TXOne Networks

ANNUAL REPORT

# Insights Into **ICS/OT Cybersecurity 2022**

TXOne Networks

ANNUAL REPORT

# Insights Into **ICS/OT Cybersecurity 2022**

txOne networks

# Insights Into **ICS/OT Cybersecurity 2022**

## Table of Contents

# Executive Summary

In 2022, many new, ecosystem-complete RaaS (such as Black Basta, Pandora, and LockBit 3.0) emerged and adopted a ruthless multiple extortion strategy, attacking vital departments in the critical manufacturing, energy, food and agriculture, and healthcare and public health industries. We've seen a heightened frequency of cyberattacks on key industry suppliers, namely those in the energy and critical manufacturing sectors. Additionally, the impact on car-related product manufacturers is particularly severe, accounting for around 24% of the victims within the manufacturing classification. As more and more car manufacturers adopt the trend of automation in their plants, measures to mitigate supply chain attacks will become a matter of do or die for these factories in the future.

Organizations are all too slowly realizing that hacker attacks can disrupt production operations, seriously affecting productivity and requiring hours or even days to recover. Adversaries can use various extortion methods to steal sensitive business information, leading to data breaches, property loss, and violations that weaken customer trust and harm brand value. In response to Industry 4.0 becoming a critical aspect of corporate competitiveness, management and cybersecurity leaders should prioritize OT network protection at the top of their cybersecurity strategy. The dangers of insufficient cybersecurity are at the door, and organizations are due for a very rude awakening. First, they need to learn that ICS/OT requires a different set of security solutions, skills, processes, and methods than IT. They need to build specific cyber defenses to manage OT/ICS security risks in order to protect our critical infrastructure and industries for the future.

In the hopes of casting a spotlight on the seriousness of the situation, TXOne Networks commissioned Frost and Sullivan to conduct a global survey on the current state of OT/ICS cybersecurity in the manufacturing industry. Armed with awareness, organizations would ideally be poised to defend themselves or even fight back against the increasing number of threats and intruders. Key insights from the survey include:

- **94% of IT security incidents have also impacted the OT environment as IT and OT become more integrated.**
- **Increased complexity of OT and lack of visibility into third-party security capabilities are becoming serious security challenges for organizations.**
- **93% of organizations have deployed at least one OT cybersecurity solution and 85% of organizations still plan to increase their OT security capabilities next year.**
- **Despite increased investment in OT security, 70% of organizations are still considering adopting IT security solutions for the OT environment.**
- **Only 6% of organizations have 100% of their Windows devices protected by endpoint security solutions.**
- **The future of OT security must be comprehensive, integrated, performant, and accessible.**

## About TXOne Networks Inc.

TXOne Networks Inc., offers cybersecurity solutions that ensure the reliability and safety of industrial control systems and operational technology environments through the OT zero trust methodology. TXOne Networks works together with leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. TXOne Networks offers both network-based and endpoint-based products to secure the OT network and mission-critical devices in a real-time, defense in depth manner.

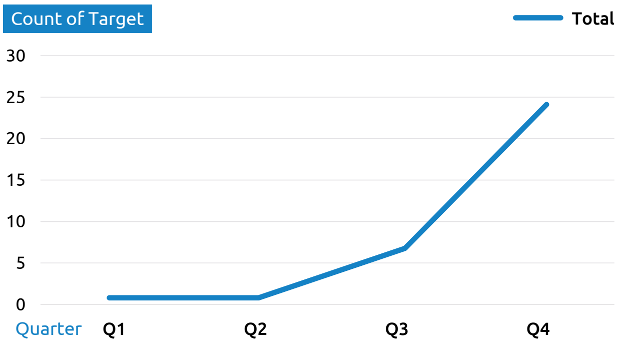
## About Frost and Sullivan

For over six decades, Frost & Sullivan has helped build sustainable growth strategies for Fortune 1000 companies, governments, and investors. Frost & Sullivan has applied actionable insights to navigate economic changes, identify disruptive technologies, and formulate new business models to create and implement a stream of innovative, sustainable, and manageable growth opportunities that drive future success.

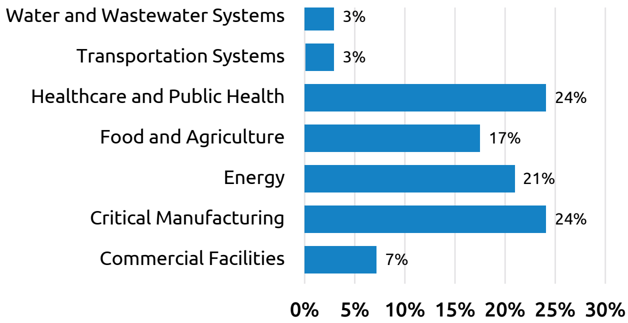
# Insight Into 2022 ICS/OT Cyber Incidents

## Multiple Extortion Ransomware Continues to Spike

CASES OF LOCKBIT ATTACKS IN 2022



INDUSTRIES MOST AFFECTED (EXAMPLE: LOCKBIT)



### 1. Ransomware-as-a-Service (RaaS) continues to adopt the multiple extortion model

In 2022, numerous RaaS with full ecosystems (e.g., Black Basta, Pandora, LockBit 3.0) were predicted to emerge, adopting various extortion tactics such as destroying data, holding data for ransom, selling data on the dark web, threatening customers or suppliers, and targeting industries like Smart Manufacturing, Energy, Food & Agriculture, and Healthcare & Public Health. Overall, after the release of LockBit 3.0, we saw an increase in activity related to LockBit 3.0 in Q4 2022.

### 2. Ransomware adds anti-analysis measures

To enhance security, some ransomwares use advanced techniques to prevent analysis, such as requiring a pass parameter to parse the main program (e.g., Egregor, LockBit 3.0). This makes it difficult for researchers to analyze and deepens the impact of an attack on organizations.[1]

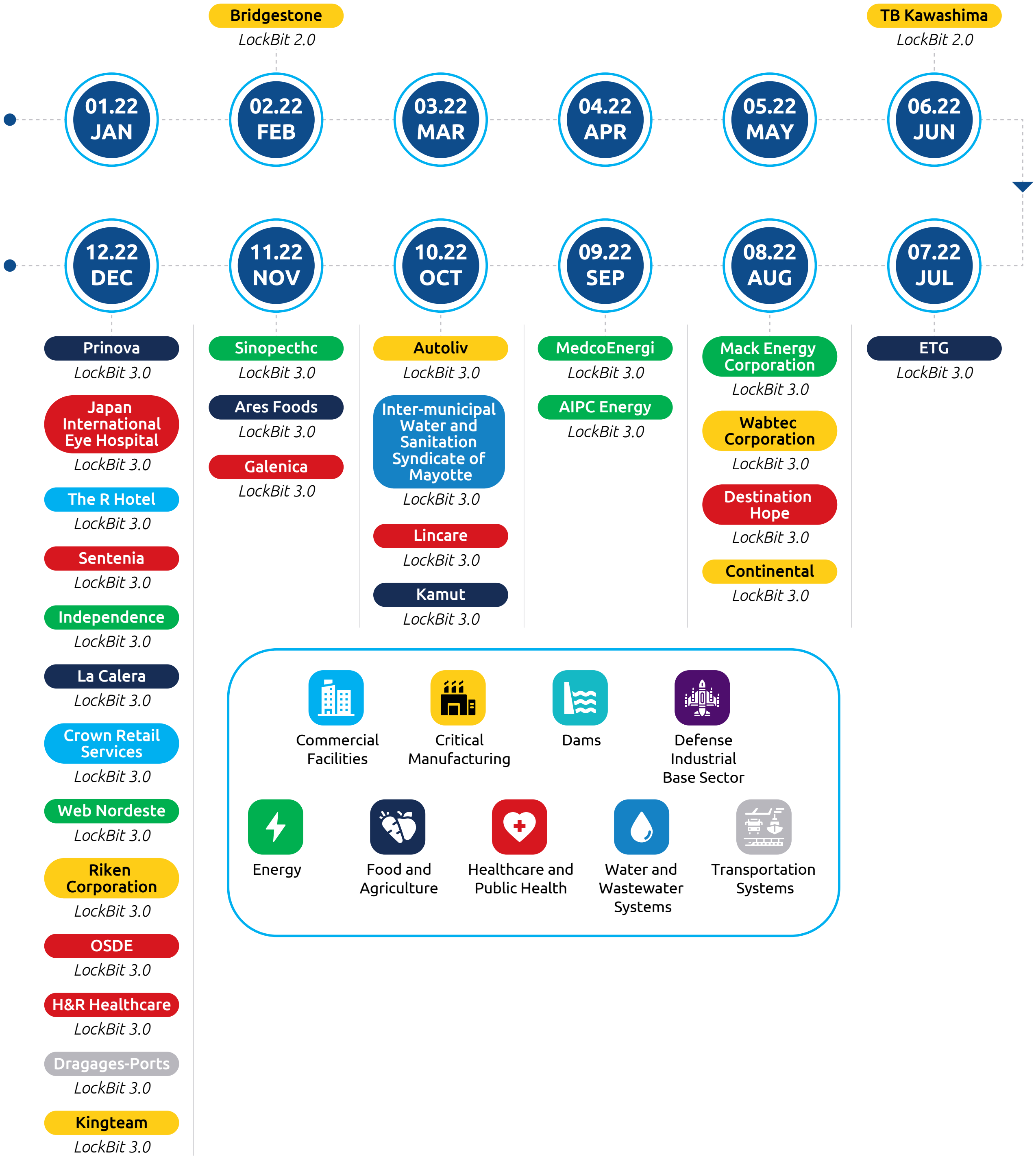
### 3. Ransomware employs fast encryption and better methods

Ransomware is using fast encryption methods and hardening tactics to evade detection and prevent attacks. For example, some use intermittent encryption that encrypts files in 16-byte increments, reducing the intensity of file I/O operations and avoiding statistical analysis and detection methods. Hackers are also exploiting vulnerabilities (e.g., Log4j) and using legitimate Windows/Microsoft Defender tools to download malicious DLL files and encrypted Cobalt Strike payloads. They can also shut down specified services (e.g., antivirus, backup, Volume Shadow Copy Service, sql) and then implant the ransomware.

## 4. Critical infrastructures face ongoing large-scale ransomware attacks

Large-scale ransomware attacks are not limited to power grids, oil, gas, or water treatment plants and are now targeting medical and public health units. The Healthcare and Public Health sector must remain vigilant in defending against ransomware attacks.[2]

### Cybersecurity Incidents Affected by LockBit Attacks in 2022



01.22 JAN

02.22 FEB
Bridgestone
*LockBit 2.0*

03.22 MAR

04.22 APR

05.22 MAY

06.22 JUN
TB Kawashima
*LockBit 2.0*

07.22 JUL
ETG
*LockBit 3.0*

08.22 AUG
Mack Energy Corporation
*LockBit 3.0*
Wabtec Corporation
*LockBit 3.0*
Destination Hope
*LockBit 3.0*
Continental
*LockBit 3.0*

09.22 SEP
MedcoEnergi
*LockBit 3.0*
AIPC Energy
*LockBit 3.0*

10.22 OCT
Autoliv
*LockBit 3.0*
Inter-municipal Water and Sanitation Syndicate of Mayotte
*LockBit 3.0*
Lincare
*LockBit 3.0*
Kamut
*LockBit 3.0*

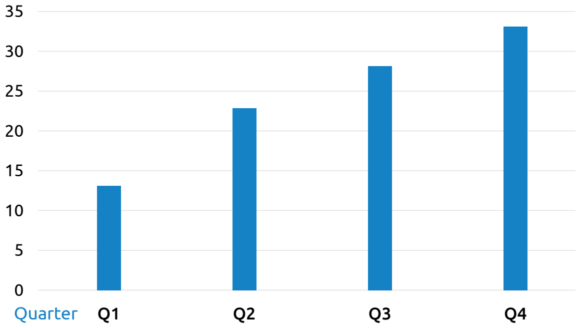
11.22 NOV
Sinopecthc
*LockBit 3.0*
Ares Foods
*LockBit 3.0*
Galenica
*LockBit 3.0*

12.22 DEC
Prinova
*LockBit 3.0*
Japan International Eye Hospital
*LockBit 3.0*
The R Hotel
*LockBit 3.0*
Sentenia
*LockBit 3.0*
Independence
*LockBit 3.0*
La Calera
*LockBit 3.0*
Crown Retail Services
*LockBit 3.0*
Web Nordeste
*LockBit 3.0*
Riken Corporation
*LockBit 3.0*
OSDE
*LockBit 3.0*
H&R Healthcare
*LockBit 3.0*
Dragages-Ports
*LockBit 3.0*
Kingteam
*LockBit 3.0*

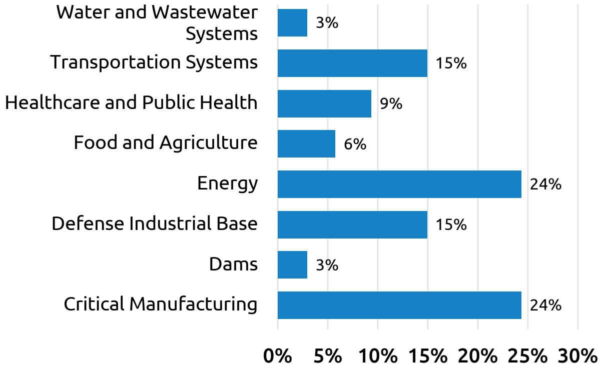
Commercial Facilities
Critical Manufacturing
Dams
Defense Industrial Base Sector
Energy
Food and Agriculture
Healthcare and Public Health
Water and Wastewater Systems
Transportation Systems

# Supply Chains Require Thorough Risk Assessments

ACCUMULATED CYBERSECURITY INCIDENTS IMPACTED BY SUPPLY CHAIN ATTACKS IN 2022



THE INDUSTRIES MOST IMPACTED BY SUPPLY CHAIN ATTACKS



## 1. Supply chain attacks threaten key industries

Supply chain attacks against crucial industries have surged in 2022, as seen in the attacks on SolarWinds and Kaseya. For instance, in H1 2022, Toyota had to halt production at 14 auto factories due to cyberattacks on its suppliers of plastic parts and electronic components. Meanwhile, Shell suffered a loss in oil production because of a cyberattack on its logistics and storage supplier. These incidents demonstrate the direct impact of supply chain attacks on key industries.[3]

