## Protecting Critical Assets:

# Navigating Cybersecurity Regulations and Compliance for OT in Critical Infrastructures

**Understanding *NIS2*, *NERC CIP*, *NIST SP 800-82 Rev3*, and *IEC 62443* Standards**

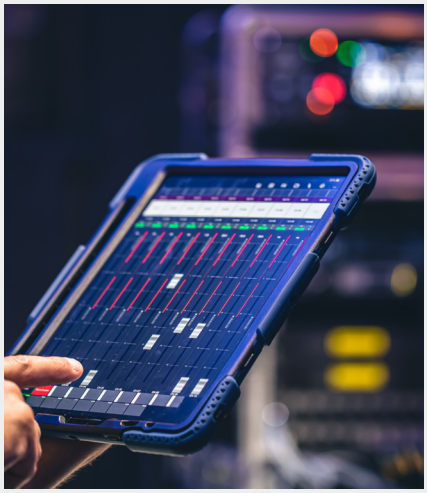
SALVADOR TECHNOLOGIES

8.2024

## More Connection Means More Risk

More and more industrial control systems (ICS) and operational technology (OT) networks are being connected to business networks through the internet, opening a new world of possibilities. However, with legacy operational networks still predominant in the industrial world, utility, manufacturing, maritime, and other organizations are particularly susceptible to cyberattacks against their critical infrastructures.

While industrial enterprises are stepping up their investment in preventive security solutions to keep their mission-critical operations safe, ransomware, political sabotage, and other malicious attacks continue to breach their cyber defenses with success. Moreover, industrial business environments are often subject to employee errors and lapses that can lead to significant breaches.



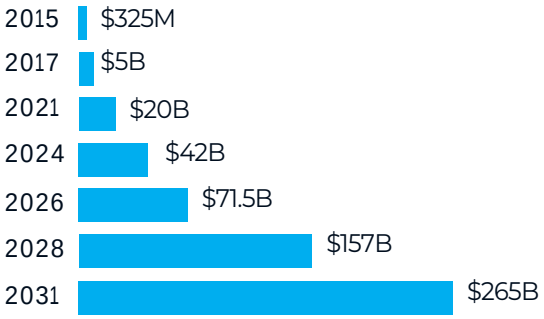
## Ransomware damage on the rise

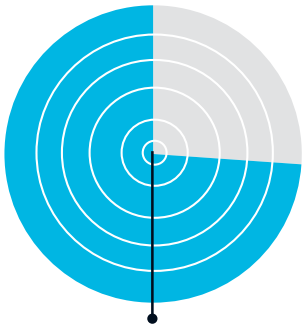
As bad actors further refine their modus operandi – a new cyberattack against businesses or consumers is perpetrated every 2 seconds, according to Cybersecurity Ventures – no slowdown is in sight. Given the low prosecution rates and the tendency of victims to meet attacker demands to save their businesses, ransomware is set to take an even bigger bite into the global economy. Cybersecurity Ventures predicts that annual ransomware damages to victims will surge from $42 billion in 2024 to $265 billion by 2031.

**$10M**

**median cost of a ransomware attck in 2022**

### Global Cost of Ransomware



The **human element** was responsible for **74%** of attacks in 2022


Ransomware will attack a company every **2 seconds** by 2031

### As a result

- Security awareness training market is expected to surge to $10 billion by 2028
- Ransomware-related cyber insurance claims rose 77% in the first quarter of 2023

While all business sectors are potential targets, manufacturing and industry – which have experienced 45 percent of all such attacks in the US in Q1 2023 – are most susceptible to ransomware incidents.

## Catastrophic economic costs

The damage caused by ransomware and other cyberattacks can be catastrophic. Organizations must bear the potential costs of downtime, system recovery and remediation, cyber forensics, upgrades, compensation, and legal issues.

At the same time, however, consumers and the public are often stuck with covering hidden economic costs. For example, a company may pass to its customers remedial costs. University disruptions may impact students and their access to education. And healthcare organizations may be forced to cut budgets, scale back their workforce, and limit care options, thereby increasing the length of time before patients can return to work.

Internal or external attacks can also cause significant damage to the environment and the public at large.

## Recovery standards to the rescue

Regulatory bodies worldwide recognize the danger that OT organizations face without deploying an effective cyber recovery solution. As such, new recovery standards across myriad sectors and geographies are continuously being added and updated.

As a global provider of recovery and downtime prevention solutions for industrial organizations, Salvador Technologies understands the synergistic relationship between ICS/OT security and regulatory compliance for maintaining business continuity and operational integrity. The Company's comprehensive recovery solution ensures regulatory compliance, boosts critical infrastructure resilience to reduce downtime and mitigate financial loss, and empowers organizations in their longstanding battle against cyberattacks.

