WHITE PAPER

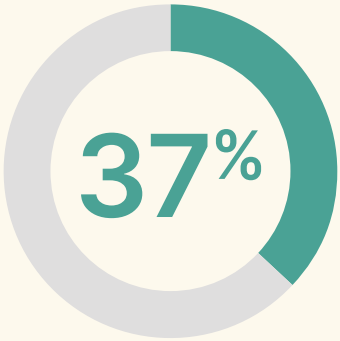
Mitigating the Hidden Threat of Shadow OT in Manufacturing

COPIA

Cybercrimes are a growing threat that are expected to cost businesses $9.5 trillion globally in 2024 (exceeding $10 billion in the U.S. alone), and to grow in excess of $10.5 trillion in 2025. A 2023 Claroty survey found that 37% of global respondents experienced a ransomware attack within the past year that impacted both IT and OT environments, up 10% in just the last two years. One of the ways hackers make their way into corporate systems is by exploiting a hidden malevolent asset many manufacturers don't even know they have: Shadow OT.

Shadow OT is the collective accumulation of both approved and unapproved devices, software, files, and improvised hotfixes that, while perhaps introduced with completely benign intent, represent the hidden corners of an enterprise. And where there are unknowns, there are potential security vulnerabilities.

This white paper examines the rising threat of Shadow OT and provides recommendations for securing modern manufacturing environments against these vulnerabilities.



The number of Global respondents who experienced a ransomware attack within the past year

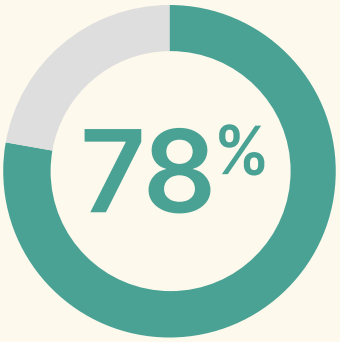
The Invisible Threat Within the Ranks

The rapid integration of IT and OT has introduced major security risks, as evidenced by high-profile cyberattacks on manufacturing facilities in recent years. The Triton attack on a critical infrastructure facility in 2017 was the first known attack targeted specifically at industrial safety systems (ISS). This attack led to a week of plant shutdowns, widespread business and process disruption, and untold revenue loss.

Ransomware has become a top threat to global manufacturing enterprises — this kind of attack on Toyota in 2022 caused 14 factories to shut down, creating a production loss of an estimated 13,000 vehicles. A 2022 survey by IBM revealed that 83% of respondents had experienced more than one data breach. Risks from such breaches include exposure of proprietary data, loss of visibility into processes, and regulatory non-compliance. In 2023, Clorox filed with the SEC to disclose an attack estimated at $356 million in addition to a drop in their stock price and the costs of re-securing their systems.

Such attacks point to the havoc that can be caused by poor OT security practices. Many facilities have a substantial number of unauthorized devices (i.e. Shadow OT) added without proper security controls. An example of Shadow OT could be as simple as a USB thumb drive that a well-meaning employee uses to upload the latest version of automation code to provide a much-needed hotfix. If those files are undocumented and not backed up, they remain outside the vision of the enterprise. This is concerning, as 78% of respondents to the soon-to-be published State of Industrial DevOps Report revealed that hotfixes are common across operations.

An unapproved device could be a host for ransomware, or present a gateway for hackers to break into the system. As manufacturing facilities adopt more industrial internet-of-things (IIoT) devices, their inherent connectivity further increases the potential risk of attack.



The number of respondents who experienced hotfixes are common across operations

The Importance of Visibility and Transparency

Securing a business requires it to maintain clear visibility of the road ahead. The further down the road it can see, the more able it is to prepare for these attacks. But forward vision is not the only perspective that helps bolster defenses. A business needs a clear 360-degree view to fully protect itself from harm. Assessing the current state of security is critical to creating a strong defense.

Transparency is another powerful tenet of organizational visibility. This is created by un-siloing departments and allows a company to surpass the perceived limits of its own visibility, seeing through barriers formed by systems architecture, processes, and policy.

While some barriers may be necessary for security, others are created as a byproduct of their environment and inhibit productivity. The ability to set the rules for visibility and transparency in an organization — providing permissions to approved people, following the Principle of Least Privilege (POLP) — can go a long way toward streamlining overall system workflows.

Surfacing Shadow OT

Surfacing Shadow OT requires more than looking around the factory floor for obvious holes and breaches. The vulnerability could be as innocuous as an approved server that an IT department installed to connect its operations to its cloud-based ERP system. If that server isn't equipped with the latest patch to protect it from a known vulnerability and no one is aware of it, it lies within the bounds of Shadow OT.

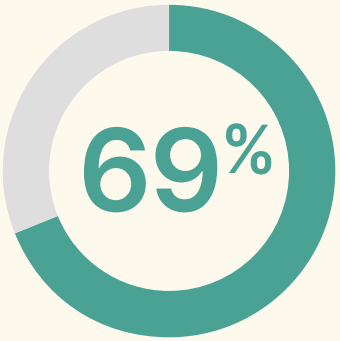
Today, it is reasonable to assume that manufacturers that have integrated their IT with their OT have some degree of Shadow OT in their midst. It is therefore important to understand what manufacturers and other businesses in industrial environments stand to lose if these risks are not mitigated.