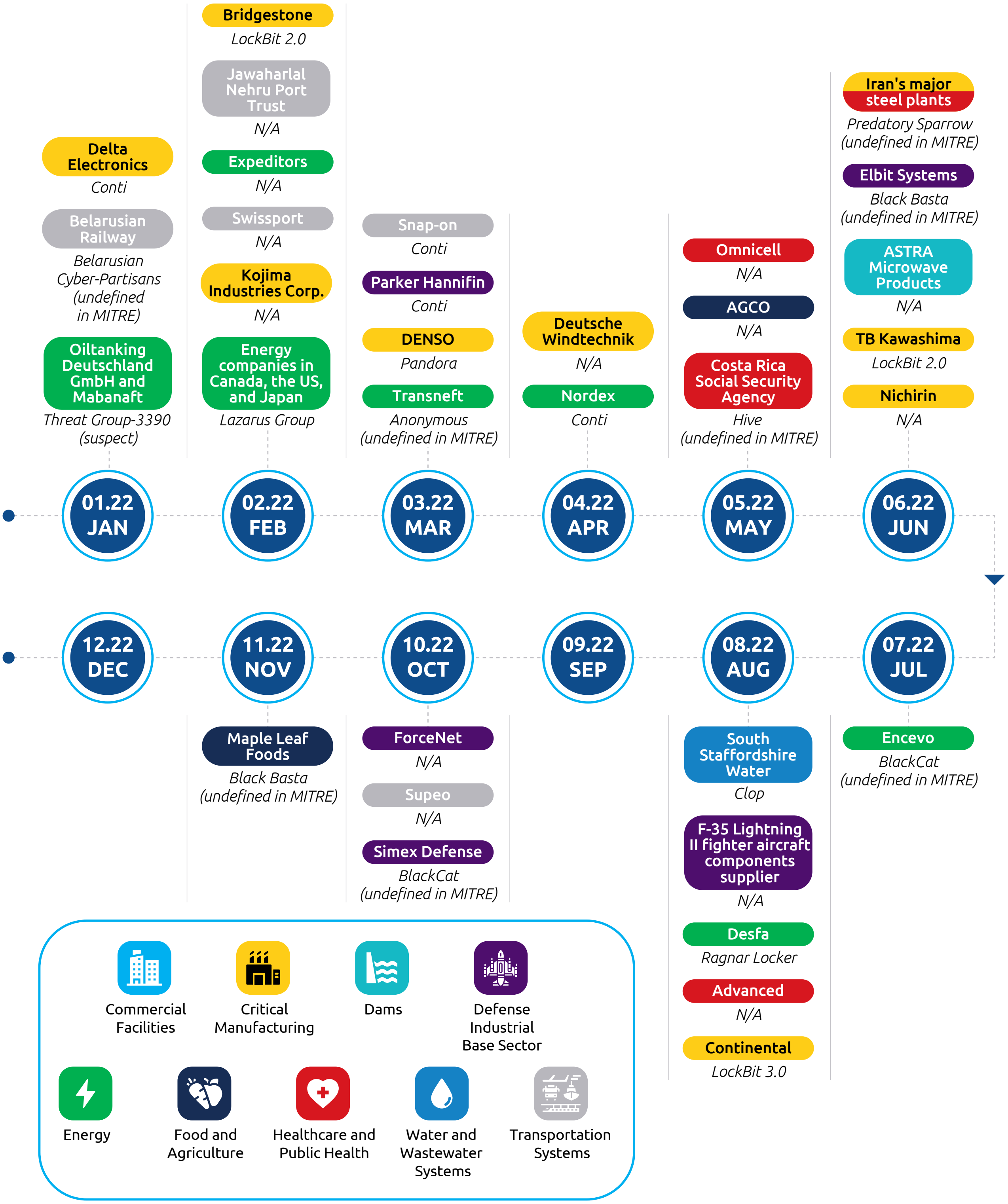
## 2. Organizations must prioritize supply chain risk assessments

To help organizations assess supply chain risks, MITRE has developed the System of Trust Framework. The SCS Hot Topics Summit in 2022 will address the specific issues of supply chain risks, due to the growing concern for the topic. The impact of supply chain attacks on key industries emphasizes the need for organizations to conduct comprehensive and consistent assessments of supply chain risks in the future.[4]

## 3. Energy and critical manufacturing industries face a high number of supply chain attacks

In 2022, cyberattacks on suppliers in key industries were recorded and it was found that the Energy and Critical Manufacturing industries were among the most affected. Critical manufacturing accounts for 24% of the total. Among them, the automotive industry makes up the majority. We have found that with the rise of automated manufacturing in the automotive industry, measures to mitigate supply chain attacks will become a key focus for automotive factories.

## CYBERSECURITY INCIDENTS IMPACTED BY SUPPLY CHAIN ATTACKS IN 2022



01.22 JAN

Delta Electronics
*Conti*

Belarusian Railway
*Belarusian Cyber-Partisans (undefined in MITRE)*

Oiltanking Deutschland GmbH and Mabanaft
*Threat Group-3390 (suspect)*

02.22 FEB

Bridgestone
*LockBit 2.0*

Jawaharlal Nehru Port Trust
*N/A*

Expeditors
*N/A*

Swissport
*N/A*

Kojima Industries Corp.
*N/A*

Energy companies in Canada, the US, and Japan
*Lazarus Group*

03.22 MAR

Snap-on
*Conti*

Parker Hannifin
*Conti*

DENSO
*Pandora*

Transneft
*Anonymous (undefined in MITRE)*

04.22 APR

Deutsche Windtechnik
*N/A*

Nordex
*Conti*

05.22 MAY

Omnicell
*N/A*

AGCO
*N/A*

Costa Rica Social Security Agency
*Hive (undefined in MITRE)*

06.22 JUN

Iran's major steel plants
*Predatory Sparrow (undefined in MITRE)*

Elbit Systems
*Black Basta (undefined in MITRE)*

ASTRA Microwave Products
*N/A*

TB Kawashima
*LockBit 2.0*

Nichirin
*N/A*

07.22 JUL

Encevo
*BlackCat (undefined in MITRE)*

08.22 AUG

South Staffordshire Water
*Clop*

F-35 Lightning II fighter aircraft components supplier
*N/A*

Desfa
*Ragnar Locker*

Advanced
*N/A*

Continental
*LockBit 3.0*

09.22 SEP

10.22 OCT

ForceNet
*N/A*

Supeo
*N/A*

Simex Defense
*BlackCat (undefined in MITRE)*

11.22 NOV

Maple Leaf Foods
*Black Basta (undefined in MITRE)*

12.22 DEC

Commercial Facilities

Critical Manufacturing

Dams

Defense Industrial Base Sector

Energy

Food and Agriculture

Healthcare and Public Health

Water and Wastewater Systems

Transportation Systems

# Critical Infrastructure Assets Remain Under Attack

Recently, cybersecurity has become a matter of national security as critical infrastructure has been put in the crosshairs of various malicious actors. Critical infrastructure organizations (such as power companies, water treatment plants, oil and gas transportation companies, and hospitals) face persistent security risks and high costs when incidents occur because they are attacked by both mercenaries and groups that intend to cause civil unrest with their antics. Recent examples include the attack on Ukraine's power grid, which resulted in power outages for hundreds of thousands, and the attack on Dusseldorf University Hospital in Germany, which forced the hospital to close its emergency room and resulted in a patient's death during the process of transferring to another hospital. The shutdown of Colonial Pipeline's pipeline system in response to a ransomware attack resulted in jet fuel shortages for airlines, commercial fuel shortages and rising oil prices at gas stations. In 2023, the combination of energy shortages, geopolitical tensions, and advancements in attack technology is likely to increase attacks on critical infrastructure, particularly between the US and its allies. Governments must confront these facts:

## 1. The energy industry is a prime target for cyberattacks on critical infrastructure

Analysis of global critical infrastructure attacks in 2022 shows that the energy sector accounted for 31% of all incidents, making it the most targeted industry. This is due to the increasing connectivity between the operational technology (OT) systems of power grids and wind farms with information technology (IT) systems, enabling attackers to gain access and control these systems. The industry is facing new security challenges, and concerns are growing over rapidly accelerating emerging threats.

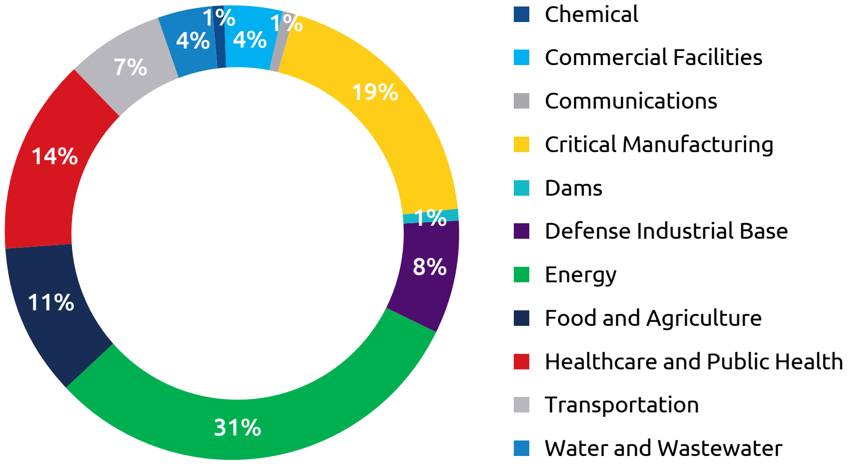
In the second half of 2022, critical infrastructure sectors experienced the highest number of known ransomware attacks among industries closely related to the ICS/OT environment. For example, in August, the Clop ransomware group claimed to have compromised a British water supply company, attaining access to the internal network of the industrial control system, and disrupting the flow of water, as evidenced by the publication of the water plant's HMI screen. Additionally, SEKOIA.IO[5] reports that Conti, LockBit, and Hive are the RaaS strains that occur most frequently in Utilities, with Conti and LockBit each accounting for one-third of all attacks.

- ***Conti:*** Malicious emails and stolen RDP credentials are common initial access methods. As of January 2022, Conti has victimized over 1,000 entities and been paid over $150 million in ransom, making it one of the most financially damaging ransomware families. Notably, Conti has been observed to behave aggressively towards its victims and may still leak data even after receiving the ransom payment.[6]

- ***LockBit:*** In 2022, LockBit has seen a significant increase in the number of attacks and, in July, announced the availability of free and searchable victim data leaks. LockBit 3.0 poses a challenge for security researchers as it requires a pass parameter to parse the main program, making it difficult to analyze. By creating a difficult-to-analyze environment, LockBit underscores the impact an attack can have on a victim organization as it struggles to counter their attack.

- ***Hive:*** Hive primarily targets energy, healthcare, and finance industries. Like Conti, Hive often uses malicious emails and stolen RDP credentials as an initial means of exploitation. In July, Hive upgraded its code from GoLang to Rust, making it relatively harder for analysts to reverse engineer. As of November 2022, Hive has received approximately $100 million in ransom from over 1,300 victimized businesses.[7]

### ANALYSIS OF CRITICAL INFRASTRUCTURE CYBER INCIDENTS IN 2022



## 2. Geopolitical conflicts are escalating critical infrastructure security risks

Although outright war hasn't been declared, the beginnings of technological warfare are well under way as radical hackers are already parlaying their skills to threaten national stability and the daily lives of civilians. Due to the critical nature of national infrastructure, such as energy, transportation, and communication, a successful compromise could seriously impact a country. As such, critical infrastructure is a desirable target for state-supported or politically motivated attackers. For instance, Lazarus, an APT organization supported by North Korea, continues to target energy companies in Canada, the United States, and Japan. In addition to connecting the victim computer to the C&C Server, they also attempt to obtain the adfind.exe tool from the victim endpoint Active Directory information to identify potential endpoints for lateral movement. The Russian

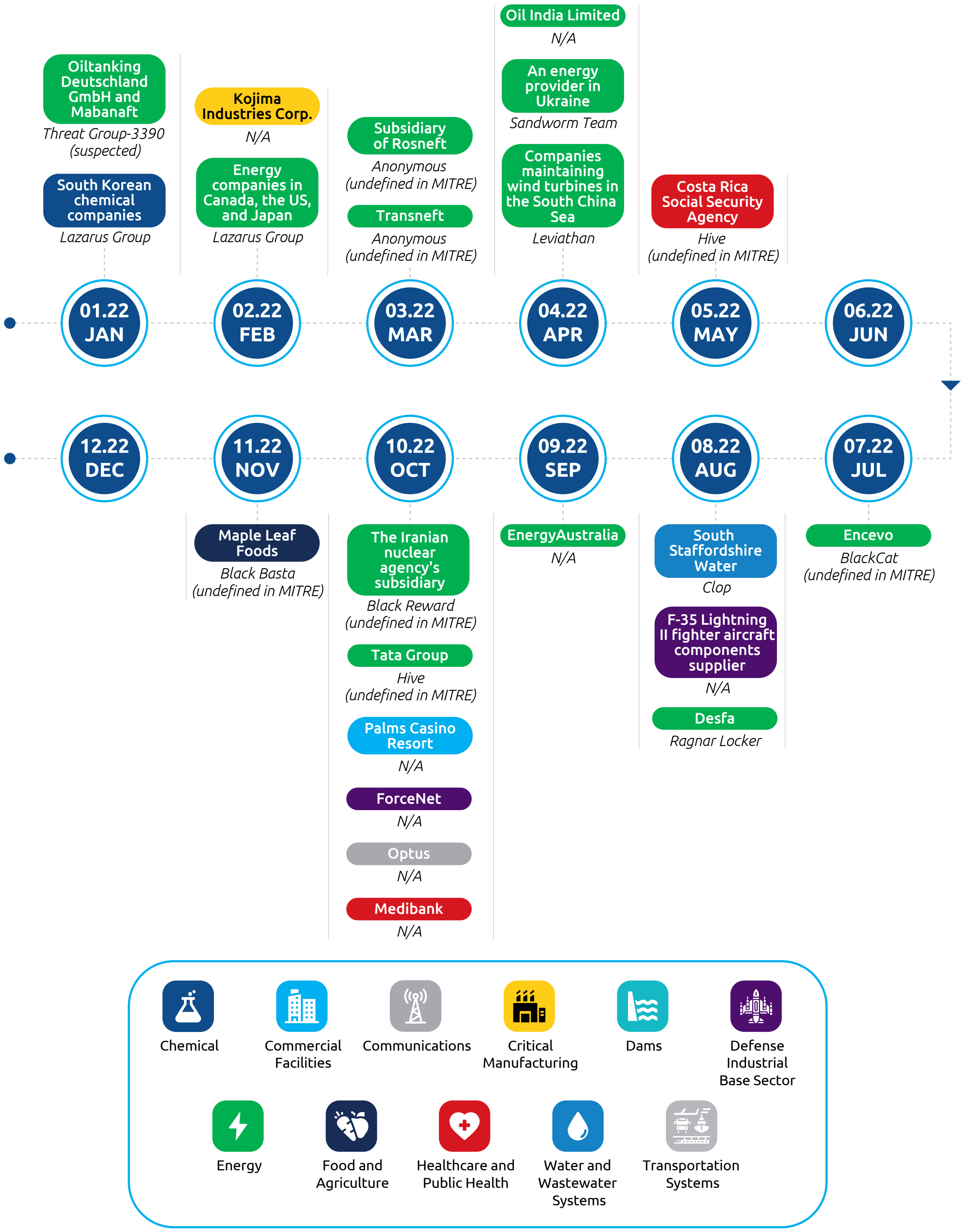
APT organization Sandworm attempted to use the Industroyer2 malware, which targets power supply system-based infrastructure, to attack multiple substations in Ukraine. They also utilized disk wiping tools to damage energy companies' Windows, Linux, and Solaris servers, making it difficult for victims to restore power. Moreover, the pro-Russian attack group Killnet launched DDoS attacks against major US airports, leading to network crashes at airports in Atlanta, Chicago, Los Angeles, New York, Phoenix, and St. Louis.

