



CYBERTHEORY ICS/OT RISK REPORT JUNE 2022



ICS OT SECURITY INCIDENTS ARE GROWING RAPIDLY

ICS/operational technology (OT) security is an emerging technology category that is rapidly growing in importance.

In the past twelve months, we've seen high-profile cyber-attacks on Colonial Pipeline, an American oil pipeline system that carries gasoline and jet fuel to the Eastern Seaboard, JBS Foods, a food processing company supplying meat and beef products throughout the US, NEW Coop, a grain distribution and storage services company serving 36 locations across the country, a water treatment facility in Florida and several other lower profile operations.

Critical infrastructure (electric utilities, oil and gas, and community water systems) have been early adopters of ICS/OT security, but increasingly, manufacturers, food and beverage, and pharmaceutical asset owners are also evaluating their options for protection in an increasingly hostile environment.

***U.S. ON HEIGHTENED
ALERT FOR CRITICAL
INFRASTRUCTURE
ATTACKS***

ICS/OT owners are seeking technology-agnostic security solutions that provide broad asset discovery, identification and visibility regardless of vertical.

Solution providers who have a heritage grounded in control systems enjoy a marked advantage over vendors trying to enter this market with only an internet-of-things (IoT) security background. Despite organizations increasingly connecting their factories to the cloud, the gap between ICS and IoT is still huge. While IoT sensors collect data from the physical environment to improve decision making in enterprises, industrial control systems use microprocessors to manipulate the physical world.

THE ZERO TRUST APPROACH WOULD BE TO PRIORITIZE VULNERABILITY REMEDIATION FOR “CROWN JEWEL” ASSETS



EXPERTS AGREE THAT ORGANIZATIONS CAN'T FULLY PREVENT DETERMINED ATTACKERS FROM COMPROMISING THEIR NETWORKS.

The annual “Global ICS/OT Risk Report” from CyberX (now a Microsoft company) is based on analyzing real-world traffic from more than 1,800 production ICS/OT networks across a range of sectors worldwide, making it a more accurate snapshot of the current state of ICS/OT security than most survey-based studies.

Experts agree that organizations can't fully prevent determined attackers from compromising their networks.

As a result, the Zero Trust approach would be to prioritize vulnerability remediation for “crown jewel” assets — critical assets whose compromise would cause a major revenue or safety impact — while implementing compensating controls such as continuous monitoring and behavioral anomaly detection to quickly spot intruders before they can cause real damage to operations.



SUMMARY OF KEY FINDINGS AND THE DANGER ZONE

Broken Windows: Outdated Operating Systems. 62 percent of sites have unsupported Microsoft Windows boxes such as Windows XP and Windows 2000 that no longer receive regular security patches from Microsoft, making them especially vulnerable to ransomware and destructive malware. The figure rises to 71 percent with Windows 7 included, which reached end-of-support status in January 2020.

Hiding in Plain Sight: Unencrypted Passwords. 64 percent of sites have unencrypted passwords traversing their networks, making it easy for adversaries to compromise additional systems simply by sniffing the network traffic.

Excessive Access: Remotely Accessible Devices. 54 percent of sites have devices that can be remotely accessed using standard management protocols such as RDP, SSH and VNC, enabling attackers to pivot undetected from initial footholds to other critical assets.