Internal vs. External Threats

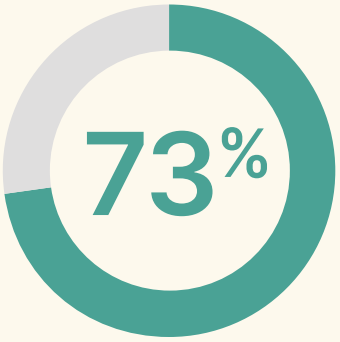
While the internal threat of Shadow OT is very real, we should not forget that external threats are also on the rise with a very costly impact. According to a 2023 survey, 69% of organizations targeted by ransomware paid the ransom demanded of them; more than half of those who paid ransoms suffered damages of $100,000 or more.

The truth is that many victimized organizations have no choice but to pay the ransom rather than risk prolonged plant shutdowns. Phishing (social engineering schemes to garner protected information) and the risks of exposure from third-party vendors all compound the challenge of securing operations.

A recent report found that 73% of surveyed organizations permitted third-party access to OT environments with scores of third parties granted such access in each organization. While external attacks garner headlines, insider risks are equally important. Unauthorized changes made by personnel with direct equipment access can introduce vulnerabilities or safety issues, such as in the case of the employee with a USB thumb drive. Strict access controls and change management processes are essential to a tight security policy.



Organizations targeted by ransomware and paid the ransom demanded



Permitted third-party access to OT environments

The Price of Poor Cybersecurity

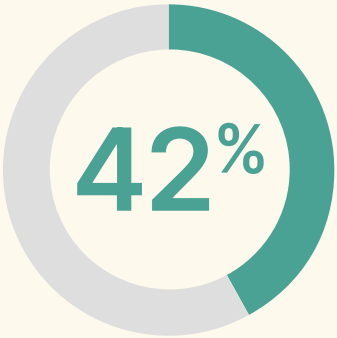
The financial impacts of cyberattacks in manufacturing go far beyond immediate equipment damage or ransom payments. Think of how much a business spends keeping its production line humming. It fine tunes the delivery of raw materials, its machinery, and its packaging to maximize output and uptime. The faster it goes, the more efficient it becomes. But that level of efficiency is glaring when its production line comes to a full stop. Each day it remains stuck is another day of compounding losses.

Recovering from an attack is expensive — organizations spend millions to replace hardware and audit controls. Extended downtime also erodes customer trust, damages brand reputation, and negatively impacts market share. Downtime also presents an opportunity for competitors to move into the marketplace.

Most customers will look elsewhere rather than wait for a business to get its factory back online. Proactive monitoring and defense is the only way to keep these risks at bay.

Best Practices for Mitigating Risk

To reduce Shadow OT risks, enterprises need to thoroughly document their processes and code changes. It is no secret that the status quo in OT is that automation code is often fragmented and not backed up. Copia Automation's forthcoming State of Industrial DevOps Report shows that 42% of respondents are using or adopting industrial coding software to achieve compliance with cybersecurity standards, while 41% use it for data integrity features and 39% for secure coding guidelines and vulnerability scanning.



Respondents using or adopting industrial coding software

OT environments are historically more static than IT environments, and for good reason. If a company is making the same product over a course of years, and the system is working, there's less incentive to introduce changes to the process that may disrupt the status quo. For this reason, operating in a closed environment makes sense. But changes to code still occur to make fine adjustments for equipment changes, specifications, and product enhancements. If those changes are not documented in a way that can be easily accessed and restored upon failure, that code becomes part of a company's Shadow OT.

By applying some of the best practices of IT—beginning with Git, a distributed version control system for tracking changes made to computer code over the course of its development—to operational technology, industrial enterprises can bring Shadow OT to the foreground. This will enhance the visibility of code changes across multiple vendor devices and, at the same time, provide a much-needed backup and disaster recovery system.

Where to go Next: Emerging Trends and Technologies

Global investment in cybersecurity is on the rise — Gartner estimates that global end-user spending on cybersecurity and risk management will surpass $215 billion in 2024, an increase of 14% over the previous year. The future focus is clearly on building security into processes from the outset rather than reacting to threats.

The OT security landscape, in particular, is evolving rapidly. Secure-by-design networks, Zero Trust architectures, micro-segmentation, and edge computing all help limit risks. Cloud-based monitoring platforms leverage big data analytics to detect anomalies and catch intrusions early. Machine learning and AI are rapidly being applied for user behavior analysis and

Estimated increase of spending on cybersecurity and risk managment in 2024

intelligent threat detection. Blockchain-based solutions ensure integrity of industrial data transactions and equipment software through algorithmic checks and gateways.

The Copia Industrial DevOps Platform uniquely empowers companies with unparalleled visibility and control of code across a diverse industrial environment to promote continuous quality control, streamlined production, and preemptive crisis management. It does so by providing a reliable single source of truth for code across various devices, languages, and locations to eliminate system malfunctions and downtime, expedite disaster recovery, and enforce quality control to optimize operations and increase revenues. The Copia Platform proactively documents and backs up OT code to shine a light on Shadow OT as a means of identifying and eliminating security risks.

As manufacturing facilities integrate IT and OT, Shadow OT will continue to pose significant risks to security and business continuity. Both external attacks and insider threats can lead to costly outages and safety incidents. Addressing security proactively across people, processes, and technology is essential for every manufacturer. The recommendations provided in this white paper can help secure sensitive OT environments against escalating threats and avoid disruptive incidents.

To speak to a Copia Automation representative about how the Copia Industrial DevOps Platform can shine a light on the Shadow OT in your enterprise and help manage your automation workflow more effectively, visit copia.io.