According to the European Union Agency for Cybersecurity (ENISA), the Russia-Ukraine conflict has led to a rise in radical hacking activities, with 128 government agencies in 42 supporting countries falling prey to state-sponsored hacker groups. As soon as conflict began, hacker groups rose to the occasion to add their disruptive activities to the mix. This shows how quickly hacking can be wielded as weapons against entire nations and governments. Countries such as China, Iran, and North Korea are also increasing their espionage activities, and national hacker organizations have targeted countries such as Southeast Asia, Japan, and Australia. As geopolitical tensions persist in Asia, these national hacker groups have targeted countries with close ties to Taiwan, including EU member states like the Czech Republic and Poland. These attacks often exploit zero-day vulnerabilities or target OT networks, with a focus on critical infrastructure. Social engineering, disinformation, and data threats are also common attack methods used by national hackers.

## 3. Interdependence in utilities industries and the threat of APT and ransomware attacks on suppliers

Critical infrastructure industries are often interconnected, with coal mining and transportation systems serving as an example of the interdependence between energy and transportation. The green symbol in the figure denotes critical infrastructure suppliers. In the event of a cyberattack on a supplier, the corresponding industry may be unable to provide stable public infrastructure services. In January 2022, German oil storage company Oiltanking suffered a cyberattack that prevented it from providing services to trucks, making Shell a victim of the incident. This highlights the potential impact on national economies if the fuel supply of a company like Shell were to be disrupted. In October of the same year, Supeo was hit by ransomware, causing Danish train drivers to lose access to key operational information and resulting in several hours of train service disruption. These incidents underscore the significant impact of supply chain attacks on critical infrastructure and the importance of comprehensive risk assessments.

## Critical Infrastructure Targeted in 2022



01.22 JAN

Oiltanking Deutschland GmbH and Mabanaft
*Threat Group-3390 (suspected)*

South Korean chemical companies
*Lazarus Group*

02.22 FEB

Kojima Industries Corp.
*N/A*

Energy companies in Canada, the US, and Japan
*Lazarus Group*

03.22 MAR

Subsidiary of Rosneft
*Anonymous (undefined in MITRE)*

Transneft
*Anonymous (undefined in MITRE)*

04.22 APR

Oil India Limited
*N/A*

An energy provider in Ukraine
*Sandworm Team*

Companies maintaining wind turbines in the South China Sea
*Leviathan*

05.22 MAY

Costa Rica Social Security Agency
*Hive (undefined in MITRE)*

06.22 JUN

07.22 JUL

Encevo
*BlackCat (undefined in MITRE)*

08.22 AUG

South Staffordshire Water
*Clop*

F-35 Lightning II fighter aircraft components supplier
*N/A*

Desfa
*Ragnar Locker*

09.22 SEP

EnergyAustralia
*N/A*

10.22 OCT

The Iranian nuclear agency's subsidiary
*Black Reward (undefined in MITRE)*

Tata Group
*Hive (undefined in MITRE)*

Palms Casino Resort
*N/A*

ForceNet
*N/A*

Optus
*N/A*

Medibank
*N/A*

11.22 NOV

Maple Leaf Foods
*Black Basta (undefined in MITRE)*

12.22 DEC

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base Sector
Energy
Food and Agriculture
Healthcare and Public Health
Water and Wastewater Systems
Transportation Systems

# OT Security Market Driving Forces

Facing the constantly rising tide of OT/ICS cybersecurity threats, it is necessary for us to understand the underlying causes. In this chapter, we will a) explore the importance of OT security from a technical, legal, and economic standpoint and b) examine the responses of governments and businesses to the rapidly escalating global OT threats.

## IT and OT Systems are Converging

The concept of IT/OT convergence, which aims to integrate physical equipment and devices into the digital realm, is not new. However, it has only recently gained significant traction in the industry. A 2019 report by IoT Analytics stated that around 50% of industrial assets in factories will be connected to local or remote data collection systems starting in 2020.[8] This projected trend has been further accelerated by the COVID-19 pandemic, which highlights the importance of the Industrial Internet of Things (IIoT) for enhancing organizational resilience in the face of catastrophic events. In the manufacturing sector, Industry 4.0, which is also known as the Industrial Internet of Things, is seen as a key driver for reducing downtime, developing new business models, and improving the customer experience.

### The Killer Application of IT/OT Convergence

Typically, a successful digital transformation in the industry begins by identifying key application cases, and then implementing them on a small scale in factories. During the process, data is shared, and the intelligence of IT systems is applied to the physical assets of OT systems to achieve new efficiencies, streamline operations, foster innovation, and introduce new services. Common OT devices include sensors, programmable logic controllers (PLCs), distributed control systems (DCSs), computer numerical control (CNC) systems, building automation systems (BAS), and supervisory control and data acquisition (SCADA) systems. These devices can communicate wirelessly through standardized network protocols to transmit relevant data from each physical system back to a central server for monitoring and analysis. The results of this analysis can then be communicated back to the physical system, resulting in the following IT/OT convergence applications:[9]

- **Energy sector:** IT and OT teams can remotely access operational data to help industries (such as power grids, oil, and gas) optimize preventive maintenance of industrial control equipment, perform damage assessments, and handle inventory monitoring, or optimize energy distribution.
- **Manufacturing sector:** IT and OT teams can use automated material transfer systems and robotic arms for automated production, adjust production processes in real-time, improve production efficiency, and reduce manufacturing costs and waste. For example, data analysis can be used to reduce electricity costs or reduce redundant inventory.

- **Transportation sector:** IT and OT convergence can help rail, bus, delivery, and other transportation organizations better understand asset coordination, conditions, and usage to guide short-term maintenance, route optimization, and long-term planning for asset replacement and safety.

- **Pharmaceutical sector:** The integration of IT and OT allows more medical devices to measure products that can detect physiological parameters, which can provide insight into health or physiological conditions. Data analysis systems can be used to improve pharmaceutical manufacturing and ensure product quality or collaborate with health services to achieve better patient analysis and outcomes, along with predicting disease incidence.

- **Retail sector:** By using OT devices such as shelf sensors, product labels, IP cameras, and POS devices, more data can be provided to IT departments for analysis, thereby optimizing inventory and sales sites, saving costs, and generating greater revenue while improving the shopper's experience.

## The New IT/OT Converged Organization

This phase of the process focuses on facilitating communication and collaboration between IT and OT teams, which is crucial for the overall success of the organization. Launching an organization for IIoT success also requires changes to organizational structures, collaboration types, and job profiles and roles. As a result, a new way of working and a new set of capabilities is necessary, particularly as IT and OT converge. To achieve this, the framework should include:

- **A common governance model**
- **Aligned processes that span across IT and OT**
- **Centralized data and security management**

To ensure success, IT and OT must reform their processes to accommodate each other and ensure that important projects have effective communication channels. Businesses may have specific processes for storing and securing IT data, but these processes may need to be adapted or extended for converged OT systems.

## New IIoT Technologies Creates Unprecedented Vulnerabilities

As the new Industrial Internet of Things architecture gains momentum, traditional centralized SCADA and MES system communication methods are shifting. For example, many sensors are now using IoT protocols such as LoRaWAN, SigFox, or NB-IoT to connect industrial sensors directly to the cloud. Additionally, industrial computer manufacturers are developing support for Edge Server, which can connect devices to the cloud through a software application platform. For instance, Advantech's ADAM-3600 RTU is capable of connecting to the Azure cloud.[10] Some small and medium-sized factories prefer to use open-source equipment and communication protocols, such as Linux-based HMI and gateways, or factories gradually adopt servers that support the OPC-UA protocol. However, these trends can also increase the attack surface for hackers.

## Addressing the Challenges of OT Cybersecurity

Availability is paramount in OT/ICS network architectures rather than confidentiality, and productivity is the primary consideration in most decision-making processes. Therefore, the network architecture of OT/ICS is rarely designed with cybersecurity defense functions in mind and tends to be flattened. This creates common OT/ICS cybersecurity challenges which include:

- **Incomplete cybersecurity architecture:** In the past, OT/ICS defense most commonly relied on "complete isolation" (air-gapping). This assumption has led to imperfect planning and deployment of cybersecurity countermeasures. For example, the OT/ICS network architecture does not consider the cybersecurity of regional management, or even detailed hierarchical isolation.

- **Internal/supply chain threats:** Mobile devices carried into an air-gapped environment, with lax management policies, may allow malicious programs to damage the OT/ICS environment or steal sensitive data. USB flash drives for data transfers and laptops for repairs, or even any device brought into the factory by any supplier, could become a patient zero from which malware can spread.

- **Complex OT communication protocols:** Different industries use special OT/ICS network architectures and communication protocols in their workplaces, and they may have vast differences due to variable requirements. In addition, many industrial control communications protocols are not encrypted, making it easier for hackers to manipulate factory operations and interfere with production.

- **Legacy operating systems:** Typically, OT/ICS endpoints are the weakest links in OT/ICS cybersecurity because there are many legacy OT/ICS endpoints in the environment that perform critical operations or operate on production line decisions. At the same time, the software and firmware of the key assets that run the old system would not be updated, and newly discovered vulnerabilities would not be patched. This is why every Windows XP or Windows 7 system is a vulnerable target.

- **IT cybersecurity solutions are not suitable for OT environments:** In the semiconductor equipment industry, endpoints will be subject to special warranties or regulations, and installing additional applications would void the warranty or violate the regulations. In addition, the pharmaceutical industry also has many such assets. Due to the limitations of the system design of the equipment itself, anti-virus software cannot be installed, and special solutions are required to maintain and secure such systems.

# Renewed Government Regulatory Focus on Cybersecurity

Nowadays, countries around the world are constantly developing their own digital infrastructure and industries. The widespread use of information and communication technology has made all aspects of life more interconnected and integrated than ever before. Many traditional network boundaries have disappeared, making network threats a direct threat to governments, critical infrastructure, and private enterprises. Looking back at cybersecurity incidents in recent years, it is clear that more and more network attacks are directly impacting people's lives. Several well-known network attacks with global influence, such as Stuxnet, WannaCry, SolarWinds, Colonial Pipeline, and Russia's cyberattack on the US satellite company Viasat in the early stages of the Ukraine war,[11] serve as cautionary tales. These incidents have prompted governments to reexamine their cybersecurity regulations and policies in order to prevent hackers from threatening urban power, water supply, or stealing sensitive corporate or personal data.

## U.S. OT Cybersecurity Policies and Regulations

### Executive Order 14028 "Improving National Cybersecurity" Highlights the Importance of OT Cybersecurity

In recent years, the United States has seen a series of cyberattacks on critical infrastructure, such as the Colonial Pipeline ransomware attack, which quickly brought the potential impact of cyberattacks on the economy to the forefront, as the attack knocked out nearly half of the East Coast's fuel supply. Additionally, there was a would-be disastrous attack on water infrastructure in Oldsmar, Florida that was narrowly avoided, where an unknown hacker attempted to release lye into the town's water system, a plot straight out of a comic book villain's handbook. Recognizing the severity of the situation, on May 12, 2021, President Biden signed Executive Order 14028, "Improving Nationwide Cybersecurity". Biden's executive order, aimed at protecting critical infrastructure from further attacks by modernizing the nation's cybersecurity, emphasizes for the first time that the scope of protection and security must include the systems that process data (information technology (IT)) and the operations critical to keeping us safe (Operational Technology (OT)). Then in March 2022, President Biden signed CIRCIA into law.[12] CIRCIA provides legal protections and guidance to companies operating in critical infrastructure sectors, including requiring reporting of cyber incidents within 72 hours and ransom payments within 24 hours.

### ICS/OT of Critical Infrastructure Becomes the Focus of Cybersecurity

On July 28, 2021, President Biden signed a national security memorandum on improving the cybersecurity of critical infrastructure control systems.[13] The National Security Memorandum (NSM) establishes a voluntary initiative to advance collaboration between the Federal Government and the critical infrastructure community to help stakeholders understand cyber threats to critical ICS/OT systems and adopt minimum cybersecurity standards. Examples include the introduction of multiple performance-based directives by the Transportation Security Administration (TSA) in 2022 to improve cybersecurity resilience in the pipeline and rail sectors, and measures in 2022 addressing the cyber needs of the aviation sector. At the same time, cybersecurity performance goals were released to help illuminate the investment results of headlining cybersecurity.

### Pre-think Security for New Digital Infrastructure

The U.S. government has passed bipartisan infrastructure law to reinforce cybersecurity investment in the modernization of the U.S. infrastructure in order to ensure that it is both smart and safe. An example of modernization lies in expanding the national electric vehicle charging station network, building it to last and enabling it to meet modern safety and security standards, which include stronger network protection. In addition, the bill also brings high-speed Internet to underserved areas of the country while bridging the digital divide. To that end, it introduced the first cybersecurity grant program specifically targeted at state, local and territorial (SLT) governments across the country, providing state and local cybersecurity with a four-year grant program that allocates $1 billion in funding to SLT partners to ensure investment in digital security.[14]

### US OT CYBERSECURITY OVERVIEW

Ongoing regulatory developments will apply to US manufacturers as most meet the criteria for critical infrastructure

**Current Landscape**

- North America is the largest OT cybersecurity market, which accounted for 39.7% of the market in 2019. The US represents the largest market in this region and is one of the most mature markets in cybersecurity awareness, including OT cybersecurity technology adoption.
- The US manufacturing sector does not have overarching, mandatory cybersecurity regulations, but many manufacturers meet the criteria for critical infrastructure, which is highly regulated.
- Overall cybersecurity in manufacturing is under **NIST**. The US is guided by the Executive Order 13636 leading to the **NIST Framework for Improving Critical Infrastructure Cybersecurity (2018)**. State-specific laws also exist such as Senate Bill 327 (for California) for the protection of smart devices connected to the internet.

**Outlook**

- The US government has been actively making regulatory developments for IT and OT security. Highly public security attacks (e.g., Colonial Pipeline attack) highlighted the need for cybersecurity protection.
- In May 2021, the President's Executive Order 14028 was issued. It includes the whitepaper Baseline Security Criteria for Consumer loT Devices, which aims to improve cybersecurity mandating multiple bodies, including NIST, to ensure a secure software and loT devices supply chain.
- In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. This will pave the way for more regulatory development for both IT and OT security, impacting several industries.

