EBOOK

Ransomware Ready Playbook for Operational Technology

COPIA

Introduction:

The Unseen Threat to OT — Ransomware

Ransomware, a type of malware that encrypts files and systems, demanding payment for their release, poses a severe and escalating threat to Operational Technology (OT) environments. The impact of a successful ransomware attack on OT can be devastating, leading to prolonged unplanned downtime, significant financial losses, disruption of essential services, potential safety incidents, and damage to an organization's reputation. The increasing convergence of Information Technology (IT) and OT, driven by Industry 4.0 and the Industrial Internet of Things (IIoT), has expanded the attack surface, making robust cybersecurity measures more critical than ever. This playbook provides a strategic roadmap to enhance your organization's OT ransomware readiness, helping you prepare for, prevent, detect, respond to, and recover from these insidious attacks.

> This playbook provides a strategic roadmap to enhance your organization's OT ransomware readiness, helping you prepare for, prevent, detect, respond to, and recover from these insidious attacks.

01 Understanding Your OT Environment: The First Step to Resilience

Effective ransomware preparedness begins with a deep understanding of your OT landscape. You cannot protect what you cannot see.

Architecture Development:

- **Why:** An in-depth evaluation of your current network architecture is critical for preparing for a security incident, identifying network weaknesses not utilizing a secure-by-design methodology, and beginning to understand how your architecture does or does not support your business workflows while maintaining security.
- **What:** Develop an OT architecture diagram including where segmentation exists, ingress / egress data flows, critical management assets, and sensitive data stores.
- **How:** Achieve this by collecting existing diagrams and documentation, interviewing key engineering and operations personnel, utilizing passive network discovery tools, performing physical site inspections, tracing critical data flows and protocols, and applying standardized diagramming notations such as the Purdue Model.

Comprehensive Asset Discovery & Inventory:

- **Why:** A complete inventory is the foundation of any cybersecurity program. It's essential for identifying critical assets, understanding interdependencies, and planning security controls.
- **What:** Catalog all OT assets, including PLCs, HMIs, SCADA systems, industrial PCs, network devices, IIoT sensors, and their configurations, firmware versions, installed software, communication paths, and criticality to operations.

01 Understanding Your OT Environment: The First Step to Resilience (continued)

- **How:** This is accomplished by deploying specialized OT passive discovery tools, integrating data from CMMS and engineering systems, conducting manual verification and physical inspections, enriching asset data with detailed attributes like firmware and criticality, establishing a centralized inventory database, and implementing an ongoing process for inventory updates.

Risk Assessment:

- **Why:** Not all assets and vulnerabilities carry the same level of risk. A thorough risk assessment that considers important factors to your business helps prioritize security efforts and investments.
- **What:** Evaluate the likelihood of ransomware exploiting identified vulnerabilities and the potential impact on safety, operations, and business continuity. Consider both direct impacts (e.g., system lockout) and indirect impacts (e.g., supply chain disruption). This assessment should inform your security roadmap and incident response planning.
- **How:** Conduct the assessment by adopting a recognized risk framework (such as NIST or ISA/IEC 62443), identifying system vulnerabilities and credible threat actors, analyzing the likelihood of threat event occurrence, assessing potential impacts on safety, operations, and business, determining risk levels by combining likelihood and impact, prioritizing these risks, and documenting findings along with recommended mitigation actions.

02 Building a Defensible OT Infrastructure: A Staged Approach to Security

Strengthening your OT environment against ransomware is an ongoing process, not a one-time project. Adopting a phased approach can make this journey manageable and effective.

Phase 1: Foundational Visibility & Control

- **Goal:** Establish a clear understanding of your OT assets and their current security posture.
- **Actions:**
  - **Business Workflow:** Interview your business partners to learn about the business workflows. In-depth understanding of your business workflows is critical for developing a usable secure-by-design architecture.
  - **Deploy Asset Discovery Tools:** Implement solutions that automatically discover and inventory all OT assets and their detailed characteristics.
  - **Network Baselining:** Understand normal operational network traffic patterns to help identify anomalous behavior later.
  - **Develop Basic Security Policies:** Start drafting or refining policies for access control, remote access, and change management specific to OT.

02 Building a Defensible OT Infrastructure: A Staged Approach to Security (continued)

Phase 2: Network Protection & Access Hardening

- **Goal:** Implement fundamental network security controls and strengthen access management.
- **Actions:**
  - **Network Segmentation:** Isolate the OT network from the IT network and utilize VLANsegments and Zero Trust Network Access (ZTNA) technologies within the OT environment to isolate critical systems. This help to limit the lateral movement of attackers if a breach occurs.
  - Secure Remote Access: Implement a remote access solution that supports multi-factor authentication (MFA),audited access, and session controls for all remote connections to OT systems, whether for employees or third-party vendors. Scrutinize and limit all external connections and ensure contractual controls are in for all third-party connections.
  - **Strengthen Access Control Policies:** Enforce the principle of least privilege, ensuring users and systems only have the access necessary for their roles. Regularly review and update access rights.
  - **Firewall Rule Review & Hardening:** Ensure firewalls between IT and OT (and within OT segments) are properly configured and regularly reviewed and consider the use of data diodes to enforce unidirectional data flows.

