Research

TPR Survey Report

Ransomware Attack Recovery: are industrial enterprises prepared?

Sponsored by Salvador Technologies

Executive Summary

No organization can detect or prevent 100% of cyberattacks

Industrial enterprises invest millions each year in solutions that are designed to keep mission-critical industrial operations safe from cyberattack. They employ a vast array of cybersecurity equipment and software to identify, protect, and detect all kinds of threats and attacks and to respond to them as quickly as possible. Traditionally, cyber security programs have focused on prevention – on keeping the attacks at bay. However, even with all the investment in prevention, ransomware and other malicious attacks are still breaching cyber defenses. When a breach occurs in the cyber-physical world and damage begins, the need for a fast and effective recovery process becomes painfully clear.

Fact

No organization can detect or prevent 100% of attacks.

Therefore, every organization should have a recovery plan for "the moment after" a breach occurs. This is especially true for industrial enterprises, whose mission-critical operations run 24/7 non-stop, and are extremely averse to downtime. Unplanned disruptions to water delivery, electricity distribution, oil/gas pipelines, chemical processing, manufacturing production lines, etc. can be devastating in numerous ways.

Solutions for **Cyber Attack Recovery** are gaining importance and recognition for the critical role they play in avoiding downtime after an attack and getting industrial operations fully back on track. While Recovery is included in the NIST (National Institute of Standards and Technology at the U.S. Department of Commerce) Cybersecurity Framework (CSF), the recovery function has been woefully underinvested in favor of preventative measures such as incident identification, protection and detection.

The potential to wreak havoc and extort large payouts make industrial enterprises an attractive target for ransomware, political sabotage, and other attacks both internal and external. Additionally, in OT/ICS environments, breaches and damage caused by employee mistakes and lapses are often extremely damaging and difficult to fix. It is folly to depend on incident prevention measures alone.

How fast can OT/ICS systems recover from cybersecurity incidents?

We asked industrial enterprises of varied sizes and sectors to tell us what Cyber Attack Recovery processes they have in place, and how quickly their OT/ICS systems

can recover from a Ransomware attack or other incidents.

This TPR Survey Report gives you the inside scoop on what OT/ICS cybersecurity professionals think about Cyber Attack Recovery in general and in terms of their own industrial enterprise. Since a high percentage of respondents are members of an OT or Plant cybersecurity team, their experience and insight provide valuable and highly germane perspectives on the state of Cyber Attack Recovery in industrial enterprises.

Highlights of Findings

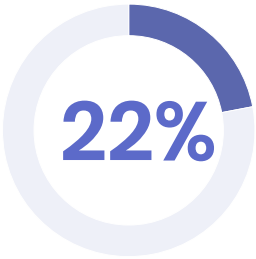
Respondents say their current Cyber Attack Recovery plan does not adequately support OT/ICS

Respondents are not confident in their Cyber Attack Recovery plan (i.e., business continuity) for critical OT workstations and machines

Respondents say OT/ ICS environments differ dramatically from IT and require an OT-specific approach to cyber securitymachines

Report that the Recovery process in their organization is owned by IT teams

This dissonance may be putting OT systems at risk for costly downtime following an attack.



While OT downtime can be devastating, only 22% of respondents aim for a Recovery Time of minutes or less. The expectation that Recovery "takes time" may be the result of underinvestment in OT Attack Recovery strategies and solutions

Only 10% of respondents perform continuous or weekly validation of OT workstation/system backups and restoration. Most verify their OT backups once a year or once a quarter because the process is so invasive and time-consuming

In light of these findings, many industrial enterprises may be living with a false sense of security.

We are confident this report will be of particular interest to OT Cybersecurity teams who are seeking cybersecurity solutions **that are designed for the needs of OT/ICS environments.** We also believe that corporate cybersecurity teams who traditionally hail from the IT side of networking and tend to oversee incident recovery efforts, will find this survey report of great interest.

Ransomware Rising

Ransomware is on the rise in OT environments and becoming ever more disruptive. From the extortionist's perspective, it makes perfect sense. The more damage and downtime they can cause, the more ransom they can demand from their victims. What could be more disruptive than taking down a gas pipeline that brings energy to thousands of homes and businesses or interfering with critical water purification or manufacturing operations?

One of the hallmarks of Ransomware extortionists is that they are always upping their game and improving their methods. In recent years, they have demonstrated their growing ability to penetrate IT systems and consequently bring OT system to a halt as noted in the breach of the Colonial Pipeline, causing energy outages along the East Coast of the United States in May 2021. Likewise, ransomware attackers nearly shut down the power grid of Queensland's CS Energy in Australia in November 2021.