## EU OT Cybersecurity Policies and Regulations

### EU NIS 2.0 Establishes a Response Command Center to Defend Against Cyberattacks

As a landmark moment in the legalization of the EU's cybersecurity management regulations, the "Network and Information System Security Directive" was officially announced and implemented in 2016. Its full name is Security of Network and Information Systems, or NIS Directive for short. By the end of 2020, in response to increasingly serious cyber threats, the European Commission (EC) proposed an amendment proposal NIS 2 Directive, the purpose of which was to update the NIS directives to meet current and future needs. It would also be in line with the cybersecurity situation in the post-COVID-19 era and the 5G era. Most of the objects covered by this upgrade are critical infrastructure such as energy systems, medical networks, and transportation services.[15]

After comparing the old and new versions of the EU's Network and Information System Security Directive, we found that the new version (NIS 2.0) expanded the scope of regulated objects to include 11 additional management agencies, such as district heating and cooling facilities, hydrogen energy-related agencies, and government administrative departments. Additionally, NIS 2.0 established a response center called EU-CyCLONe to assist EU countries in monitoring and responding to major cyberattacks. EU member states will have 21 months to incorporate these new rules into their national legislation.

In February 2022, several large refineries in Belgium and the Netherlands were hit by cyberattacks.[16] Hackers paralyzed the automatic loading and unloading process of oil depots, rendering ships waiting to load and unload crude oil products inoperable and disrupting almost the entire region's trading of petroleum products. This shows us that even as regulations are evolving, the threat of cyberattacks remain ever-present, so we must exercise constant vigilance.

### EU Cyber Resilience Act Promotes Product Security by Design

On September 15, 2022, the European Commission (EC) proposed the Cyber Resilience Act (CRA) to enhance the cybersecurity of EU digital products and streamline existing regulatory framework.[17] The CRA imposes a number of cybersecurity obligations on digital products, including software, and is closely related to other EU regulations such as the NIS 2 Directive, the Artificial Intelligence Act, and the General Data Protection Regulation (GDPR). It has the potential to be one of the most significant EU cybersecurity laws.

The CRA applies to all digital products that are directly or indirectly connected to another device or network. A digital product is defined as "any software or hardware product and remote data processing solution thereof, including software or hardware components placed on the market separately". Internet-connected products must comply with basic cybersecurity requirements, including design, development, and production, risk-based cybersecurity, and the absence of known exploitable vulnerabilities. Businesses that violate the cybersecurity requirements and obligations of manufacturers outlined in Annex I of the CRA may be fined up to €15,000,000 or 2.5% of their global annual turnover for the previous financial year, whichever is higher, instating concrete consequences for reckless or negligent cyber hygiene.

## GERMANY OT CYBERSECURITY OVERVIEW

**Germany is a leading industrial hub requiring advanced OT cybersecurity solutions to remain competitive**

**Current Landscape**

- European organizations are leveraging OT and loT to enhance manufacturing processes. Since Germany is a leading industrial and manufacturing hub, German enterprises require the most advanced OT cybersecurity solutions and services. This includes OT and IT integration.
- The German government recognizes the risk from industrial cyberattacks. **The Industrial Strategy 2030** includes improving cybersecurity under its main pillars. The government also adopted the **Cybersecurity Strategy 2021-2025** to improve cybersecurity across the board, including OT.
- For vendors, EU is a highly regulated market especially when it comes to privacy and data regulation. This can give regional vendors and inherent advantage.

**Outlook**

- Last November, the EU adopted the **NIS2 Directive**. It sets the baseline for cybersecurity risk management measures. Member States must transpose NIS2 into national laws by Sept. 2024.
- Although OT is not the highlight in NIS2, OT security will be in scope for NIS2 along with the **CER Directive**. The directives will address current and future online and offline risks, from cyberattacks (NIS2) to physical attacks and natural disasters (CER). CER focuses on physical rather than digital resilience measures for critical entities.
- Not yet into law, the proposed **EU CRA** introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. It will apply to manufacturers, importers, and distributors of these products across their life cycles. It will also stipulate requirements for vulnerability and incident handling for manufacturers and obligations for operators.

## Japan OT Cybersecurity Policies and Regulations

In keeping with the rest of the world, the Japanese government has placed a renewed emphasis on securing critical infrastructure and industrial control systems in its National Security Strategy. On December 14, 2022, the government officially released a new version of this, which highlighted the need to improve response capabilities in the field of cybersecurity to ensure the safe and stable use of national cyberspace, particularly for key infrastructure. The strategy aims to bring Japan's cybersecurity response capabilities to or above the level of leading countries. Specific measures outlined in the strategy include:[18]

- Establishing a mechanism to continuously assess the security of government agencies' information systems, improving responses based on the latest cyber threats, and continuously managing vulnerabilities in government agencies' information systems
- Introducing "active cyber defense" to preempt the possibility of serious cyberattacks that could raise national security concerns for government and critical armed attacks
- Further strengthening information collection and analysis capabilities in the field of cybersecurity and establishing a network active defense system, including promoting public and private information sharing, detecting attacked devices, and launching network countermeasures
- Reorganizing the National Cybersecurity Incident Preparedness and Strategy Center (NISC) into a new agency to coordinate policy in the field of cybersecurity
- Coordinating with allied countries and other countries to strengthen information collection and analysis, attribution, and publication, and develop international frameworks and rules; to this end, Japan's Ministry of Economy, Trade and Industry (METI) and US Department of Homeland Security (DHS) signed a cybersecurity cooperation in the MOU, demonstrating that the security of industrial control systems is one of the four key cooperation projects

In addition to these efforts, the Japanese government is focusing on promoting smart industrial safety as an international cooperation project. The Ministry of Economy, Trade and Industry (METI) established the Industrial Cybersecurity Research Group in December 2017 to identify challenges faced by Japanese industrial companies in the field of cybersecurity and promote relevant policy measures. The ministry also established working groups to discuss industry-based cybersecurity policies and published guidelines for cyber-physical security measures for building and plant systems.

METI also cooperates with other countries such as Indonesia and Thailand to develop smart industrial safety policies. On January 25, 2022, METI and the Ministry of Industry of the Republic of Indonesia signed a memorandum of cooperation (MOC) to "strengthen smart cooperation",[19] and on September 28, 2022, METI and the Ministry of Industry of Thailand (MOI) signed a Memorandum of Cooperation (MOC) agreeing on the promotion of smart industrial safety cooperation.[20]

## JAPAN OT CYBERSECURITY OVERVIEW

Japan is leading the OT cybersecurity market in Asia-Pacific, which will further grow driven by regulatory developments

### Current Landscape

- Asia-Pacific is the fastest-growing region, with China and Japan leading the OT cybersecurity market .
- According to the NICT, there has been a significant increase in the number of cyberattacks on IoT devices. This prompted the government to establish new legislation, strategies, and facilities.
- **Society 5.0** is a national policy achieved by integrating cyberspace and physical space in a sophisticated manner. **Connected Industries** is another national policy for creating new value added by connecting a variety of goods, industries, and people.
- METI aims to ensure security in the new supply chains through the **Cyber/Physical Security Framework 2019 (CPSF)**. It presents an overview of security measures for industrial society.

### Outlook

- With the evolving threat landscape, Japan is continuously trying to improve their IT and OT security environment.
- Japan is seeking bilateral cooperation to operationalize its cybersecurity priorities. Agreements with the US Dept. of Homeland Security aim to improve and collaborate on curbing cyber threats faced by the governments.
- In July 2021, the Japanese government released a new cybersecurity strategy for the next three years. The enhanced deterrence was prompted by the suspected involvement of the Chinese and Russian governments in cyberattacks.
- In November 2022, METI issued the Cyber and Physical Security Guidelines for Factory Systems to provide reference concepts and steps for implementing security measures for factory systems.

# Rising Trade Protectionism Leads Countries to Establish Local Manufacturing Hubs

Over the past few decades, globalization has been considered a practically irreversible trend. Numerous manufacturing industries around the world have stretched their supply chain fronts and placed their production bases in mainland China and India, which can provide low-cost labor, land, and services, so as to establish a far-reaching model known as the ever-changing multinational enterprise empire. However, with the rise of the “Industry 4.0” revolution in recent years, more and more companies have begun to reflect on whether the long-chain model is truly beneficial to all.

The U.S.-China trade dispute, coupled with the catalyst of COVID-19, has led countries to experience unprecedented supply chain shocks, such as shortages of automotive chips and medical supplies. Governments and companies in various countries have begun to discover that they must be able to produce the required products within their own country in order to ensure safe domestic operations. This consideration based on people’s livelihood and national security has further established “localization” and “regionalization” instead of “globalization” in production. In recent years, companies have begun to abandon cheap labor and land as the primary considerations for layout and started a “return” strategy to transfer production lines back to their home countries.

In recent years, developed countries such as the United States, Germany, Japan, South Korea, and the United Kingdom have actively promoted the reshoring of manufacturing industries. The rapid progress of technological innovations such as new materials, 3D printing, and smart manufacturing has deepened the division of labor in their domestic production chains. With the building of new factories, enterprises are more inclined to consider ICS/OT cybersecurity when equipment initially enters the site, so as to lay a better foundation for future security.

## Increasing Awareness about Potential Losses Within the OT Environment

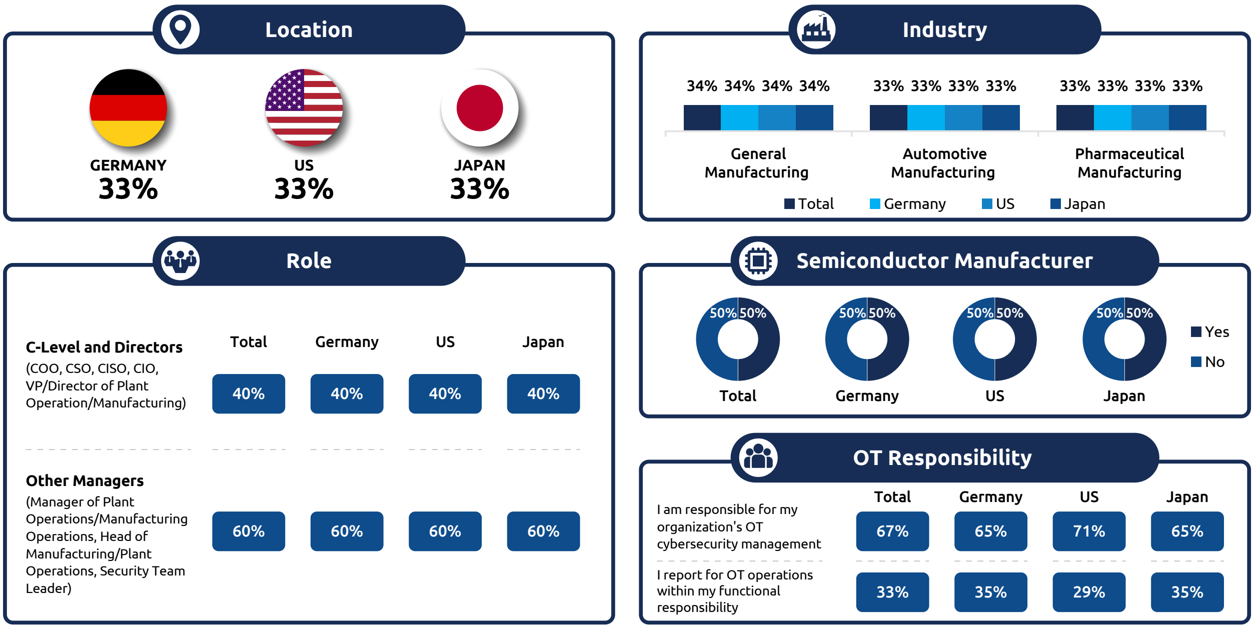
The rise in attacks targeting manufacturing and critical infrastructure highlights the gravity of OT (Operational Technology) attacks, emphasizing the need for security. Businesses now understand that ransomware attacks can disrupt production line operations, seriously hinder productivity, and take hours or longer to recover. Hackers may use multiple extortion methods to steal sensitive corporate information, leading to data breaches, property damage, and violations that can erode customer trust and harm brand value. Therefore, as Industry 4.0 becomes a crucial aspect of corporate competition, corporate management and information security leaders should make protection of the OT network a top priority in their information security strategies. In the interests of providing the groundwork on which this new cybersecurity architecture can be built, we have invested in research based on 2022 manufacturing companies' experience.

## OT Security End User Survey

In 2022, TXOne Networks commissioned Frost and Sullivan to conduct a global survey on the current state of OT/ICS cybersecurity in the manufacturing industry. The study interviewed decision makers or leaders in advanced manufacturing countries such as the United States, Japan, and Germany, involving 300 OT/ICS stakeholders. This survey investigates the way decision makers within organizations perceive OT security, the challenges they face and establishes their general level of vulnerability and resilience. Three major verticals were surveyed, dividing the subjects up with roughly equivalent sample sizes. 34% were from general manufacturing, 33% were from automotive manufacturing, and 33% were from pharmaceutical manufacturing. From the general manufacturing vertical, half of them are semiconductor manufacturers, factories that require specialized equipment which can be critically compromised.

The roles of those sampled are in management and extend up to the tier of C-Level executives and directors. 40% are in the C-suite of management, while 60% of the participants are managers of plant operations, heads of manufacturing, or leaders of security teams. This was deliberate, since the survey is looking to gain insight into the minds of those who would make security and cybersecurity-based decisions, so these groups of people were the ones most directly relevant. In terms of OT-centric responsibilities, majority of them (65% or above) described themselves as "responsible for [their] organization's OT cybersecurity management". Therefore, it can be assumed that these are the people who deal with cybersecurity problems and are accountable for solving those problems in their day to day lives. The remainder classify themselves as those who "report for OT operations within [their] functional responsibility". TXOne Networks hoped to gain a closer look at the threat landscape of OT security from the viewpoint of those that would be on the ground floor.

