Rockwell Automation

WELCOME TO YOUR CUSTOM

OT Cybersecurity Preparedness Assessment Report

Contents

OT Cybersecurity Preparedness Report

Thank you for taking the Rockwell Automation Cybersecurity Preparedness Assessment. The goal of this report is to help provide a quick benchmark of your organization's cybersecurity preparedness, based on action steps in each category of the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover.

Introduction

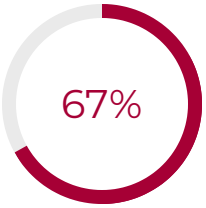
Assessment Categories & Scores

Overall Assessment Scores

Introduction

This report will help identify strengths and weaknesses, as well as show a comparison of your organization's self-reported scores with other industrial organizations who have answered the same questions. Example recommendations are offered at each level, providing a jumping off point for conversations within your organization or with an outside cybersecurity partner such as Rockwell Automation. Let's jump into your results.

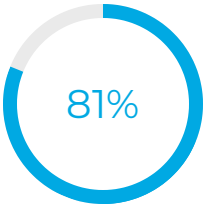
Your Organization's Overall Cybersecurity Preparedness Score



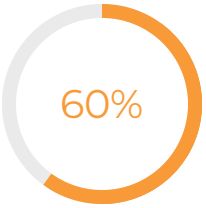
Your overall **Moderate** score indicates that your preparedness is inconsistent. You're doing some work to protect your organizations from cyberattacks, but you're not acting fast enough to cover all important gaps.

NIST Category Scores

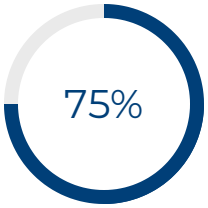
The NIST Cybersecurity Framework is widely adopted across all industries. Rockwell Automation recommends this framework to all Critical Infrastructure providers and industrial organizations as a fundamental roadmap for managing cybersecurity risks. Assessment questions are categorized by the NIST core function areas identified below. In the next few pages we'll discuss each category and explain what your results mean, key steps to raise your score, and how you compare to your industry peers.



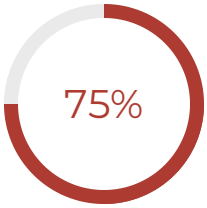
Identify



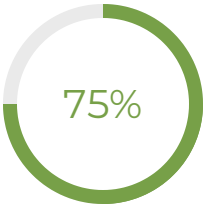
Protect



Detect



Respond



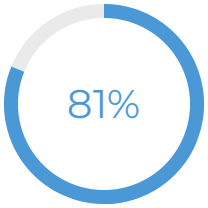
Recover

NIST Category: **Identify**

Your Identify Score and What It Means

The Identify category includes a series of steps to discover your current cybersecurity landscape, expose gaps, and understand risks and vulnerabilities – internal and external – and to document and prioritize business-critical systems and available resources. The steps under the Identify category help you prioritize risks so you can direct your limited resources to the areas of highest impact.

Activities within this domain are risk and vulnerability assessments; network architecture assessments; asset inventory analysis; penetration testing; supply chain evaluation; employee cybersecurity hygiene levels and more. These areas should be assessed within the context of the organization's specific environment, including industry; number and locations of sites; potential impacts to the organization and its customers in the event of cyberattack downtime and/or damage; government or industry compliance requirements; cybersecurity insurability; and environmental influences.



YOU SCORED

MODERATE / SOMEWHAT PREPARED

You scored in the middle of the preparedness scale, which means you're heading in the right direction — but you still have some work to do in ensuring your organization is fully protected. Threat actors are constantly searching for any weaknesses they can exploit to gain access inside critical infrastructure providers. With automated tools, they can look for vulnerabilities at scale, and any gap that remains puts your infrastructure at risk of attacks.

Before you implement an effective cybersecurity strategy, focus on identifying your risks and prioritizing them. Are your inventory assessments frequent enough? Are you assessing your supply chain risks? Have you identified your business-critical systems and their risks? Until you answer these and other risk-related questions with confidence, all the efforts you devote to the other areas of the framework will fall short.

In the next section, we'll recommend some steps to get you started.

