Manufacturing Cyber Risk Report

Insure24 manufacturing insurance downloadable report

A manufacturing cyber-risk report linking government cyber statistics to production downtime, ERP outage, ransomware, supplier portals and cyber insurance evidence.

Headline findings

- Manufacturing cyber risk should be framed around operational continuity: production planning, quality records, dispatch, stock control and supplier integration.
- Ransomware and phishing can become business interruption events when systems control orders, schedules, labels, tests or deliveries.
- Cyber insurance submissions are stronger when manufacturers evidence MFA, backups, patching, incident response and senior ownership.

Manufacturing Cyber Risk Scenarios

Scenario | Operational impact | Insurance evidence
- Ransomware locks ERP | Production scheduling and dispatch stop | Backups, recovery testing and incident response
- Phishing compromises supplier portal | Orders, invoices or delivery data are manipulated | MFA, user training and payment controls
- OT or test-data outage | Quality records or connected machinery are unavailable | Network segmentation and manual workarounds
- Customer data breach | Notification, investigation and reputation cost | Data mapping, legal response and cyber policy limits

Methodology

This report uses the Cyber Security Breaches Survey and manufacturing insurance scenarios to explain cyber as an operational risk, not only a data breach issue.

Related cover and report links

- Cyber Insurance for Manufacturers: https://www.insure24.co.uk/business-insurance/manufacturing/cyber-insurance/
- Business Interruption: https://www.insure24.co.uk/business-insurance/manufacturing/business-interruption/
- Manufacturing Risk Index: https://www.insure24.co.uk/business-insurance/manufacturing/risk-index/

Sources used

- Cyber Security Breaches Survey 2025: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025