EBOOK

The Proactive Defense: Streamlining Cyber Insurance and Recovery with Industrial DevOps

COPIA

Introduction:

The Rising Stakes of Cyber Insurance in Manufacturing

In today's interconnected industrial landscape, the question is no longer if you'll face a cyber threat, but when. As a result, cybersecurity insurance has shifted from a "nice-to-have" to a critical component of any manufacturer's risk management strategy.

However, simply having a policy is not enough. Insurers are now demanding that companies prove they have a robust and tested cyber recovery plan in place. Without one, you risk policy denial, exorbitant premiums, or a voided claim when you need it most.

> Cybersecurity insurance has shifted from a "nice-to-have" to a critical component of any manufacturer's risk management strategy

This ebook will explore the challenges of meeting these stringent requirements and introduce a modern, proactive approach to building and maintaining a cyber recovery plan that satisfies insurers and, more importantly, truly protects your operations.

The Challenge: The Insurance Hurdle and the Recovery Plan Gap

For many industrial organizations, providing a detailed cyber recovery plan is a significant challenge. Insurers need to see evidence of:

- **Systematic Backups:** How do you ensure all critical automation code and configurations are consistently backed up?
- **Change Management:** How do you track and approve every change to your control systems to prevent unauthorized or malicious modifications?
- **Rapid Recovery:** How quickly can you restore operations to a known-good state after an incident?
- **Auditable Proof:** How do you provide a clear, auditable trail of all these activities to prove compliance?

Many manufacturers rely on manual processes, disparate tools, and institutional knowledge, making it nearly impossible to meet these demands effectively. This creates a dangerous gap between having an insurance policy and having a resilient operation.

> Many manufacturers rely on manual processes, disparate tools, and institutional knowledge

The Foundation of Resilience: Industrial DevOps and ICLM

To build a modern cyber recovery plan, we need to adopt a modern methodology. This starts with **Industrial DevOps**, which applies Lean, Agile, and DevOps principles to the entire lifecycle of industrial cyber-physical systems. It's a holistic approach focused on increasing resilience, accelerating development, and improving overall system quality.

But how is this methodology put into practice? The technical foundation of Industrial DevOps is **Industrial Code Lifecycle Management (ICLM).**

ICLM is the systematic management of all industrial automation code as a critical asset. It treats your PLC, robot, and HMI programs not as static files, but as dynamic assets that must be protected, tracked, and optimized throughout their lifecycle. An effective ICLM strategy includes:

1. **A Single Source of Truth:** A centralized, secure repository for all automation code.
2. **Automated, Reliable Backups:** Regular, automated backups of all critical devices.
3. **Complete Version History:** The ability to see every change made, by whom, and when.
4. **Collaborative Workflows:** A structured process for reviewing and approving changes.
5. **Rapid Restore Capabilities:** The means to quickly roll back to any previous version.

Essentially, a robust ICLM strategy is the tangible proof of a modern cyber recovery plan—it's exactly what insurers are looking for.

How Copia Automation Enables ICLM and Cyber Recovery

Copia Automation's platform is purpose-built to deliver on the promise of Industrial DevOps by providing a comprehensive ICLM solution. By treating your industrial code as a critical asset, Copia directly addresses the core requirements of cyber insurers.

Key Features for Cyber Resilience:

- **Git-based Source Control:** Creates a single source of truth for all your automation code. Every change is tracked, providing a complete, auditable version history that satisfies compliance and audit requirements.
- **DeviceLink™ Automated Backups:** Continuously backs up the code running on your PLCs and other industrial devices. This ensures you always have a recent, secure restore point, dramatically reducing your Mean Time To Recovery (MTTR).
- **AI-Powered Diff Descriptions:** When changes are detected, Copia's AI automatically generates a clear, human-readable summary of what was altered. This allows your team to instantly spot unauthorized or risky modifications, a key component of a proactive defense.
- **Collaborative, Approval-Based Workflows:** Enforce a structured process for code changes. This ensures that every modification is reviewed and approved before deployment, reducing human errors and improved detection capabilities of malicious attacks changes.
- **Disaster Recovery, Tested and Proven:** In the event of a ransomware attack or system failure, Copia gives your team the confidence and the tools to support your team as they restore operations from the last known-good state in minutes, not days. This proven ability to recover is precisely what insurers need to see.

The Copia Advantage: From Compliant to Confident

For companies with or seeking a cybersecurity insurance policy, Copia Automation provides:

- **De-Risked Operations:** Dramatically reduce your risk profile with a systematic approach to code management and recovery.
- **Simplified Audits:** Effortlessly provide insurers with the auditable proof they need.
- **Lower Premiums & Better Coverage:** A provably resilient operation makes you a more attractive client to insurers.*
- **Peace of Mind:** Move beyond simply having a policy to having a truly resilient operation, ready to weather any storm.

*Insurance premiums and coverage terms are determined by individual underwriters and are subject to their specific risk assessment criteria at the time of evaluation.

Conclusion:

Ready to build a cyber recovery plan that satisfies insurers and secures your operations?

Learn how Copia Automation can transform your approach to industrial cybersecurity.

Request a Demo

Connect with the Copia Team

Schedule a demo now or reach out to us directly at contact@copia.io for a personalized consultation.