Recommendations: **Identify**

Key Actions to Raise Your Score

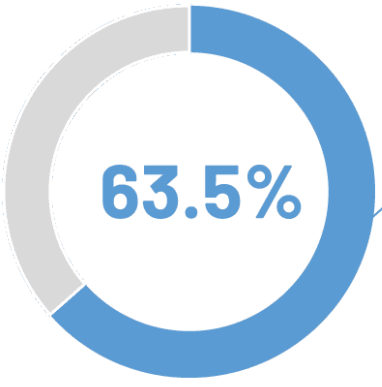
Your **Moderate** score shows you've already implemented some best practices for identifying, understanding and prioritizing cybersecurity risks. In a recent Rockwell Automation survey on Critical Infrastructure cybersecurity preparedness, respondents had an average score of 63.5%, and your result means you're doing as well as many of your peers.

However, gaps remain in terms of gaining a complete picture of your threat landscape. The recommendation is to continue to identify and close critical exposures, moving with urgency to design and implement all needed protections. If you're not fully assessing all your risks, as your Moderate score suggests, cyber attackers can likely uncover weakness in your infrastructure.

Recommendations:

- Conduct network inventory assessments at least daily, and many organizations are moving to real-time inventory capabilities.
- Implement automated threat detection tools directly or through a managed services provider to simplify assessments step and help eliminate manual errors or oversights.
- Identify and prioritize the systems that are critical to core business functions such as plant production. This activity supports the Zero Trust architectural strategy, allowing additional controls to be placed close to critical systems in priority order.
- Ensure the integrity and security of your supply chain by conducting supply chain risk assessment, which will help you understand the cybersecurity practices and processes your vendors follow and how they affect your own organization's risk. If you haven't started this process or are not performing these supply chain assessments regularly, start now and make it a priority.
- Conduct an end-to-end cybersecurity assessment across systems and processes at least once per year. Working with a highly experienced partner who understands the unique requirements and the environments of industrial operations, and of OT cybersecurity, can provide high assurance of leaving no stone unturned in terms of regular, thorough assessments.

ROCKWELL AUTOMATION SURVEY RESULTS: 2022



Industry Average Score: Identify

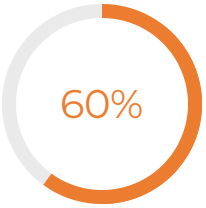
LOW to MODERATE / SOMEWHAT PREPARED

NIST Category: **Protect**

Your Protect Score and What It Means

The Protect category focuses on designing, developing and implementing safeguards for protecting the systems, assets, applications, data, people and other components that enable the delivery of your critical services.

The safeguards needed should be outlined from assessments and reviews taken in the Identify phase. These safeguards should include gap-closing measures such as updating network design with IDMZ and segmentation; continuous threat monitoring and asset inventory auditing; CIP product-level controls; identity and access controls, including secure remote access; removable media management; OT patching; employee awareness and training; data security, information protection processes and procedures; and incident response and recovery planning.



YOU SCORED

MODERATE / SOMEWHAT PROTECTED

A **Moderate** score means you're doing some things right, but not doing enough of the right things. You're likely missing critical safeguards which continues to leave your infrastructure exposed. The frequency of cyberattacks targeting Critical Infrastructure sectors means it's only a matter of time before your organization is hit with a costly attack. You may have already experienced downtime and/or damage from cybersecurity incidents.

If your organization is among the many undertaking digital transformation initiatives to connect operations, expand IoT and gain efficiency, the ongoing convergence of IT and OT can also expose your environment to new threats. This creates its own urgency to address gaps quickly. The longer you wait, the more complex your environment will grow.

Read the next section for our recommendations.

Recommendations: **Protect**

Key Actions to Raise Your Score

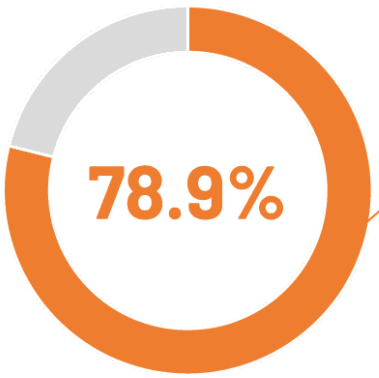
Your **Moderate** score indicates you're likely doing well in protecting your systems, advancing in some areas but struggling in others. Based on the comparison between your results and the average score of 78.9% for this category in our 2022 survey, you may also have some work to do to catch up to many of your peers.