## OT SECURITY END USER SURVEY OVERVIEW



**Location**

| GERMANY | US | JAPAN |
|---|---|---|
| 33% | 33% | 33% |

**Industry**

**Role**

| | Total | Germany | US | Japan |
|---|---|---|---|---|
| **C-Level and Directors** (COO, CSO, CISO, CIO, VP/Director of Plant Operation/Manufacturing) | 40% | 40% | 40% | 40% |
| **Other Managers** (Manager of Plant Operations/Manufacturing Operations, Head of Manufacturing/Plant Operations, Security Team Leader) | 60% | 60% | 60% | 60% |

**Semiconductor Manufacturer**

**OT Responsibility**

| | Total | Germany | US | Japan |
|---|---|---|---|---|
| I am responsible for my organization's OT cybersecurity management | 67% | 65% | 71% | 65% |
| I report for OT operations within my functional responsibility | 33% | 35% | 29% | 35% |

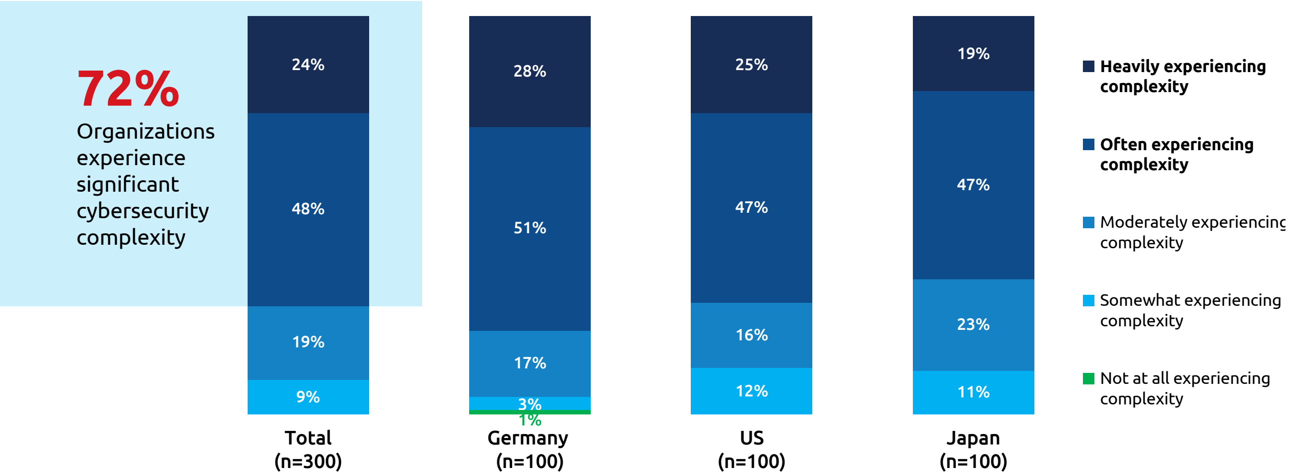
# The Landscape of Today's OT Security

This report is based on interviews conducted in three major manufacturing countries. The countries were chosen because the US, Japan and Germany have long been recognized as giants in the realm of manufacturing and cutting-edge technology. Based on the feedback from respondents, we clarify the thoughts of those most involved. From this analysis, we compared the security challenges faced by different countries in the past year and identified five key insights into the global manufacturing industry's OT cybersecurity situation. The survey's results show that organizations are becoming increasingly concerned about the security of their OT infrastructure, but there are still blind spots and a need to strengthen their efforts in preventing OT threats.

## INSIGHT 1 Cybersecurity Complexity has Fixable Contributing Factors

In the past, when information was confined to a singular physical object, such as a computer hard drive or a floppy disk, it was relatively simple to keep track of the whereabouts of information and therefore protect it. However, with Industry 4.0, and the way connectivity has become the trend, this task has become incredibly unwieldy and unpredictable. Problems that arise in trying to maintain the security of information are grouped under the umbrella term of cybersecurity complexity. In this survey, 72% of organizations face cybersecurity complexity, demonstrating how much of an issue it has become and why it is urgent for companies to upgrade their own protective architectures before cyber attackers take advantage and run amok. From those aforementioned organizations, 24% report heavily experiencing complexity, while 48% report often experiencing complexity. This constitutes a majority of organizations experiencing complexity, and the main bulk of that majority experiencing it often. With increased complexity comes a requisite higher level of expertise from security teams to manage and mitigate these complexities. Therefore, security teams are heavily impacted by this rapidly evolving threat landscape and they face numerous human resource challenges.

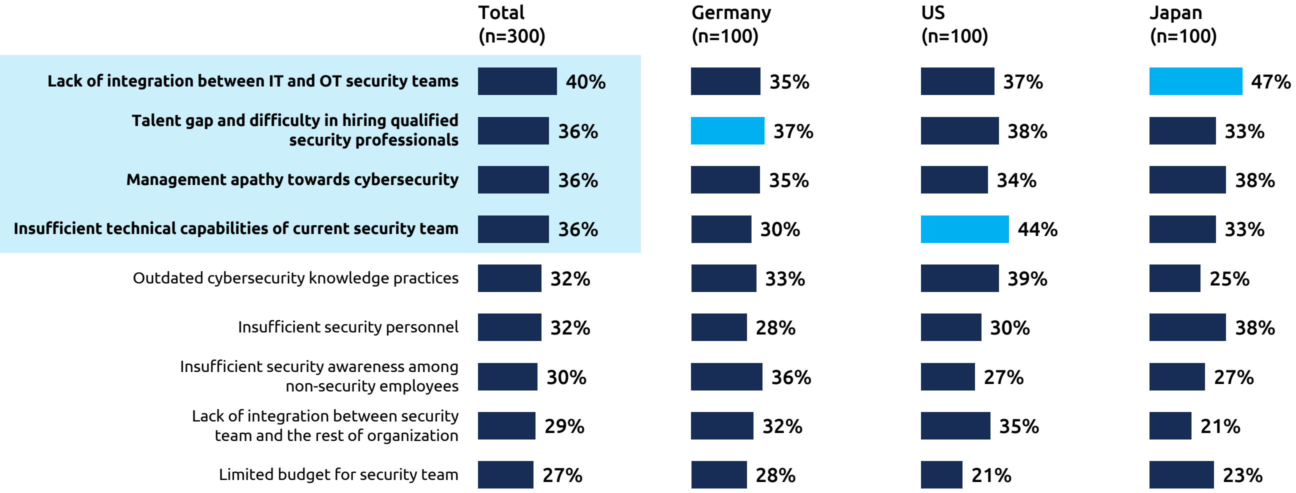
## CYBERSECURITY COMPLEXITY AMONG ORGANIZATIONS



*Q - To what level is your organization experiencing cybersecurity complexity? (Rate from 1 - not at all experiencing complexity to 5 - heavily experiencing complexity)*

*Source: Frost & Sullivan*

## KEY SECURITY HUMAN RESOURCE CHALLENGES



*Q - What are the key security human resource challenges your organization has faced over the last 12 months?*

*Source: Frost & Sullivan*

## IT and OT Security Teams Need to Collaborate

The largest challenge facing organizations is a lack of coordination between IT and OT security teams. 40% of the 300 companies cite lack of integration between IT and OT security teams as their stumbling block. Up until recently, most security was centered around IT, and was dealt with using software such as anti-viruses and firewalls. In terms of operational technology, simple measures were taken such as air-gapping, where secure computer networks were safe from unsecured networks due to physical separation. However, this meant that they were offline and unable to upgrade their systems, leaving them unpatched by security updates. If they were to be suddenly connected to a network in order to update their security, all of those missed upgrades and patches would compromise the system in a way that makes their attempt to upgrade their security an inadvertent exposure to much more danger. This is just one of many ways that IT and OT systems conflict with each other in terms of security. The OT device is safe so long as it's offline and physically separated from other devices. But, for it to be usable in this day and age, it needs to be online and connected. As technology advances, both sides must coordinate corresponding strategies and work more closely together to ensure end-to-end information security. In Japan, this lack of integration between teams is at its severest, posing a challenge to 47 out of 100 companies.

## Increase Hiring of Qualified OT Security Professionals

The next challenge lies in the difficulty of hiring qualified security professionals from a limited talent pool. Considering how quickly technology has advanced in recent years, it is no surprise that the population of people who are completely up to date and well trained is a limited one. Not only is cybersecurity a difficult field to break into but its constant evolution spurred on by leaps in technological innovation creates a situation that is always in flux. Germany suffers the most from this problem, with 37% of their companies facing this issue. This indicates that a dedicated training program or curriculum for cybersecurity within a company would be advisable and could cut down on many negative impacts in the future. Excellent OT security professionals possess the necessary skills and experience to manage the security of the OT network, and they are helpful in areas such as pre-preparation, planning, support, training, threat and response identification during an incident, and reducing impact, elimination, and recovery after an incident.

## Establish Commitment of Management to OT Cybersecurity

Aside from the lack of experience and knowledge in cybersecurity that is prevalent in many companies, there is also the issue of attitude. In fact, more than a third of those in management are apathetic towards cybersecurity in general and appear not to take it as a serious threat, averaging 36% of companies that were surveyed. This could be because the field of cybersecurity is still a fairly niche and specialized area of expertise, and management may be slow to acknowledge the need to acquire a whole new skillset along with a steep learning curve. In addition to this reluctance to adapt, there is the factor of complacency as well. Up until this point, it appears that most companies assume that their IT security is enough to cover the bases of OT security. Considering that 48% of the companies surveyed faced OT security incidents in 2022, while 47% of the companies surveyed faced IT security incidents in 2022, it's clear that there is a discrepancy between management's perception and the reality of the world. Hackers are advancing in leaps and bounds and have set their sights on vulnerabilities that are exposed as companies play catch up in modernizing their equipment in order to remain a competitive force within their verticals. On top of that, 94% of IT incidents have impacted the OT environment within these organizations as well. Demonstrably, IT solutions do not cover the vulnerabilities of OT security, whereas IT problems do span both sectors and negatively impacts OT security. This situation is unsustainable to say the least. They need to understand the critical importance of protecting the security of both IT and OT environments, and that commitment and support from management is instrumental to the success of an OT security plan.

## Proactively Mitigating Cybersecurity Complexity Can Reduce Negative Impact

There are many negative consequences that stem from cybersecurity complexity, and many organizations deal with this as a matter of operational routine. The main victim is the process time—47% of companies surveyed reported that their process time is lengthened substantially. Germany suffered in this area the most at 52%. In the realm of manufacturing, the damage this causes an organization can be quite devastating, both financially and reputationally. In addition to that, organizations also have to spend more on maintenance costs as well, a problem that 44% of organizations face. Again, integration is another issue, as 41% suffer from too little integration across solutions. There are increased manpower costs as well, affecting organizations at an average of 40%. Lower threat detection and response efficacy has the widest range, with 28% of companies from Germany finding this a challenge, whereas 45% of Japanese companies are hit by this issue. Increased human error has been reported at an average of 37% and a wider threat surface has impacted 31% of the companies surveyed.

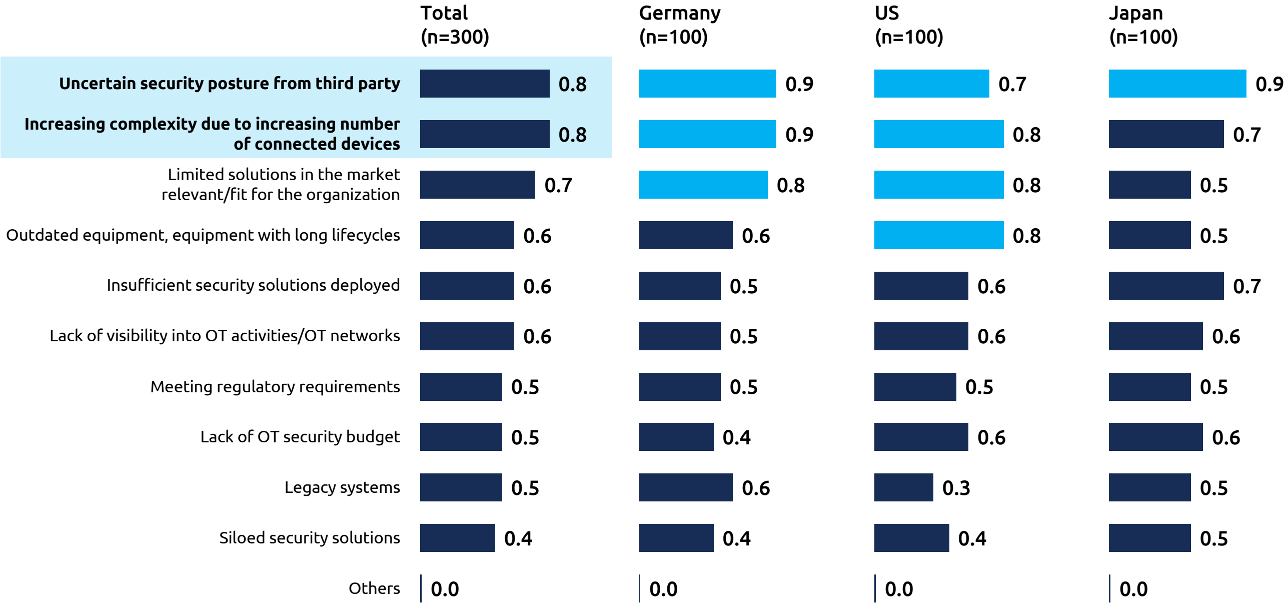
INSIGHT 2

# New Defense Requirements in OT Cybersecurity to Address Specific Challenges

Aside from increasing complexity, enterprises also face new attack methods, legacy equipment, an ever-evolving technological environment, and resource constraints. According to this research survey, these are the biggest challenges faced in securing ICS/OT technologies and processes. They are ranked as such:

1. **Uncertain security posture from third party**
2. **Increasing complexity due to increasing number of connected devices**
3. **Limited solutions in the market relevant/fit for the organization**
4. **Outdated equipment, equipment with long lifecycles**
5. **Insufficient security solutions deployed**

## TOP OT CYBERSECURITY CHALLENGES



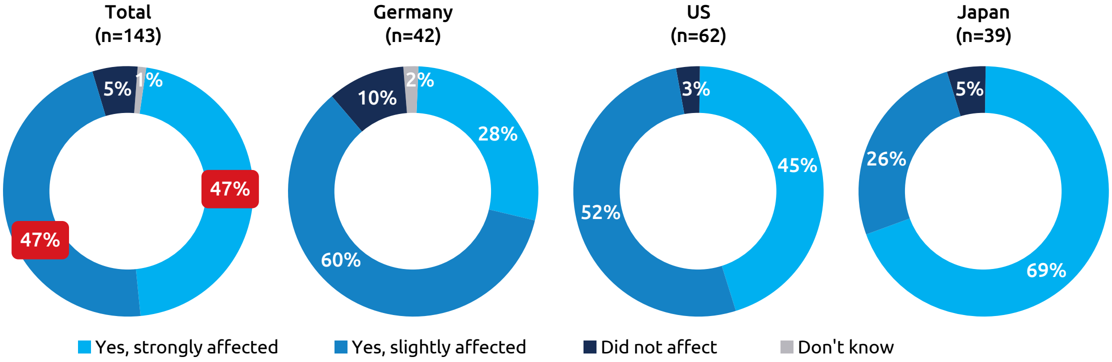
*Q - What are the top OT cybersecurity challenges faced by your organization? Please select top 3 answers. (ranked average score)*

*Source: Frost & Sullivan*

## IT SECURITY INCIDENTS AFFECT ORGANIZATION'S OT ENVIRONMENT

**94%**

of IT security incidents have also impacted the OT environment



*Q - Did these IT security incidents also affect your organization's OT environment?*

*Source: Frost & Sullivan*

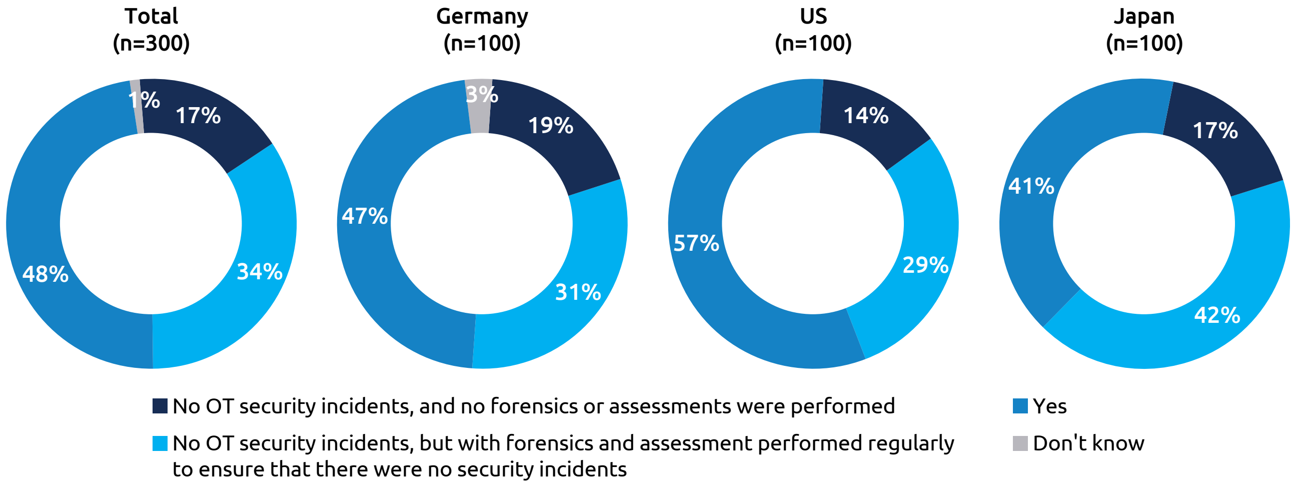
Enterprises believe that the greatest challenge is the element of the unknown that a third-party supplier brings into the supply chain. Sophisticated hackers will search for the weakest links in the supply chain and conduct supply chain attacks through these trusted companies. Second, the ever-increasing number of connected devices, along with legacy and aging ICS/OT technologies, open up even more avenues for enterprises to be attacked. Notably, as OT facilities face the fact that traditional IT security technologies were not designed for control systems and can cause disruptions in ICS/OT environments, organizations are looking for a solution that fits ICS-specific controls to protect their priority assets.