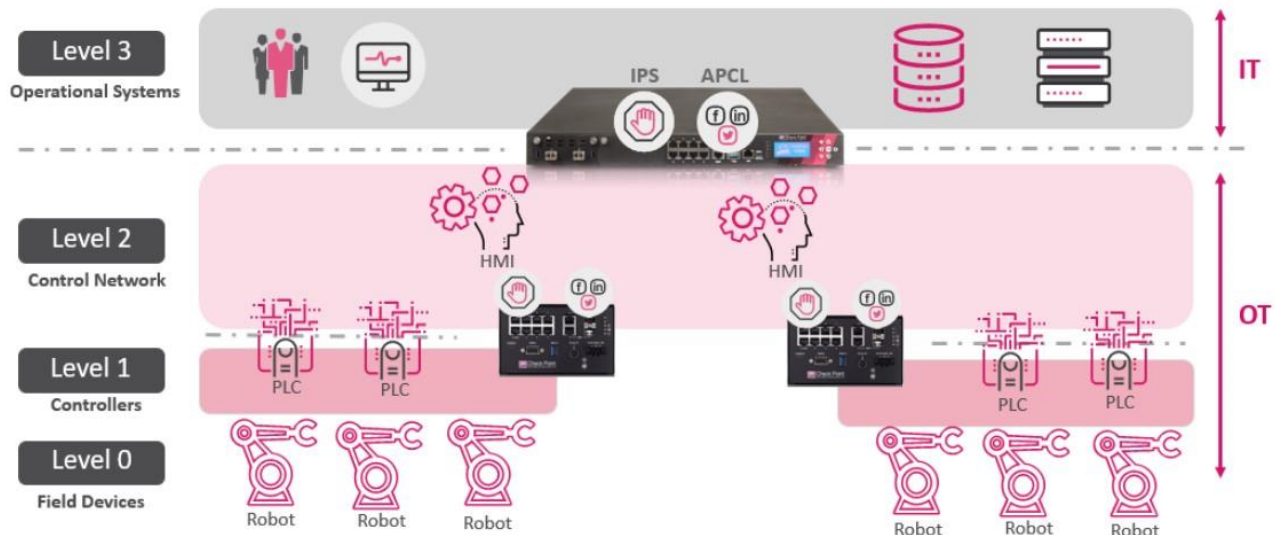
For example, during the TRITON attack on the safety systems in a petrochemical facility, the adversary leveraged RDP to pivot from the IT network to the OT network in order to deploy its targeted zero-day malware.


Clear and Present Danger: Indicators of Threats. 22 percent of sites exhibited indicators of threats, including suspicious activity such as scan traffic, malicious DNS queries, abnormal HTTP headers, excessive number of connections between devices and malware such as LockerGoga and EternalBlue

MORE GRANULAR TELEMETRY

All OT solutions will mimic traditional IT network stacks which limit monitoring telemetry down to level 2, while ICS requires visibility into telemetry at level 0 and 1, where electromagnetic signals will travel seeking vulnerable ICS control targets, and cannot be seen by traditional Purdue network topologies running heritage IT network monitoring tools.

The Purdue Model





***SENSING AND MANIPULATING
PHYSICAL PROCESSES
OCCURS AT LEVEL 1, WITH
PROCESS SENSORS,
ANALYZERS, ACTUATORS, AND
RELATED INSTRUMENTATION.***

IT/OT CONVERGENCE

Supervisory control and data acquisition (SCADA) software is used to supervise, monitor, and control physical processes. SCADA can manage systems over long distances from the physical location of the plants, while the distributed control system (DCS) and programmable logic controllers (PLCs) are usually deployed within the plant.

The human-machine interface (HMI) connected to DCS and PLCs allow for basic controls and monitoring, while the SCADA systems aggregate data and send it upstream for recording by the historian in level 3. PLCs typically do not have keyboards and monitors. Remote Terminal Units (RTUs) allow operators to log in to the SCADA systems.

Siemens, Schneider Electric, ABB, GE Digital, and Rockwell Automation are some of the major providers of SCADA systems. Devices and strategies at this layer typically communicate over the Modbus and dnp3 protocols, and data diodes can help bolster security.

Sensing and manipulating physical processes occurs at level 1, with process sensors, analyzers, actuators, and related instrumentation. To drive efficiencies, sensors are increasingly communicating directly with their vendor monitoring software in the cloud via cellular networks.

**VENDORS WILL NEED TO
DEMONSTRATE THAT THEY
CAN MONITOR, DETECT AND
REMEDiate THREATS FROM
LEVEL ZERO UP THROUGH
LEVEL 7**



LEVEL ZERO

Level 0 – Physical process: Defines the actual physical processes. It is essentially the machine language of the hardware providing direction for packet formation and routing to the IT network in level 3.

To offer a holistic OT/ICS Cybersecurity solution, vendors will need to demonstrate that they can monitor, detect and remediate threats from level zero up through level 7 on the OSI and TCP/IP network protocol stacks.

Safety, availability, and resilience are paramount characteristics of industrial environments, and they require unique expertise and technology to defend against an expanding Cybersecurity threat landscape.

