevent supply disruptions and ensure resilient operations

» 2022 industrial cybersecurity survey report in manufacturing, electric utilities, oil, and gas

CONTENTS

INTRODUCTION

The purpose of this survey is to reveal the current state and challenges of industrial cybersecurity, especially in promoting secure smart factories or critical infrastructures. Manufacturing, electric utilities, and oil and gas companies around the world are amid of digitizing their infrastructure and operations for sustainable growth. At the same time, cybersecurity threats that could hinder that growth are becoming a top concern for organizations.

As IT and OT become increasingly interconnected, resilient operations are a critical issue in industrial cybersecurity. Cybersecurity threats execute across these environments in a mixed- technology environment. In contrast, even when attempting to deploy cybersecurity control, ICS/OT environments have different restrictions.

Our study will provide you with tips and best practices for further advancing industrial cybersecurity through understanding the cyber incidents and the implementation state.

METHODOLOGY

- **Objective**

This report looks at the current state and challenges facing ICS/OT systems in manufacturing, electricity, oil and gas industries and what cybersecurity leaders should focus on when it comes to cybersecurity.

This is achieved by analyzing the key industries of manufacturing, electric utilities, and oil and gas for three countries, the United States, Germany, and Japan, based on three perspectives:

1. Impact due to cyberattacks, damages, causes
2. Maturity of cybersecurity
3. Drivers for cybersecurity

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**

February 2022 to March 2022

- **Respondents**

- Total of 900 respondents

- Manufacturing (314), electricity (310), oil and gas (276)

- Countries: US (300), Germany (300), Japan (300)

- Company profile: Organizations with 1,000+ employees

- Role of respondents: IT, OT
  Decision makers determining cybersecurity measures in ICS environments
  IT Department: Information Technology, IT Security
  OT Department: Production Management, Production Engineering, Maintenance Management/Equipment Maintenance, Plant engineering, Automation/Control engineering, Operations, OT cybersecurity

EXECUTIVE SUMMARY – RESULTS OF ALL THREE INDUSTRIES

CYBERATTACK IMPACT

What consequences did cyberattacks make in the organizations in the last 12 months?

Supply Affected
89%

Disruption 4 days or more
56%

Average amount of damage
$2.8 million

LIKELIHOOD AND RECOGNIZED CAUSES

How many times did the organizations face disruptions in the last 12 months?

6-10 times disrupted
in the last 12 month
44%

1 to 5 attacks in OT

1 to 5 attacks in IT

MATURITY OF CYBERSECURITY

Which tier of NIST CSF are their IT and OT going on?

IT **About 40%** is in a state where risks are recognized at organizational level (Tier 2).

OT **About 30%** is in a state where risks are partially addressed (Tier 1)

REASON OF IMPLEMENTATION

What is the current driver to strengthen ICS/OT security?

Top reason is
to prevent recurrence of incidents

POST INCIDENT IMPROVEMENT

Did organizations take actions to reduce future risks after incidents?

48%
don't always make improvements

Survey Results

1. IMPACTS AND DAMAGES DUE TO CYBERATTACKS

How many organizations are experiencing disruptions due to cyberattacks? Is what we see in the news just the tip of the iceberg? Our study revealed that most organizations in manufacturing, electricity and oil and gas utilities were disrupted with their supply. Moreover, we investigated the duration of the disruption and the amount of financial damage as consequences of those cyberattacks.

Most organizations have impacts on their supply due to cyberattacks.

- 89% of respondents had manufacturing, energy supplies affected due to cyberattacks.

Figure 1. Supply affected due to cyberattacks

Q12. Has your organization's ICS/OT system disruption due to a cyberattack impacted your organization's supply chain in the last 12 months? (N = 900)

Since there is no difference by industry, it can be said that cyberattacks are a common threat that can have a significant impact regardless of industry.

ICS/OT disruptions lasted for 4 days or more in almost half of the organizations.

- 56% of respondents whose ICS/OT was disrupted due to cyberattacks said the disruption lasted 4 or more days. The average duration of the ICS/OT disruption lasted 5 days.
- By industry, oil and gas utility has a relatively large number of respondents (65 %) that experienced disruptions lasting four or more days. On the other hand, the number of respondents in the manufacturing industry was lower (50 %).
- On average by industry, the disruptions lasted 6 days for oil and gas, electricity and 5 days for manufacturing.