## Organizations Should Integrate IT-OT Joint Defense Into Their Security Plans

Ransomware attacks on organizations like Colonial Pipeline and JBS Foods have drawn attention to the dangers IT attacks pose to OT systems. Though these attacks may not initially target OT systems, a compromise on IT systems can force OT teams to manually shut down operations for security reasons, leading to indirect impact on OT. 94% of surveyed enterprises acknowledge the likelihood of IT security incidents impacting the OT environment. With ransomware being capable of lateral movement, relying solely on either OT or IT systems is insufficient. These incidents underscore the urgency of incorporating IT-OT fusion defenses in security strategies.

However, according to the survey of this research, 48% of organizations reported experiencing ICS/OT security incidents in 2022, while 17% stated that they had not experienced any, but had not conducted any forensic or security assessments either. Conversely, only 34% of organizations reported having completed detailed security incident investigations and assessments, stating that no incidents had occurred. In reality, a small number of companies may appear secure on the surface but have not actually implemented security assessments or forensics activities, so the actual situation of companies experiencing ICS/OT security incidents may be more severe than reported. For example, 57% of companies surveyed in the US region reported ICS/OT security incidents, and there may also be some companies that have not yet detected ICS/OT security incidents. This highlights that ICS/OT security is an issue that corporate leaders must urgently address in the future.

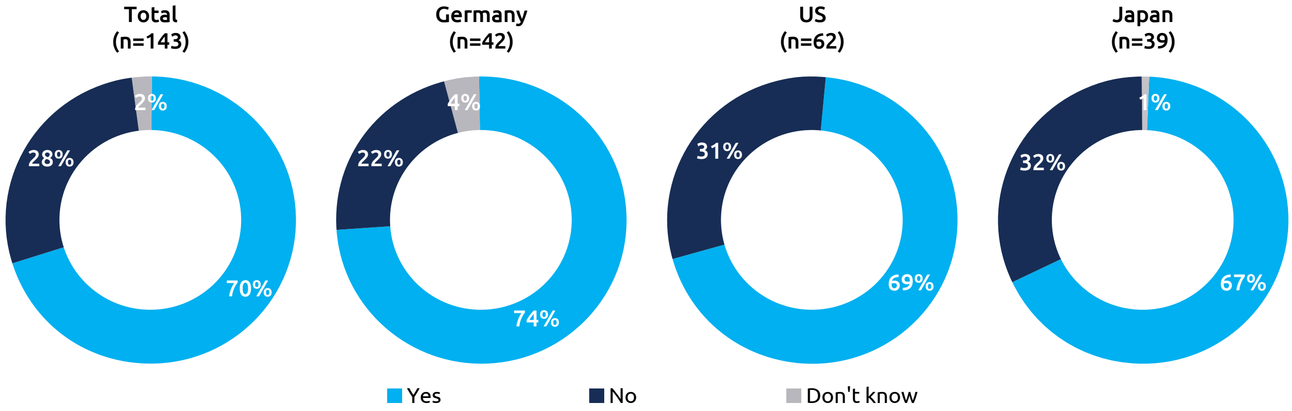
## ORGANIZATIONS WHO EXPERIENCED AN OT SECURITY INCIDENT



*Q - Has any OT security incident occurred in your organization in the last 12 months?*

*Source: Frost & Sullivan*

## ORGANIZATIONS WHO EXPERIENCED DATA OR OPERATIONS HOSTAGE



*Q - Has your data or operations ever been held hostage?*

*Source: Frost & Sullivan*

## Strengthening an Organization's Resilience Plan Can Mitigate Impact

When asked "Has your data or operations ever been held hostage?", 70% of organizations responded that they have experienced data or operations hostage. For years, attacks similar to ransomware have resulted in significant losses and economic damage. The most common tactic is holding companies' data and operations hostage, which echoes what was discussed in the previous paragraph regarding data only reflecting a part of reality, the tip of the iceberg with undiscovered danger lurking beneath.

The organization should not assume that OT hacker attacks will never occur, but rather must consider how to respond in the event of such an attack. Therefore, based on lessons learned from past crises, the organization should provide innovative and adaptable solutions for future OT disruptions. The development of a resilient plan for the organization must be forward-looking and require continuous learning and revision based on experience.

### Respond to Frequent Attacks with Automated Tools

Aside from cybersecurity complexities and the time, manpower and money dedicated to solving the problems that arise, organizations are also under siege from malware and ransomware attacks. In fact, 20% of organizations reported dealing with ransomware attacks on a weekly basis and 19% reported experiencing virus or malware infiltration on a weekly basis. In the last year, 70% of organizations had their data or operations held hostage by malicious actors. Organizations facing frequent cybersecurity attacks, coupled with a shortage of manpower, must rely on more automated cybersecurity tools to quickly respond.

### ORGANIZATIONS EXPERIENCE REPEATED OT SECURITY ATTACKS

| | Frequency of OT Security Incidents | | | | | |
|---|---|---|---|---|---|---|
| **Incident** | **Weekly** | **Monthly** | **Quarterly** | **Half-Yearly** | **Yearly** | **Unsure** |
| Virus or malware infiltration | 19% | **38%** | 31% | 5% | 5% | 2% |
| Ransomware attack | 20% | **26%** | **26%** | 17% | 11% | 0% |
| Vulnerability of unpatched systems | 17% | 24% | **41%** | 15% | 12% | 0% |
| Phishing emails | 15% | **39%** | 28% | 7% | 11% | 0% |
| Advanced Persistent Threat (APT) attack | 14% | 32% | **34%** | 16% | 2% | 2% |
| Distributed Denial of Service (DDoS) attack | 18% | **33%** | 26% | 21% | 3% | 0% |
| Human Error (unintentional) - Employee Actions | 17% | 30% | **33%** | 17% | 0% | 2% |
| Malicious Motives - Employee Actions | 12% | 32% | **38%** | 8% | 4% | 6% |
| Identity theft, fake login credentials | 16% | **40%** | 20% | 16% | 7% | 2% |
| Third-party vendor or supplier compromise | 18% | **33%** | 31% | 11% | 4% | 2% |

*Q - How often did these OT security incidents occur in your organization over the last 12 months? (Base Varies)*

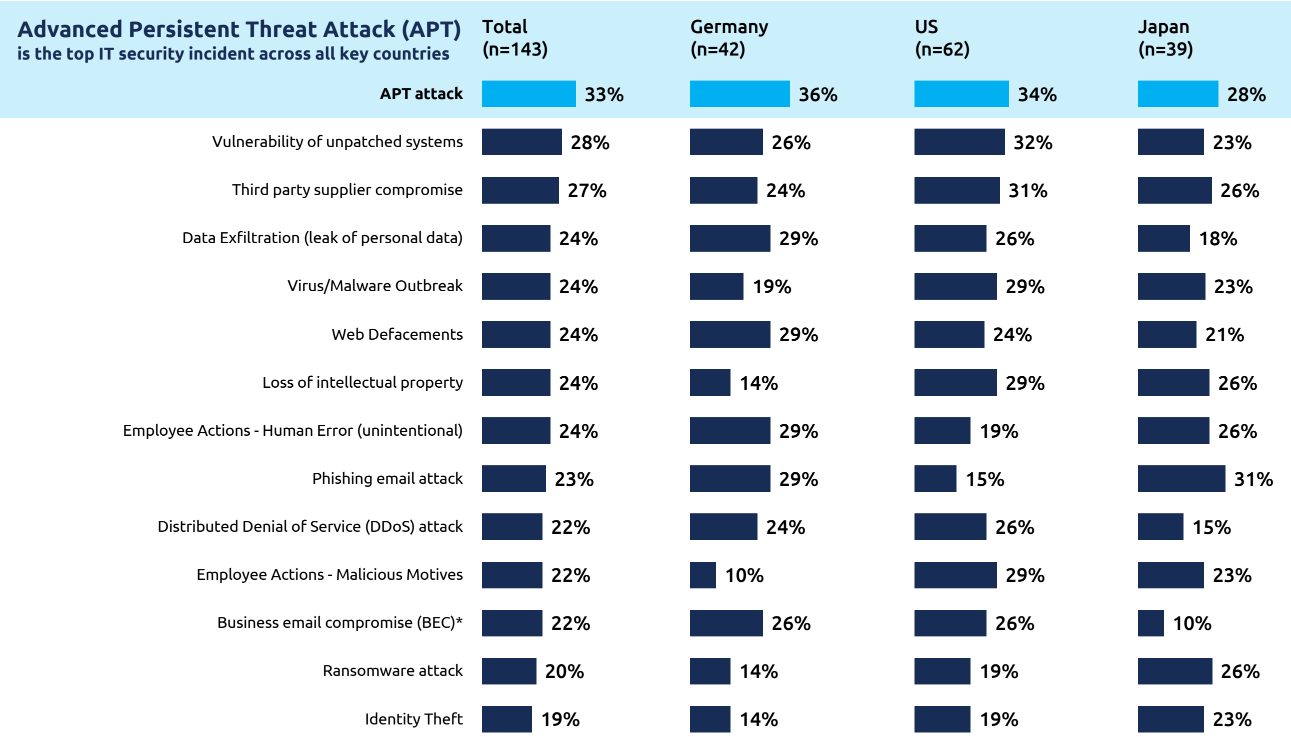
*Source: Frost & Sullivan*

**INSIGHT 3**

## Take Extra Precautions for New Assets in the OT field

In the realm of IT, APT (advanced persistent threat) attacks rank as the highest IT security incident in all 3 countries. The problem with this type of attack is that its goal is to establish and maintain access over time; this is not a hit and run, but a malignant poison nested within the organization. Germany has suffered the most from this type of attack at 36%.

## TYPE OF IT SECURITY INCIDENT EXPERIENCED

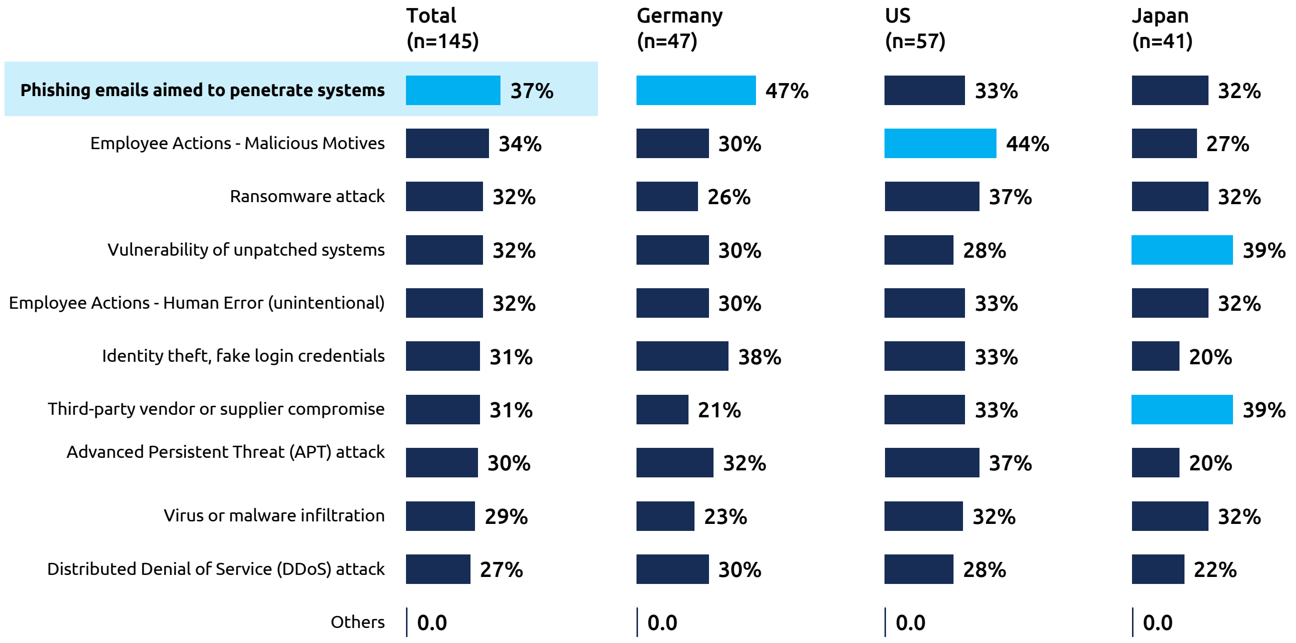


*Q - Which of the following IT security incidents have you encountered in your organization in the past 12 months?*

*Source: Frost & Sullivan*

On the other hand, OT attacks mainly consists of phishing emails that are aimed to penetrate systems by using the naivete or carelessness of workers within the company. Again, Germany suffers from this type of attack the most, with 47% of their companies falling victim. Within the US, employee actions with malicious motives make up 44% of OT incidents. Therefore, US companies are more likely to deal with a situation where the call is coming from inside the house. In Japan, their greatest weaknesses are actually twofold: the vulnerability of unpatched systems and third-party vendor or supplier compromise. Legacy systems may not have connectivity capabilities or may deliberately be kept offline to maintain security and allow the machines to keep working. However, in keeping these walls up to keep out danger, they also block themselves off from updated security measures that can help them if they are successfully infiltrated. Third-party vendor or supplier compromises are issues where equipment from another company that enters the factory work floor can contain malware or viruses that can damage the organizations' systems. These two types of security incidents make up 39% of the OT incidents they must handle in Japan.

