# Industrial control system (ICS) or operational technology (OT) threat landscape

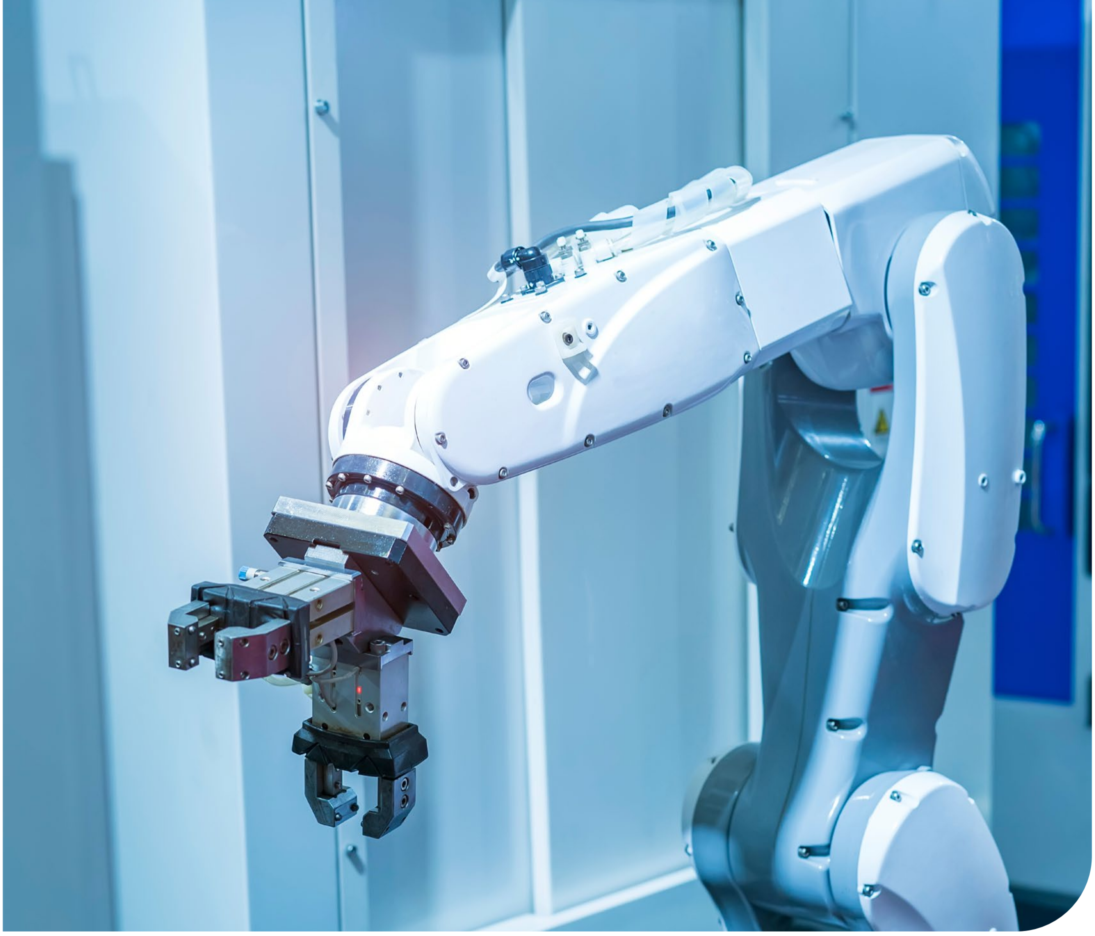
## A new frontier for cyber attacks

April 2024

kpmg.com/in

KPMG. Make the Difference.

# Table of contents



01

# Introduction

Operational technology (OT) covers everything that is linked to monitoring and/or controlling industrial control systems (ICS), supervisory control and data acquisition (SCADA), or programmable logic controller (PLC) environments.

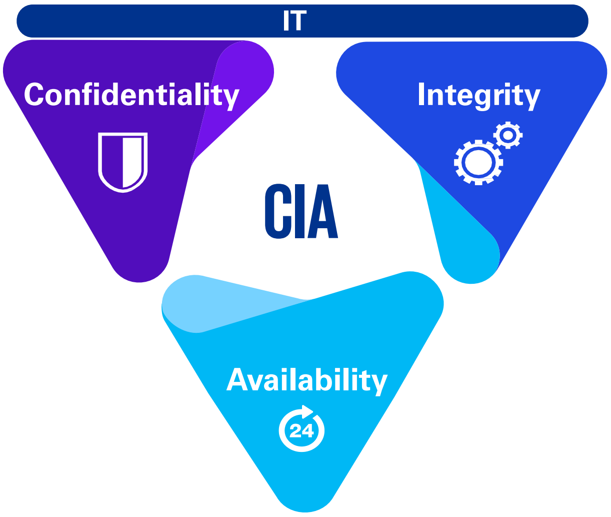
Using OT monitoring or controlling, facility managers and supervisors can manage plant operations smoothly and in a pre-planned way. With a rapid increase in digitisation, OT today spans across internet-enabled sensors, to cloud-based controllers up to different other use cases which are driving the Industry 4.0 revolution and disrupting the traditional Purdue model.

With the widespread use of OT across industries, some of the threats connected to these control and monitoring systems have emerged in sophistication over the last few years.

Today OT systems control almost everything from critical infrastructure such as airports, power plants (including nuclear plants), water filtration systems and manufacturing plants to seemingly innocuous ones such as connected sensors, smartwatches and smart houses.

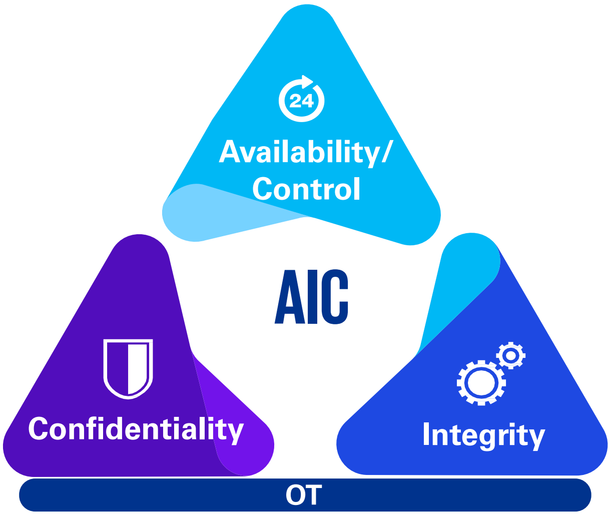
**The typical OT security priority triad often seen in comparison to IT is as below:**

**IT / IOT**



Confidentiality and integrity are the top priority in IT.

**OT / IIOT**



Control and Availability are the top priority in OT.

OT systems were progressively built over a period of 2-3 decades, and were never designed keeping security needs in mind, inherent security controls common in the IT world such as authentication, authorisation and data validation were not implemented in view of prioritising availability over security.