Figure 2. How long is ICS usually disrupted

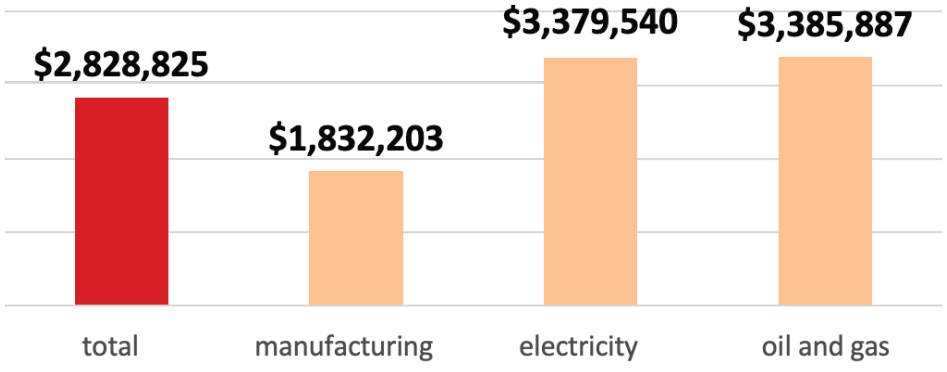
Q9. Thinking about the last 12 months, how long is your organization's ICS/OT system operation usually disrupted for, as a result of a cyberattack?

(Only for those who answered in Q5 that the ICS/OT system was disrupted at least once, N = 829)

The average financial damage amounts to approximately $2.8 million USD.

- Respondents who said there has been at least some disruption in the three industries incurred an average of $2.8 million in financial damages over the 12 months because their ICS/OT systems being disrupted by the cyberattack.
- On average by industry, the financial damage amounts to approximately $3.3 million for oil and gas and electricity, approximately $ 1.8 million for manufacturing.

Figure 3. Average financial damage



Q11. How much financial damage was caused by your organization's ICS/OT system disruption in the last 12 months, due to the cyberattack?

(Only for those who answered in Q5 that the ICS/OT system was disrupted at least once, N = 829)

For this survey, the amount of financial damage is the total amount of losses and expenses shown below.

- Expenses paid for cyber incident response
- Expenses paid for recovery, such as extortion by ransomware
- Expense to build recurrence prevention measures
- Extra expenses to run business, such as hiring additional staff or purchasing third-party services.
- Sales loss due to system inoperability
- Expenses paid for damage such as loss of others and information leakage

The magnitude of the impact varies by industry. There is a possibility that this is a characteristic of the business.

In addition, when it comes to financial damage, it is easy to see the damage due to ransomware, but it is inferred that there are other types of financial damage as well.

Due to a longer disruption period in the oil and gas and electricity industries, the financial damage can be larger than the damages incurred in the manufacturing industry.

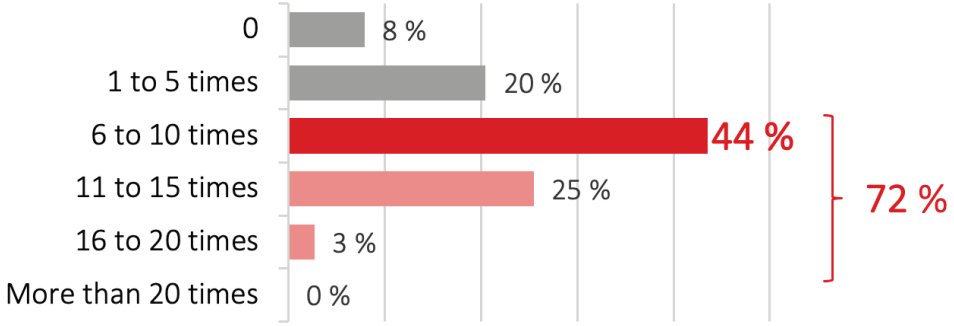
2. THE NUMBER OF SYSTEM DISRUPTIONS AND RECOGNIZED CAUSES

How often did ICS / OT disruptions occur? Are the risks of cyberattacks common? We also asked how they recognize whether these disruptions were due to cyberattacks on IT or OT.

