Minutes Matter, Seconds Count

Industrial Cybersecurity Practices That Reduce Downtime

Rockwell Automation

Table of Contents

INTRODUCTION

In February 2022, a system administrator at an auto parts manufacturer rebooted a file server to resolve an unexpected file error. The administrator didn't see the normal boot screens one might expect, but was instead greeted with a threatening message, providing the first sign that an active cyberattack was underway.

The attack would continue to ripple through the automotive supply chain for days. By the time the full scope of the attack was discovered, this leading worldwide automaker was forced to suspend operations in 28 production lines across 14 plants, cutting global capacity by one third, representing hundreds of millions of dollars in losses.

Today's industrial networks are increasingly connected and vulnerable to OT cybersecurity threats. The costs of a cyberattack come in many forms, including expenses to restore lost data, repair or replace damaged equipment, compensate victims, and pay fines or legal fees. In industrial settings, however, the largest cost typically comes from operational downtime.

CONNECTING CYBERATTACK RISKS TO THE COST OF DOWNTIME

For plant owners, unplanned downtime costs related to cyberattacks can add up fast. A small-to-medium business might lose $8,000 or more for each hour of downtime, while for a large industrial organization the hourly losses can easily top $1 million per hour[1] or more.

Meanwhile, the frequency of cyberattacks on industrial operations is increasing, driven heavily by phishing or spear phishing exploits that start in IT and migrate to OT infrastructure; or through removable devices, which abound in industrial settings and can carry malware.

Bigger dangers are on the horizon. The use of AI to find and exploit vulnerabilities is growing, and Critical Infrastructure is increasingly targeted by adversarial nation-states intent on disruption.

Combine the high cost of downtime with the rising frequency of cyberattacks, and it's clear the risk calculus is significant for industrial organizations. Improving defenses can literally reduce plant downtime from cyberattacks and therefore provide a significant impact to the bottom line, making it a top priority for anyone managing production operations.

Let's explore a few modern industrial cybersecurity practices using the five NIST Cybersecurity Framework categories. These practices can help reduce risks and the duration of downtime during a cyberattack.

[1] Pingdom, https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/

NIST Category 1:
IDENTIFY

When a cyberattack strikes, defenders usually have more questions than answers. But it's important for incident responders to answer specific questions early on to quickly scope and respond, including: "What's affected?" and "Where are we vulnerable?"

Answering these crucial questions requires a complete, up-to-date inventory of assets that are most critical to the operation of production environments. In typical industrial organizations, assets number in the thousands to tens of thousands. Manufacturing operations, for example, have production line equipment and controllers, smart devices, sensors, and a host of other connected assets.

This volume, which is also frequently changing, can make asset inventories challenging to assemble. And collecting this information after an attack can cause massive delays, contributing to extended downtime. Ad-hoc asset inventory scans can take hours or even days of waiting for a maintenance window to avoid additional disruption. What's more, many organizations infrequently perform asset analysis in the first place, contributing to a higher vulnerability of cyberattack.

A key step in reducing downtime from cyberattacks is to implement a robust asset and vulnerability management program. Regular, automated asset inventories performed as often as daily, hourly, or in real time in some cases, confirms that defenders are always prepared with an accurate picture of the landscape. Gaining this visibility, you can determine if rogue assets have appeared on your network, and also if legitimate assets are exhibiting behaviors that point to threat actors. This brings fast focus to your efforts to prevent and respond to attacks, ultimately saving downtime in a cyberattack.

NIST Category 2:
PROTECT

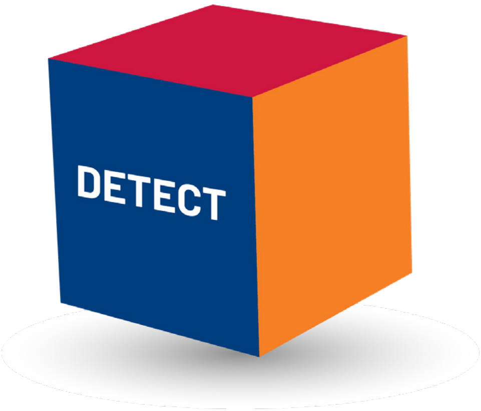
Implementing certain proactive measures can also minimize downtime from cyberattacks, by blocking threats before damage can occur.

One defensive priority for any organization is network segmentation. Network segmentation creates strict boundaries between systems, controls the flow of traffic and minimizes the risk of an attack spreading to other parts of the network.

In industrial organizations, a DMZ (Demilitarized Zone) is an architectural boundary between IT and OT networks, providing a critical air gap. With most industrial attacks starting in IT and migrating to OT, DMZ deployment is a key network segmentation strategy to limit IT attacks from gaining access into plant operations. (See Anatomy of 100+ Cybersecurity Incidents in Industrial Operations for more insights about industrial cyberattacks.)