While ICS/OT security requires unique expertise, buyers seek a holistic security view across the enterprise. In industries such as manufacturing, distribution and energy, technical evolutions are transforming operations and driving innovation, yet at the same time, devices, endpoints, and networks across both IT and operational technology (OT) environments are more connected than ever. The upside is undeniable, but the security implications of IT/OT convergence are still challenging.



**THE CHALLENGES OF
SECURING INDUSTRIAL
CONTROL SYSTEMS (ICS)
AGAINST CYBER THREATS
CONTINUES TO DOMINATE
THE EVERYDAY TO-DO LISTS
OF OT TEAMS.**

CHALLENGES

We tapped independent research conducted by Fortinet who surveyed industry leaders who manage and maintain OT infrastructure, and have used some of their findings to identify and validate some of the defining security trends and practices that impact operations and demand an effective security strategy.

As operators of critical infrastructure (CI) continue to converge the cyber and physical aspects of their businesses, many have achieved more efficient and effective monitoring of critical processes, as well as an increased ability to virtually leverage data from enabled sensors, industrial applications, medical devices, and software-defined production processes.

This range of capabilities, better known as the Industrial Internet of Things (IIoT), affords decision making in real-time and significant cost savings in terms of power consumption and employee efficiency.

However, the challenges of securing industrial control systems (ICS) against cyber threats continues to dominate the everyday to-do lists of OT teams. Absent of an effective OT security plan, these systems are left vulnerable to cyberattacks that could result in financial loss, reputational damage, diminished consumer confidence, and even threaten the safety of citizens and national security.

MOST COMMON IT/OT SECURITY CONCERNS

OT SYSTEMS THAT WERE TRADITIONALLY BUILT UPON LEGACY SOFTWARE ARE MUCH LESS LIKELY TO BE PATCHED.

With the rise of IIoT and subsequent IT/OT convergence, industries have lost the “air gap” that historically protected OT systems from hackers and malware. OT systems that were traditionally built upon legacy software are much less likely to be patched, and the convergence with IT is resulting in the expansion of an attack surface that enables greater access to an environment where vulnerabilities exist.

This connectivity not only brings added risk, but also opens the door for cybercriminals in a way that was not possible when these systems were isolated.

With this in mind, the survey found that 96 percent of respondents foresee challenges as they move toward IT/OT convergence.

As a result, these organizations have taken deliberate, careful movements to better protect these connected systems. Among the respondents, more than one-third reported concerns about the following OT security challenges:

- Third parties lack security expertise needed to assist with converged technology
- Sensitive or confidential data will be leaked
- When a breach occurs, organizations are not able to isolate or contain the threat
- Organizations are facing increased regulatory pressures for ICS

THE RISE OF OT SECURITY BREACHES

IT IS NO SURPRISE THAT THERE HAS BEEN A STRONG DRIVE TO COMMIT GREATER RESOURCES ON SECURITY, WITH 78 PERCENT PLANNING TO INCREASE THEIR ICS SECURITY BUDGETS THIS YEAR.

In addition, compliance has become a growing concern for those managing OT systems. 70 percent of respondents reported mounting compliance pressures over the past year, and 78 percent feel this trend will continue for the next two years. According to the report, the regulations making the most significant impact are:

- The EU Data Protection Directive (GDPR)
- International Society (ISA) Standards

The rate of cyberattacks on OT infrastructure is increasing, and these breaches are causing real damage.

For example, in 2020 we witnessed the appearance of the 'Ekans' ransomware, which specifically targets ICS systems in the industrial space.

Among those surveyed for the study, only 10 percent reported that they had never experienced this type of threat.

In contrast, 58 percent of organizations surveyed have suffered an OT breach in the past 12 months, and as a result, more than 75 percent expect regulatory pressure to increase over the next two years. If this period of consideration is extrapolated to 24 months, the breach rate rises to 80 percent, illustrating that OT systems are indeed cyber adversary targets of primary interest.

OT SECURITY MEASURES REMAIN CHALLENGING

**53 PERCENT REPORTED THAT SECURITY SOLUTIONS
HINDER OPERATIONAL FLEXIBILITY AND HALF
REPORTED THAT THEY CREATE MORE COMPLEXITY.**

The study also found that between 36 percent and 57 percent of organizations lack consistency when it comes to measuring items on a list of standard metrics. Among the most commonly tracked and reported areas are vulnerabilities (64 percent), intrusions (57 percent), and cost reduction resulting from cybersecurity efforts (58 percent).