About half of the organizations faced ICS disruptions once every two months.

- 72% of respondents experienced at least six ICS/OT disruptions in the last 12 months due to cyberattacks.
- When we look at the number of individual times, 44% say it was 6 – 10 times

Figure 4. The number of disruptions



Q5. How many times in the last 12 months has your organization's ICS/OT system operation been disrupted due to cyberattacks? (N = 900)

Respondents' recognition is that the cyberattacks causing disruptions occur in both IT and OT.

- Looking at cyberattacks recognized as causes of disruptions by area of occurrence, 1 to 5 incidents were the most common for both OT and IT side (OT 45%, IT 56%).

Figure 5. The number of times (OT side)

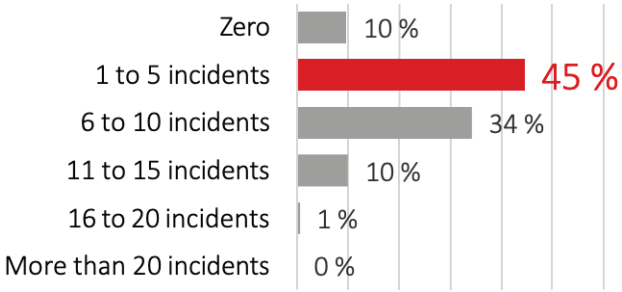
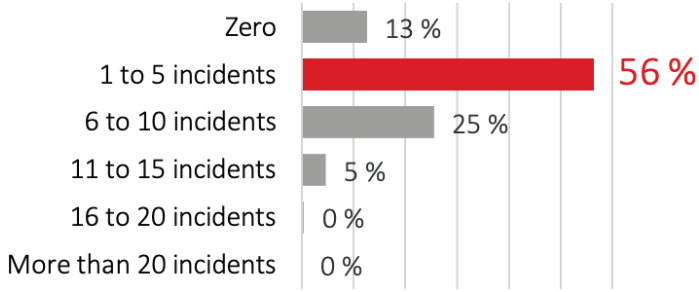


Figure 6. The number of times (IT side)



Q6. How many cyberattacks in the last 12 months that caused the disruption to the ICS/OT system occurred on the IT side, and how many occurred on the OT side?
(Only for those who answered in Q5 that the ICS/OT system was disrupted at least once, N = 829)

ICS/OT disruptions have occurred multiple times in a short period of time.
Furthermore, we asked where cyberattacks occurred, not entry points and paths of attack, in this survey. Looking at Figure 5 and 6, we can see that respondents recognize that cyberattacks causing disruptions occur in both IT and OT.

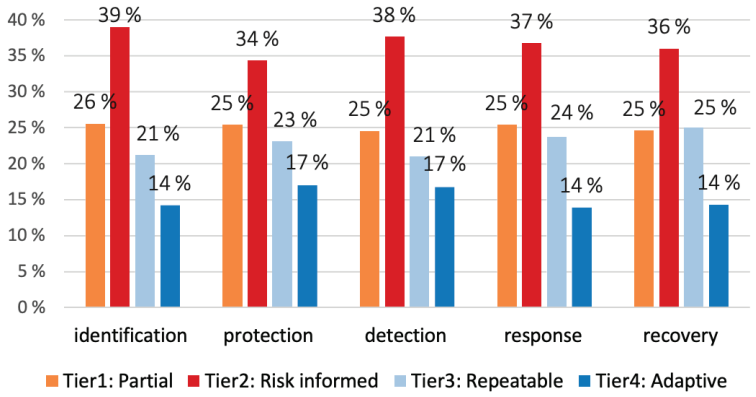
3. MATURITY OF CYBERSECURITY

This study examined the maturity of IT and OT cybersecurity. We asked them to answer the state of their cybersecurity function with reference to the tiers 1 to 4 for each of the five functions of NIST Cybersecurity Framework(CSF).

Many organizations are in a state of partial implementation, regardless of IT or OT areas.

- In IT, nearly 40% of respondents say that they are in the state where risks are informed (Tier 2) in each function, which is outstanding. The next largest group is 25% in a partial state (Tier 1).