Therefore, attackers and nation-state actors are capitalising on these weaknesses to effect large-scale disruption and facility shutdowns.

Traditionally, plant operators have also relied on isolating or air-gapping OT systems to prevent unauthorised access to them. Air gapping ensured that these systems were digitally isolated from the internet. However, with the advent of Industry x.0 and rapid digitisation fueled by the pandemic, air gapping is no longer a feasible option.

Further, in some cases, an IT-based security approach was transposed on OT systems to secure them, worked effectively for various reasons.

The deployment architecture and unidimensional information exchange present clear barriers to the adoption of IT-based cybersecurity practices such as encryption of data and digital signature

Safety and availability are paramount and compromise of either of the two could lead to catastrophic outcomes and severe regulatory penalties

Legacy OT systems do not support traditional IT protocols, and OEM support for new versions are often not available or the upgrade/update is extremely expensive

IT systems such as ERP and others are often required to be connected to plant systems for operations, monitoring and for demand planning and forecasting.

## What is at stake (value at risk) ?

Recent cyber security incidents in plants have shown that the impact monetarily and reputationally from a cyber security incident is very high –

JBS Meat Supplier

**USD11 million[1]**

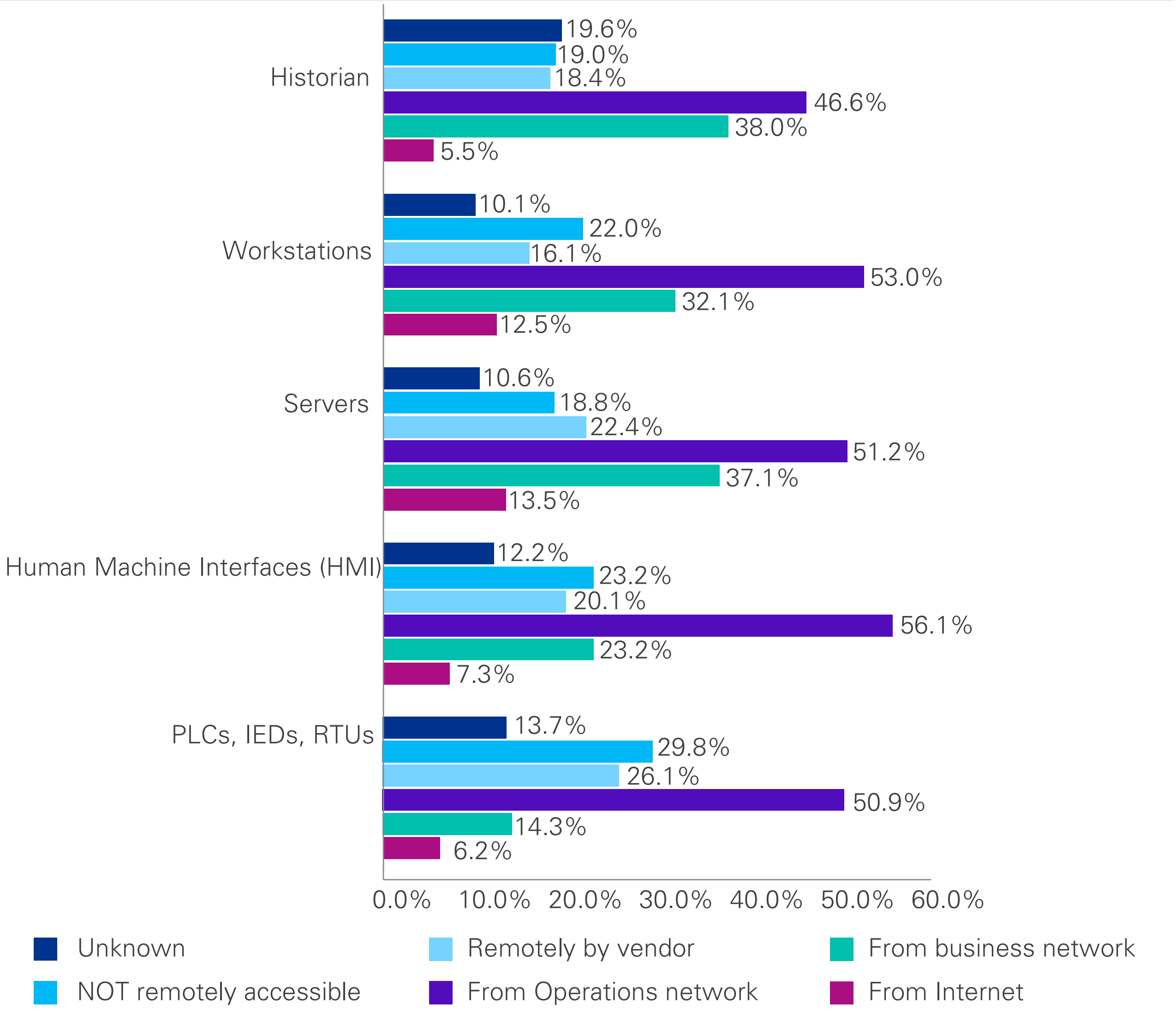
Colonial Pipeline

**USD5 million in ransom (2.3 million recovered)[2]**

Maersk

**USD300 million in losses[3]**

### The KPMG CS2-AI 2020 Survey puts cyber security risk to ICS components as below

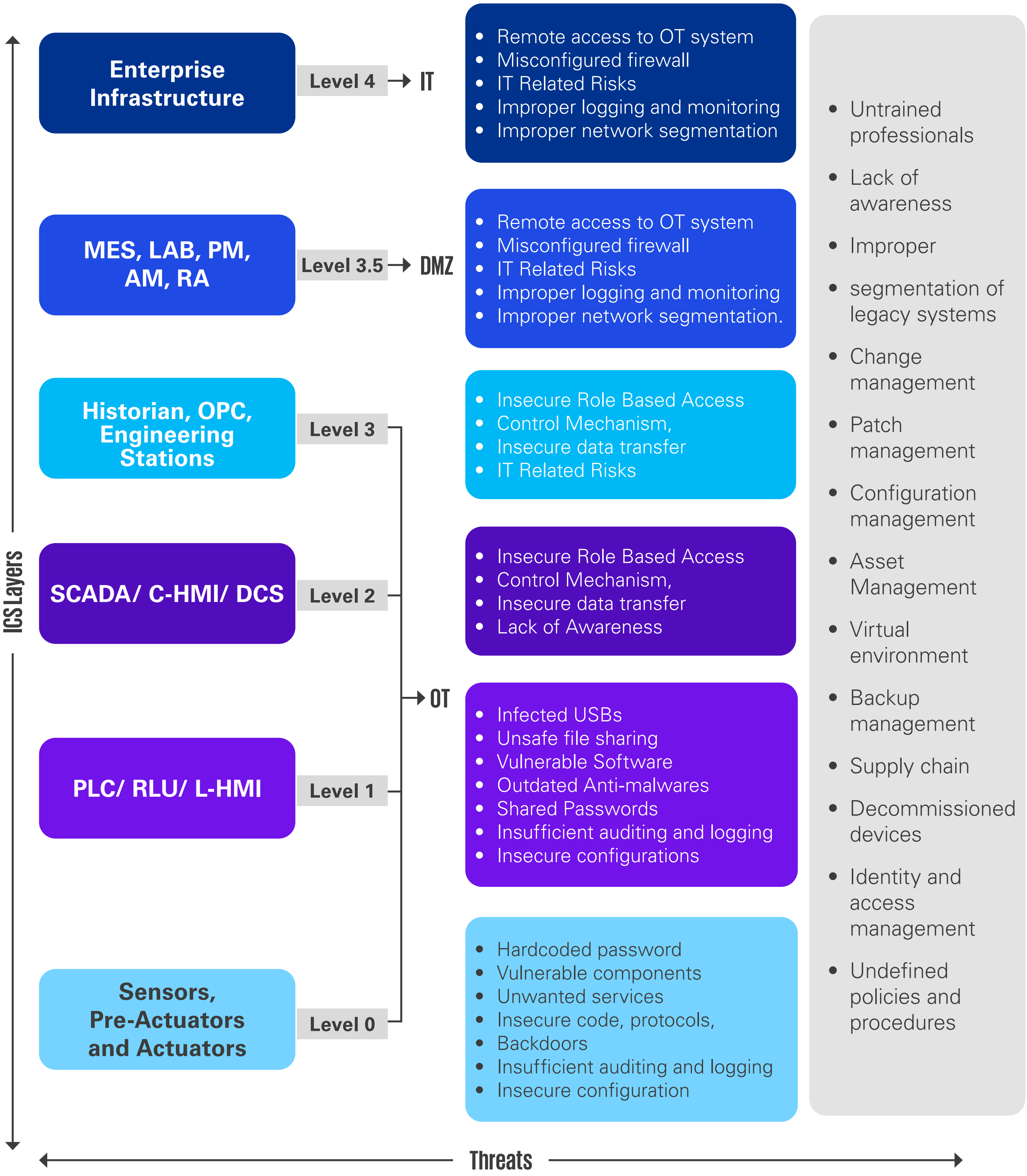


*Source: $(CS)^2$ AI-KPMG 2019 Control System Cyber Security Survey*

