# Manufacturing

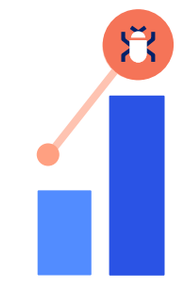
## Benefits of a Smart Cyber Insurance Policy

CORVUS BY TRAVELERS

### 1 The Big Picture

Historically, manufacturing companies have believed that they're an unlikely target for a cyber attack. This overlooks the industry's value to threat actors as a hub of valuable data, like credit card information and health records.

### 2 What's New?



**+1177%**

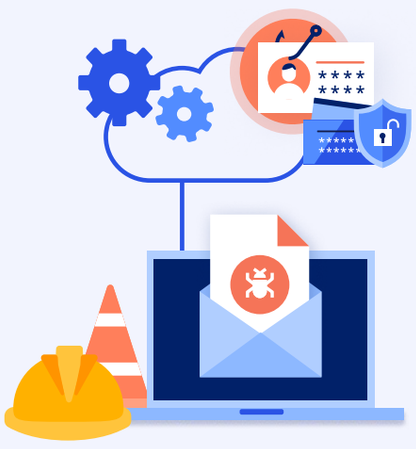
The industry faces timely challenges, such as increasing reliance on IoT products and a shift towards automation. The frequency of ransomware attacks on the manufacturing industry increased 1177% between Q1 2021 and Q1 2023.

### 3 The Risk Management Solution

Adequate cyber liability coverage and risk management practices are now essential. Companies in the Manufacturing industry should carry insurance to cover the cost of a cyberattack, including first- and third-party coverages such as ransomware and social engineering attacks.

# Cyber Claims Examples

## Phishing Email Scam

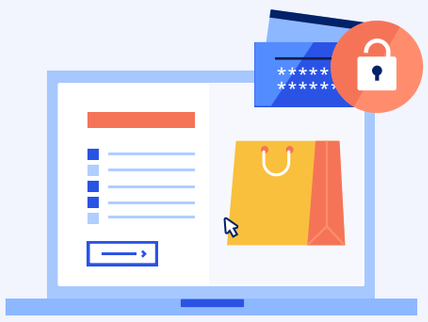


An employee at a manufacturer opened a phishing email that infiltrated its centralized network, exposing names, addresses, Social Security numbers and financial information such as credit card and bank account numbers of 5,000 of its customers.

A computer forensic investigator was hired and determined that Personally Identifiable Information (PII) was compromised.

The manufacturer notified the affected customers, offered free credit monitoring for one year and hired a public relations firm in anticipation of bad publicity because this was not the first time the manufacturer experienced a breach. Several states launched investigations and fines were imposed for the repeated failure to protect PII.

## Payment Card Data Breach of Online Ordering System

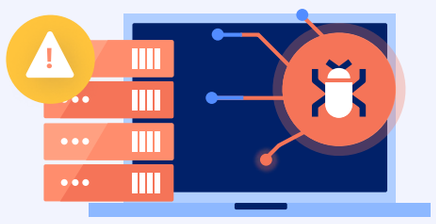


A clothing and accessories manufacturer with an online ordering system that supports 50% of its revenue suffered a cyberattack. The FBI notified the company that a hacker it had arrested had the credit card numbers of 500,000 of the company's customers in their possession.

After hiring a forensic investigator it was determined that the cybercriminal had compromised the online ordering system over a six-month period and exfiltrated customer names, addresses, credit card numbers, expiration dates, card security codes and email addresses.

The Payment Card Industry Agreement required the manufacturer to hire a certified forensic investigator to examine the company's systems and related infrastructure. The company also incurred significant costs as state law required the company to notify its affected customers and offer one year of free credit monitoring. The company ultimately hired a public relations firm to maintain customer confidence and limit reputational damage.

## Computer Virus



The server at a manufacturing plant was infected with an undetectable malware. Through this attack cybercriminals gained access to the manufacturing plant's production system, causing a shutdown that lasted several days. After discovering the incident, the manufacturer immediately retained a computer forensic expert to investigate. The manufacturer incurred substantial costs associated with repairing and restoring its systems. In addition, the company suffered significant revenue loss associated with the shutdown.

# Smart Cyber and Cyber Excess Policy Highlights

### Coverage for Privacy Laws & Fines/Penalties

There is a nationwide patchwork of privacy laws in effect across industries, and a manufacturer's failure to comply can lead to significant fines or penalties from state or federal agencies. Cyber coverage can respond to regulatory fines or penalties.

### Coverage for Third-Party Risk

Manufacturing companies increasingly transfer or entrust data to third-party vendors such as cloud storage companies. Third-party cyber coverage can respond when manufacturers face a breach, regardless of which organization's system was breached, or where the data resided at the time of the compromise.

### Risk Prevention Services

Through tailored threat alerts and partnership with in-house cyber experts, we're here to help policyholders reduce the likelihood of a cyber attack at their organization — and at no additional cost beyond their policy premium.

### In-house Claims Handling

When a security breach happens, every minute matters. Our in-house incident response and claims teams are available through the entire breach response process — before, during, and after an incident.

# Industry Benchmarks

**Limit Benchmarks**

While recommended limits will vary by the specifics of each risk, these benchmarks approximate the Smart Cyber Insurance coverage purchased by organizations grouped by gross annual revenue. (Corvus offers limits of up to $5m for primary and excess Cyber policies)

| Annual Revenue | Typical Limit Purchased |
|---|---|
| Up to $50m | $2m |
| $50m - $200m | $2m |
| $200m - $300m | $3m |
| $300m+* | $5m |

**Data reflects Corvus primary policies only. Policyholders may be achieving aggregate limits greater than $5 million through excess policies.*

## About Corvus

Corvus Insurance, a wholly owned subsidiary of The Travelers Companies, Inc., is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners.

Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance® and Smart Tech E+O®.



**Brian Alva**
Senior Vice President
Cyber TEO Underwriting

10/01/24