# Specialist Cyber Protection: *For Manufacturing Firms*

Manufacturing firms not a cyber risk? *Think again*.

## The Key Exposures Facing Manufacturing Firms

### Convergence of IT and OT security

Routine IT procedures, such as antivirus updates and software patching, can lead to significant production disruptions and have the potential to temporarily shut down entire production lines. To further complicate the already challenging task, software updates are not always available for Operational Technology (OT) assets, leaving critical operational and production assets susceptible to security vulnerabilities.

### Interconnected risks from new technology

While new technologies have the benefit of increasing productivity, the complexity of such advancements also poses significant supply chain risks. Global malware events that impact supply chains may cause devastating widespread disruption and delay, often derailing the critical manufacturing processes.

### Business interruption and domino impact

While the Internet of Things improves efficiency in manufacturing with network-connected devices, it also provides increased exposure to attacks that can cripple ICS or supervisory control and data acquisition (SCADA) systems. Such disruptions can grind ordinary business to a halt and force manufacturers to incur significant costs to get back on-line and resume operations.

## How our Specialist Coverages Respond to the Threats Facing Manufacturing Firms:

We protect manufacturing firms against cyber threats by building resilience and minimising risk

**01** Broad definition of Dependent Business as a third-party entity that provides necessary products and services to the Insured Organisation pursuant to a written contract, including supply chain-related interruptions.

**02** Incorporates a qualifying period approach to business interruption coverage instead of a waiting period.

**03** Computer System definition includes technology such as Industrial Control Systems (ICS), Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA).

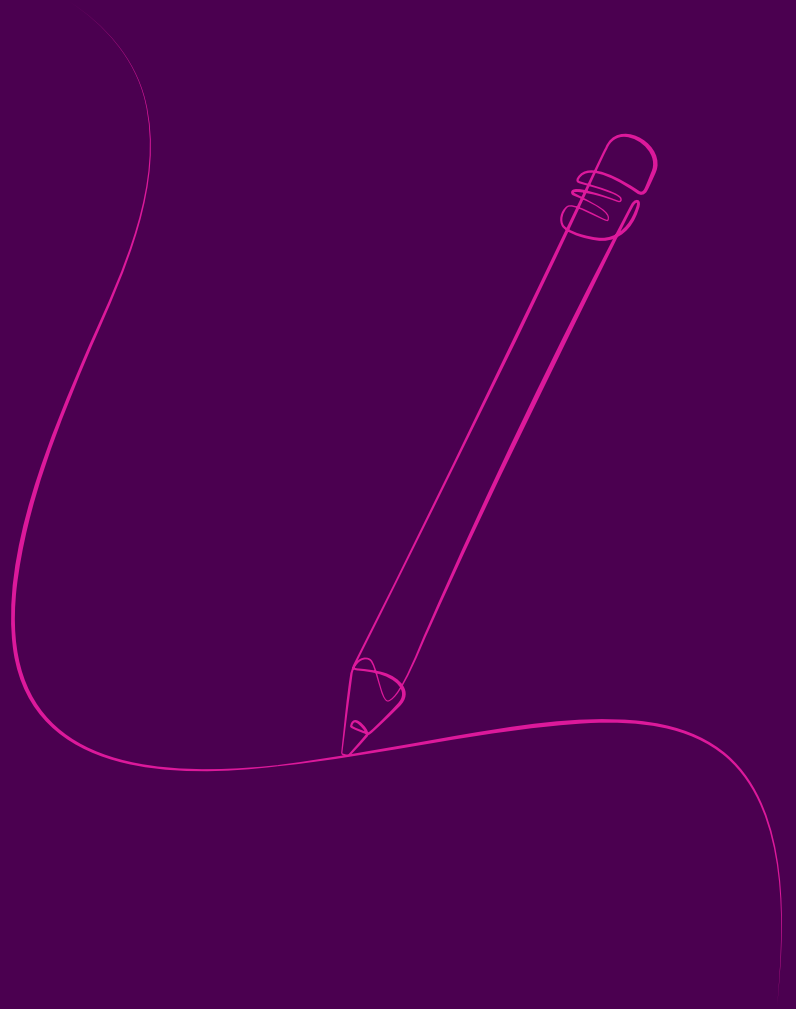
**04** Third party liability coverage for bodily injury claims arising from cyber incidents, available up to $250,000 sub-limit.