In the case of Queensland CS Energy, OT downtime was averted. Others have not been so lucky.

- We all remember the devastating NotPeyta cyberattack on Merck in June 2017. The successful attack disrupted production of the company's HPV vaccine, cost $850 million in damages, and precipitated $400 million in lost sales that year. The attack also affected thousands of other companies who do business with Merck.
- Norsk Hydro, one of the largest manufacturers in the global aluminum industry, was forced to halt production processes and switch to manual operation for several weeks following a LockerGoga ransomware attack in March 2019. The disruption cost the company $52 million.
- In April 2020, Energias de Portugal (EDP), a large Portuguese energy company reported a ransomware attack involving Ragnar Locker malware, which left the company's systems encrypted. The criminals claimed to have stolen terabytes of company files before the encryption, and threatened to disclose the private information unless they were paid a ransom of nearly $11 million.

According to the CyberSaint State of Ransomware Attacks Report 2022, Utilities, Energy, and Oil companies are increasingly popular targets for ransomware attacks, and 43% of those who are attacked, end up paying the ransom.

Even when the ransom is paid, there is no guarantee that the cybercriminals will honor their end of the bargain. Furthermore, many argue that every ransom payment becomes an incentive for criminals to attack again and again. Clearly, industrial enterprises need a better way out of the ransomware trap and the specter of OT downtime.

The specter of OT downtime from cyber attacks

To recover from a ransomware attack and avoid crippling downtime, industrial enterprises must be much better prepared for when things go wrong. When OT systems are breached, those who are not prepared risk harmful impacts on their business including:

- Direct costs and projected losses from the disruption to OT/ICS operations, production lines, etc.
- Direct costs of attack remediation and downtime recovery, which may take longer than expected.
- Direct costs of ransomware payments, or rise in premiums if insurance has to pay.
- Indirect expenses resulting from litigation (e.g., class-action lawsuit) and or regulatory fines.
- Breach and potential disclosure of sensitive company data.
- Brand and reputation damage.

The importance of a Cyber Attack Recovery Plan

Having a Cyber Attack Recovery plan that is OT-savvy and fully validated plays a critical role in avoiding downtime and quickly getting industrial operations back on track after an attack. The National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) recognizes the importance of the "Recover" process and made it one of the pillars of the NIST Cybersecurity Framework (CSF), which is designed to help businesses of all sizes to better understand, manage, and reduce their cybersecurity risk and to protect their networks and data.