Recommendations:

- **OT patching:** Since downtime is a big concern, working with an outside expert specializing in OT and Critical Infrastructure security can resolve these difficulties and deliver appropriate patching, with an eye on preserving operational uptime; a trusted partner who understands the dynamics of industrial environments can devise solutions to patch OT systems with minimum of disruption and downtime. In some cases, the easiest patching solution is to implement Infrastructure-as-a-Service. These managed services solutions provide the high benefits of improved operational performance and appropriate cybersecurity controls, such as OT patching. What's more, these solutions help organizations avoid high CapEx costs and issues around IT and security staffing shortages.
- **IAM:** If your organization uses remote access, an identity and access management (IAM) system provides complete visibility into all access requests and enforces Zero Trust. **Multi-factor Authentication** is another recommended practice for better securing remote access.
- **Network segmentation:** Segmenting networks helps harden perimeters around key operational infrastructures, limiting damage from spreading in the event of a successful breach.

If you're not on your way to Zero Trust already, start those conversations now. The Zero Trust approach is especially effective for protecting OT environments such as Critical Infrastructure organizations, removing excess trust from systems that can lead to poor protection. There are many ways to implement Zero Trust, which means you can likely leverage some of the strategies you already have In Place or on your cybersecurity roadmap.

ROCKWELL AUTOMATION SURVEY RESULTS: 2022



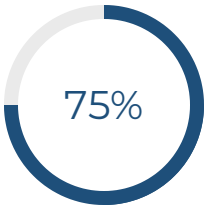
Industry Average Score: **Protect**

MODERATE / SOMEWHAT PREPARED

NIST Category: **Detect**

Your Detect Score and What It Means

The Detect category in the NIST Cybersecurity Framework deals primarily with continuous threat monitoring so that your organization can effectively detect threats. The faster you can discover a security incident, the more successful you'll be at blocking the threat or minimizing the damage if the breach was successful. Anomalies and events, continuous monitoring and threat detection processes are the three categories within this function.



YOU SCORED

MODERATE / SOMEWHAT PREPARED

Defense strategies, however robust, are not fool-proof. Threat actors are resourceful and constantly updating their techniques, and you should always assume that a compromise of your systems may have already happened.

That's why threat detection is so critical. The faster threats are identified, the less likely adversaries will be to carry out their malicious objectives. Fast detection also enables you to respond quickly to reduce the damage from a potential breach.

Your **Moderate** score indicates that your organization does not yet have strong enough threat detection capabilities to spot attacks on your OT systems, which hinders your response to threats. It's important to work quickly to eliminate this gap. Until then, your organization remains at high risk of threats, such as ransomware, or stealthy actors moving through your system to prepare for an eventual large-scale attack.

Read the next section for steps that you can take to close this gap.

Recommendations: **Detect**

Key Actions to Raise Your Score

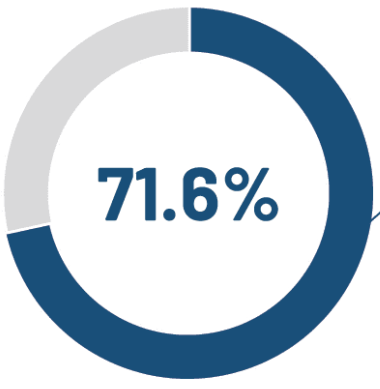
Critical Infrastructure organizations are being encouraged, and in some cases mandated, to follow Zero Trust security strategies. Core tenets of Zero Trust include continuous monitoring, as well as the assumption that your organization has already been breached. Even if you haven't started working on a Zero Trust model or are just beginning your journey, your security should be built on these ideas, making threat detection an essential capability.

Your **Moderate** score in this category means you have implemented some important threat detection practices, but may still have gaps. Your score also means you're doing nearly as well as the industry—the average in this category on the 2022 Rockwell Automation survey was 71.6%. However, any gaps continue to put your organization at risk. Strengthening threat detection will improve your organization's ability to identify and block or respond to and recover from cybersecurity attacks, which lowers risks of downtime and financial losses from these incidents.