In this research, it was found that the digital attacks targeting organisations ICS and OT assets increased by over 2,000 per cent between 2018 and 2020. Ransomware attacks against organisations accounted for 23 per cent of security incidents in the industrial sector in 2020 and ICS vulnerabilities were also 49 per cent more prevalent in 2020 than they were the year before.[4]

1. Meat giant JBS pays $11m in ransom to resolve cyber-attack, BBC News - 2020
2. Attackers Breached Colonial Pipeline Using Compromised Password, Bloomberg - 2020
3. The Cost of a Malware Infection? For Maersk, $300 Million, Data Insider - 2020
4. Tripwire : State of ICS Security /

## Typical OT threat landscape



ICS Layers

**Enterprise Infrastructure** – Level 4 → IT

- Remote access to OT system
- Misconfigured firewall
- IT Related Risks
- Improper logging and monitoring
- Improper network segmentation

**MES, LAB, PM, AM, RA** – Level 3.5 → DMZ

- Remote access to OT system
- Misconfigured firewall
- IT Related Risks
- Improper logging and monitoring
- Improper network segmentation.

**Historian, OPC, Engineering Stations** – Level 3

- Insecure Role Based Access
- Control Mechanism,
- Insecure data transfer
- IT Related Risks

**SCADA/ C-HMI/ DCS** – Level 2

- Insecure Role Based Access
- Control Mechanism,
- Insecure data transfer
- Lack of Awareness

→ OT

**PLC/ RLU/ L-HMI** – Level 1

- Infected USBs
- Unsafe file sharing
- Vulnerable Software
- Outdated Anti-malwares
- Shared Passwords
- Insufficient auditing and logging
- Insecure configurations

**Sensors, Pre-Actuators and Actuators** – Level 0

- Hardcoded password
- Vulnerable components
- Unwanted services
- Insecure code, protocols,
- Backdoors
- Insufficient auditing and logging
- Insecure configuration

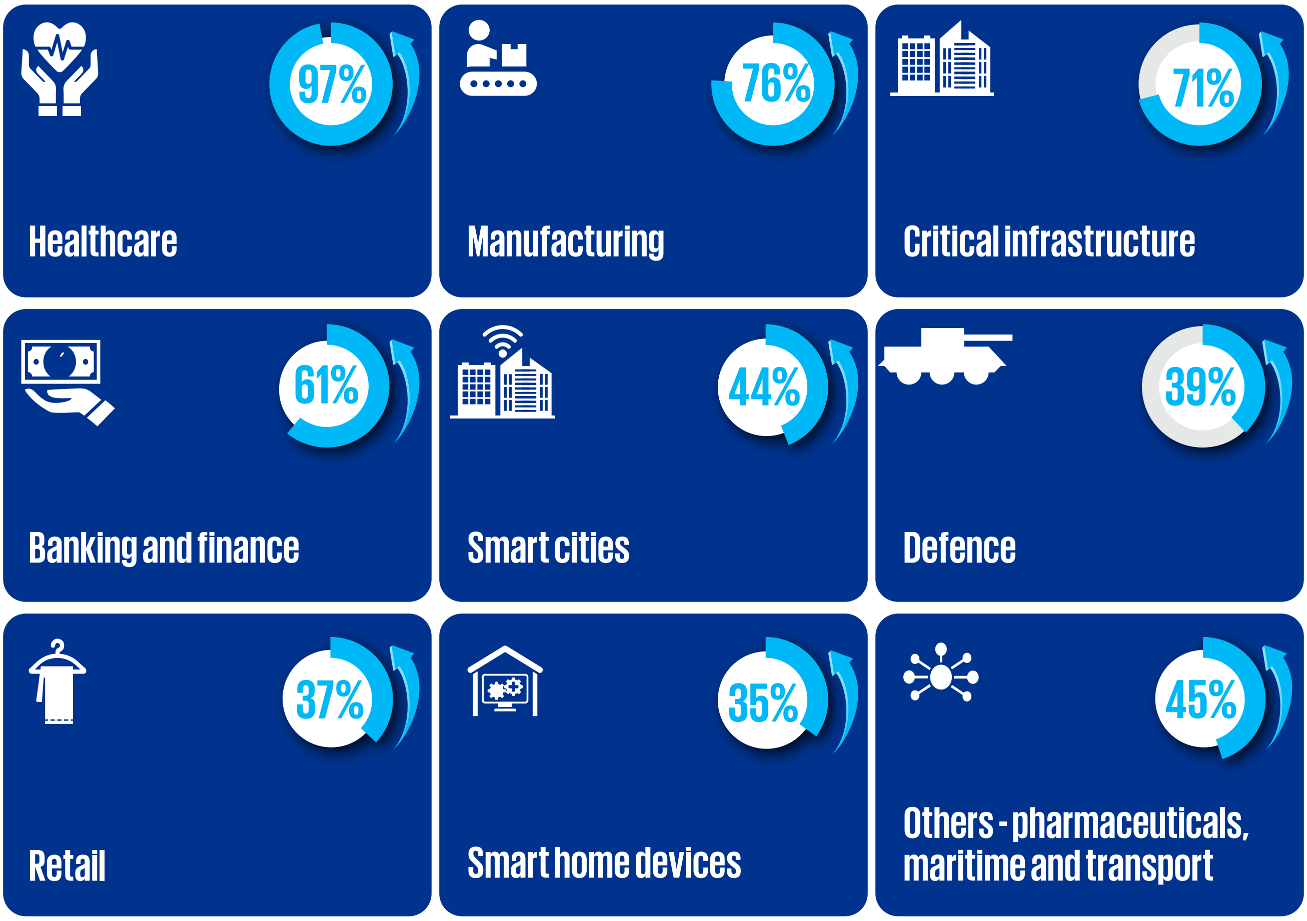
- Untrained professionals
- Lack of awareness
- Improper
- segmentation of legacy systems
- Change management
- Patch management
- Configuration management
- Asset Management
- Virtual environment
- Backup management
- Supply chain
- Decommissioned devices
- Identity and access management
- Undefined policies and procedures