Conversely, less than half of surveyed organizations (43 percent) are known to report on tangible risk management outcomes, and 39 percent to 50 percent do not routinely share basic cybersecurity data with senior executive leadership.

Respondents also cited security analysis, monitoring, and assessment tools as among the most essential features in security solutions, with the majority (58 percent) ranking these specific attributes in the top three. Despite the prioritization of these features, however, 53 percent reported that security solutions hinder operational flexibility and half reported that they create more complexity.

As security concerns for OT infrastructure rise, it's important for businesses to also consider the implications for their partners. To prevent breaches impacting third party organizations, it's critical that businesses grant limited and privileged access to appropriate personnel only.

PROTECTING BUSINESS PARTNERS

**PROTECTING THE OT ENTERPRISE IS CRUCIAL TO
BUSINESS SUCCESS.**

The study found that the organizations that were most successful with securing the OT environment were also 129 percent more likely to severely limit or even deny infrastructure access to their business partners.

Similarly, these businesses were 45 percent more likely to keep certain security functions in-house rather than outsourcing them.

Protecting the OT enterprise is crucial to business success.

As industrial systems continue to evolve, OT leaders are faced with new security challenges that have led to new priorities.

To appropriately protect high-value cyber-physical assets, those who manage and maintain critical infrastructure must keep abreast of the latest security trends, especially those related to IT/OT convergence, and understand how to secure their migration into this broader, digitally transformed landscape.

Historically, OT security was limited to protection of the physical plant because OT systems were not connected to the internet.

Strong perimeter gates, and human-based access controls, such as security guards, were the standard, and highly visible deterrents to intrusions. The protection of the technology was highly conspicuous.

WHY ARE OT NETWORKS AT RISK?

CAN INDUSTRIAL NETWORKS BE SECURED WITHOUT CAUSING ANY DISRUPTION IN OPERATIONS?

Internet connectivity introduces ease of operability, but apart from the inherent benefits introduced earlier, this transformation has exposed the system to vulnerabilities that cannot be stopped by a physical armed guard.

Can industrial networks be secured without causing any disruption in operations?

According to the 2020 Global IoT/ICS Risk Report, 71% of these networks have outdated operating systems that are no longer receiving security updates, 64% are using insecure passwords, and 66% are not updated with the latest antivirus updates. These conditions present some difficult problems:

- Most organizations have direct connections to the public internet. We all know that only one internet-connected device is enough to provide a gateway for attackers to introduce malware into OT networks.
- Operators have been using insecure passwords for convenient entry to the networks. This makes it easy for attackers to use brute-force discovery of credentials to gain unauthorized operator access.
- Many industries have at least one misconfigured wireless access point that many devices such as laptops can access.
- An outdated operating system that no longer receives security updates is extremely vulnerable to security attacks.

A SMARTER SECURITY OPERATIONS CENTER

IT WILL BE ESSENTIAL TO ESTABLISH DIFFERENT ACCESS FOR DIFFERENT USERS SECURED BY MFA.

Over the past years, several OT threat detection tools and software have come onto the market. But there are few challenges in OT threat detection:

- Limited cybersecurity skills in operations and manufacturing knowledge in the Security Operations Center (SOC).
- Threats are continuously changing, and adversaries are advancing their techniques.
- No single tool or sensor can provide visibility into all threats.

Sensitivity in Industrial Control System environments requires many tools to be passive, meaning that they cannot automatically trigger a shut-down event in the absence of a bona fide failure.

Managing operational technology security is one of the most critical tasks for organizations that operate plants and manufacturing facilities.

To secure an OT environment from any type of cyber threat, organizations can create a Smarter Security Operations Center using the MITRE ATT&CK framework.

The information in MITRE ATT&CK will help organizations identify the threats, active in the wild who now have your numbers to protect the castle and then themselves.

A few important processes that may immediately help you in securing your OT environment include:

- Regardless of degree of difficulty, it will be essential to establish different access for different users via various access routes.