Another key area to review is endpoint monitoring. Monitoring endpoints in real time enables you to spot anomalies and identify suspicious activities early that may indicate a security incident. Additionally, consider deploying a **Security Information and Event Management**(SIEM) solution if you don't have one in place.

If you don't yet have an OT Security Operations Center (SOC) for fast threat detection, we strongly recommend you consider this strategy if you haven't already. An OT SOC partner like Rockwell Automation brings deep expertise and a highly trained team for real-time, 24/7 monitoring, greatly increasing your preparedness to respond to threats. Managed OT SOC services also help avoid large capital expenditures (CapEx), moving cybersecurity to operating expenditures budgets (OpEx).

ROCKWELL AUTOMATION SURVEY RESULTS: 2022



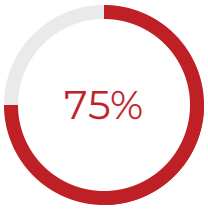
Industry Average Score: **Detect**

MODERATE / SOMEWHAT PREPARED

NIST Category: **Respond**

Your Respond Score and What It Means

The Respond core function helps you develop and implement your actions in response to a cybersecurity incident, with the goal of containing the impact. Respond activities fall into five main categories: response planning, communications, analysis, mitigation and improvements.



YOU SCORED

MODERATE / SOMEWHAT PREPARED

Fast and effective incident response is important for all industries. It's even more amplified for Critical Infrastructure providers, considering the stakes are high and a full-scale incident can cause tremendous harm potentially impacting thousands or even millions of people.

Your **Moderate** score indicates that your organization's ability to bounce back from an attack is at least somewhat limited, with potential implications including extended downtime, large financial losses and service interruption.

This is an area of struggle—and another uncertainty—for many organizations, partly due to the constantly changing nature of threats. If you don't have an effective response plan, your organization will continue to have a difficult time in maintaining or regaining full operations after an attack.

In the next section, we provide recommendations for how to improve your capabilities.

Recommendations: **Respond**

Key Steps to Raise Your Score

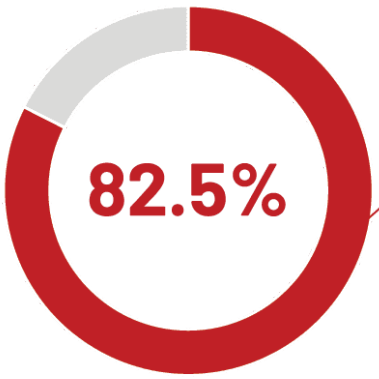
Based on your **Moderate** score, it appears your organization is not able to consistently contain incidents before they become a bigger problem.

You're also lagging behind the industry in this category—the average among the 2022 Rockwell Automation survey respondents was 82.5%. If you don't yet have the capabilities for threat analysis, containment, and mitigation, your first course of action is to develop a plan. Once you have a plan that includes incident containment and intrusion eradication protocols, your team doesn't have to second-guess their actions and can respond more confidently based on the incident type.

Most Critical Infrastructure providers also don't have the ability to detect threats and anomalies in real time. Threat detection platforms for malicious OT/ICS behavior get better all the time, and we highly suggest you invest into such a platform if you don't already have one in your security stack.

If you lack in-house expertise and talent to develop an incident response plan or **implement an OT SOC** so you can monitor and respond in real time, work with an outside expert. A partner can both help you plan your incident response and manage it for you. An OT SOC provider takes the pressure off your team to mitigate incidents 24/7, offering deep OT security expertise and training, as well as the latest best practices—boosting your preparedness.

ROCKWELL AUTOMATION SURVEY RESULTS: 2022



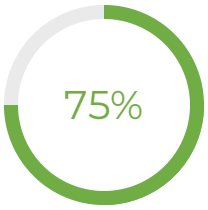
Industry Average Score: **Respond**

MODERATE to HIGH / SOMEWHAT PREPARED

NIST Category: **Recover**

Your Recover Score and What It Means

The final core function of the NIST framework focuses on your ability to restore services and operations. Successful recovery reduces the impact of a cybersecurity incident while also helping your organization become more resilient. The three categories in this process include recovery planning, improvements and communications.