Threats

02

# Defining the threat landscape

## Rising attacks on OT installations across key sectors



% rise of sectors

*Source: Sectrio IoT and OT Threat Landscape Assessment Report – 2022*

*Note: This table captures the percentage rise in cyberattacks on OT installations globally logged in the year 2021 over 2020 as calculated on 31 December 2021 (11:59 PM, PST).*

## Trends in the evolution of OT threats

Between January and November 2021, an unnamed hacker group affiliated to PLA Unit 61486 operating independently targeted multiple OT-based businesses across Southeast Asia. The attack was done ostensibly to gather information on common SCADA system designs. The attackers hijacked a series of resident tools to attack machines involved in SCADA design and management. The tools used included those linked to DLL hijacking, browser hijacking through a fake plugin, keylogger and a downloader. Only native system tools or programs were used in these attacks as attackers wanted to minimise the chances of detection.

In these attacks, in addition to obtaining information related to specific SCADA system configuration information attackers targetteduser credentials and information related to key systems as well. Through lateral movement, the attackers ran scans and collected vital network information as well. Through such attacks, the hacker group is also trying to build a model for targeting businesses that are running similar systems with slightly varying configuration. By using a model-based approach, the effort involved in successfully breaching multiple targets to be brought down which frees up attackers for targeting more P1 (high priority) targets.

Attacks on OT networks require months, if not years of planning. By gaining information on the design and architectural aspects of OT deployments, attackers are trying to reduce the time taken to target OT systems. Further, such APT groups are also well ahead of traditional goals such as stealing IP to new goals such as long term control of the hijacked systems. This includes having the ability to shut down parts of a utility plant at will, increase or reduce output (power or water) and shut down plants completely.

PLA Unit 61486 carries out extensive target network scans to locate weaknesses that it can pass on to its affiliate groups. In some instances, the affiliate group exploits the weakness, plants a malware or steals credentials and reports back to 61486. Threat actors from 61486 will then take over the hijacked systems to steal more information or maintain a backdoor to key systems for future activity.

## Over the years, attacks on the OT networks have evolved gradually from Stuxnet in 2014 to focused attacks such as Colonial Pipeline and JBS Meat Suppliers.

### 2010 - Stuxnet

- Designed to disrupt the SCADA system in ICS environments.
- Uncovered in Iran's nuclear facility and was suspected to have been injected through USB sticks.

### 2014 - Havex

- First occurrence in ICS environments during the spring of 2014.
- Identified to be targeting the OPC servers and was also used as data collection malware.
- Colonial Pipeline, one of USA's largest gasoline, diesel and natural gas distributor, was impacted by a ransomware attack in 2021, May. DarkSide, a Russian cybercrime group was responsible for the attack. Colonial paid a USD4.4 million ransom in Bitcoin (USD2.3 million of it was recovered by the U.S.)

### 2015 - Blackenergy + 2016 - Industroyer

- Blackenergy was initially identified in 2007 as a HTTP based toolkit built to perform DDoS
- (Distributed Denial of Service).
- First occurrence of Blackenergy in ICS environment was seen in Ukrainian Power Grid.
- In December 2016, the Ukrainian Power Grid was again infected with a malware called

Industroyer. The malware was used to create a backdoor in the ICS environment and gain control over the industrial systems.

### 2017 - Triton

The malware was first discovered in Saudi Arabian petrochemical plant.

Malware made it possible for the attackers to take over the systems remotely.