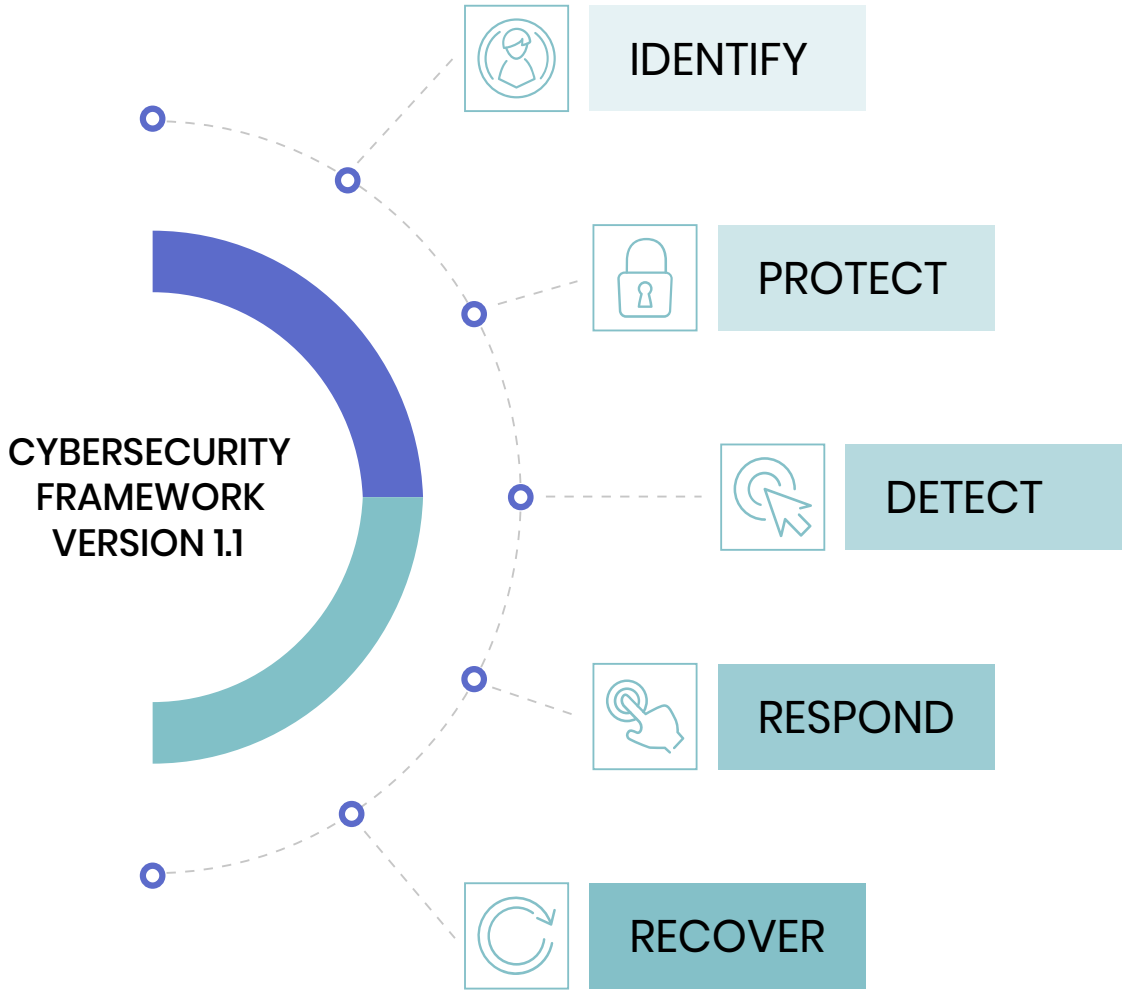


Figure 1: NIST Cybersecurity Framework

The NIST CSF was conceived by IT security experts as a guideline. Adherence is very helpful, but entirely voluntary. Traditionally, CISOs have focused their budgets on the prevention pillars of the cybersecurity framework (i.e., Identify, Protect and Detect) with the aim of building defenses that could not be breached. But in the hacker game of cat and mouse, it's only a matter of time until an attack is successful. The Offense is always one step ahead of the Defense. Therefore, incident recovery is critical, especially in the industrial sector.

How fast can OT/ICS systems recover from cybersecurity incidents?

Industrial enterprises have a lot to lose from downtime in the wake of an attack. They should be seeking solutions that enable the OT environment to recover rapidly and completely by keeping OT systems and assets up and running and by making sure critical data and configurations can be fully and quickly restored.

Attack Readiness and Resilience

The Model for Incident Resilience (developed by TP Research) plots IT-centric versus OT-centric backup-and-restore processes in terms of the NIST Cybersecurity Framework and in terms of the time or velocity with which these processes can be accomplished.