> ***"Regulations in the operational technology sector are vital to safeguarding our critical infrastructure against emerging cyber threats, ensuring that we maintain not only compliance, but also the resilience of our energy systems."***
>
> J.G, U.S. Secretary of Energy

## Understanding Recovery Regulations

Given the significant impact of unplanned critical infrastructure disruptions and shutdowns, there is no shortage of ICS/OT regulatory standards and frameworks. Some are general, others industry-specific. Some are regional, others global. But all are focused on one goal – to ensure that organizations implement the right measures for maintaining business continuity. Below is a short list of some of the most prominent cyber recovery standards.

| Standard | Region | Industry |
|---|---|---|
| NIS 2 | Europe | General |
| NERC CIP-009 | North America | Electricity |
| NIST SP 800-82 Rev3 | United States | General |
| GAMP5 V2 | Global | Pharmaceutical |
| IEC 62443 | Global | General |
| IACS UR E26, E27 | Global | Maritime |

### NIS2

The European Union's NIS2 Directive aims to achieve a high, standard level of cybersecurity across the region. The directive provides legal measures, based on an all-hazards approach, to help EU organizations prepare for business continuity in the event of a major cyber incident. Among the regulations, which are mandatory for the Directive of European Critical Infrastructures, are cyber recovery considerations and up-to-date backups

### NERC CIP-009

Part of a set of standards developed by the North American Electric Reliability Corporation (NERC) to protect the continent's bulk electric system from cyberattacks, NERC CIP-009 mandates that organizations establish comprehensive backup and recovery procedures for critical infrastructure. These include preparing detailed recovery plans for critical cyber assets, which must specify recovery time objectives (RTOs) and recovery point objectives (RPOs) to minimize downtime and data loss during disruptions. The standard includes restoration tests, conducted at least once every 15 months, to ensure that systems can be restored within predefined RTOs.

## NIST SP 800-82 Rev3

The National Institute of Standards and Technology (NIST) SP 800-82 Rev3 focuses on establishing capabilities to recover from cybersecurity incidents and to restore impaired assets and services to their pre-incident state. This includes creating reserve systems and processes to back up an OT system's relevant data, configuration files, and programs at regular intervals. It also calls for securing backups according to access control requirements, establishing recovery processes and procedures, verifying backups for reliability and integrity, and maintaining a list of all backups.

## GAMP5 V2

In pharmaceutical manufacturing, adherence to the Good Automated Manufacturing Practice (GAMP) guidelines, particularly GAMP5 v2, is crucial for ensuring product quality and regulatory compliance. These guidelines outline stringent requirements for the management of automated systems, including backups and recovery strategies. Compliance with GAMP5 v2 requires implementation of robust backup and recovery mechanisms to safeguard critical data and ensure operational continuity. Backup strategies must align with disaster RPOs, including determining the frequency and granularity of backups to minimize data loss in the event of system failures or disasters. Additionally, recovery procedures must be documented and regularly tested to verify their effectiveness and compliance with regulatory standards. By following up on GAMP5 v2 regulations, pharmaceutical manufacturers can mitigate risks, maintain data integrity, and uphold the highest standards of quality assurance in their operations.

## IEC 62443

Part of a series of international standards that provides specific guidance for securing industrial control systems, the International Electrotechnical Commission (IEC) 62443 outlines crucial backup and recovery requirements for safeguarding industrial operations, including cyber recovery. It covers data integrity, redundancy, access controls, and incident response strategies to strengthen organizations' abilities to respond to incidents and to restore integrity swiftly. According to the standard, organizations must regularly perform recovery tests to identify weaknesses in their backup and recovery capabilities and to make necessary improvements. While compliance is not universally mandatory, regulatory bodies increasingly endorse it to ensure cybersecurity resilience in industrial settings. While the standard is maintained by IEC, various bodies contribute to it. Sectors such as energy, manufacturing, and transportation often mandate its compliance to mitigate risks.

### IACS UR E26,E27

The International Association of Classification Societies (IACS) UR E26 and E27 regulations became mandatory for new ship construction at the outset of 2024. In compliance with IACS regulations E26 and E27, vessels must possess backup and restore capabilities for rapid recovery after a cyber incident. Data restoration from secure copies is mandated with consideration for offline backups to enhance resilience against ransomware and malware. The measures ensure that vessels can swiftly regain operational functionality and maintain safety at sea.

## Complementing Compliance with Backups

While backups can protect an organization from an attack, not every deployment guarantees success. In the 2021 ransomware incident against Israel's Hillel Yaffe Medical Center, for example, the hospital's backups were not air gapped, according to reports. So while the backups should have enabled the hospital to return to normal activity in just hours, [as the regulation recommends,] the systems had been hijacked and were inaccessible to IT personnel. It is likely that the attackers extracted all patient data and treatments, including the backups, before blocking the systems.

Deploying a successful backup strategy is a best practice that can help organizations protect their data and comply with regulations. One popular strategy, the 3-2-1 rule, has been extended to the 3-2-1-1-0 rule as explained below.

**3**-2-1-1-0 – Maintain at least 3 copies of your data (i.e., primary data plus 2 more backups).

3-**2**-1-1-0 – Don't store 2 copies of the backup on the same type of storage media.

3-2-**1**-1-0 – Keep at least 1 copy of the backup away from the physical location (i.e., where the primary data and backup are located).

3-2-1-**1**-0 – Keep at least 1 backup copy offline, which is an integral part of Salvador Technologies' unique offering.