02 Building a Defensible OT Infrastructure: A Staged Approach to Security (continued)

Phase 3: Proactive Threat Management & Exposure Reduction

- **Goal:** Actively monitor for threats and reduce the overall attack surface.
- **Actions:**
  - **Continuous Monitoring & Threat Detection:** Deploy OT specific network monitoring solutions capable of monitoring OT network traffic to detect anomalous behavior, vulnerabilities, and known threat signatures in real-time.
  - **Comprehensive Vulnerability Management Program:** Establish a regular cadence for vulnerability scanning, risk assessment, and remediation. Track and manage vulnerabilities systematically.
  - **Vendor and Supply Chain Risk:** Evaluate third-party devices and services for enforcement of strong security hygiene and implement contractual requirements to maintain a security baseline including regular security patches.
  - **Physical Security Review:** Ensure physical access to OT assets and control rooms is adequately restricted and monitored.

02 Building a Defensible OT Infrastructure: A Staged Approach to Security (continued)

Phase 4: Strengthening Resilience with Industrial DevOps & Secure Code Management

- **Goal:** Implement advanced practices for managing industrial code, automating backups, and ensuring robust recovery capabilities.
- **Actions:**
  - **Version Control for Industrial Code:** Implement a centralized system for versioning all critical automation code (PLC programs, HMI configurations, SCADA projects, robot programs). This allows tracking of all changes, who made them, when, and why.
  - **Automated & Verified Backups:** Establish automated, regular backups of all critical OT system configurations, application software, and industrial code. Ensure backups are stored in multiple secure locations (including offsite/offline), and regularly test the restoration process to verify integrity and speed.
  - **Formalized Change Management Processes:** Implement and enforce a structured change management process for all modifications to OT systems and code. This should include review, approval, testing, and documentation.
  - **Secure Development & Acquisition Practices:** For any custom-developed OT software or when acquiring new systems, ensure security is a key consideration throughout the lifecycle.

03 Detecting Ransomware in OT: Early Warnings are Key

The sooner a ransomware attack is detected, the more effectively it can be contained.

- **Leverage Continuous Monitoring:** Utilize OT-aware monitoring tools to detect:
  - Anomalous network traffic (e.g., unexpected communication patterns, large data transfers to unknown destinations).
  - Unusual system behavior (e.g., unexpected process execution, high CPU/memory usage on controllers or HMIs).
  - Unexpected file modifications or encryption on engineering workstations or servers connected to the OT environment.
- **Endpoint Detection & Response (EDR) (where applicable):** For operating systems (Windows, Linux, and others) within the OT environment (e.g., HMIs, engineering workstations), consider deploying EDR solutions tailored for industrial settings.
- **Log Analysis:** Collect and analyze logs from network devices, servers, and critical OT systems. Centralized logging (SIEM) can help correlate events and identify suspicious patterns.
- **User & Operator Vigilance:** Train operations staff, engineers, and IT personnel to recognize phishing attempts, social engineering tactics, and early signs of a cyber incident. Establish clear procedures for reporting suspicious activity immediately.

04 Responding to a Ransomware Attack: Containing the Damage

A well-rehearsed Incident Response Plan (IRP) is crucial for minimizing the impact of an attack.

- **Develop a Specific OT Incident Response Plan:**
  - **Defined Roles & Responsibilities:** Clearly outline who is responsible for what during an incident (e.g., OT team, IT security, management, legal, communications).
  - **Communication Strategy:** Establish secure communication channels and protocols for internal teams and external stakeholders (including regulatory bodies if required by frameworks like NIS2).
  - **Containment Procedures:** Define steps to quickly isolate affected OT segments or systems to prevent further spread. This may involve disconnecting network segments or shutting down specific processes if deemed safe.
  - **Eradication Strategy:** Plan how to remove the ransomware from affected systems.
  - **Evidence Preservation:** Outline procedures for preserving evidence for forensic investigation.
  - **Decision-Making Framework:** Establish a clear process for making critical decisions, including whether or not to pay a ransom (law enforcement and cybersecurity experts generally advise against this, focusing instead on robust recovery capabilities).
- **Practice the Plan:** Regularly conduct tabletop exercises and simulations to test the IRP and ensure all team members understand their roles.

05 Recovering from Ransomware: Restoring Operations Safely & Efficiently

Recovery is not just about restoring data; it's about restoring trusted operations.