Industrial Cyber Incident Resilience - Maturity Model

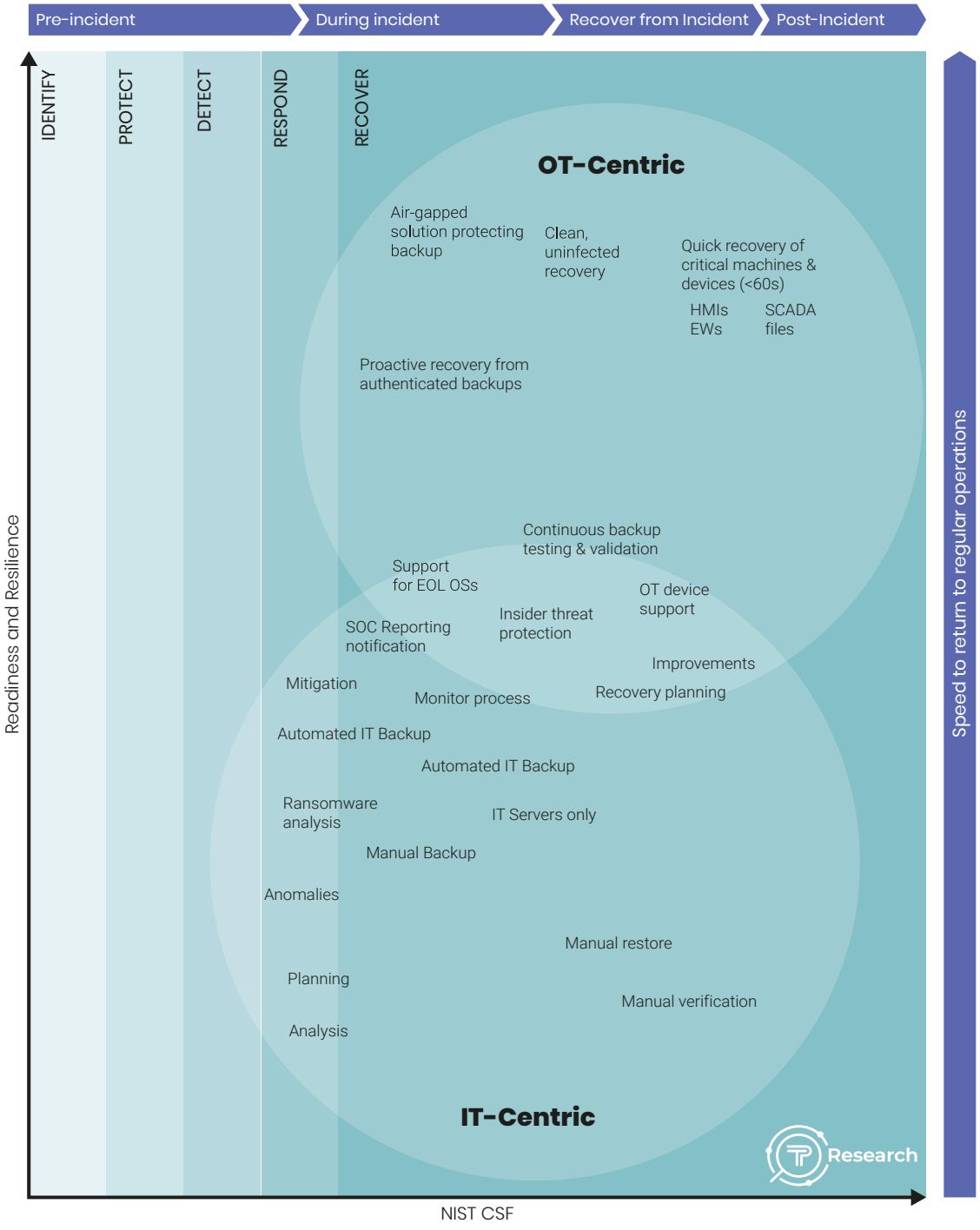


Figure 2: The bulk of OT-centric cybersecurity activity happens in the Recovery phase

To date, a significant percent of industrial Recovery strategies are planned and managed by the CISO and IT teams, who are responsible for cybersecurity across the entire organization (and have been for the past 30 years!). Preparing an actual recovery plan can be tricky, particularly across critical infrastructure and industrial environments that are separated from corporate IT and cloud networks by complex segmentation.

Using IT-centric Backup & Recovery strategies for OT environments is fraught with significant shortcomings, including:

- Need to restore hundreds of engineering workstations, HMIs, etc., often throughout an entire factory or production line. Hours or days may be tolerable for recovering a single or a few workstations. However, when numerous workstations have stopped, it will take several days or weeks to restore them all.

- Cloud and other IT expertise needed. Restoration of cloud backups to workstations in the OT environment is not trivial and it requires expertise and experience, which may be in short supply during a downtime crisis. For example, when a 5-person IT team has to restore hundreds of workstations, it creates a huge hurdle that costs time and money to overcome.

- Cloud and network bottlenecks can hamper recovery: Even when recovery experts are on hand, the sheer volume of OT systems and assets that need to be restored often cause significant delays.

- Recovery processes in the OT environment are often unverified because it's practically impossible to "shut down" a 24/7 industrial process just for testing. When OT backup and restore processes are not validated continuously, Recovery teams often discover that they cannot rely on the backups.

These shortcomings may add greatly to OT system downtime before full recovery is achieved and have far-reaching repercussions on business continuity, safety, and profitability.