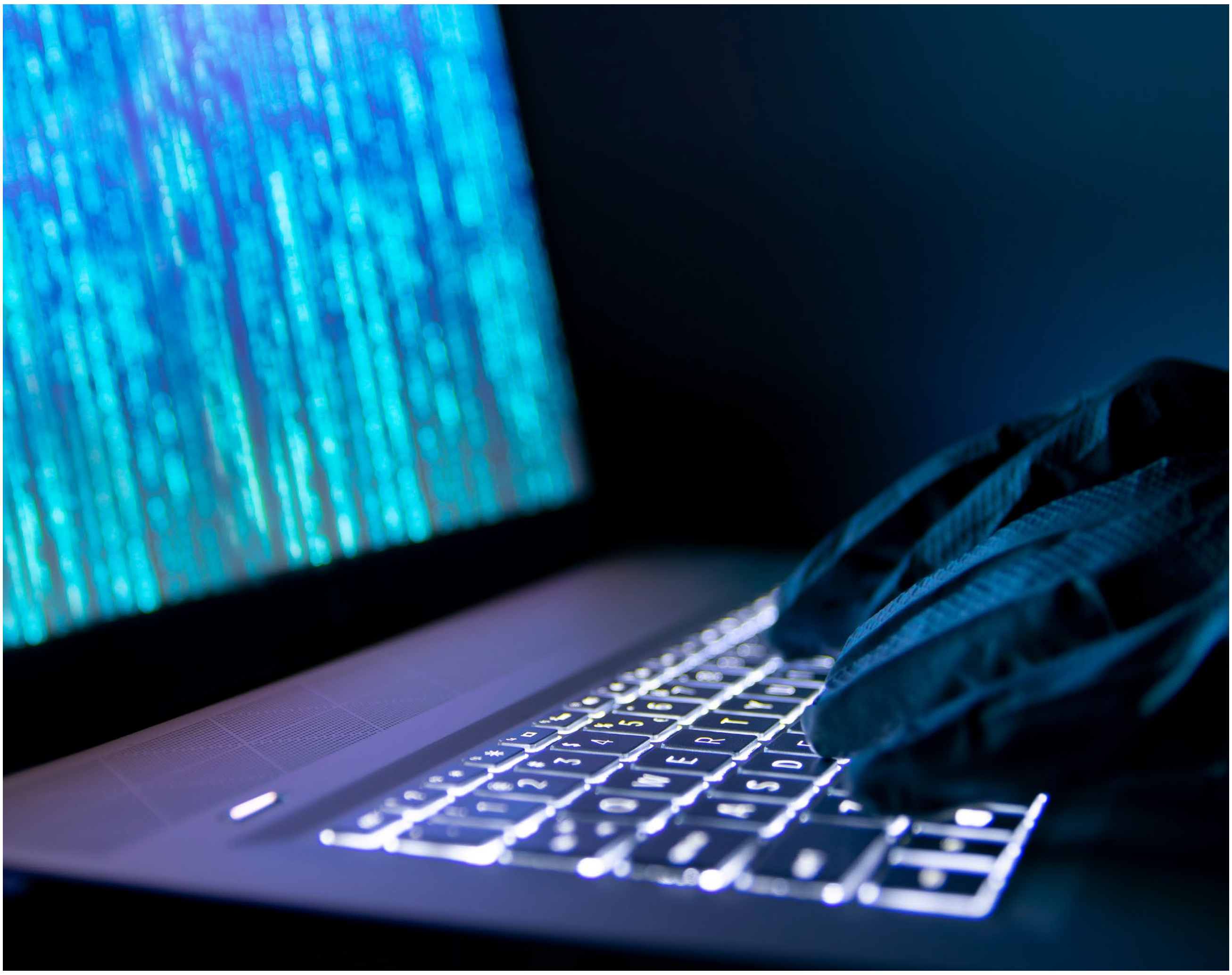
- drinking water at a water treatment facility in Oldsmar. However, the operators inside the facility detected two intrusions from outside the plant and reverted the changes.

### 2018-19 - Shamoon 1, Shamoon 2

- EKANS has been designed to take down the entire network rather than individual systems. The attack is relatively new and is actively targeting ICS environments for financial gain.
- 64 ICS processes were targeted in the ransomwares "kill list".
- 2021 – Colonial Pipeline, JBS, Oldsmar, Florida Water Treatment Facility
- Early 2021, an attacker remotely changed the levels of sodium hydroxide in residential and commercial

### 2020 - EKANS, WannaCry

JBS, the world's largest meat supplier, was attacked by a ransomware group called REvil.This led to a shutdown of plants in Australia, Canada and the U.S. resulting in disruption of one-fifth of their meat processing capacity. However,JBS maintained a backup system and was able to resume operations by restoring the data backup. JBS reportedly paid the attackers an USD11 million ransom.



### Key trends in the evolution of OT cyberattacks in the last decade:

- Attackers have realised that the value at risk in plants is far higher, leading to ransomware becoming more targeted and destructive. Speed of monetisation of cyberattacks is an important consideration for bad actors
- As many as 66 percent of CISOs polled in a June 2022 CISO survey admitted that they do not have sufficient visibility into their networks. Lack of visibility implies lack of control and creates gaps in security posture such as surfaces that are exposed to the internet and can be exploited by attackers.
- Isolated and targeted attacks on OT are often not monetised immediately. Sophisticated actors are focusing on maintaining access to target systemsfor as long as possible
- Direct attacks on OT through targeted attacks, supply chain poisoning or attacks on SCADA and PLC systems result in operational impairment. Attackers use such windows of downtime to put added pressure on victim enterprises to yield to their ransom demand
- Attackers have weaponised the techniques to access, study, map, and eventually exploit the ICS and OT components
- Multi-modal reconnaissance involving the use of dormant malware to study IT and OT networks is providing malware developers and operators with information on target systems and infrastructure.

## Crown jewels that attackers are targeting

The key systems and their impending objectives that are leading to attackers going after OT systems are as below:

