Petri IT Knowledgebase Resource
A BWW Media Group Brand

Petri IT Knowledgebase

# Solving the 7 Major Pain Points for Manufacturing Availability

Sponsored by
Acronis

# CONTENTS

The processes running on the factory floor are critical for manufacturing businesses – any downtime immediately results in lost productivity and revenue. This means that protecting critical manufacturing applications like process control servers and keeping them highly available have always been a priority.

However, this need for high availability also presents several IT challenges that are unique to the manufacturing industry. For example, applications are usually highly specialized for different discrete processes but they often run on out-of-date operating systems like Windows XP. Software is mostly very stable and rarely (if ever) updated.

This whitepaper discusses the costs of manufacturing downtime, explores the main challenges in maintaining uptime, and considers data protection solutions that can support manufacturing IT infrastructure.

## Manufacturing Downtime is Expensive

The manufacturing industry depends on reliable, continuous production processes – every minute of downtime is extremely costly. Even so, downtime is not at all an unusual event for the sector. Industry studies show that almost every factory loses at least five percent of its productive capacity to downtime, and many lose up to 20 percent.

> On Average Manufacturers Have To Deal With Up To 800 Hours Of Downtime Annually

According to Aberdeen Research, 82 percent of companies have experienced unplanned downtime over the past three years. Research from Arimo shows that on average manufacturers have to deal with up to 800 hours of downtime annually. Factory downtime adversely affects the business in several vital areas:

- **Lost production** – Reliable manufacturing processes equate directly to profits. Production time losses directly impact the business's bottom line and reduce profits.

- **Lost capacity** – Factory downtime decreases overall productive manufacturing output.

- **Increased direct labor costs** – Direct, fixed labor costs remain the same whether the factory is producing or not. Downtime means that labor costs increase per goods produced.

- **Reputation damage** –Downtime decreases order fulfillment and product delivery, which can damage customer relationships as well as diminish the company's brand and valuation.

- **Financial loss from cyberattacks** – In addition to causing downtime, targeted cyberattacks like ransomware can force the business to pay cybercriminals in order to restore essential services and damage a company's reputation.

A recent report by Aberdeen estimates that unplanned downtime inflicts annual losses of $50 billion on the sector, with system failures accounting for 42 percent of outages. Per Aberdeen, "The cost of unplanned downtime can be devastating, ranging from an estimated $10,000 to $260,000 per hour for industrial plants."

While businesses may already be aware of these reports – or have experienced the impact directly – efforts

to improve reliability face several challenges that must be addressed. Fortunately there are solutions that can make reliability not only possible, but also easy and efficient to achieve.

# 1 Legacy data protection solutions are slow, complex and inadequate

Factory floor IT deployments typically include multiple servers performing discrete specialized tasks, with a different backup for each. Many applications run on older operating systems like Windows XP. Multiple backups yield operational complexity and increased manual intervention, prolonging recovery times.

## Solution

Use a data protection solution that can support a wide range of platforms (physical, virtual, cloud), operating systems, and application workloads that may or may not have network access to a centralized management console. Prioritize solutions that can create highly automated backup plans with a management interface that is intuitive enough for non-IT personnel to operate.

> "...downtime can be devastating, ranging from an estimated $10,000 to $260,000 per hour for industrial plants."

# 2 Ransomware and cryptojacking malware also attack uptime and performance

Ransomware is among the most pervasive malware threats to the manufacturing sector, encrypting the files of targeted servers to extort a ransom for the key to unlock them and restore service. Many ransomware variants include worm components that enable their proliferation over the network to other targets, including backup servers.

For example, in 2019 the Norwegian aluminum manufacturer Norsk Hydro was forced to shut down its internal network following a ransomware attack. This instance is not an exception to the rule – manufacturing is one of the most popular targets for cybercrime attacks, according the 2019 Global Threat Intelligence Report by NTT Security:

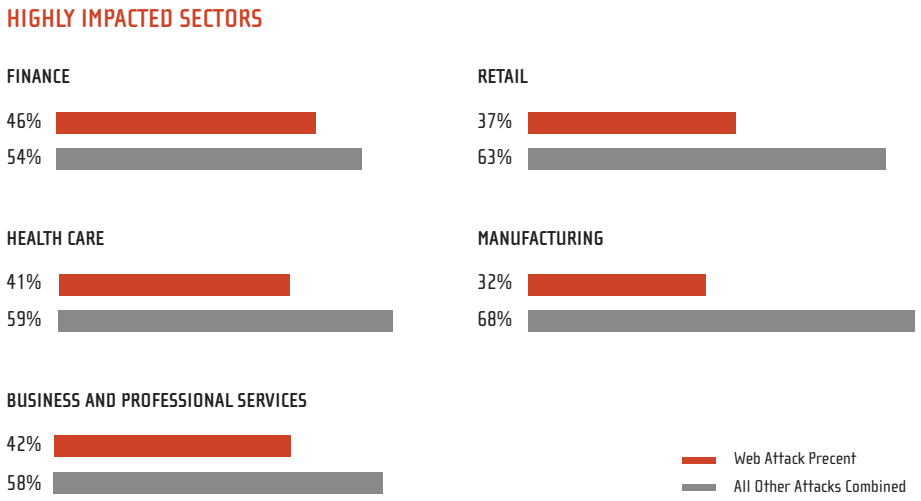


Figure 1 - Threat Impact by Industry

Cryptojacking is another pervasive malware threat that surged by 450 percent in 2018, per IBM's X-Force Threat Intelligence Index 2019. Servers and workstations infected with cryptojacking malware are used to surreptitiously mine cryptocurrency on behalf of remote cybercriminals, stealing system resources (CPU cycles, memory, power and cooling). The result is reduced system performance and availability, shortened hardware operating life due to increased wear-and-tear, and higher power and HVAC costs.

### Solution

Deploy a data protection solution that includes behavioral anti-malware features based on artificial intelligence and machine learning. These advanced technologies can be leveraged to identify and terminate high-priority threats like ransomware (including zero day attacks) and cryptojacking.

## 3 Factories lack skilled IT support staff

An Enterprise Strategy Group 2018 survey reported that 26 percent of the businesses surveyed identified backup and recovery as an area hampered by an IT skills shortage within their organization: Manufacturing is no exception. Plant engineers with limited IT skills often only have written procedures to rely on when it comes to restoring failed IT systems from backup.

> Deploy a data protection solution ... that enable[s] push-button backup and recovery for the entire factory environment

### Solution

Deploy a data protection solution that is easy for any administrator or staffer to manage, with automation features that enable push-button backup and recovery for the entire factory IT environment.

## 4 Manufacturing environments include aging operating systems and applications

Many manufacturing applications are ancient and stable. They are rarely updated and often run on antiquated hardware and operating systems. According to ARC Advisory Groups, "A significant percentage of today's global installed base of automation systems are at least 20 years old and becoming increasingly difficult and costly to maintain properly." A 2018 survey by Enterprise Strategy Group indicated that for 31 percent of businesses, modernizing data backup and recovery was the area they intended to invest in most significantly.

The imperative to keep these applications and their underlying OSes and hardware in a steady state complicates data protection. The conscious choice not to install new OS revisions or apply patches opens up security vulnerabilities that can be exploited by various malware attacks.

### Solution

Deploy a data protection solution that can restore any physical, virtual or cloud platform – running any operating system

and application workload – to dissimilar hardware if necessary.

## 5 Slow data protection is labor-intensive and yields incomplete backups

Legacy data protection solutions used in manufacturing typically require extensive manual intervention and significant man-hours to operate. Outages directly reduce productive hours and increase direct labor costs. Slow, labor-intensive backup operations can result in missed backup cycles and gaps in data protection. When the organization does encounter a system failure, the recovery process is often complex, multi-step, error-prone and potentially ridden with data gaps.

**The conscious choice not to install new OS revisions or apply patches opens up security vulnerabilities.**

### Solution

Deploy a high-performance data protection solution that is fast enough to meet the organization's recovery-time and recovery-point objectives, with automatically scheduled backup plans and fast restoral operations.

## 6 Recovery from backup is too slow

Most businesses experience an average of two outages per month, with each event lasting around six hours according to an Infonetics study. Meanwhile, Industry Week reported that restoring data from traditional backups is a long, highly manual process, taking hours or even days to complete.

**Deploy a high-performance data protection solution that can restore failed systems in minutes not hours, and can perform bare-metal and automated restoral operations.**

While it can take time to diagnose the problem and determine if there is a need to restore the system, most often significant, additional downtime results because the restoral process itself is lengthy. In some cases, older backup and restoral technologies can take hours to recover a single failed system.