Report Findings – Insights from the OT Cybersecurity Front Lines

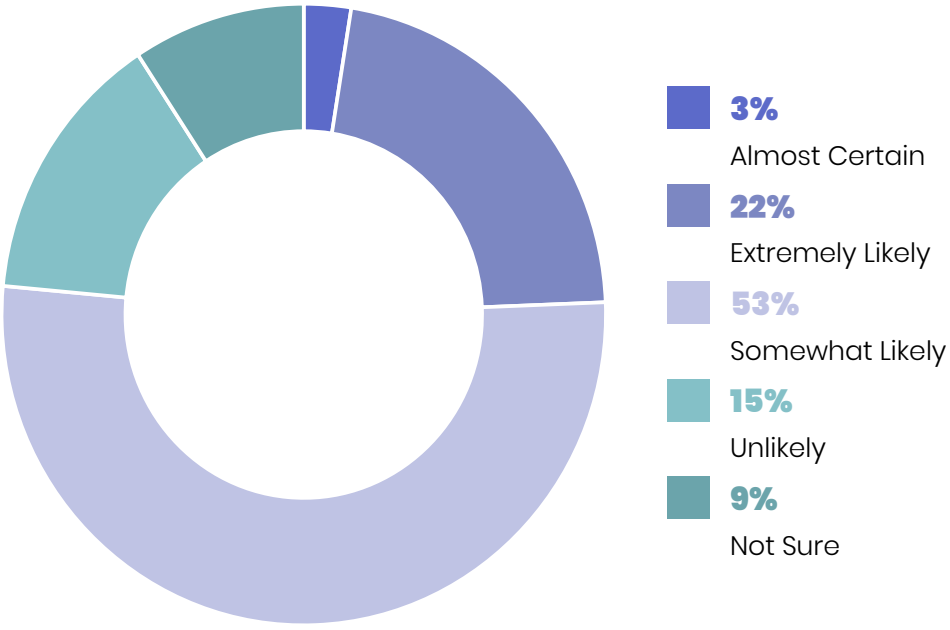
We asked 100+ industrial managers, experts, and leaders from different companies to tell us what they are doing in terms of Recovery from a cyber incident. Here's what they told us.

Survey demographic

What are the chances of your OT/ICS business being attacked?

In your opinion, how likely is it that your company's production will fall victim to a ransomware attack in the next 12-24 months?

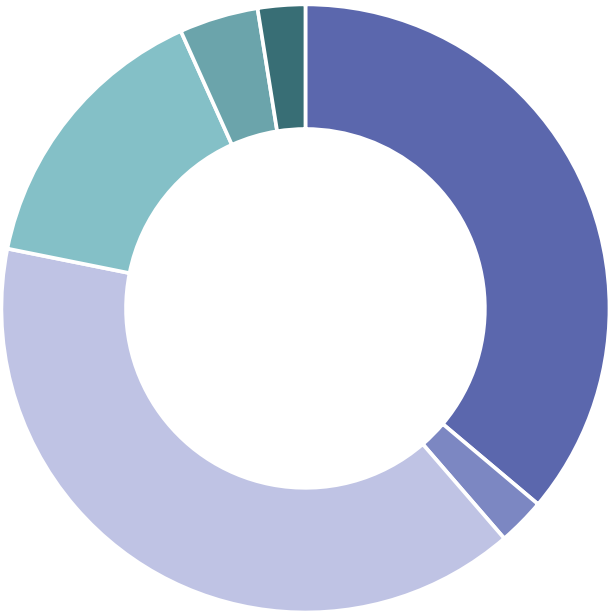
78% of respondents think a Ransomware attack will hit their business, which means they anticipate having to respond and recover and should have a Cyber Attack Recovery plan in place.



How well can you Recover from an attack on OT/ICS?

Who currently owns the OT/ICS Recovery process in your organization?

While industrial cybersecurity traditionally has been the responsibility of Corporate IT Operations and cybersecurity teams, our findings show that OT teams are taking more responsibility for the security of the OT environment. Nearly 60% of respondents put OT cybersecurity in the hands of OT teams.



37%
CISO/Cybersecurity team

3%
CIO/IT team

40%
Cybersecurity team

15%
Engineering or Operations team

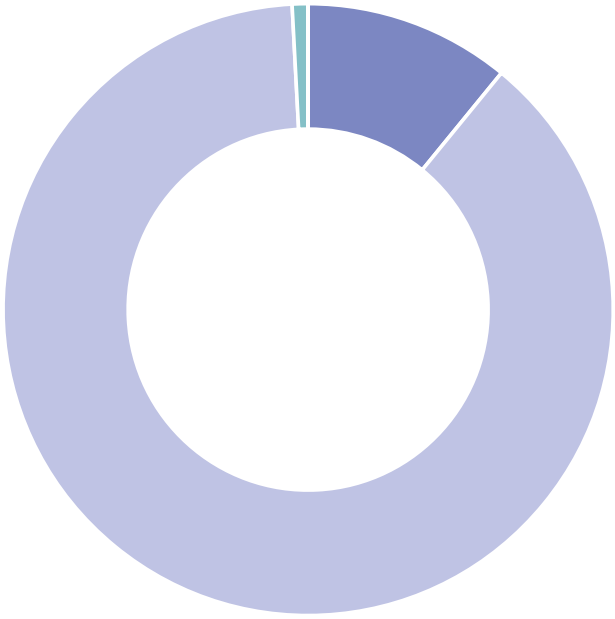
4%
Individual plant/site manager/engineer

3%
Other

Who should own the OT/ICS Recovery process?