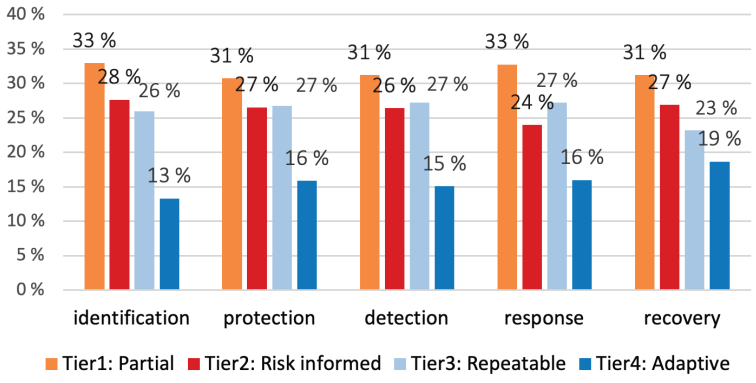
Figure 7. Maturity of cybersecurity (IT)



Q13 – Q17. For each of the following cybersecurity areas, which approach best describes how your organization implements cybersecurity functions? (N = 900)

- In OT, the largest number of respondents (about 30%) are in Tier 1 of each function. The next largest group (about 25%) is in Tier 2 or Tier 3, depending on the function.
- Unlike IT, there is a gradual decrease from Tier 1.

Figure 8. Maturity of cybersecurity (OT)



Q13 – Q17. For each of the following cybersecurity areas, which approach best describes how your organization implements cybersecurity functions? (N = 900)

In general, Tier 1 and Tier 2 account for 60 - 70% of the total in the IT and OT areas.
To be in Tier 3 or above requires regular reviews and flexible adaption based on lessons learned.
This would be a major challenge.

4. DRIVERS TO STRENGTHEN CYBERSECURITY

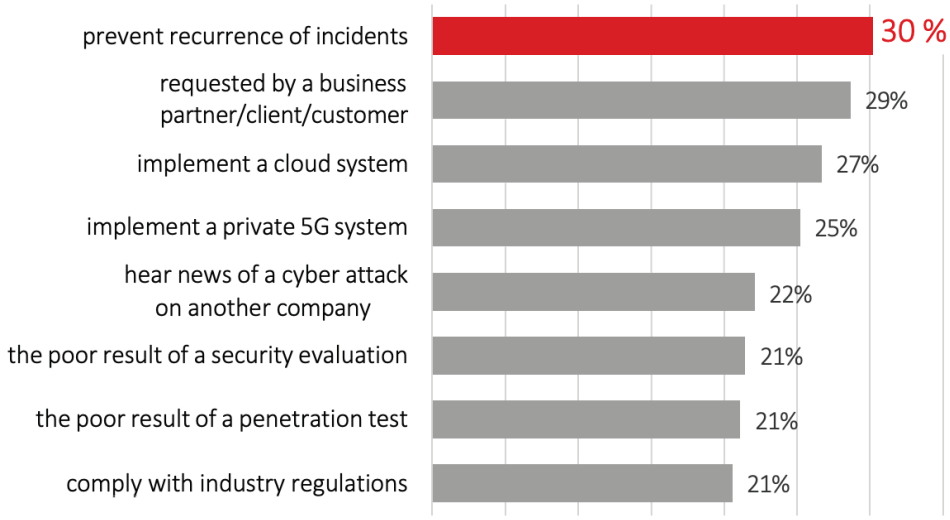
This study looked at why organizations have implemented security controls for ICS/OT. Many organizations are experiencing incidents, but we wanted to know if they took actions to prevent recurrence after the incident is over.

In addition, we investigated the reasons why they would strengthen ICS/OT cybersecurity in the next 3 years to understand the outlook for the future.

The current top reason is to prevent recurrence of incidents.

- ICS/OT systems are most likely to be protected to prevent the recurrence of specific incidents (30%).
  The second most likely reason is a request was made by a partner/client (29%).

Figure 9. Reasons for industrial cybersecurity

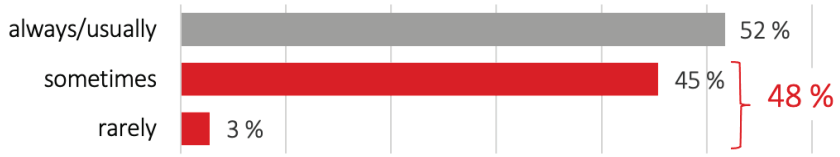


Q19. Up until now, what have been your organization's top two reasons for implementing cybersecurity measures to protect your ICS/OT systems? (N = 900)
(Please select the top two reasons)

Nearly half of respondents do not always work on improvement after an incident.