- **Prioritized Restoration:** Your Business Continuity Plan (BCP) should define the order in which systems and processes are restored based on their criticality to safety and operations.
- **Utilize Verified Backups:** This is where your investment in automated and verified backups pays off. Restore systems, configurations, and code from the last known-good backups.
- **System Validation and Hardening:** Before bringing restored systems back online, ensure they are clean of malware and apply any necessary patches or hardening measures identified during the incident.
- **Monitoring During Restoration:** Closely monitor restored systems for any signs of reinfection or unusual activity.
- **Post-Incident Review & Analysis:** After operations are restored, conduct a thorough review of the incident:
  - Identify the initial attack vector.
  - Analyze how the ransomware spread.
  - Evaluate the effectiveness of the response and recovery efforts.
  - Document lessons learned and update security controls, policies, and the IRP accordingly.

06 Fostering a Culture of OT Cybersecurity & Continuous Improvement

Ransomware readiness is an ongoing commitment that requires a security-conscious culture.

- **Bridge IT & OT Collaboration:** Foster strong collaboration and communication between IT and OT teams. Develop a unified cybersecurity strategy that addresses the unique needs of both environments.
- **Comprehensive Training & Awareness:** Conduct regular cybersecurity awareness training for all employees, tailored to their roles. This should cover topics like phishing, strong password hygiene, secure remote access practices, and incident reporting. Promote basic cyber hygiene as a shared responsibility.
- **Adherence to Compliance & Governance Frameworks:** Implement and maintain controls aligned with relevant industry standards and regulations (e.g., NIS2 Directive, ISO 27001, SOC 2, ISA/IEC 62443). Document processes and controls to facilitate audits and demonstrate due diligence.
- **Regularly Test & Update the Playbook:** The threat landscape is constantly evolving. Schedule regular reviews and updates to this playbook based on new threat intelligence, lessons learned from incidents (internal or industry-wide), and results from drills and simulations.

07 How Copia Automation Secures Your OT Environment Against Ransomware

Copia Automation's Industrial DevOps Platform is a cornerstone of a robust OT cybersecurity and ransomware readiness strategy. It empowers enterprises with unparalleled visibility, governance, and control over their critical automation code and configurations. Here's how Copia specifically helps:

- **Git-based Source Control — Your Foundation for Code Integrity & Visibility:**
  - **Unparalleled Visibility & Control:** Provides a centralized, version-controlled repository for all automation code (PLCs, HMIs, robots, SCADA configurations). This "single source of truth" ensures you know exactly what code is running on your devices and how it got there.
  - **Detailed Audit Trails:** Every change to your industrial code is tracked – who made the change, what was changed, when, and why. This is invaluable for forensic analysis after an incident to understand if code was tampered with and for demonstrating compliance.
  - **Secure Change Management:** Facilitates robust and auditable change management workflows. By enforcing reviews and approvals before deployment, it reduces the risk of unauthorized or malicious code modifications that could create ransomware entry points or exacerbate an attack.
  - **Rapid Identification of Malicious Changes:** Visual differentiation (diffs) allows engineers to quickly spot unexpected or unauthorized alterations to code, which could be indicators of compromise.

07 How Copia Automation Secures Your OT Environment Against Ransomware (continued)

- **DeviceLink™ — Automated Backups for Rapid & Reliable Recovery:**
  - **Automated & Secure Backups:** DeviceLink automates the backup process for critical industrial device configurations and code, eliminating manual errors and ensuring consistency. Backups are stored securely, providing reliable recovery points.
  - **Reduced Recovery Time Objective (RTO):** In the event of a ransomware attack that corrupts or encrypts device programs, DeviceLink enables rapid restoration to the last known-good state, significantly minimizing downtime and operational impact.
  - **Disaster Recovery & Business Continuity:** Forms a critical component of your disaster recovery plan, ensuring that your essential automation logic can be recovered quickly and efficiently, maintaining business continuity.
  - **Auditable Backup Evidence:** Provides clear, auditable proof that backups are being performed regularly and systematically, supporting compliance with frameworks like NIS2 and ISO 27001.

- **Copia Copilot™ — Enhancing Secure Coding Practices:**
  - **Improved Code Understanding & Documentation:** While primarily an AI tool for code generation, translation, and summarization, Copia Copilot aids in creating well-documented and understandable code. This clarity helps reduce human errors during development and maintenance, which can inadvertently create security vulnerabilities.

Conclusion:

By integrating Copia Automation's Industrial DevOps Platform into your OT cybersecurity strategy, you significantly enhance your ability to prevent, detect, respond to, and rapidly recover from ransomware attacks, safeguarding your critical industrial operations.

Connect with the Copia Team

To learn more about how Copia Automation's Industrial DevOps Platform can help bolster your approach to OT Cybersecurity, we invite you to connect with our team.

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