In terms of business continuity strategy post cyber incident (attack, breach, ransomware, insider), how would you consider the approach of IT versus OT?

A whopping 90% of respondents say the OT/ICS Recovery process should be owned by OT professionals and not by IT, due to the considerable differences between OT and IT environments. While progress has been made in this regard (see the graph above) there still is a considerable shift that needs to occur in order to put OT/ICS Recovery in the hands of OT.



0%
IT and OT environment should be considered identical in every way

11%
The environments are quite similar: we can use the same approach we use in IT with a few minor tweaks to OT

90%
The OT environment differs considerably from IT in terms of the aims and in terms of the technology deployed. We need a specialized approach to OT

1%
Not Sure

How well does your current backup/restore business continuity solution support OT (select all relevant)

40% of respondents are using advanced solutions for attack recovery (e.g., air-gapping, full recovery of OS, backup automation, legacy support, etc.). The 60% who do not have these solutions are likely to suffer from sub-optimal recovery methods.

While current IT and cloud-based solutions are able to restore/recover - they cannot do it quickly or without the intervention of expert personnel. This creates serious bottlenecks and often results in hidden costs, delays and risks.

31%
Air gapped backup with multiple recovery points

5%
Fast recovery (<60 seconds) of critical machines and systems

57%
Full recovery of OS, configuration and files

36%
Support for end-of-life OS (Windows 95, XP, 2000)

27%
Non-intrusive, continuous testing and validation of backup

39%
Automated backup/restore of critical machines and systems

48%
Clean (malware/virus free) backups

24%
None of the above or Other

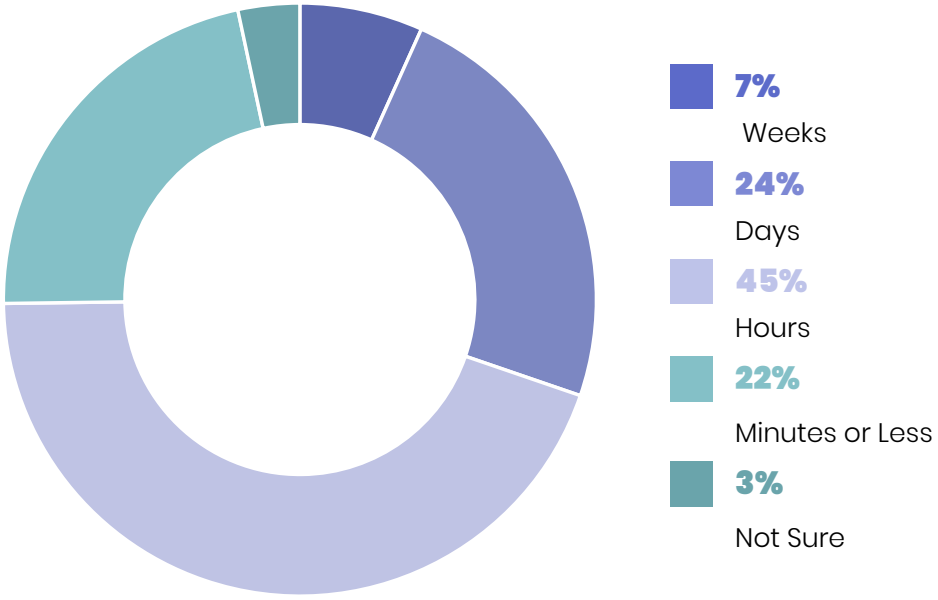
What should OT/ICS Incident Recovery goals be?

What is your optimal TTR (Time-to-Recovery) for OT/ICS workstations and HMIs?

69% of respondents think that hours or days are an optimal Recovery Time Objective (RTO). Hours or days may be acceptable for recovering a single or a few workstations. However, when numerous workstations in a production environment are down, it can take several days or weeks to restore them all.