YOU SCORED

MODERATE / SOMEWHAT PREPARED

After you've mitigated a cybersecurity incident, you still need to restore your operations to normal as quickly as possible. If your systems were affected severely, full recovery could take weeks and even months, especially if you don't have an established plan.

Based on your **Moderate** score, your organization has made headways in this area, but doesn't have a fully effective strategy. This means you're still at high risk of significant consequences, such as mounting financial costs and widespread customer disruption.

As a Critical Infrastructure provider, you understand how your organization's resilience impacts your customers and your community. Continue to strengthen your practices in this area and make it as important as the other core cybersecurity functions.

Read the next section for recommended strategies.

Recommendations: **Recover**

Key Steps to Raise Your Score

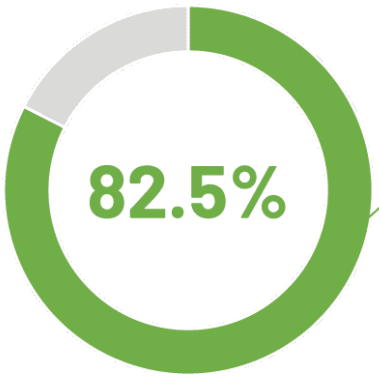
A **Moderate** score indicates that fast restoration of critical operations is limited, and your organization may face more lengthy and damaging consequences as a result. You're also behind the industry average of 82.5% that the 2022 Rockwell Automation survey showed.

Any incident can escalate into a large-scale attack with deep consequences if not stopped and if recovery processes are not at the ready. This could be anything from large financial losses to physical harm or loss of life.

Start by evaluating existing recovery procedures, identifying the areas that still fall short and then creating an action plan based on those gaps. For example, frequent data and systems backup are essential to your ability to restore application data and return to production quickly. Once you've covered the most critical operations and systems, move on to those that are of less consequence if affected.

After recovery, it's also important to thoroughly investigate cybersecurity incidents to identify root causes. This allows you to spot inadequacies, initiate improvements and **strengthen your attack resilience.** If you haven't implemented this process and your team doesn't have the expertise to conduct these investigations, engage an industrial security services team to provide the support you need.

ROCKWELL AUTOMATION SURVEY RESULTS: 2022



Industry Average Score: **Recover**

MODERATE to HIGH / SOMEWHAT PREPARED

Final Review: **Key Findings**

Your Overall Preparedness and Looking Ahead

Unmitigated critical infrastructure weaknesses can have serious implications, ranging from high costs of downtime and halted operations to customer disruption and human harm. While your overall Medium score of **67%** shows you're making headway, it's imperative you devote more attention and resources to closing your remaining preparedness gaps. If you've completed the fundamental steps such as a cybersecurity plan, risk and vulnerability assessments, and continuous threat monitoring, implement more advanced practices that can improve your organization's cybersecurity maturity. Additionally, continue to make progress on your journey to Zero Trust by implementing additional controls that support this model. Use the resources below to help you get started.

Rockwell Automation Cybersecurity Services: Securing What The World Relies On.

Rockwell Automation provides a range of industrial security solutions and services to help you manage threats and boost the resiliency of your OT and IT ecosystem. Our experts can help you build a robust and secure network infrastructure while helping to defend against threats and rapidly respond to incidents. In addition to deep expertise and knowledge of the latest best practices, we bring production operations wisdom from more than 100 years in industrial automation. Our worldwide locations enable customers to apply cybersecurity protections on a global scale across multiple sites with logistics as finely tuned as you'd expect from the industry leader in industrial automation.

Resources to Help You Get Started

- For more insights into the state of Critical Infrastructure, download Rockwell Automation's report,"Cybersecurity Preparedness in Critical Infrastructure."
- Use ourOT Cybersecurity Plan Template and checklist, a planning guide that can help to quickly develop a high level view of gaps and action areas for further build out. US State, Local and Tribal Critical Infrastructure organizations: use the Plan Template to help prepare for cybersecurity grant funding coming soon as part of the 2021 infrastructure bill.
- Talk to a Rockwell Automation expert and learn how we can help you with the right OT cybersecurity program to best protect your industrial operations.

www.rockwellautomation.com