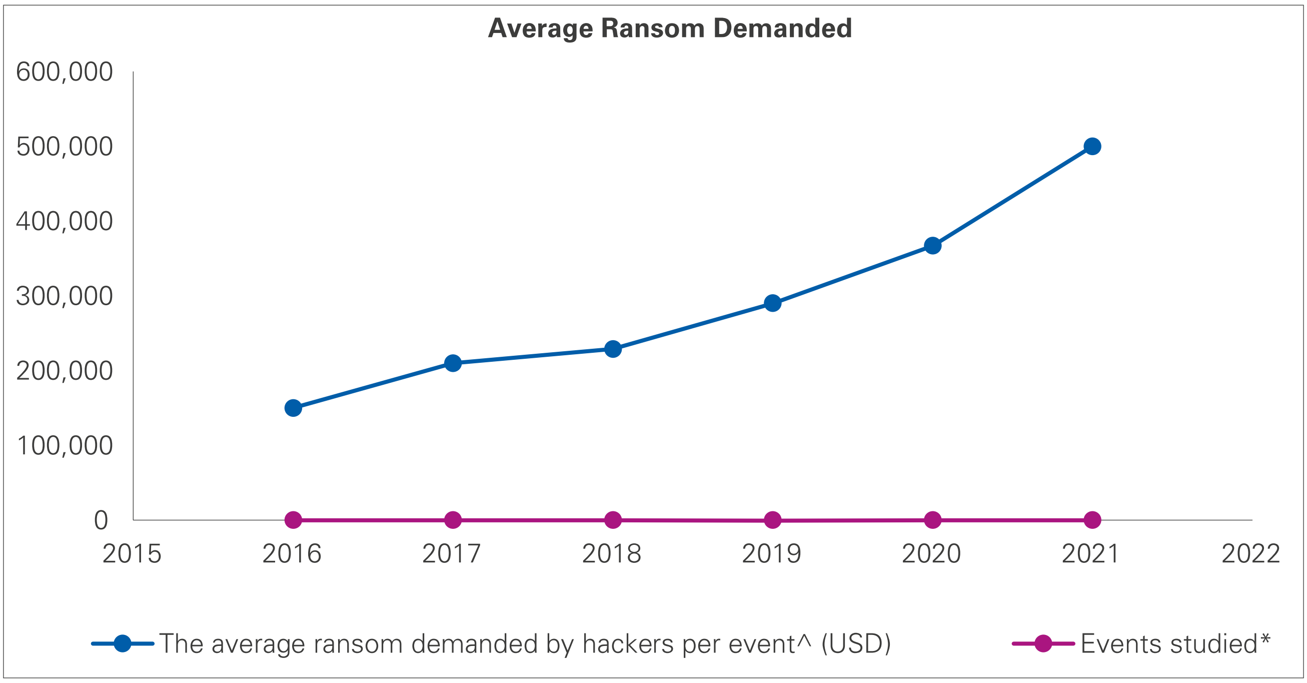
| Sector | Target | Impact |
|---|---|---|
| Manufacturing | Safety systems, IIoT deployments, shop floor, assembly line controllers, HMIs, monitoring systems, PLCs, DCS, protocol converters and field devices | Data theft, ransom, large scale disruption, geopolitical factors for impacting the economy, safety parameter change leading to safety issues |
| Healthcare | Ventilator systems, MRI, Radiology systems, CT Scan, water and oxygen supply systems, elevators, electronic doors, lighting, Emergency Lighting and Medical gas systems | Patient data theft, ransom, disruption of critical / emergency medical equipment |
| Defence | Communication systems, controllers, weapon maintenance systems, SCADA systems linked to onshore hardware and situation monitoring, weapon systems, naval vessels with ICS, radar and power and water treatment systems within bases, position, navigation and timing (PNT) systems | Disruption<br>Misfired Left of launch attacks, compromised command and control of missile systems, malfunction of detection systems such as radars, disruption of position and navigation information to missiles, disruption of inter missile communication |
| Pharmaceutical/ drug manufacturers | Assembly lines, production system controllers and HMIs, Laboratory Information Management System (LIMS), Formulation Systems, Packaging Systems, LAMS, CMS, Laboratory Quality Management System (LQMS) | Disruption of vaccination manufacture and manufacture of critical drugs, Ransom attacks on critical systems, patient data theft, manipulation of pill formulation, revenue diversion, disruption, theft of proprietary recipes and production batch sequence step |
| Power and Utilities | HMIs, SCADA, control systems at various levels, and monitoring systems, Grid function management systems relay Distribution Management Systems (DMS) and Remote Terminal Units<br>Power Meter, Energy Meter, Power Quality Analyzer, Turbine Monitoring System, DCS, Electrical Switchyard Systems, Terminal Acquisition System, smart meter, smart grid, nuclear reactors, nuclear cooling systems | Geopolitical factors for impacting the economy, ransom, data theft, manipulation of bills, and revenue diversion, disabling electricity substation, damage the power grid, uncontrolled reactions in nuclear plants |
| Oil and gas | Flow management systems, production management systems, health, environment, and safety systems, SCADA systems, rail and road systems, corrosion monitoring systems, vibration monitoring system, ESD, Marine oil terminal, crude oil terminal, Dispatch, Fire and Safety, POS, HMU, VFD | Geopolitics, compromise of generation data, disruption of drilling and production systems, disruption fuel stations – POS, disruption of safety systems, leakage of hazardous chemicals |
| Maritime | Ships, navigation and communication equipment, offshore OT installations connected with cargo management, GNSS, GMDSS, Nautical System Support, Propulsion and Power Control Systems (Engine Control Room Console, Bow Thruster Control System, Anchor and Mooring Winch Control System)<br>Power Management<br>CCTV, BNWAS, SSAS, ECDIS, AIS<br>VSAT(SATCOM), VOIP, WLAN | Ransomware attacks, piracy, Manipulation of CCTV network, AIS Data Manipulation or ECDIS Data Manipulation leading to collision, Rogue Man Overboard signals leading to false distress calls, Disruption of communication |

## The rising cost of ransom linked exclusively to OT environments

The cost of ransom has been rising consecutively for the last three years. In 2021, the average cost of recovering a part or whole of the infrastructure was in millions. With companies relying on legacy OT systems for monitoring operations, collecting, and processing data, criminals have understood the importance of OT for businesses, and this has emboldened them to ask for higher ransom payouts after each event.

The willingness to pay on the part of the victims is primarily driven by the loss that a business must incur for every minute a critical facility is not operational. Due to production and supply commitments, OT operators find it easier or cheaper rather to pay out the ransom than to deal with a prolonged loss of production capacity.

### Ransom Demanded By Cybercriminals Between 2016-2021



*Source: Global ransomware damage costs predicted to exceed USD265 billion by 2031," Cybersecurity Ventures, June 3, 2021*

** Number of incidents studied where the information was sufficient to arrive at the ransom numbers*
*^ The ransom demand varies according to the threat actor, size of the data, victim, and complexity of the malware used*

### In correlation to the numbers above the leading ransomware strains by revenue as of 2023 were as below:

| | | | | |
|---|---|---|---|---|
| Conti<br>USD180 million | DarkSide<br>USD90 million | Phoenix Cryptolocker<br>USD85 million | REvil/ Sodinokibi<br>USD100 million | Cuba<br>USD60 million |
| Clop<br>USD75 million | LockBit<br>USD91 million | Hive<br>USD100 million | BlackMatter<br>USD100 million | Ryuk<br>USD150 million |

*Source: Global ransomware damage costs predicted to exceed USD265 billion by 2031," Cybersecurity Ventures, June 3, 2021*

Nearly five years ago, the average cost of ransom demanded by attackers was approximately USD150,000 (this is the ransom sought by the attackers but may or may not represent the amount paid by the victim organisation). Today, the average is in the range of USD500,000 per attack (Based on 120 publicly available reports).

| Year | The average ransom demanded by attackers per event^ (USD) | Why? |
|---|---|---|
| 2016 | 1,50,000 | 19 incidents |
| 2017 | 2,10,000 | 21 incidents |
| 2018 | 2,29,000 | 20 incidents |
| 2019 | 2,90,000 | 16 incidents |
| 2020 | 3,67,000 | 24 incidents |
| 2021 | 5,00,000 | 20 incidents |

REvil and DarkSide commanded the maximum ransom per attack while Babuk and Avaddon, DoppelPaymer, HelloKitty, and Evil Corp were the other groups that placed a huge ransom demand on their victims.