**05** “Bricking” coverage to replace computer devices or equipment stemming from a security breach related incident.

beazley

# Claims examples

## How our policy supports clients for the duration of the claim



### An automobile manufacture suffered a ransomware attack that encrypted the majority of systems and temporarily shut down production.

| | How our solution responded |
|---|---|
| The policyholder immediately contacted their Beazley Cyber Services Manager, who helped select expert privacy counsel and forensic experts to investigate and determine the scope of the incident. | **Cyber Services: Incident Helpline** |
| The digital forensics team determined that the threat actor did not access or exfiltrate any personally identifiable information, and privacy counsel concluded that there were no notification or regulatory reporting obligations. | **Cyber Services: Digital forensics, Legal Services** |
| Widespread encryption resulted in significant impact to business operations. Despite viable backup solutions, restoration was time-consuming. With depleted inventory and the inability to produce additional goods, the policyholder was unable to satisfy orders and suffered significant losses in income. | **First Party Loss Business Interruption** |
| While the policyholder did not incur notification costs or pay the ransom demand, the complexity of the ransomware event was costly. Significant data recovery expenses and business interruption losses resulted in the policy paying the full limit. | **Claims Support** |

### A tech device manufacturer was the victim of data theft and extortion.

| | How our solution responded |
|---|---|
| The policyholder immediately contacted their Beazley Cyber Services Manager, who quickly arranged for the services of a negotiation firm, privacy counsel, and forensic experts. | **Cyber Services: Incident Helpline** |
| The investigation confirmed that the threat actor exfiltrated sensitive proprietary data and files containing PII on numerous employees and customers. Privacy counsel concluded that the data triggered individual and state AG notification obligations. Privacy counsel drafted notices, and Beazley arranged for notification and call center services to support the process. | **Cyber Services: Digital forensics, Legal Services, Notification & Call Center** |
| The exfiltration and potential unauthorized publication of the sensitive proprietary data by the threat actor posed significant commercial risk. Beazley coordinated for a ransom negotiation firm that was able to settle the ransom event for $2M. | **First Party Loss: Cyber Extortion** |
| Post notification, the state's Attorney General responded with a data request that resulted in significant defense costs. Through the partnership of Beazley's panel regulatory counsel, the inquiry was closed without further action or penalty. | **Liability: Regulatory Defense & Penalties** |
| Beazley's policy covered the $2M extortion payment and defense expenses. The service provider fees and notification expenses were paid under the Policy's separate Breach Response coverage (outside the limit), preserving the remaining $3M of the $5M limit for potential future claims. | **Claims Support** |

beazley

# Reducing Risk –
# Cyber Security Advice For Manufacturing Firms

**01** **Incident response planning and tabletop exercises** - Create and stress test a plan regularly during tabletop exercises with key stakeholders; improve upon the issues raised during testing to improve response times.

**02** **Staff cybersecurity training -** Conduct regular phishing tests throughout the year to reduce human error.

**03** **Backups -** Develop and test backup and recovery plans; keep copies of sensitive or proprietary information in a separate and secure location. Test backups regularly to ensure both the technology, and the people, can function during a crisis.

**04** **Email security -** Properly configure spam filters, investing in antivirus protection, add multi-factor authentication, and use sandbox technologies to test for malicious messages.

**05** **Regular vulnerability scanning and penetration testing -** Engage a security firm to evaluate the attack surface and assess vulnerabilities. Determine if it is possible to move from the IT environment to the OT environment without permission. Report poor results to the executive team and create a remediation plan.

**06** **Vendor risk management -** Vet suppliers thoroughly, require Cyber Insurance for all service providers, and use standard contracts, questionnaires and forms for uniformity. Consider who is responsible for notification obligations if the vendor suffers an incident.

**07** **Enhance security by segmenting the IT network from the OT environment and segmenting OT from the internet.**

- Create separate user credentials to access the OT environment.
- Require and enforce MFA for remote access to the OT environment.
- Include OT as part of your logging and monitoring.
- Develop a plan for end-of-life assets: assess which assets can be decommissioned and restrict access where applicable.
- Annually assess the capability of security tools that are deployed across OT endpoints.

beazley

# Our Cyber Solution for Manufacturing

## Key coverages include:

- **Breach response:** Notifications, Forensics, Public Relations, Legal, Crisis Management
- **First party:** Cyber Extortion, Business Interruption, Dependent Business Interruption, Data Recovery, Extra Expense
- **Third party:** Data and Network Liability, Regulatory Defense and Penalties, Payment Card Liability
- **eCrime:** Fraudulent Instruction, Funds Transfer Fraud, Telephone Fraud

**Click here for more guidance in our Beazley Manufacturing BI Guide**

## Manufacturing Appetite