When the Line Goes Down: Cyber Risk and Insurance Considerations for Manufacturers

Sep 29, 2026

Categories:

Publications

Authors:

John T. Wolak

Manufacturing is under attack.

For several consecutive years, manufacturing has held an unwelcome distinction: the most heavily targeted industrial sector, accounting for more than two-thirds of all industrial ransomware incidents. Compounding this problem, a cyber incident at a manufacturer is rarely limited to unauthorized access to personal information or confidential data.

Instead, many ransomware attacks lead to operational and technology shutdowns that may halt production lines, delay shipments, disable safety systems, disrupt quality control, and compromise customers' personal and financial data and the company's trade secrets. And of course, a production shutdown delays revenue, strains customer relationships, and creates potential downstream contract, tort, and regulatory consequences.

Cybersecurity and privacy, therefore, should be treated by manufacturers as an enterprise risk sitting at the intersection of operations, contracting, legal, technology, and risk mitigation — not as just a technology line item.

Manufacturing Week 2026

Five informative sessions. Offered daily, virtually. Covering critical issues impacting manufacturers across their operations, workforce, and supply chains.

Learn More

Sector-Specific Cyber and Privacy risks

Every manufacturing operation has a unique cyber and privacy risk profile that is shaped by numerous potential vulnerabilities.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

Operational technology (OT) and information technology (IT) convergence: Industrial systems were historically kept separate from corporate networks, but for many companies, connectivity and efficiency gains have eroded — if not eliminated — that separation. In addition, manufacturing operations are often interconnected between multiple locations and different countries. When these discrete systems are connected or integrated, a single compromised corporate credential can ultimately lead to lateral access into the production environment and the ability to launch direct protocol exploits.

Ransomware and business interruption: A ransomware event that causes any operational downtime directly affects inventory, delivery schedules, and revenue. As a result, ransomware incidents remain a dominant driver of business interruption losses, and the magnitude of such loss for the company frequently dwarfs the cost of the underlying incident response, remediation, and notification.

Supply chain and vendor risk: Manufacturing breaches often involve a third party. For example, many manufacturers have suffered a cyber incident as a result of vendor access that was provided without adequately vetting the vendor's security program. In addition, even a cyber incident that is confined to a third-party vendor can indirectly cause substantial disruption and loss if mission-critical services or components are delayed or no longer available.

Insider threats and human risk: Human error is the most common pathway to credential theft, and business email compromise schemes — fake invoices and fraudulent bank detail changes — thrive in manufacturing's competitive, fast-moving and demanding business environment. And unfortunately, insider threats remain a recurring category of loss from employees, contractors, and temporary workers who intentionally misuse access to steal proprietary designs and formulas and disrupt operations.

Privacy obligations: Manufacturers collect, process, and store a broad range of data sets, including employee HR, payroll and health records, customer data, supplier information, biometrics, and vehicle or video recordings. There is no comprehensive federal

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

privacy statute, but manufacturers may be subject to sector-specific federal privacy and security obligations. It is likely that most manufacturers are also subject to a patchwork of state privacy statutes and regulations and the corresponding compliance obligations. In addition, sensitive non-public and proprietary information — whether company- or customer-owned — often requires special administrative, technical and physical controls to protect that information.

The Role of Cyber Insurance in Risk Mitigation

Manufacturing is a complex orchestration of facilities, machinery, supply chains, labor, contracts, and customer relations, and the associated cybersecurity and privacy exposures are real and can have a devastating impact on the business. Insurers have steadily limited or eliminated so-called "silent-cyber" coverage (i.e., coverage for cyber-related losses under policies not explicitly designed for cyber and privacy risks) through broad electronic-data, access-or-disclosure, and related exclusions. Therefore, manufacturers are at significant risk if they rely on traditional coverages for the range of potential cyber and privacy-related losses. A cyber policy often addresses the gaps in coverage under traditional policies, providing broader protection in the event of a cyber incident and any corresponding losses, costs, and expenses.

Cyber policies differ materially in definitions, triggers of coverage, exclusions, sub-limits, waiting periods, conditions, and endorsements. However, a typical cyber policy provides first-party coverage that includes the costs for forensic and legal services, notification and call center services, restoration or re-creation of data and systems, public relations and crisis management, and ransom payments. In addition to this coverage, manufacturers should assess the need for business interruption coverage to respond in the event of income lost from disruption of its own operations, as well as contingent business interruption coverage when a cyber incident at a vendor disrupts supply or services, and in turn affects the manufacturer's own operations. A typical cyber policy also includes third-party coverage for liability to others (including the costs of defense) arising out of individual claims or

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

consumer class actions, credit card issuer suits, and regulatory investigations.

A Risk Assessment and Insurance Planning Framework for Manufacturers

In order to assess its true cyber and privacy risk profile, a manufacturer should periodically assemble a cross-disciplinary group of stakeholders — from legal, risk management, IT, information security, finance, supply chain management, HR, compliance, and operations — to evaluate its risk exposure, including the following issues:

- What type(s) of data does the business collect, process, and maintain?
- What is the process and cost to recreate each data set if one or more is lost or inaccessible?
- What systems, data, facilities, and processes are essential to production and ongoing operations?
- How are IT and OT environments connected, segmented, and remotely accessed?
- Which vendor's services or supply could interrupt production if delayed or lost?
- What contractual, regulatory and notification obligations may be triggered in the event of a cyber incident?
- Which losses are retained, which are transferred by contract, and which are potentially insured?
- Do policy limits, retentions, waiting periods, definitions, and exclusions align with current and expected operations?

By completing this assessment, a manufacturer can effectively develop and implement an integrated risk mitigation and resiliency framework built on cybersecurity, privacy compliance, and insurance well before a cyber incident demands it and the production line — and the business behind it — comes to a halt.

Deeper Dive: Manufacturing Week 2026

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

On Friday, October 30, as part of our Manufacturing Week 2026 series, FBT Gibbons Partner John Wolak will present a webinar more closely examining the cyber risk equation for manufacturers. Attendees will gain practical insights into cyber insurance coverage, incident preparedness, breach response, and risk mitigation strategies that can strengthen organizational resilience. To view the full lineup and register, visit the **FBT Gibbons Manufacturing Week 2026** event page.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons