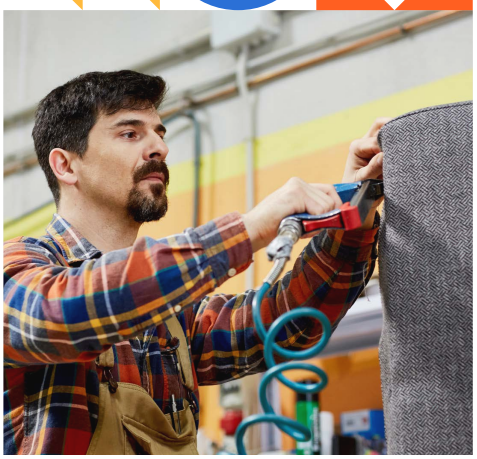
Coalition



THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Manufacturing Industry

Manufacturers rely significantly on both emerging and legacy technologies to operate efficiently and at scale. The critical nature of these technologies, however, make them a frequent target of cyber attackers looking to disrupt businesses and capitalize on high-value, often unprotected assets.

The manufacturing industry faces increased cyber risks due to the use of operational technology (OT) for automation and remote access, as well as interconnected systems — all of which are critical to the manufacturing process. Ransomware attacks can knock these systems offline, causing serious delays, disruptions, and even unauthorized access to sensitive data and physical equipment. In particular, industrial control systems (ICS) in manufacturing facilities are often outdated and lack proper security protocols. The possibility of physical damage to manufacturing equipment due to a cyber attack is also a unique concern for the industry, underscoring the need to prioritize cyber security measures that protect their operations.

Claims Insights

It's just a little security incident. How bad could it be?

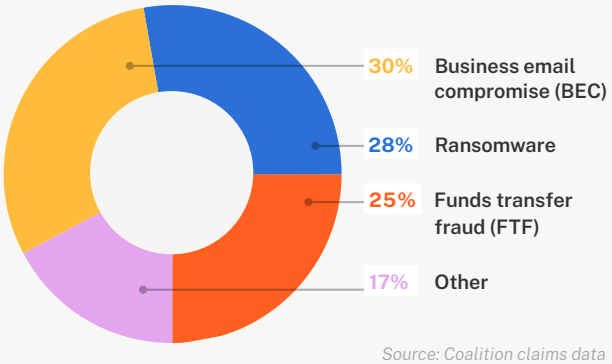
$224,000

Average cost of a cyber insurance claim for manufacturers

Claim Examples

ORGANIZATION	INCIDENT	LOSS
Electrical Discharge Machining	Business Email Compromise	$200,000
Laser Systems Manufacturer	Ransomware	$757,000
Skin Care Manufacturer	Funds Transfer Fraud	$331,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Although it's not the leading event type, the average FTF loss for organizations in the manufacturing industry is more than $391,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Unique Exposures

Most manufacturing businesses use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Email

Business email compromise (BEC) is the leading cause of cyber insurance claims for manufacturers, which can trigger data breaches, business interruption and even reputational damage.

End-of-life software & hardware

Organizations may use outdated technologies with the belief that upgrading would be expensive, time-consuming, and disruptive. However, technologies no longer supported by the manufacturer often have known security vulnerabilities and may lack important security features to protect against modern threats.

Enterprise resource planning (ERP) systems

ERP systems are crucial to manufacturing operations, consisting of processes, workflows, master data, and numerous interconnections with other internal and external systems. Cyber attackers are keenly aware of the valuable assets within these systems and frequently target them for the purposes of encryption and disruption.

Human-machine interfaces (HMI)

HMIs are used to control or monitor machinery, making them a common target of cyber attackers looking to disrupt manufacturing businesses. Unauthorized access to an HMI can cause operators to lose control of a machine and result in asset damage, destruction, or serious bodily injury.

Payment processing software

Funds transfer fraud and invoice manipulation are often major drivers of cyber claims. For manufacturing companies that use electronic payments, even one fraudulent transfer can have dire financial consequences.

Programmable logic controllers (PLC)

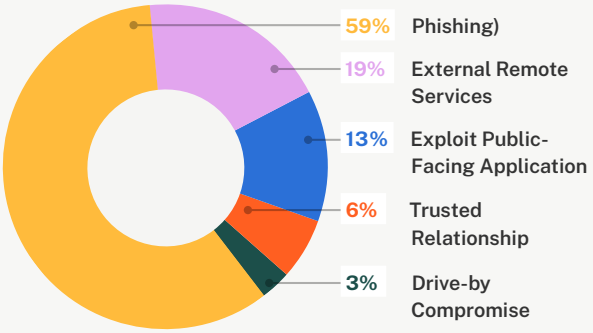
Similar to other industrial control systems, PLCs are used to monitor and control equipment in industrial and commercial environments. They're also vulnerable to cyber threats that can compromise an entire business operation, including network-based attacks, physical attacks, and malicious software attacks.

Supervisory control and data acquisition (SCADA systems

SCADA systems are a core component of manufacturing operations, used to manage and supervise machines and industrial processes. The devices used to run SCADA systems are typically connected to other IT systems and discoverable on the web, making them vulnerable just like any other internet-connected device. SCADA systems can also be difficult to secure with traditional cybersecurity technology and require compensating controls to sufficiently defend against cyber attacks.

Cyber Claims in the Manufacturing Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims.**



Source: Coalition forensics survey data

Coalition

Sensitive Data Can Increase Business Liability

Financial data

Collecting and processing financial information requires adherence to industry standards. Mishandling or unauthorized disclosure of financial data can cause direct harm to customers or vendors and trigger industry and regulatory investigations.

Legal and contractual data

Manufacturers may have access to contracts, legal agreements, and disputes, including settlements, judgments, and court orders. Mishandling confidential data can cause significant damage to the data owner.

Non-sensitive personal information

Some data may be publicly available and not considered protected, but a breach can still impact trust and public image if it appears the organization did not handle the situation appropriately.

Sensitive employee information

Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data can cause direct harm to employees.

Personally identifiable information (PII)

PII is any data that can potentially identify a specific person. PII can be used to launch cyber attacks or gain access to networks to initiate attacks. Organizations that mishandle PII or do not respond to a breach appropriately can be subject to fines, penalties, and other damages.

Intellectual property

Manufacturing companies may work with patents, designs, prototypes, proprietary processes, and other sensitive information that they must keep confidential to maintain a competitive advantage and protect products from copying or theft. Unauthorized access to proprietary manufacturing methods or production equipment data can undermine an organization's competitive advantage.

Protected health information (PHI)

Some manufacturers may have access to health-related information, such as disabilities or injuries, for the purposes of accommodation and compliance. All PHI must be protected to ensure medical privacy and comply with Health Insurance Portability & Accountability Act (HIPAA) regulations.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- HIPAA & business associate agreements
- International data privacy and consumer protection regulations
- State data privacy & consumer protection laws
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$4.47 million

Average total cost of a **data breach** for manufacturers[1]

1. IBM Security, Cost of a Data Breach Report 2022

Coalition

Business Impacts

What can manufacturers expect after a cyber incident?

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, most commonly first-party expenses. If a construction business experiences BEC and sensitive data is involved, it can trigger a need for additional legal counsel, forensic investigation, victim remediation, and notification. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. Relevant insuring agreements may include:

- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

Many manufacturers face new and unexpected exposures after a cyber event. Though most do not collect large amounts of sensitive personal information, they may have access to corporate confidential data and systems; some must also comply with industry standards or government requirements for protecting data. This type of information and access is typically addressed in contracts and often carries strict information security and disclosure requirements in the event of a breach, exposing firms to cyber liability they may not anticipate. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 3rd Party
- Multimedia Content Liability
- Network and Information Security Liability
- PCI Fines and Assessments
- Pollution
- Regulatory Defense and Penalties

Business interruption and reputation damage

Many manufacturers maintain a traditional IT environment for business applications, like email and ERP systems, as well as an OT environment for manufacturing activities. A cyber event that impacts either environment can have a significant impact on an organization's ability to manufacture and ship products. Even short periods of disruption can lead to direct loss of revenue due to delays, missed shipments, or physical damage to production lines. Delays can also affect contractual obligations and have a negative impact on client retention and acquisition. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a manufacturer or its clients — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, a business can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to clients, customers, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, a manufacturer may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