## TYPE OF OT SECURITY INCIDENT EXPERIENCED



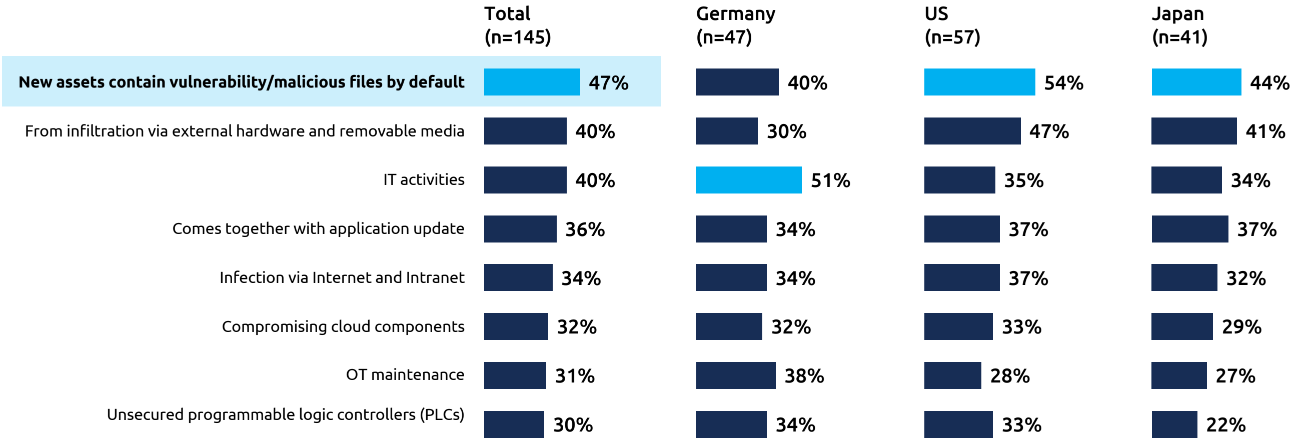
*Q - Which of the following OT security incidents have you encountered in your organization in the past 12 months?*

*Source: Frost & Sullivan*

## Most OT Security Incidents Come from New Assets

New assets are where the majority of OT security incidents stem from, as they contain vulnerabilities, and they can be carrying malicious files by default. In the US, this is an issue for 54% of the sample size, whereas in Japan this happens 44% of the time. Germany is the outlier here, with 51% of their OT security incidents stemming from IT activities instead of from new assets. These challenges result in both financial losses and badly compromised productivity.

## SOURCES OF THE OT SECURITY INCIDENTS

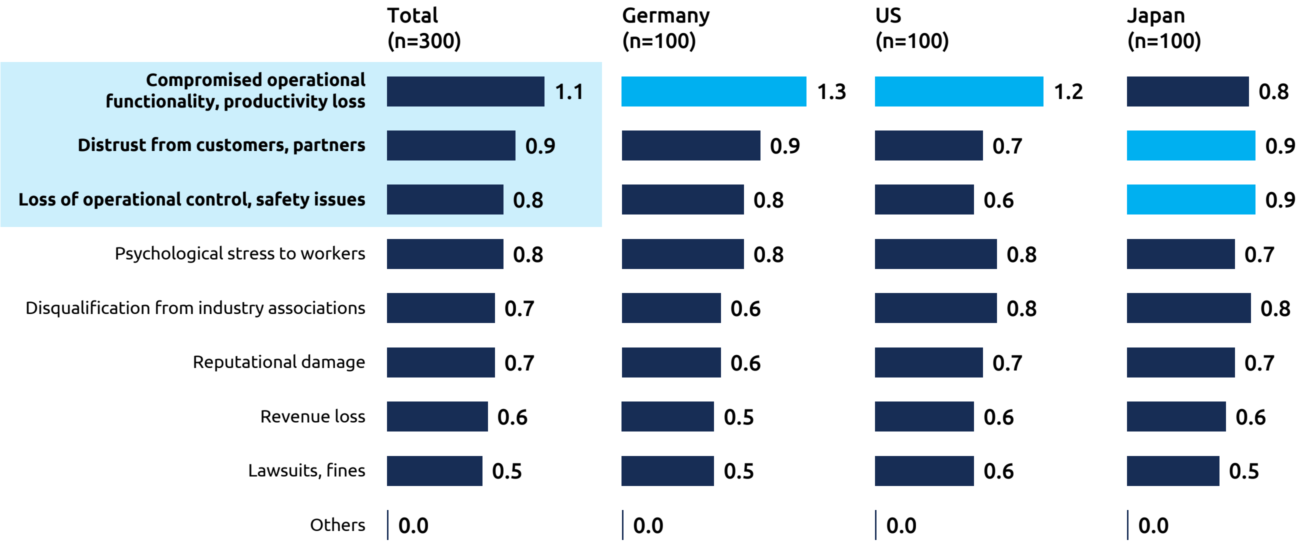


*Q - What are the sources of the OT security incidents that occurred in your organization from the past 12 months?*

*Source: Frost & Sullivan*

Despite these heavy financial losses, organizations are most concerned about productivity loss instead. The impact of security incidents on productivity ranges from compromised operational functionality and literal productivity loss, to distrust from customers and partners and to loss of operational control and safety issues. There's also the psychological stress to workers, disqualification from industry, reputational damage, revenue loss, and lawsuits or fines to contend with. All told, the impact of these security incidents is multifaceted and very difficult to recover from.

## MOST CONCERNING IMPACT OF SECURITY INCIDENTS



*Q - Which of the following impacts from security incidents is your organization most concerned about? Please select top 3 answers. (ranked average score)*

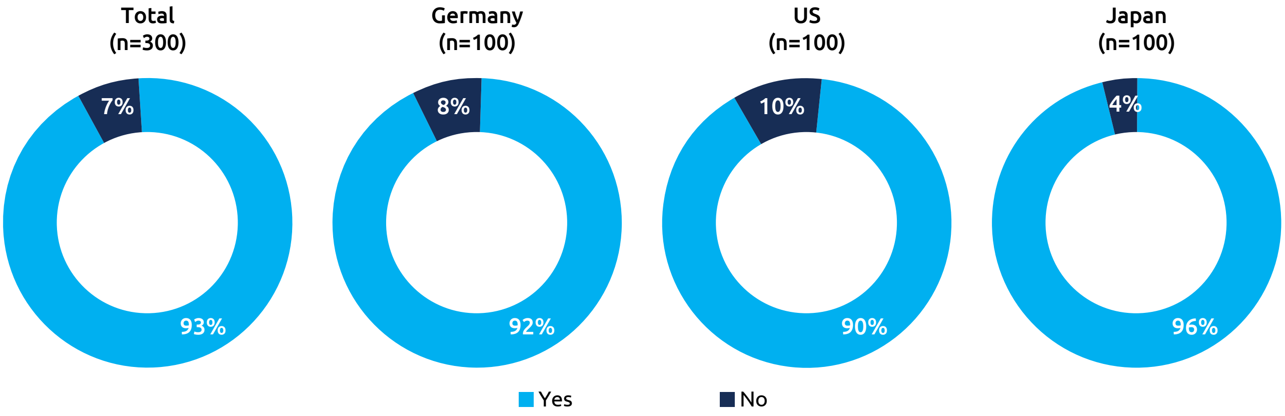
*Source: Frost & Sullivan*

## INSIGHT 4 OT-specific Cybersecurity Solutions are Necessary

According to the study, 93% of companies have already used cybersecurity solutions, which have been applied in OT environments. As mentioned in the first chapter, this shows that companies have increased their cybersecurity awareness for the OT environment and deployed solutions to avoid potential losses. However, it raises questions about why cybersecurity incidents still occur frequently. Based on our observations, the potential factors are as follows:

1. **Using IT solutions rather than OT cybersecurity solutions in the OT environment. Around 70% of organizations are considering reusing previously deployed IT solutions in the OT space.**
2. **Insufficient manpower. Japan has markedly minimal staff assigned to security. In fact, their average is only one staff member for every 101-200 devices, and the most severe situation has 1 staff member for every 301-400 devices.**
3. **Incomplete deployment of solutions. 61% of organizations have unprotected Windows devices.**
4. **Human error.**
5. **Outdated systems unable to receive enough technical support.**

### CURRENTLY USING CYBERSECURITY SOLUTIONS

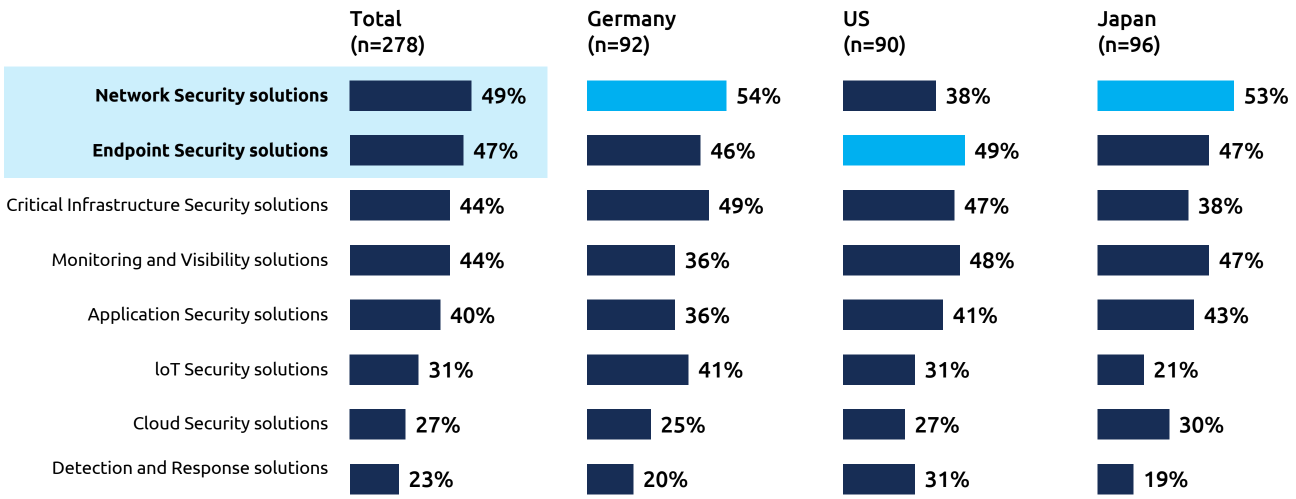


*Q - Is your organization currently using cybersecurity solutions for OT security?*

*Source: Frost & Sullivan*

Given that many organizations have deployed cybersecurity solutions, it is important to determine which solutions are most important for organizations. 49% of respondents stated that Network Security solutions have been deployed, followed by 47% for Endpoint Security solutions. Third place was tied between 44% for Critical Infrastructure Security solutions and 44% for Monitoring and Visibility solutions. In general, the manufacturing industry considers the most effective way to prioritize OT defense is through the use of firewall and intrusion detection products, followed by endpoint protection, then protection of critical infrastructure such as production line machines, and lastly, monitoring and visibility solutions for cybersecurity.

## CYBERSECURITY SOLUTIONS USED FOR OT SECURITY



*Q - Which of the following cybersecurity solutions are currently being used in your organization for OT security (by category)?*

*Source: Frost & Sullivan*

However, deploying an endpoint protection solution typically takes 3 to 6 months for solution validation, in order to learn its workings and how to integrate into the organization's existing systems and workflows. For example, 14% of endpoint protection respondents said they need 3-6 months. Network security solutions had 20% of respondents stating they need 3-6 months. Considering that 20% of organizations experience ransomware attacks on a weekly basis, this amount of time taken to deploy a protection solution is a compounding issue for organizations. The above data shows that companies need a more perfect OT security solution in order to greatly simplify their environment and reduce deployment or functional validation barriers, especially to avoid overlapped workflows.

## TIME TAKEN TO VALIDATE A SOLUTION

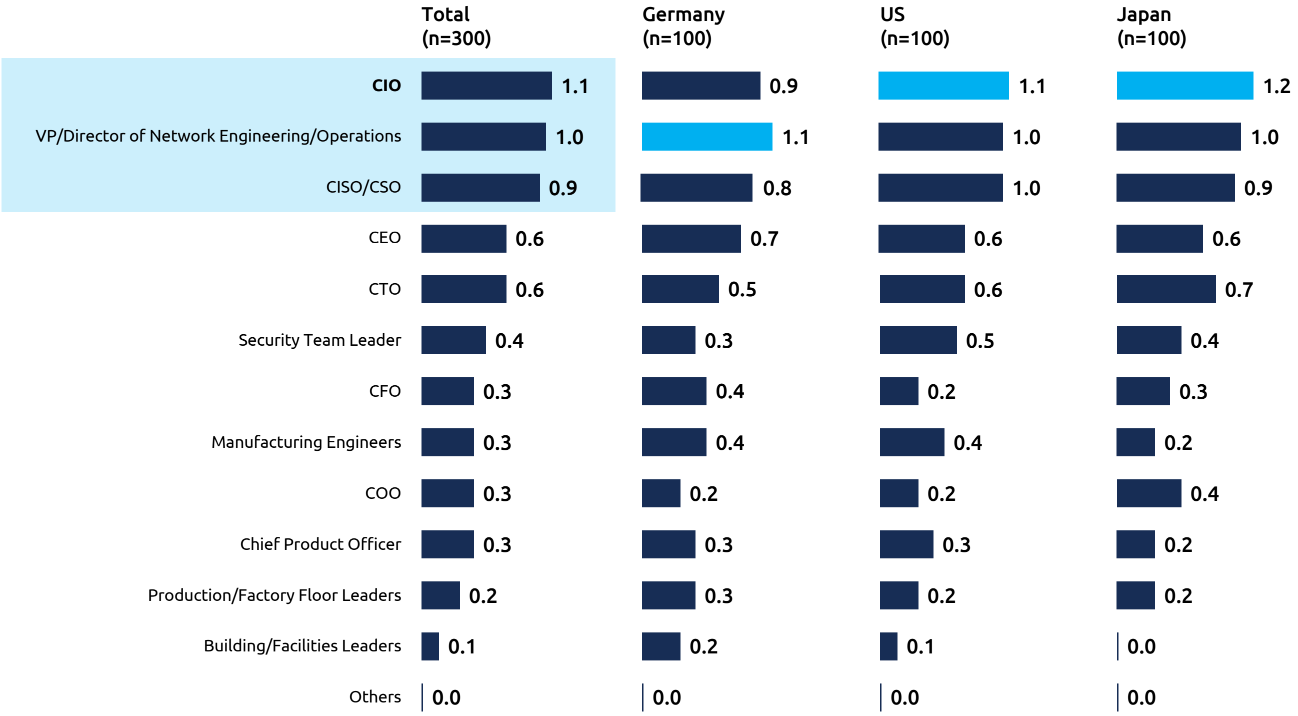
| | Time Taken To Validate a Solution | | | | | |
|---|---|---|---|---|---|---|
| Incident | Less than a month | Between 1-3 months | Between 3-6 months | Between 6-9 months | Between 9-12 months | More than 12 months |
| Endpoint Security solutions | 13% | 12% | **14%** | 1% | 2% | 1% |
| Network Security solutions | 5% | 11% | **20%** | 6% | 3% | 0% |
| Critical Infrastructure Security solutions | 3% | 11% | **17%** | 8% | 1% | 0% |
| Application Security solutions | 7% | 8% | **14%** | 8% | 0% | 1% |
| Cloud Security solutions | 4% | **9%** | 5% | 5% | 2% | 0% |
| loT Security solutions | 3% | 7% | **12%** | 6% | 1% | 0% |
| Monitoring and Visibility solutions | 6% | **17%** | 12% | 3% | 2% | 1% |
| Detection and Response solutions | 3% | 6% | **8%** | 3% | 1% | 0% |

*Q - How long does it take to validate a solution in each of the following categories? (Base: Total (n=300))*

*Source: Frost & Sullivan*

The Vice President/Director of Network has the most influence on a company's approach to cybersecurity, closely followed by the CISO, CSO, and CIO. Thus far, most organizations use endpoint security solutions, with 88% of companies following this strategy.