PROPER HYGIENE IS CRITICAL

AGAIN, ANOTHER TENET OF ZERO TRUST REQUIRES AN ACCURATE ACCOUNTING OF ALL INFORMATION SYSTEMS, INCLUDING OT.

In addition, user access should be secured with multi-factor authentication.

Centralized logging helps to manage and analyze all logs to identify security gaps, and optimize defense.

- **As we've pointed out, many OT systems face a lack of visibility. Most organizations do not know the exact number of OT systems they have in their domains. As a part of asset management, every organization must have a full and accurate inventory of their OT systems.**

This will enable them to know what they are protecting, and plan accordingly. Again, another tenet of Zero Trust requires an accurate accounting of all information systems, including OT.

- **Organizations must be cognizant of the all software versions, updates, and compatibility with the OT systems in the environment. Vulnerability scanning is also an important part of understanding where weaknesses may exist. The guideposts are published and available.**

- **Patching is also an important part of hardware and software stewardship. Organizations must know the patching requirements of the assets in their possession. OT patching is a complex process, so the process must be handled judiciously.**

This means that sometimes, automatic OT patching may not be possible and you will need a plan for outliers, like complex network servers.

NETWORK SEGMENTATION

THE AIM IS TO DIVIDE LARGE NETWORKS ACCORDING TO THEIR RESPECTIVE FUNCTIONS.

- **Network segmentation is the clear demarcation between unrelated networks.**

The aim is to divide large networks according to their respective functions. Segmentation can assist in isolating a compromise.

For example, an attack against the development network will not affect the sales network.

Instead of creating a new network, a company should follow an established procedure, such as the Purdue Model to establish system-to-system connectivity, and make sure that you have created protect surfaces around your most critical assets, another Zero Trust principle.

OT security is a high-priority challenge for organizations of every size, but is essential to be addressed in light of the shifted focus toward physical infrastructure.

Which attack would have the most leverage in a Ransomware negotiation?

For security solution vendors, the window is closing. It is now time to integrate a complete OT managed service offering that includes a SIEM, SOC and SOAR function, Intel, all designed around a Zero Trust model of execution, and go to market.

For end users, it is past time to prepare for that first OT Ransomware attack by adopting the principles of Zero Trust and presenting them in a way that makes it far more difficult for the bad guys to pull off a successful breach.

MARKET LEADERS

12 VENDORS LEAD THE PACK BASED ON 27 CRITERIA INCLUDING CURRENT OFFERING, STRATEGY AND MARKET PRESENCE.

Forrester Research evaluates ICS/OT vendors against 27 criteria, including

Current offering. Key criteria include ICS protocol support, asset discovery and identification, vulnerability risk management, APIs and integrations.

Strategy. Forrester evaluates product vision, execution roadmap, planned enhancements, and supporting products and services.

Market presence. Forrester's market presence scores reflect each product revenue, number of customers, and average deal size.

Forrester assessed these 12 vendors: Bayshore Networks, Cisco, Claroty, Dragos, Forescout Technologies, Fortinet, Microsoft, Mission Secure, Nozomi Networks, OPSWAT, Tenable, and Verve Industrial Protection.

Each of these vendors has:

Significant business in energy (electric utilities or oil and gas) or community water systems.

A non-internet-of-things heritage; the vendor's ICS security solutions did not begin as an IoT security solution.

A platform of capabilities specific to meet the safety, reliability, and availability needs of industrial automation and controls engineers.

Significant interest from Forrester clients; Forrester considered the level of interest and feedback from their clients based on our various interactions, including (but not limited to) inquiries, advisories, consulting engagements, and other interactions.



ABOUT US

CyberTheory is a full-service cybersecurity marketing advisory firm, providing brand stories, advertising, marketing, content, digital strategy, messaging, positioning, event management and media publishing.

We manage broad demand generation programs with extremely high conversion rates. In addition to our resident CISO team and 40+ member Customer Advisory Board, our broad subscriber network with 1st party data, allows us to personalize the targeting of each and every Cybersecurity buyer persona.

With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always aligned with the latest industry demands.

More information at www.cybertheory.io

This report is based on several surveys conducted by IBM, Fortinet, CheckPoint, CyberX' s Global ICS/OT Risk Report and Forrester Research, supplemented by insights from our own OT/ICS research team at the CyberTheory Institute.