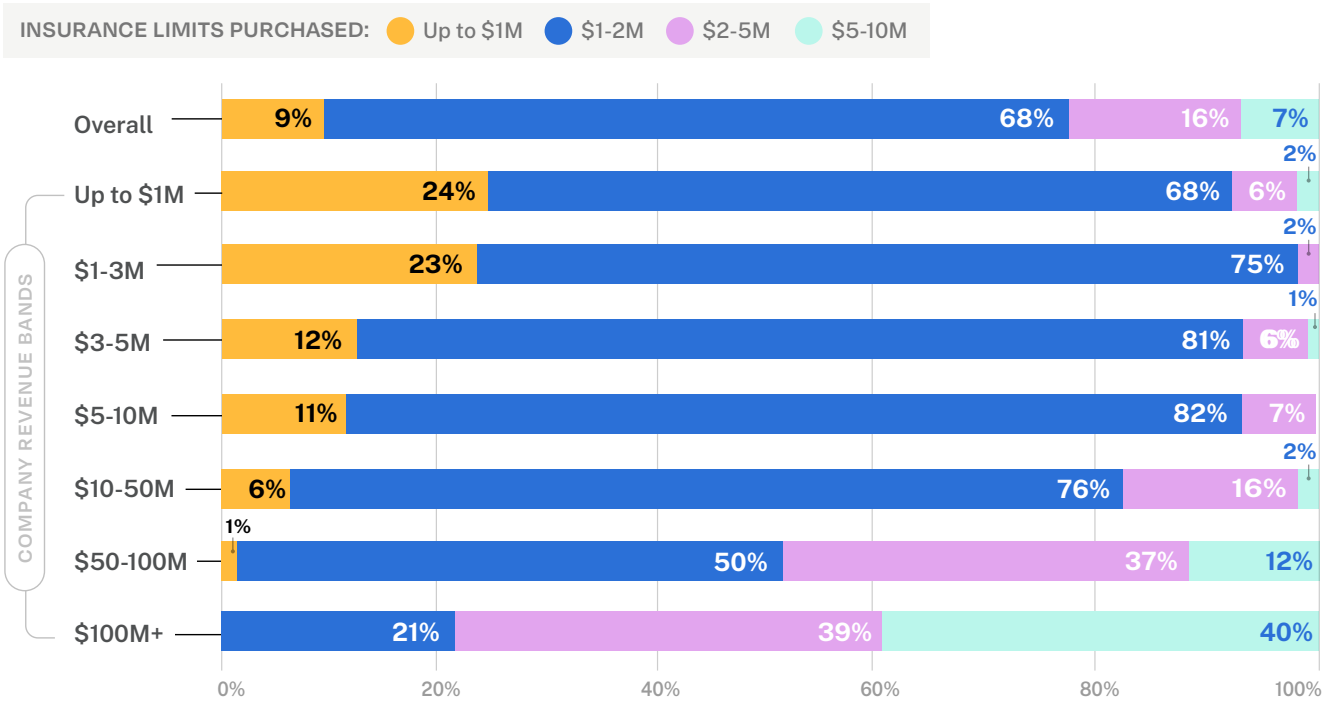
↓ 22%
Year-over-year decrease in Coalition claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the manufacturing industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT —— Most small and medium-sized businesses in the manufacturing industry purchase $1M-2M in limits, while many mid-market organizations purchase $5-10M in limits. For those needing more than $10M in limits, Coalition offers primary and excess terms for businesses up to $5B in revenue.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

The Power of Active Insurance

Why do manufacturers choose Coalition?

47%	43%	5 minutes
Reported cyber events handled with no cost to policyholder	Reduction in critical vulnerabilities among policyholders in 2022	Average response time to a cyber incident

Active Insurance* is designed to help prevent digital risk before it strikes.
Our new approach to managing digital risk provides **three layers of support**:

Active Protection

Monitoring and alerting to identify and prevent risk before it strikes

Active Response

Access to in-house resources that accelerate response and coverage if an incident occurs

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers

Get appointed today at signup.coalitioninc.com

Manufacturers

Get a free risk assessment at control.coalitioninc.com