WHO IT’S FOR
Manufacturing organizations of all sizes who are seeking cyber and operational coverage beyond what is typically covered under a cyber insurance policy.

WHAT YOU GET
Tailored policy wording that addresses manufacturers’ specific cyber and operational risks, including:
• Supply chain interruption from cyber-attacks against your organization or suppliers.
• Invoice manipulation resulting in payments being misdirected or fraudulently directed.
• Technology disruption affecting operational and industrial controls, hardware and/or software.
• eCrime losses from payment or delivery of money or securities as a result of fraud.

WHO IT’S FOR
Manufacturing organizations of all sizes who are seeking cyber and operational coverage beyond what is typically covered under a cyber insurance policy.

WHAT YOU GET
Tailored policy wording that addresses manufacturers’ specific cyber and operational risks, including:
• Supply chain interruption from cyber-attacks against your organization or suppliers.
• Invoice manipulation resulting in payments being misdirected or fraudulently directed.
• Technology disruption affecting operational and industrial controls, hardware and/or software.
• eCrime losses from payment or delivery of money or securities as a result of fraud.

MANUFACTURING & AUTOMOTIVE
Manufacturer’s First Response, A Marsh and Beazley Breach Response Initiative

Manufacturers face a range of increasing cyber and operational risks that can cause significant economic loss. Even with the best systems, controls, personnel, and procedures in place, no manufacturer is immune.

Yet, current insurance offerings have not kept pace with the changing cyber risk landscape for manufacturers, and the unique nature of those risks.

To help modern manufacturers address fast-evolving cyber threats, Beazley and Marsh designed Manufacturer’s First Response, a Marsh and Beazley Breach Response initiative and continue to add and enhance coverages to respond to new and emerging risks.

Cyber Exposures for Manufacturers

Artificial Intelligence and Machine Learning:
The digital world has transformed many manufacturers into technology companies. From autonomous vehicles to avionics to consumer electronics, manufacturers are increasingly designing software and providing components driven by software. The potential failure or underperformance of these systems can expose manufacturers to new dimensions of risk that they have not traditionally faced.

Supply Chains:
New technologies have advanced supply chains, making them more productive than ever but also increasingly complex. With these new complexities, global malware events have the potential to cause wide-spread disruption and delay, or to derail critical manufacturing processes.

Industrial Control Systems (ICS):
Ubiquitous connectivity via the Internet of Things means manufacturers are susceptible to attacks that can disrupt networks and 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.

MANUFACTURING & AUTOMOTIVE
MANUFACTURING & AUTOMOTIVE
Manufacturer’s First Response, A Marsh and Beazley Breach Response Initiative

Manufacturers face a range of increasing cyber and operational risks that can cause significant economic loss. Even with the best systems, controls, personnel, and procedures in place, no manufacturer is immune.

Yet, current insurance offerings have not kept pace with the changing cyber risk landscape for manufacturers, and the unique nature of those risks.

To help modern manufacturers address fast-evolving cyber threats, Beazley and Marsh designed Manufacturer’s First Response, a Marsh and Beazley Breach Response initiative and continue to add and enhance coverages to respond to new and emerging risks.

Cyber Exposures for Manufacturers

Artificial Intelligence and Machine Learning:
The digital world has transformed many manufacturers into technology companies. From autonomous vehicles to avionics to consumer electronics, manufacturers are increasingly designing software and providing components driven by software. The potential failure or underperformance of these systems can expose manufacturers to new dimensions of risk that they have not traditionally faced.

Supply Chains:
New technologies have advanced supply chains, making them more productive than ever but also increasingly complex. With these new complexities, global malware events have the potential to cause wide-spread disruption and delay, or to derail critical manufacturing processes.

Industrial Control Systems (ICS):
Ubiquitous connectivity via the Internet of Things means manufacturers are susceptible to attacks that can disrupt networks and 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.
Specialized Coverage for Manufacturers

**Manufacturer’s First Response**, a Marsh and Beazley Breach Response initiative, offers the following coverages tailored specifically to cyber and operational risks faced by manufacturers (New and enhanced coverages are noted):

- **Supply chain interruption** — The policy provides coverage for supply chain interruptions caused by cyber-attacks against a manufacturer’s suppliers, in addition to attacks against its own organization.

- **Invoice manipulation** — Hacking and malware were the top cause of loss for manufacturers in 2019, according to Beazley data. The policy offers protection if a hacker breaks into a manufacturer’s system to manipulate invoices and redirects shipments of finished product to fraudulent or non-existent recipients.

- **Cryptojacking** — Coverage for loss and utility costs sustained from unauthorized use of access to computer systems to mine for digital currency. New

- **Technology disruption** — Computer system definition includes technology such as operational and industrial controls, as well as hardware and software used by manufacturers.

- **eCrime** — The policy addresses losses resulting directly from a manufacturer transferring, paying, or delivering money or securities as a result of fraudulent instruction, funds transfer, and telephone fraud.

- **Voluntary Shutdown** — Coverage for business interruption loss resulting from the voluntary and intentional shutdown of computer systems to limit loss from unauthorized access or use or infection of computer systems, or as required by regulatory or governmental entity. No prior content required from underwriter. Enhanced

- **State Consumer Privacy Acts endorsement** — Penalties and claims expenses related to violation of certain state consumer privacy laws. New

- **Reputation loss** — Coverage for losses resulting from adverse media publication of a data breach, security breach or extortion threat, and for claims preparation costs. New

WHY BEAZLEY?

Beazley, a leading insurer of technology and information security risks, has developed Beazley Breach Response, a solution to privacy breaches and information security exposures tailored to the needs of manufacturers. Beazley offers a complete privacy breach response management and information security insurance solution which includes a range of services designed to help manufacturers respond to an actual or suspected incident effectively, efficiently, and in compliance with the law. Beazley was the first insurer to establish a dedicated in-house breach response services team, BBR Services, that has helped thousands of clients manage cyber incidents successfully. BBR Services also provides a full range of resources to help mitigate risks before an incident occurs.

WHY MARSH?

Marsh’s Manufacturing and Automotive Industry and Cyber Practices are comprised of more than 750 colleagues who can help you understand, measure, and manage the risks facing your industry through market-leading analytics and risk assessment solutions. Marsh has more than 25 years of experience as a cyber insurance market broker and product innovator, working with industry leaders to better serve the needs of our clients. With more than 230 dedicated cyber specialists, Marsh’s Cyber Practice places more than $1 billion in premiums annually for more than 6,000 clients, with a client retention rate of more than 90%.