- Less than half of those who have experienced at least some disruption (48%) , don't always make improvements to minimize the future cyber risks.

Figure 10. Post incident improvement



Q10. Thinking about the last 12 months, post-incident, does your organization make cybersecurity improvements in order to minimize the risks of future attacks?
(Only for those who answered in Q5 that the ICS/OT system was disrupted at least once, N = 829)

Preventing incidents from recurring is a top reason for strengthening security, however some organizations are not always able to improve. There appears to be a gap between ideals and reality. It can be inferred that some organizations tend to deal with cyberattacks on a case-by-case basis rather than strategically.

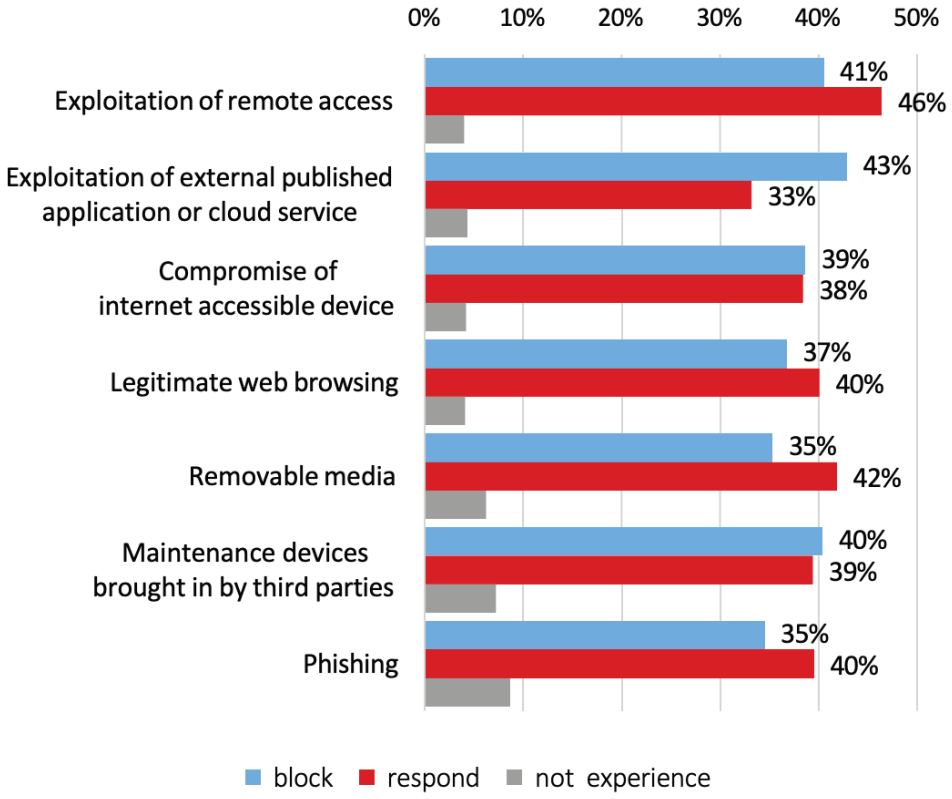
How to deal with initial attacks

This study looked at what types of initial attacks the organization experienced. Furthermore, we asked if they blocked the attacks or if they could not block it and had to respond.

For any initial attacks, around 40% could not block them.

- 35 - 43% of respondents said that they blocked the attacks, and 33 – 46% said they could not block the attacks and needed to respond.

