MARSH

Marsh's Financial & Professional Liability Practice (FINPRO)

ENHANCED COVERAGE FOR INTERNET OF THINGS PRODUCT MANUFACTURERS

Industrial control systems, smart buildings and homes, pacemakers, cameras, and even fish tanks — all of these Internet of Things (IoT) devices have been hacked by cyber-attackers looking to disrupt networks and extort users. As cyber criminals increasingly use IoT devices as a gateway to larger computer networks, the companies that manufacture IoT products face significant risks.

Marsh's Internet of Things insurance product provides manufacturers with coverage for a variety of risks that are often not insured under traditional general liability, cyber, errors and omissions, and property policies. The policy provides enhanced coverage for privacy, security, product services, intellectual property infringement, and cyber extortion risks stemming from connected devices.

IoT RISKS FOR MANUFACTURERS

The Internet of Things is the network of physical devices embedded with electronics, software, sensors, actuators, or network connectivity. These devices may collect and exchange data, control processes, or be controlled remotely. Some examples include smart homes, cars, and industrial products connected to the Internet with sensors for remote controlling and to report performance metrics.

Hackers are increasingly targeting manufacturers and IoT devices. Manufacturers were the most frequently targeted industry group in cyber-attacks in the second quarter of 2017, according to a NTT Security report. And researchers believe the use of industrial control systems and other IoT devices will lead to even more attacks.

Most manufacturers of both consumer and industrial products either have or

Who it's for

- Companies that design, manufacture, and sell IoT-enabled consumer, industrial, and medical products.
- Companies that provide services related to IoT products.

What you get

- Coverage for IoT-related risks that are generally not covered by traditional insurance policies, including:
  - Errors and omissions in the design, manufacture, service, and support of IoT devices, including those that result in a security or privacy event.
  - Copyright or trademark infringement by the software and firmware in the IoT device.
  - Cyber extortion threats stemming from IoT products.

soon will start to make their products "smart" by embedding electronics, software, sensors, actuators, or network connectivity. That opens the door for a number of critical risks, including:

- **Privacy:** Many connected consumer products collect and transmit personally identifiable information (PII) or confidential corporate information. An error or omission in the design or manufacture of an IoT product could result in a breach of customer privacy.
- **Security:** Some connected products might allow hackers to gain access to consumers' homes and/or networks or to extort money from consumers. An IoT attack could also allow hackers to take control or gain access to corporate or industrial networks, which may control HVAC systems, manufacturing facilities, electrical facilities, and more. And IoT products can be used in denial of service attacks.
- **Product Services:** Alleged errors or omissions could arise as a result of the design, manufacture, or support of IoT products, including data hosting, maintenance, and software patches/updates.
- **Intellectual Property Infringement:** Embedded software and firmware and the branding or labeling of IoT products could result in allegations of copyright and trademark infringement.
- **Cyber Extortion:** An IoT manufacturer could receive an extortion threat based on a potential attack against customers using deployed IoT devices.

MARSH'S IoT INSURANCE PRODUCT

Marsh's IoT insurance product provides two critical forms of coverage for IoT product manufacturers:

- **Liability coverage** for an act, error or omission, neglect, misstatement, or misleading statement in an insured's performance of IoT product services for others, including:
  - The creation, design, manufacture, development, distribution, license, lease, sale, or training relating to the use of an IoT product.
  - Hosting of data generated by an IoT product.
  - Prediction or performance of maintenance and servicing of an IoT product, including issuing software updates, services packs, patches and other maintenance releases provided for such products.
- **Cyber extortion coverage** for expenses from a threat directed against or using an IoT product.

For more information, contact:

SANDY CODDING
Managing Director
Marsh FINPRO
+1 617 385 0277
sandy.codding@marsh.com

ELISABETH CASE
Managing Director
Marsh FINPRO
+1 312 627 6819
elisabeth.case@marsh.com