## OT CYBERSECURITY DECISION MAKERS

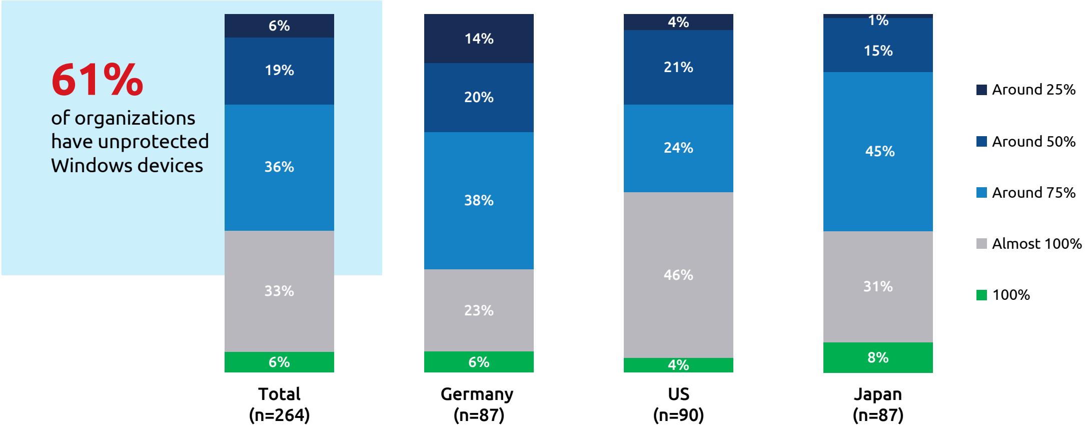


*Q - Which internal leaders have the most influence on your organization'sOT cybersecurity decisions? Please select top 3 answers. (ranked average score)*

*Source: Frost & Sullivan*

However, not all companies take the opportunity to protect their devices, specifically when it comes to Windows devices. Many of them have unprotected Windows devices (61% on average) and only 6% of organizations have 100% of their Windows devices protected by endpoint security solutions. It is up to the vendors to expand their services and offerings in order to encourage adoption of greater security solutions in the coming years. Even though incidents are common across the board, many organizations are actually confident of their OT security. This is why publications such as this one is important, to enumerate the actual situation and dangers that are posed to these organizations if they don't take cybersecurity more seriously. We can see how meaningless their confidence is when it comes to actual situations, because when security incidents do occur, most organizations look outward for help and seek external support.

## PERCENTAGE OF DEVICES PROTECTED BY ENDPOINT SECURITY SOLUTION



*Q - Provide an estimate of the percentage of Windows-based PCs and devices protected by any endpoint security solution.*

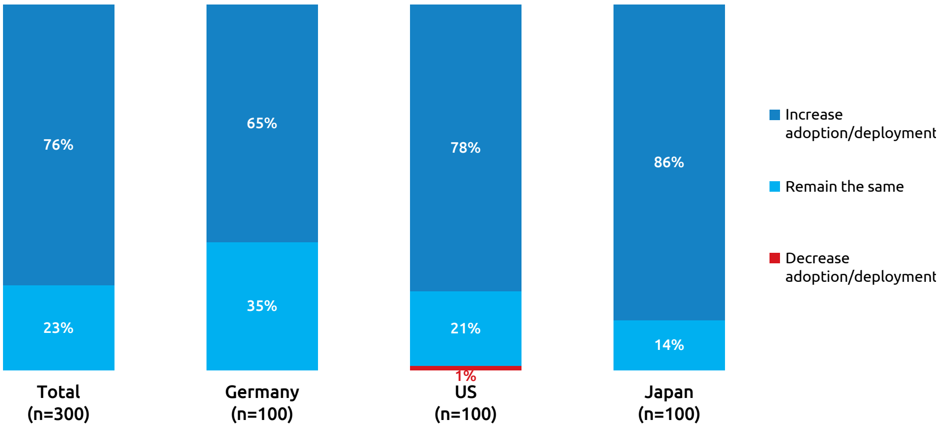
*Source: Frost & Sullivan*

## INSIGHT 5 Budget Allocation for OT Security Will Increase

### The Future of OT Security

However, within the next 12 months, key countries around the world are planning to improve their OT security management and strengthen their protective architecture within themselves. 85% of the participants in this survey have stated that they intend to improve OT security management. To that end, budget allocation for OT security is predicted to increase in the next year. At this point, OT security is still assigned a separate budget allocation from IT security despite the fact that IT-OT convergence is becoming unavoidable. This survey's findings point to a high growth potential for the OT cybersecurity market, with 76% of organizations across key countries reporting that they intend to increase adoption which entails more spending on OT cybersecurity. Their spending would primarily be used on network security solutions, critical infrastructure security solutions and endpoint security solutions. These purchase categories are good foundational measures for companies to take to protect themselves from the onslaught of exploitative attacks that come their way as systems become increasingly connected. Organizations are also looking into monitoring and visibility solutions, application security, cloud security, IoT security and detection and response.

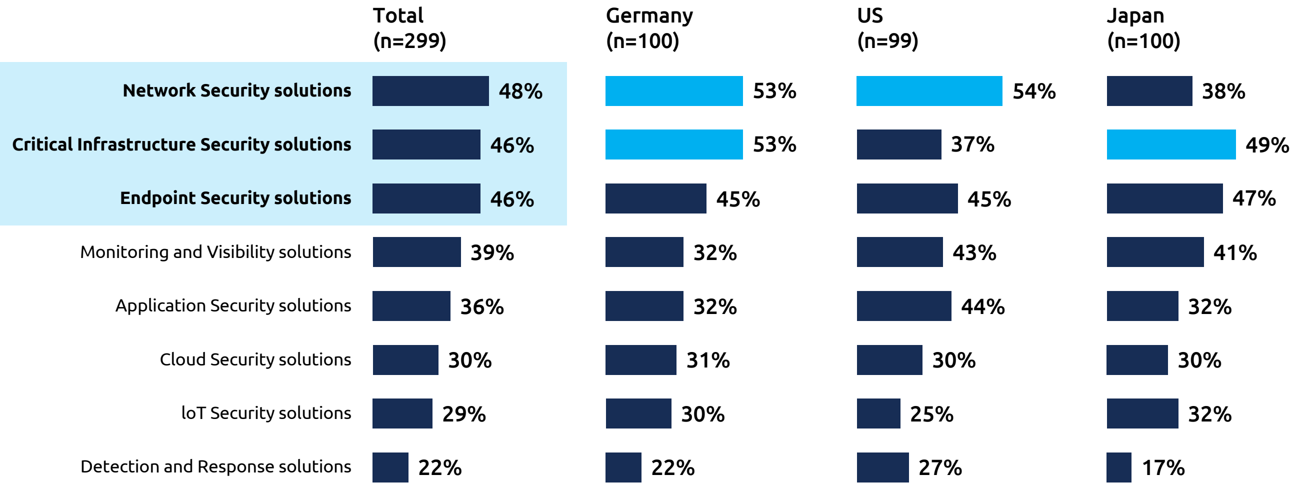
## ADOPTION/DEPLOYMENT OF CYBERSECURITY SOLUTIONS



*Q - Is your organization planning to increase or decrease adoption/deployment of cybersecurity solutions for OT security?*

*Source: Frost & Sullivan*

## CATEGORY OF SECURITY SOLUTION LIKELY PURCHASE



*Q - From which category of security solution will your organization likely purchase in the next 12 months for OT Security?*

*Source: Frost & Sullivan*

## OT Security is Not a Copy of IT Solutions

It is a rational idea for organizations to consider re-using IT solutions that have proven effective in the IT space in the past for solutions to OT security problems. This would be great if it could work, killing two birds (IT and OT security incidents) with one stone (IT solutions). If it could work, there would be much less friction as well because there wouldn't be as much of a learning curve in adopting new security solutions. However, it seems pretty clear that IT solutions will generally not cover up the holes in the OT environment completely enough to offset the amount of risk they would run by recycling old solutions for new problems.

According to the research survey, organizations are recognizing the difference between the enterprise IT and ICS/OT environments. They have not only different system types, but also technology that is not directly cross-compatible and different tasks and risk profiles - even the initial attack vectors, impacts, and event response methods are different. Currently, the main evaluation aspect for choosing a cybersecurity solution can be divided into three aspects:

1. **Strategic aspect:** Overall, aggregate quality is the most important strategic capability.
2. **Operational aspect:** Overall, the ability to integrate with other applications and technologies is the most important operational function.
3. **Performance aspect:** Overall, organizations focus on performance and availability to drive business outcomes.

# Conclusion

We anticipate that cybersecurity in 2023 will be increasingly complex and challenging, due to the emergence of numerous new Ransomware as a Service (RaaS) offerings, such as Black Basta, Pandora, and LockBit 3.0, in 2022. As the RaaS business model and revenue streams mature, attacks on the energy and critical manufacturing sectors are likely to persist, with a significant impact on manufacturers of automobile-related products.

With the drive towards the integration of IT and OT, an increasing number of automobile manufacturers are adopting automation in their manufacturing processes. Future measures to mitigate supply chain attacks will be key for these factories. Despite individual organizations having robust security, the vulnerabilities of third-party partners can still be exploited by attackers. Lack of visibility into the security capabilities of third-party partners was the primary challenge mentioned by organizations in our survey across all major countries/regions.

The Executive Order 14028 “Improving National Cybersecurity” signed by President Biden of the United States opened a key regulation in recognizing the importance of OT cybersecurity. This was followed by the National Security Memorandum signed on July 28, 2021 to enhance the security of critical infrastructure control systems, and the EU NIS 2.0 directive that became effective in December 2020, establishing cybersecurity commitments between governments and critical infrastructure communities. These are seen as useful in raising awareness among stakeholders of the cyber threats to critical ICS/OT systems and promoting the adoption of minimum-security standards. For example, the Transportation Security Administration (TSA) introduced several performance-based directives in 2022 to enhance cybersecurity resilience in the pipeline and railway sectors, and measures to address network needs in the aviation sector. The publication of cybersecurity performance objectives also helps to quantify the return on investment in cybersecurity initiatives.

Fortunately, in this survey study, 85% of organizations plan to improve their OT security capabilities in 2023. 70% of organizations also plan to increase their OT security budget allocation. This is a boost to securing critical infrastructure and smart manufacturing OT security. However, there is a concern that with the IT-OT convergence, about 70% of organizations are considering repurposing IT solutions previously deployed in the OT domain. We believe that for OT cybersecurity complexity, organizations’ security teams should have a higher level of specialized knowledge rather than copying IT solutions to the OT environment. Organizations should prioritize OT proactive defense strategies including supply chain security, asset inspection, endpoint detection and threat intelligence, network segmentation, vulnerability management, patching, and continuous monitoring to prevent potential threats. Based on OT zero-trust solutions (such as network segmentation, virtual patching, trust lists, asset hardening, and security inspections), providing a superior baseline of protection by elevating the cybersecurity standards of the network and assets from the ground up, we believe organizations can better respond to OT cyber threats that may arise in 2023.

## References

[1] *Ivan Nicole Chavez, Byron Gelera, Katherine Casona, Nathaniel Morales, Ieriz Nicolle Gonzalez, Nathaniel Gregory Ragasa, "LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities", TrendMicro, July 25, 2022.*

[2] *SickKids, "SickKids responding to cybersecurity incident", SickKids, December 19, 2022.*

[3] *Joe Tidy, "Cyber-attack strikes German fuel supplies", BBC, February 01, 2022.*

[4] *MITRE, "System of Trust Framework", MITRE, November 3, 2022.*

[5] *SEKOIA.IO Threat & Detection Research Team, "SEKOIA.IO Mid-2022 Ransomware Threat Landscape", SEKOIA.IO, Jul 28 2022, Accessed Feb 7 2023.*

[6] *Flashpoint Team, "Conti Ransomware: The History Behind One of the World's Most Aggressive RaaS Groups", Flashpoint, Oct 4 2022, Accessed Feb 5 2023.*

[7] *Sumeet Wadhwani, "What Makes the Hive Ransomware Gang That Hacked Costa Rica So Dangerous?", Spiceworks, Nov 18 2022, Accessed Feb 5 2023.*

[8] *Matthew Wopata," 5 Industrial connectivity trends driving the IT-OT convergence", IoT Analytics, August 13, 2019.*

[9] *Stephen J. Bigelow, Ben Lutkevich," What is IT/OT convergence? Everything you need to know", TechTarget, August 2021.*

[10] *Advantech, "Utilizing the ADAM-3600 Edge Sensing Device-to-Cloud Solution to Build an Wastewater Monitoring System with Multi-Point Station Data Transmission", Advantech, May 21, 2018.*

[11] *Patrick Howell O'Neill, "Russia hacked an American satellite company one hour before the Ukraine invasion", MIT Technology Review, May 10, 2022.*

[12] *CISA, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)" CISA, March 2022.*

[13] *Press Briefings "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems", The White House, July 28, 2021.*

[14] *CISA, "State and Local Cybersecurity Grant Program", CISA, September 16, 2022.*

[15] *Press release, "Commission welcomes political agreement on new rules on cybersecurity of network and information systems", European Commission, May 13, 2022.*

[16] *Joe Tidy, "European oil facilities hit by cyber-attacks", BBC, February 03, 2022.*

[17] *Policy and Legislation, "Cyber Resilience Act", European Commission, September 15, 2022.*

[18] *Christopher B. Johnstone, "Japan's Transformational National Security Strategy", CSIS, December 8, 2022.*

[19] *Commerce and Information Policy Bureau, "Japan-Indonesia Policy Dialogue on Smart Industrial Safety Held", METI, October 4, 2022.*

[20] *Commerce and Information Policy Bureau," Japan-Thailand Policy Dialogue on Smart Industrial Safety Held", METI, December 15, 2022.*

txone.com