Figure 11. How to deal with initial attacks



Q4. How has your organization dealt with the following types of cyberattacks? (N = 900)

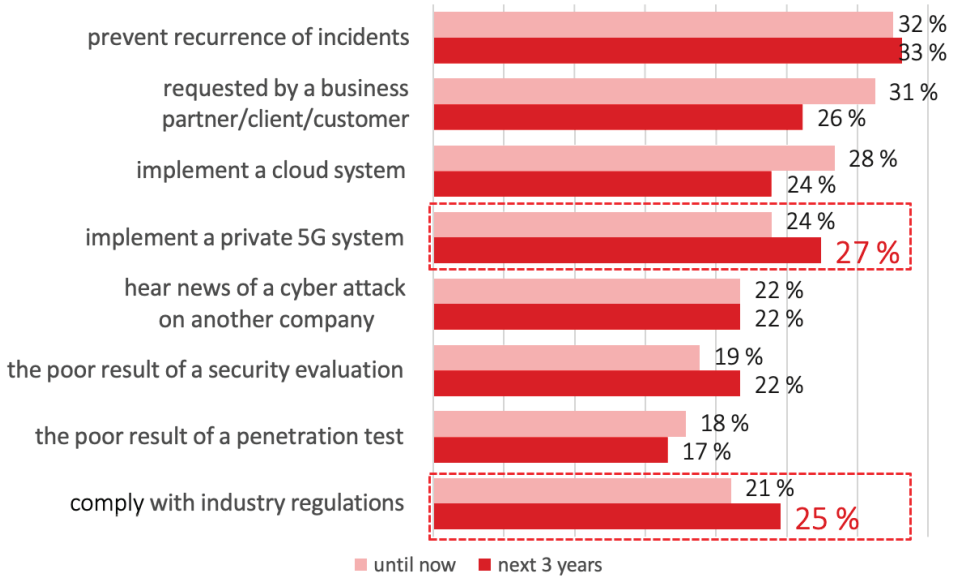
In fact, if we look at the situation of the initial attacks, in around 40% the cases, there are cases that intrusions were allowed. This situation will improve as security is strengthened.

Manufacturing

Drivers for implementing cybersecurity over the next three years (Manufacturing)

- Fewer respondents said that requests will be made by a business partner/client. Instead, more respondents said that they will protect their systems because of private 5G implementation (27%) and regulatory compliance (25%).

Figure 12. Reasons over the next three years (Manufacturing)



N = 314

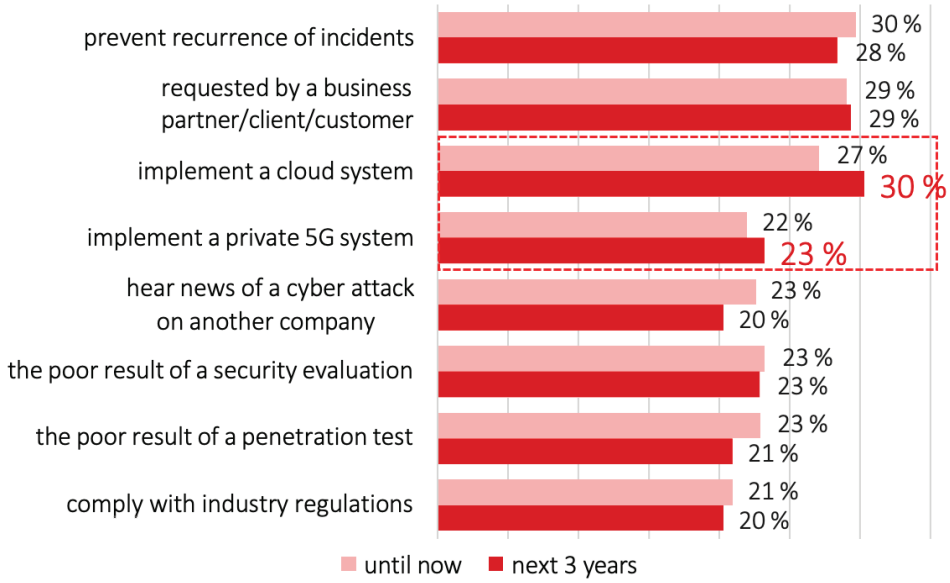
Q20. What do you believe your organization's top two reasons for implementing cybersecurity measures to protect your ICS/OT systems are over the next three years? (Please select top two reasons over the next three years)

Electricity

Drivers for implementing cybersecurity over the next three years (Electricity)

- Fewer respondents said that they will protect their systems because of prevention of recurrence. On the other hand, more respondents said that they will protect their systems because of cloud systems (30%) and private 5G implementation (23%).