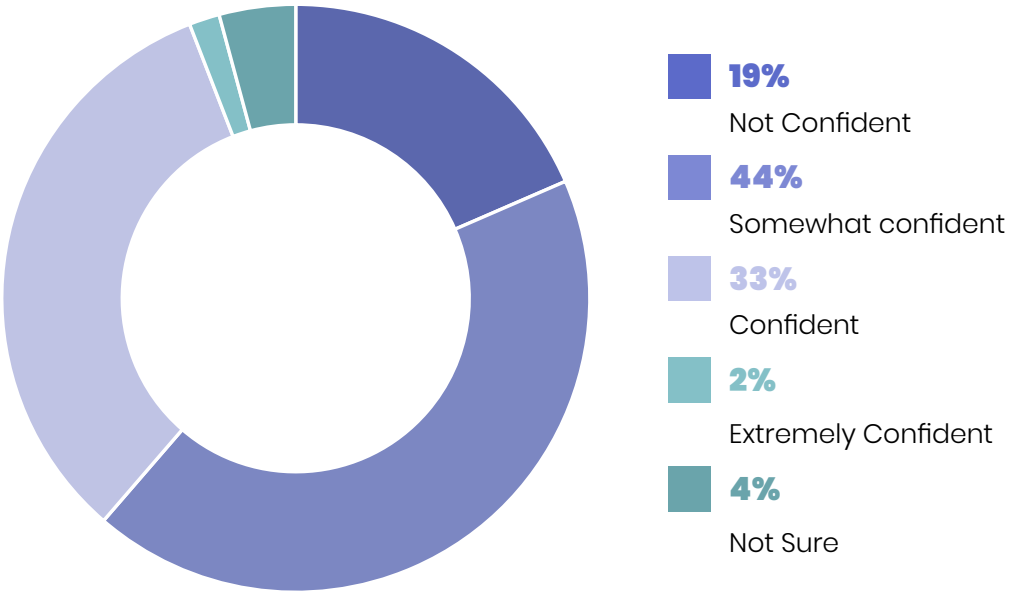
While many OT people think the IT recovery team has a handle on this, most IT professionals don't understand the complexities of the OT environment. When we consider attack recovery time across an entire factory/site, unexpected hurdles and hidden costs often arise.

In OT environments where downtime can be devastating, why do only 22% think an optimal RTO should be minutes or less? Could it be that days or weeks is the best their current solutions can do, so they don't think it is realistic to aim for less?



How confident are you that your current business continuity plan for critical machines in the OT environment will meet your RTO following a cyber incident?

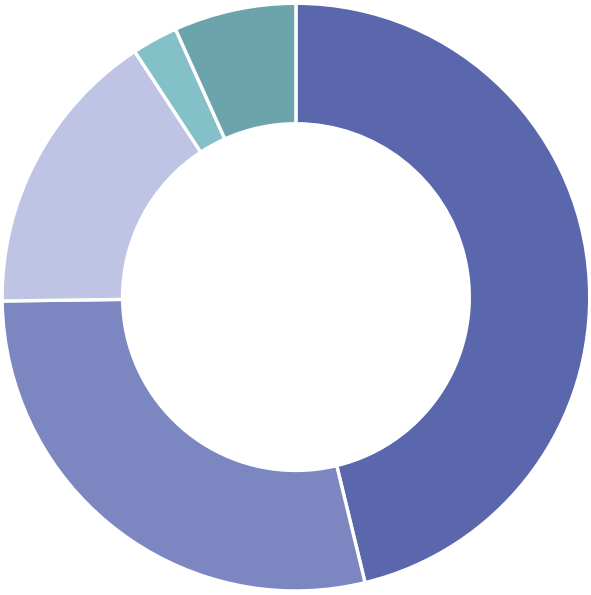
It may be telling that 67% of respondents say their optimal RTO would be hours or less (see the graph above) and at the same time, 63% are less than confident that their current Attack Recovery plan can achieve it. Here is the discord – when there is no clear OT/ICS ownership or accountability of the OT/ICS recovery process, it is almost certain that not all OT-specific factors are being considered.



Validating OT Business Continuity

How often do you check the validity of OT backups with full restoration?

The belief that your backups are valid, without verification, is a false assumption that undermines everything else in the Response/Recovery plan– and it severely impacts safety, reliability, and production. Making sure OT backups are up-to-date and easily restored often has not been done because the test process is incredibly difficult. But no longer. Today, there are elegant and simple Cyber Attack Recovery solutions that can assure no downtime of critical assets, even as broader Recovery steps are still underway.



47%
Yearly-It can be very intrusive and time consuming

29%
Quarterly-It can be somewhat intrusive and time-consuming

16%
Monthly-We have developed a less intrusive method

3%
Weekly

7%
Continuously

Survey Insights

In industrial environments, OT/ICS teams must play a role in Cyber Attack Recovery. Leaving the entire planning and implementation process in the hands of IT and cloud experts means you may be endangering the continuity of critical industrial processes – and potentially for a much longer time than is tolerable. Attack Recovery needs an equal voice in cybersecurity planning and investment.