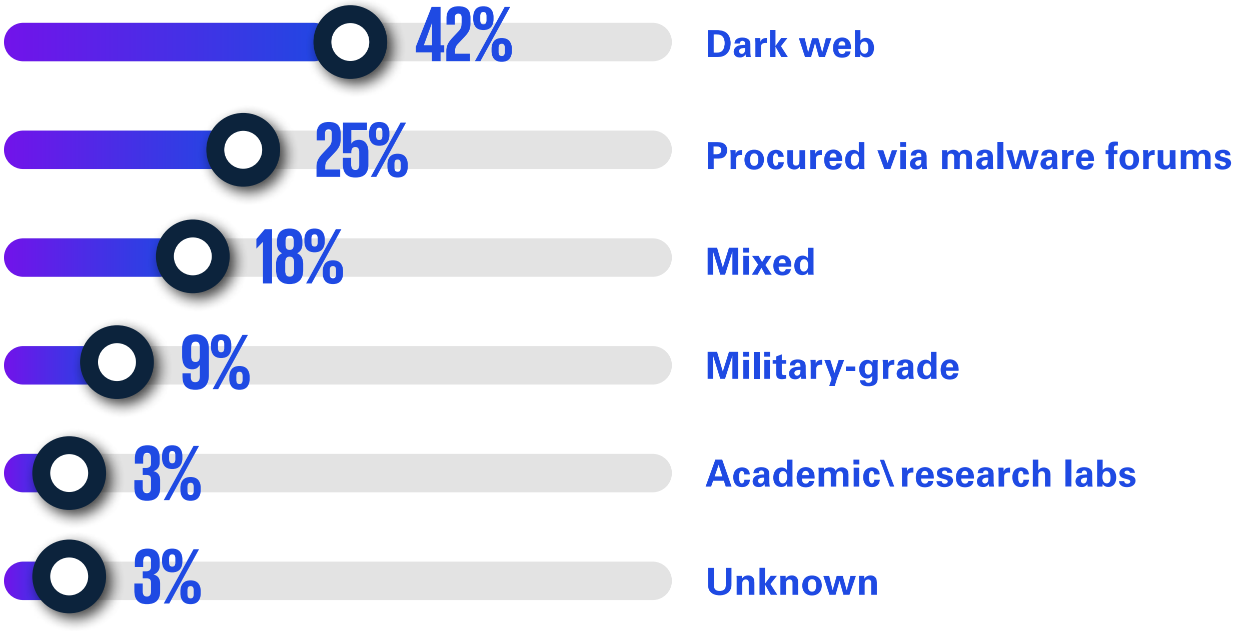
Breakaway APT groups such as those belonging to two clusters whose respective operational epicentres have been mapped to Irkutsk in Russia and Siniju in North Korea have been found to use sophisticated military/defence-grade malware that could be stolen or donated by advanced state-backed cyber offence labs.

In such instances, the ransom demand is often very high, and it can be said with a high degree of certainty that such malware brings revenue for these actors and labs and maybe even other state intermediaries.

03

# Threat actors, origins and detection

## Origin of malware



*Source: Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022*

Dark Web continues to be a major source of malware for attackers. This means that most of the malware used in attacks on OT infrastructure had passed through the Dark Web at some point before they were deployed in target organisations.

In 2021, there was an increase in the development and release of malware developed in what seems to be academic or research facilities. This is because many of these malwares had code inserts and traits that do not belong to any known malware labs run by known cyber criminals who have been signaturised in the past.

KPMG in India were able to categorise malware based on observed traits, deep content inspection, multi-layer inspection and analysis, and code slicing.

04

# Timely response is key

In 2020, there was a slight rise in the number of days taken to detect and address a cyberattack. In 2021, this number rose to an all-time high of 190 days.

The greater the delay in detecting a cyberattack, the more will be the long- and short-term impact of a breach. In an OT environment, attackers may embed their malware and wait for a larger opportunity to appear before striking. They may also transfer the control of the malware to other groups which could lead to more uncertainty and security problems.

Lack of information on vulnerabilities, patch status of key components and lack of deep visibility into network operations are together hampering the ability of security teams to respond quickly. Further, due to a lack of security drills, planning, documentation and pre-planned audits, when a cyberattack does occur, the quality of the initial response is not up to the mark, which creates more opportunities for the hacker to exploit.

### The specific problems with the response to a cyberattack on OT systems can be summarised as:

**Responsiveness to threats:** depends on the security operation team's ability to immediately inspect an alarm

**Availability of adequate logs:** this is often a challenge in the OT environment

**Time to qualify a threat:** after adequate inspection, how soon can the team classify/qualify a threat

**Qualifying the impact of the threat:** to assign adequate resources and attention to it

**Investigation time:** how much time does the team take to fully investigate and classify a threat

**Time taken to mitigate:** this refers to the time taken to fully act on and block or slow down a threat to limit its impact on the infrastructure.

In a traditional OT environment, the IT team is often tasked with looking after OT security as well. Because of this arrangement and due to the complex environment, that often hosts OT systems, deriving a structured and well-planned response to a cybersecurity event becomes a significant challenge.

Further, new regulations in India by the Indian Computer Emergency Response (CERT-In) require all service providers, intermediaries, data centres, corporates and government organisations to mandatorily report cyber incidents to CERT-In within six hours of noticing such incidents or being brought to notice about such incidents.

# Improving your OT cybersecurity posture

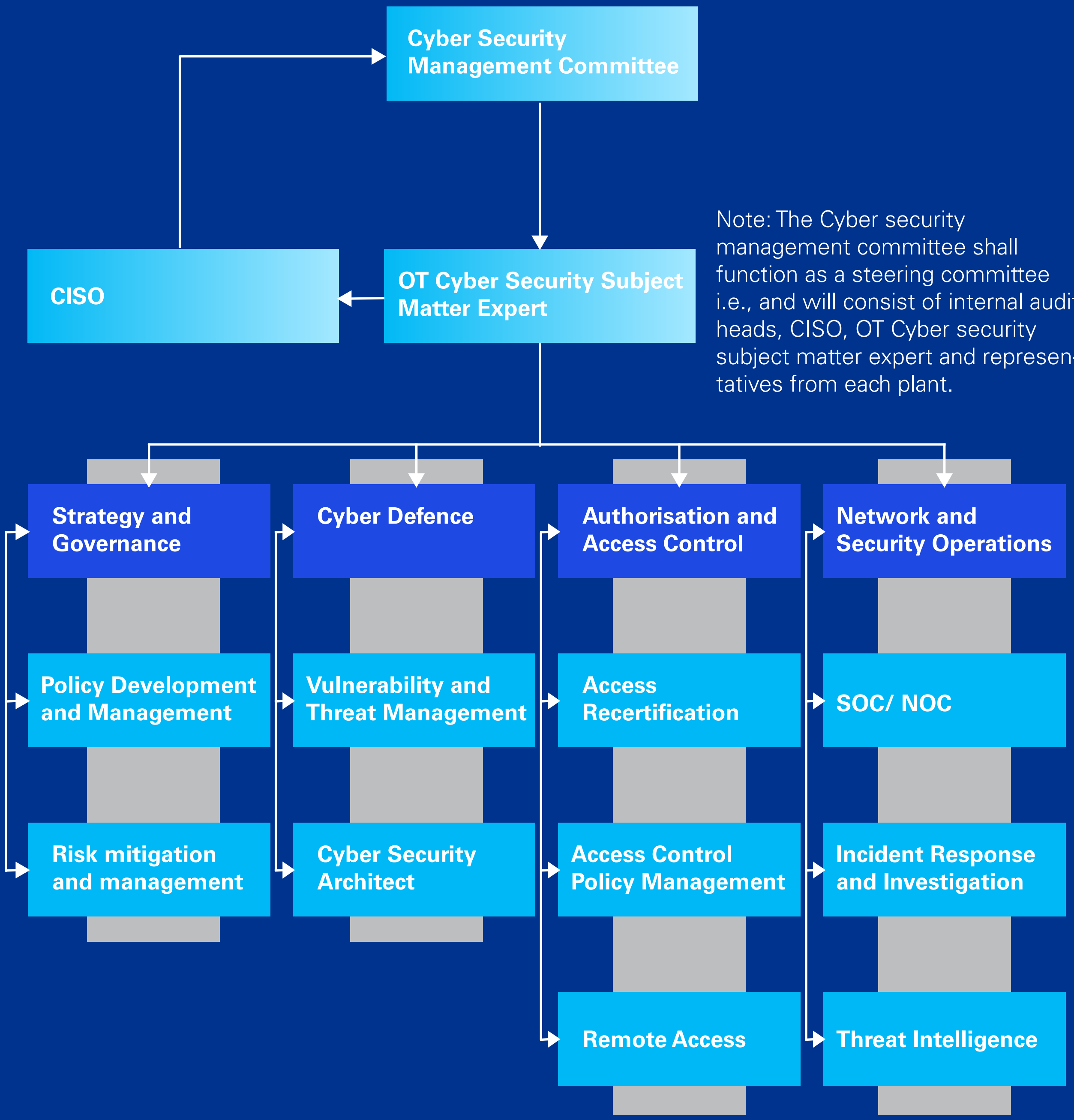
**Building an improved industrial control systems cybersecurity governance model**