3-2-1-1-**0** – Monitor the backups daily, and in the event of errors, resolve them as soon as possible so there are 0 errors. In addition, carry out tests at recurring intervals to restore data from the backups to verify that everything is under control.

# Ensuring Cyber Recovery and Resilience

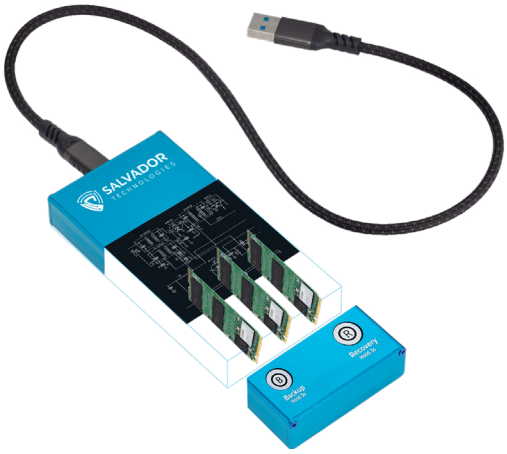
Salvador Technologies is a global provider of an advanced solution that enables organizations to ensure a swift, effective, and full recovery from a cyberattack. Based on innovative air-gapped technology, the solution recovers any computer system – be it a PC, laptop, workstation, or server - within 30 seconds after an attack or computer failure. Protecting critical OT systems and their sensitive data, the solution also improves an organization's security posture and reduces its liability in the event of an attack.

Designed to address security and compliance requirements, the solution gives organizations the following set of tools and capabilities to go beyond compliance and maintain resilience against growing cyber threats.

## OT/ICS Backup Visibility

The solution provides immediate insights into backup status, delivers real-time alerts for failures, and enables centralized monitoring through a web management system or extended log files. By meeting these key regulatory requirements, organizations can ensure the integrity and availability of their backup inventory.

## Disaster Recovery Point Objective (RPO) Alignment




The solution is anchored by a cyber recovery unit (CRU)- a disk-to-disk backup system that seamlessly aligns with regulation recommendations of backup strategies. To address the need for consistent backup scheduling aligned with disaster RPOs, the unit offers three preconfigured backup frequencies - daily, every two days, and weekly. This automation minimizes human error and ensures that backups are performed at regular intervals, according to regulation requirements.

**The CRU is physically connected to the HMI, PC, or server, but is electronically disconnected to ensure secure air-gapped backups.**

## Offsite Backup Storage

The solution's image backup capability ensures data resilience by storing backups offsite, thereby meeting regulatory requirements for geographically separated backup storage.

## Recovery Time Objective (RTO) Alignment

The solution includes an industry-leading RTO of 30 seconds, aligning perfectly with regulatory emphasis on swift data restoration.

## Test Patching

The solution enables the testing of patches in a sandbox environment. The sandbox is loaded after just a 30-second booting of the CRU. If the patch is successful, it can then be confidently applied to the production environment.

### Easy Restoration Testing

Unlike other solutions that depend on image backups, the CRU's restoration test capability does not risk copying data onto the internal hard drive. This eliminates potential risks and downtime for critical OT components during such tests.

### Portable Media and Environmental Considerations

The CRU has undergone rigorous environmental safety and electromagnetic compatibility testing to earn CE, FCC, and UKCA certifications. With a broad operating temperature range and exceptional durability that surpasses typical requirements for backup media, the CRU ensures data integrity in various environments.

## Navigating the Security Landscape with Confidence

Salvador Technologies' solution is designed with several features to enhance cyber resilience and ensure operational continuity.

- Real-time insights and alerts - provides full visibility of backup status per endpoint
- Centralized monitoring - monitors continuos production environments 24/7
- Disk-to-disk backup system - aligns with RPO recommendations
- Preconfigured backup frequencies - offers multiple options to meet an organization's specific needs
- Offsite backup capabilities - seamlessly transitions to offsite backup in the event of an attack or malfunction
- Industry-leading RTO of 30 seconds - verifies compliance through RTO requirements
- Easy, risk-free restoration testing - validates backup integrity and easily retrieves data

OT/ICS compliance is key to an organization's ability to defend itself from cyberattacks. Committed to helping organizations navigate the evolving security landscape with confidence, Salvador Technologies' cyber recovery solution facilitates regulatory compliance. This, in turn, enables them to protect their data, minimize downtime, and mitigate financial loss.

## Taking the Next Step

Depending on your RTO, your organization can implement our recovery solution to minimize downtime and meet your objectives. To learn more, contact info@salvador-tech.com.

## About Salvador Technologies

Salvador Technologies provides a cyber recovery platform for downtime prevention in Industrial Control Systems (ICS) and Operational Technology (OT) organizations. Its innovative solution minimizes downtime and regains operations immediately after a cyber-attack, IT outage, or NY Windows failure incident, in a record timeframe of 30 seconds.

The company's platform is used by some of the world's most secure critical infrastructure organizations, including manufacturing, aerospace, maritime, energy and water companies **visit us**.