While Cloud backup and recovery solutions have made great strides in efficiency, the cloud can become a bottleneck when an entire plant or OT production line needs to be restored. The first priority must be to keep OT processes running, giving you time to assess and repair the full extent of the damage without disruptive and costly OT downtime.

A harmonious approach is the best way to align the Cyber Attack Recovery expectations of management with the reality of the OT production environment. OT and IT teams must work together and share the responsibility for Attack Recovery because a one-sided approach will only achieve a false sense of security.

Checklist: What to look for in an OT-centric solution

After the Colonial Pipeline attack in the United States, CISA (Cybersecurity and Infrastructure Security Agency) and the FBI (Federal Bureau of Investigation) released a best-practice guideline requiring companies to ensure that OT backups are up-to-date, easily retrieveable and air-gapped – in other words, not in the cloud.

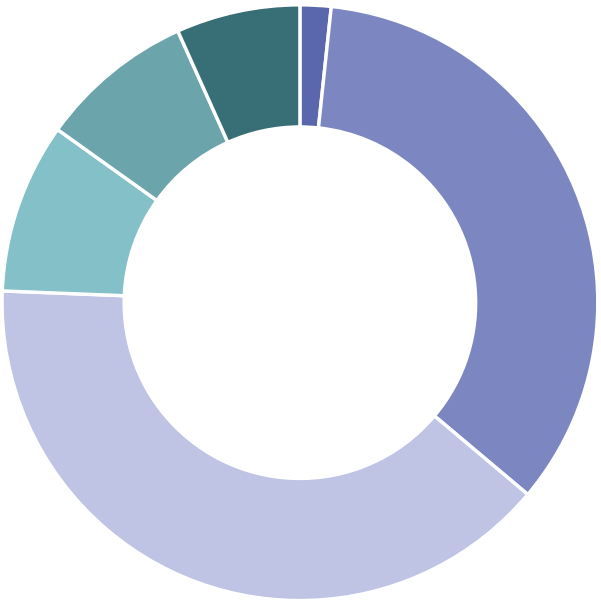
An OT-centric Attack Recovery program must be focused on assuring OT workstations and HMIs continue to operate while higher-level cleanup and recovery processes are ongoing. Backup and Restore capabilities should include:

- Air-gapped, immutable backups
- Continuous verificiation/validation of backups (with minimal or no interruption)
- Simple. Backup is automatic. Anyone can restore. No expterise needed.
- Support for every type of workstation and OS (including end-of-life operating systems)
- Full recovery starts and ends in seconds (not hours or days or weeks)
- Restore locally, as close to the workstation as possible, to avoid potential bottlenecks

Methodology

This online TPR Survey, sponsored by Salvador Technologies, was conducted during Q3-Q4 2022 with a sample size of 119 (complete) records representing professionals currently work in and around industrial enterprises. Responses came from 23 countries across the globe and multiple industries.

Which of these best describes your role?



- **2%** Member of Corporate IT Team
- **35%** Member of Corporate Cybersecurity Team
- **40%** Member of Corporate OT Cybersecurity Team
- **9%** Plant IT or Cybersecurity Team
- **9%** Plant Manager or OT Engineer
- **7%** Other

In which industry is your company?

21% Manufacturing

16% Electric Power Generation, Transmission or Distribution

14% Oil & Gas

9% Chemical

9% Transportation

6% Water & Waste

5% Pharmaceutical

3% Ports & Logistics

3% Mining

15% Other

Research

About Takepoint Research (TPR)

Takepoint Research (TPR) is a boutique industry analyst firm that provides focused research and actionable insight for industrial enterprises and those tasked with protecting them from cyber threats. TPR resources and analysis help them make informed decisions about evolving their industrial cybersecurity programs to meet the changing threat landscape. Collaboration is at the heart of our model and our mission is simply to deliver expert insight that has tangible value for your company.

SALVADOR TECHNOLOGIES

About Salvador Technologies

Salvador Technologies provides breakthrough technology solutions for operational continuity and cyberattack recovery for ICS & OT, ensuring an easy validation of the backup integrity with an instant restoration test. Our patented air-gap technology enables a full 30-second recovery from any scenario.

The company's expertise is based on more than ten years of experience in the National Cyber Unit and elite intelligence corps of the Israel Defense Forces (IDF) and on our passion for contributing to global cyber security.