Microsegmentation then provides another layer of defense. Threat actors tend to exploit the easiest pathways to achieve their ransomware and disruption goals. With a microsegmentation approach, protected segments are built around key data, applications, assets and services, with firewalls and strong access controls applied. As an added benefit, these measures are also key strategies in Zero Trust Architecture, which is an emerging compliance directive in the U.S. and other regions worldwide.

NIST Category 3: DETECT



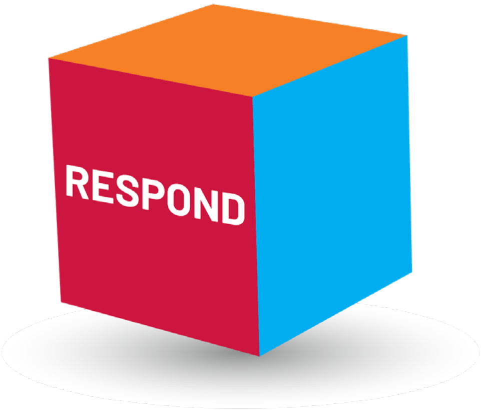
Once an adversary has breached your digital infrastructure, the race is on. Attackers know that response times are slowest at nights and on weekends and use this tactic to gain a head start.

Many well-publicized industrial attacks in the recent past began over holiday weekends. For example, malicious threat actors deployed DarkSide ransomware against Colonial Pipeline over Mother's Day weekend, and food processor JBS experienced a REvil ransomware attack over Memorial Day weekend.

Defending against modern industrial threats is not just a 'first shift' problem. It requires designing around-the-clock vigilance via network security monitoring to help ensure you're never giving the adversary a head start. Fortunately, organizations can beat the clock by deploying 24/7 network security monitoring using threat detection systems that let security teams leap into action in a matter of minutes. Continuous network security monitoring is a must-have for organizations seeking to limit downtime from cyberattacks.

Many industrial organizations find it difficult to staff a 24/7 security operations team, which is the required counterpart to detection. In these cases, a managed service can cost-effectively fill the gap, confirming defenders are always in place to detect and respond to threats quickly, minimizing downtime and preventing further damage.

NIST Category 4: RESPOND



In some industrial sectors - Life Sciences, for example - ransomware has become one of the leading sources of unplanned downtime.

Restoring systems and data is an exacting process, which can take hours or days under perfect conditions. Unfortunately, conditions are rarely perfect. Incomplete backups, incompatible software, and untrained staff can introduce complications and delays, adding days or even weeks to recovery time.

Recovery is another area where deep OT experience matters. Developing a mature recovery program takes methodical planning, backup steps, and regular testing to quickly resume normal operations and minimize downtime after a breach. And as with any complex process, practice makes perfect. It's important that each stakeholder in the recovery process understands their role and how to execute it. That can shave days or even weeks of downtime from the recovery process.

NIST Category 5:
RECOVER

In some industrial sectors - Life Sciences, for example - ransomware has become one of the leading sources of unplanned downtime.

Restoring systems and data is an exacting process, which can take hours or days under perfect conditions. Unfortunately, conditions are rarely perfect. Incomplete backups, incompatible software, and untrained staff can introduce complications and delays, adding days or even weeks to recovery time.

Recovery is another area where deep OT experience matters. Developing a mature recovery program takes methodical planning, backup steps, and regular testing to quickly resume normal operations and minimize downtime after a breach. And as with any complex process, practice makes perfect. It's important that each stakeholder in the recovery process understands their role and how to execute it. That can shave days or even weeks of downtime from the recovery process.

INVEST NOW TO SAVE DOWNTIME LATER

In industrial organizations, the potential for downtime from cyberattacks on OT infrastructure presents significant risks to operations, safety, and profitability. Implementing foundational OT cybersecurity measures can improve an organization's ability to identify, protect, detect, respond and recover from cyberattacks, reducing the risk of downtime and helping to ensure business continuity in the face of rising threats.

Rockwell Automation is the worldwide leader in industrial automation and industrial cybersecurity, with more than 100 years of experience helping organizations build solutions to complex problems. Our experts can help you to develop an industrial-strength OT cybersecurity program for excellent protection against today's sophisticated threats, enabling your production operations to keep moving.

Begin building your own business case for stronger industrial cybersecurity now. Download our free workbook, Build the Right Business Case for Your Industrial Cybersecurity Program. You can also watch a demo of a cyberattack and response on an industrial site. Or, contact us today to speak with an industrial cybersecurity expert.

Rockwell Automation

Securing What The World Relies On.

www.rockwellautomation.com

Publication GMSN-WP009A-EN-P-August 2023