Figure 13. Reasons over the next three years (Electricity)



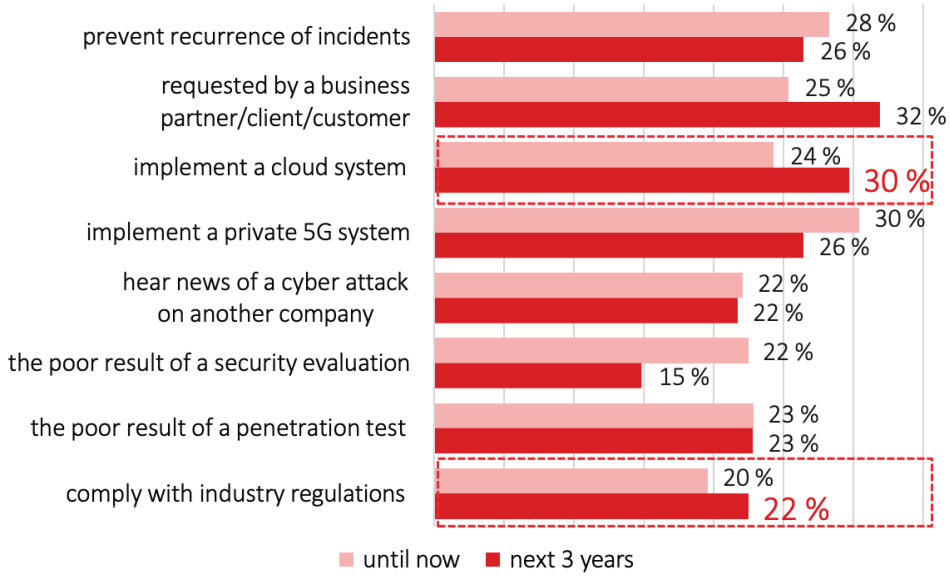
N = 310

Oil and gas

Drivers for implementing cybersecurity over the next three years (Oil and gas)

- Fewer respondents said that they will protect their systems because of prevention of recurrence. Instead, more respondents said that they will protect their systems because of cloud systems (30%) and regulatory compliance (22%).
- Implementation of a private 5G is a relatively common reason for both now and in the next three years.

Figure 14. Reasons over the next three years (Oil and gas)



N = 276

Common drivers for all three industries

- As new technologies continue to be adopted (e.g., cloud systems and private 5G) and industrial rules are tightened, industries are further aware they need to enhance their security to mitigate new risks and meet compliance regulations.
- In oil and gas industry, it is assumed that they are anticipating increased requests by a business partner and a client considering the incidents that occurred in 2021.

Conclusion and Recommendation

CONCLUSION

1. Manufacturing, electric and oil and gas utilities commonly experienced the supply disruption due to cyberattacks.

In our survey, about 90% of organizations experienced cyber incidents that affected their supply within 12 months. In addition, many organizations have experienced disruption of ICS/OT system operations more than once every two months. Cyberattacks became a common reason that impacted the availability of critical operations regardless of industry.

2. On the OT side, organizations struggled to understand what is happening. The gap between reality and recognition leads concerns.

Organizations that have had their operations disrupted by cyberattacks have recognized cyber incidents in both IT and OT. While IT and OT are inseparable, the current maturity level of cybersecurity varies widely from organization to organization. When it comes to the implementation of the detection function, most organizations are in a partial state on the OT side compared to the IT side.

To summarize, there is an issue in the ability to understand what is happening. The gap between reality and recognition in OT may be larger than in IT.

3. The current driver of cybersecurity is prevention of recurring cyber incidents, but in the future, regulations and adaptation to new technologies will increase.

Only about 40% of organizations have regularly reviewed and adapted to risks either in IT or OT. The most common reason for improving security capabilities in the ICS/OT environment is to prevent the recurrence of cyber incidents, but about half of the respondents did not take enough action to improve after experiencing a cyber incident.

In addition, the factors that will advance cybersecurity in the next three years are the requests from business partners, adaptation to new technologies such as cloud and 5G, and compliance with new regulations. There appears to be a shift in driving force for cybersecurity enhancements.

RECOMMENDATION

1. For organizations whose posture of cybersecurity is ad hoc and reactive in ICS/OT, it is necessary to establish a system that can understand what happened in their ICS/OT environment and analyze the cause of the incident.