For organisations to set cyber security hygiene, it is important to adopt existing working operating models in IT environments and implement them with necessary changes to the OT environment.

Some of the key pillars for a good OT cyber security environment are as follows –

## 1. Establish an OT security Governance Structure

- OT Cyber Security Management Committee (OT CMC) - a joint committee comprised of senior management representatives from business groups including representation from OT Cyber Security and chaired by the Chief Operating Officer or Chief Information Officer or equivalent
- Cyber Security Work Team (CWT) is formed who is mainly responsible to coordinate and enforce controls to be implemented to protect critical cyber assets from threats. CWT to perform or oversee OT cyber security evaluations of cyber assets and is expected to have representation from across teams / plants
- OT Cyber Security Subject Matter Expert : OT Cyber Security Subject Matter Expert is someone with expert level knowledge of the OT environment and is to report to the CISO on matters related to OT security. The OT SME would be responsible for ensuring coordination on key OT projects and may appoint members from their team to work with the CWT to implement OT security at a plant level. The OT SME will also be responsible to coordinate with various OT CERTs and responsible regulatory authorities
- Security Operations In-Charge : Would be a plant level (or group of plants) person to ensure implementation of OT security at the ground level.


Cyber Security Management Committee
CISO
OT Cyber Security Subject Matter Expert
Strategy and Governance
Policy Development and Management
Risk mitigation and management
Cyber Defence
Vulnerability and Threat Management
Cyber Security Architect
Authorisation and Access Control
Access Recertification
Access Control Policy Management
Remote Access
Network and Security Operations
SOC/ NOC
Incident Response and Investigation
Threat Intelligence

Note: The Cyber security management committee shall function as a steering committee i.e., and will consist of internal audit heads, CISO, OT Cyber security subject matter expert and representatives from each plant.

*Note: This governance structure represents the different technical capabilities required and not a direct mapping to the roles or a count of individuals required.*

## 2. Develop capability for monitoring ICS environments

- Establish a continuous monitoring and detection process for the facility as a whole
  - Maintain an eye-on-the-glass view of network activity
  - Identify grey areas or assets that lie outside any form of monitoring currently
- Asset inventory:
  - "You cannot protect what you cannot see" – visibility is the most fundamental cybersecurity strategy to protect any network. OT environments that we see today, were commissioned quite some time ago that have gradually evolved over the years, the number of assets deployed within the environment has only grown with time.
  - One of the most significant cyber threats that is perceived in OT is existence of 'ghost' devices. The monitoring platforms available for OT today are capable of narrowing down to a threat through means such as deep packet inspection, asset behavioural analysis and policy deviations and anomaly detection mechanisms.
- Risk management and risk assessment
  - An effective risk assessment activity may provide a holistic view of the risks the OT environment is having to deal with from a people, process and technology perspective.

## 3. Align to industry and regulatory standards available to improve baseline security

- Align the environment to industry and regulatory standards that can provide guidance on security baseline for organisations. Some of the industry standards that provide focused guidance around cybersecurity programmes and initiatives have been IEC – ISA 62443 and NIST Cybersecurity Framework.
- While the organisation has taken up initiatives to comply to standards the regulatory bodies within which the organisation lies within have also been mandating compliance to cybersecurity controls against their own custom cybersecurity standards. Some of the standards that have been published by regulatory bodies include NICS by QCert in Qatar, Cyber Security Guidelines by NCIIPC and CEA for Critical Infrastructure Environments and Power Sector Organisations in India, Cyber Security Guidelines for Critical Infrastructure by ENISA in Europe, etc.

## 4. Conduct awareness session at plant level and for security teams on OT cyber security

- Considering the traditional outlook toward IT and OT environments, the need to create cybersecurity awareness among the OT staff has largely been neglected thus far. This is because organisations have been mainly focused around safe operation of plants complying with HSSE (Health, Safety, Security and Environment) standards.
- With the increase in the number of cybersecurity threats affecting OT environments and the availability of enough examples to prove the impact such incidents are having on physical lives, organisations must address the immediate need to create awareness amongst the staff that work on the shopfloors on priority.
- The staff need to be made aware of the malpractices specific to OT and their implications on the plant networks.

## 5. Establish cyber security as an integral part of the procurement policy

- The organisation may consider contractually obliging the OEMs and system integrators to cybersecurity standards and policies applicable to the organisation. This could be to do with procuring components that have cybersecurity certifications and to comply with the organisation's cybersecurity policies and procedures post-implementation.

## 6. Conduct Indpendent Reviews of the OT Security Posture

- In addition with the increase in focus on OT security, Internal Audit teams (line of defence 3) are increasingly starting to conduct assessment of OT security assessments to provide Boards assurance on the OT security posture of the organisation.

# Acknowledgements

We are extremely grateful to senior leaders from the industry, subject matter experts, and KPMG in India team members for extending their knowledge and insights to develop this report.

## Analysis and content

- Anish Mitra
- Sony Anthony
- Pooja Chandna
- Harsha Bhat
- Pratheek S
- Vivek S

## Design and Compliance

- Anupriya Rajput
- Sameer Hattangadi

# KPMG in India contacts:

**Akhilesh Tuteja**
Global Head, Cyber Security
**E:** atuteja@kpmg.com

**Atul Gupta**
Head, Digital Trust
**E:** atulgupta@kpmg.com

**Sony Anthony**
Co-Head, Cyber Defence and Incident Response
**E:** santhony@kpmg.com

**Chandra Prakash Surywanshi**
Co-Head, Cyber Defence and Incident Response
**E:** chandraprakash@kpmg.com

Access our latest insights
on KPMG Insights Edge

**Follow us on:**

**kpmg.com/in/socialmedia**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus , Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is meant for e-communication only. (001_THL0124_AR)