### Solution

Deploy a high-performance data protection solution that can restore failed systems quickly from backups (ideally in minutes not hours), including the ability to perform bare-metal and automated restoral operations.

## 7 Backup operations are too slow to fit within allowable backup windows

In factory environments, finding suitable periods to perform backup operations is another challenge. That's because many production systems need to run 24x7, making it difficult to schedule backup times. These production environments are strictly managed and their computing resources are often limited. Slow backup operations may become even slower as data volumes grow, making it impossible to complete the current backup before the next one is scheduled to begin. This failure to fit within backup windows can result in significant data protection gaps.

## Solution

Deploy a data protection solution that has enough speed to complete backups within the allotted windows, can run concurrently with production applications with minimal performance impact, and if necessary, off-load backup management overhead to an ancillary server or virtual machine. To reduce the volume of data and the time required to perform backups, the solution should also support differential and incremental backups.

# Acronis Solves Manufacturing Data Protection Challenges

Acronis is a leading provider of data protection products and services to the manufacturing sector. Its flagship solution – Acronis Backup – delivers a unique combination of broad platform support, reliability, and simplicity that can provide complete data protection for manufacturing IT infrastructures.

Adopted by more than 500,000 businesses worldwide, it provides easy, efficient, secure backup for more than 21 platforms, including Windows XP, Linux, Mac, Windows 7, Windows 8, Windows 10 and Windows Server as well as virtualization platforms like VMware vSphere, Microsoft Hyper-V, Red Hat Virtualization and Oracle VM Server. It can restore failed systems to dissimilar hardware, including bare-metal physical servers, as well as to virtual and cloud environments.

Acronis Backup includes multiple features that address manufacturing industry pain points. Acronis Instant Restore reduces downtime by ensuring rapid restoral of complete systems from backups within minutes. Further, built-in Acronis Active Protection detects and terminates high-priority malware threats like ransomware and cryptojacking, providing AI-based behavioral anti-malware defenses that complement signature-based anti-virus solutions.

## Case Study: *The Marquardt Group Uses Acronis for Fast Recovery*

Marquardt Group, a leading manufacturer of electromechanical and electronic switches and switching systems, runs manufacturing processes in 19 locations on four continents, including the USA, China and India. The availability of its manufacturing processes is paramount – any data loss or system failure may result in costly production delays and delivery bottlenecks. Fast availability of production data and low recovery times are high priorities.

> "Acronis Backup is a secure, easy and fast backup that has brought our company a step forward..."
>
> Catalin Dragoman, System Administrator at Marquardt

Marquardt's data protection load is currently 40 terabytes of data running on 1,600 endpoints on a wide variety of operating systems. The company selected Acronis Backup as its data protection for its ability to quickly and reliably back up and restore a wide range of systems. It also found Acronis Backup to be easy to deploy and use, frugal in system and network resource consumption, and granular in its ability to recover entire systems or individual files as needed.

Catalin Dragoman, System Administrator at Marquardt says, "Acronis Backup is a secure, easy and fast backup that has brought our company a step forward since the availability of our production systems has greatly improved." Learn more about how the Marquardt Group is using Acronis to protect its critical manufacturing data here.

# Case Study: *Leading European Automaker Improves Process Control Recovery with Acronis*

A leading European automobile manufacturer wanted to improve its backup, recovery and data protection capabilities and so adopted Acronis Backup.

With its prior solution, the automaker could only restore its systems within 30 to 60 minutes, a time-consuming process that required extensive manual intervention. Each plant has an average of 100 control systems that required thousands of man-hours annually to restore. Production line maintenance windows were also time-constrained – there were many times when system backups could not be completed. Marquardt also wanted to defend production processes against the growing threat of ransomware.

Acronis enabled the automaker to centrally back up all of its systems via backup agents, without interrupting production operations, in half the time of its prior solution. Acronis Backup delivers automated backups and notifies the IT department if anything goes wrong. Within minutes, operations specialists can recover any failed system, reboot it, and get the production line running again. If a process control server is damaged beyond quick repair, integrated Acronis Universal Restore can restore it to a new replacement server, even one with a different hardware configuration. Meanwhile, built-in Acronis Active Protection automatically detects and terminates ransomware attacks, even for systems that are not running the latest patches.

Acronis

Learn more about how Acronis provides improved process control recovery for a major European automotive manufacturer here.

To learn more about Acronis Backup and download a complimentary 30-day trial, visit www.acronis.com/business.