They need to anticipate attack scenarios in the ICS/OT environment and implement appropriate security controls in the ICS/OT assets and networks.

The ICS/OT environment has different restrictions than IT, therefore the same method as IT cannot be adopted. Organizations should consider tools and methods suitable for ICS/OT as alternatives.

2. Proactive organizations that have regularly reviewed and updated IT and OT cybersecurity should plan their cybersecurity strategy assuming that cloud and 5G will be incorporated into their infrastructure.

Currently, IT and OT cybersecurity are inseparable to keep critical operations running. Soon, while promoting the use of industrial clouds and the cellular network technologies such as private 5G, they should establish cybersecurity that can adapt to mixed environments of new technologies as well as manage them in an integrated manner.

HOW CAN TREND MICRO ONE HELP ICS/OT CYBERSECURITY?

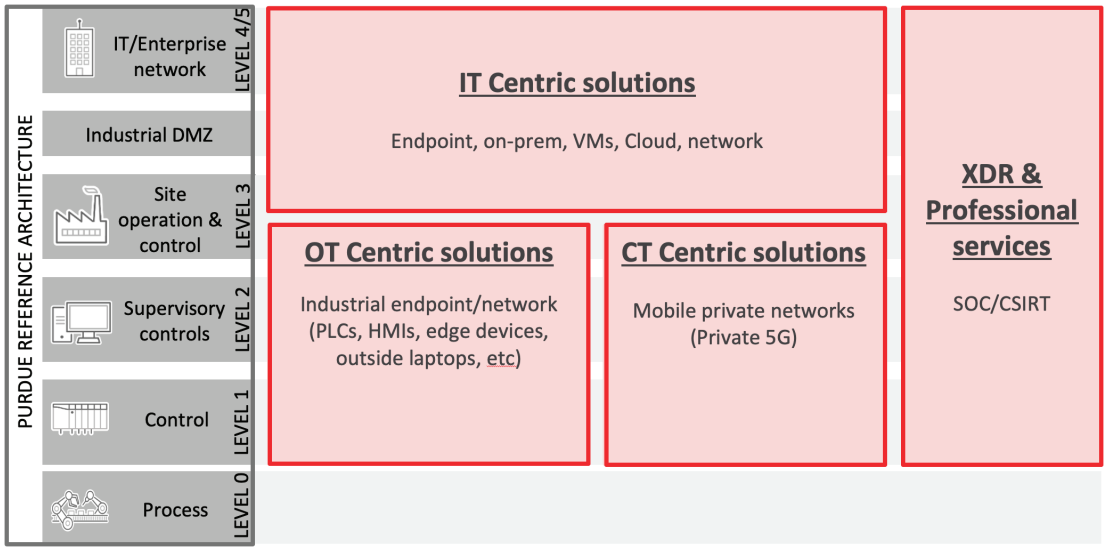
A platform securing converged environment of technologies

The current system of manufacturing, electric utilities, oil and gas is an environment in which different technologies; IT, OT and CT (Communication Technology) are combined to support businesses.

Trend Micro improves your security posture and situational awareness with OT, IT, CT, as well as XDR capabilities.

Trend Micro One unified cybersecurity platform

Trend Micro One helps solve changes in these complex environments by correlating the threat intelligence collected from around the world with data aggregated from various devices on a single cybersecurity platform.



For more details on our solutions and practices, visit our **ICS/OT security** page.

Threat research to understand cyber risks

Trend Micro's research shows that not only ICS but IT, cloud, and cellular network connections can be entry points and routes for attacks. These researches help to understand and assess cyber risks associated with attack scenarios holistically, not as a standalone asset.

Zone	Object	Research
Enterprise, control, and field network	IT endpoint > file server	Fake Company, Real Threats
	HMI	
	IT system > MES	Forward-looking security analysis of smart factories
	Application store > EWS	
	Cloud library > EWS	
	LTE/5G core network	Private 5G Security Risks in Manufacturing
Field network	Protocol gateway	A Blind Spot in ICS Security: The Protocol Gateway
	Robot programming language	The security dilemma of smart factories

TREND MICRO
Securing Your Connected World

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com

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