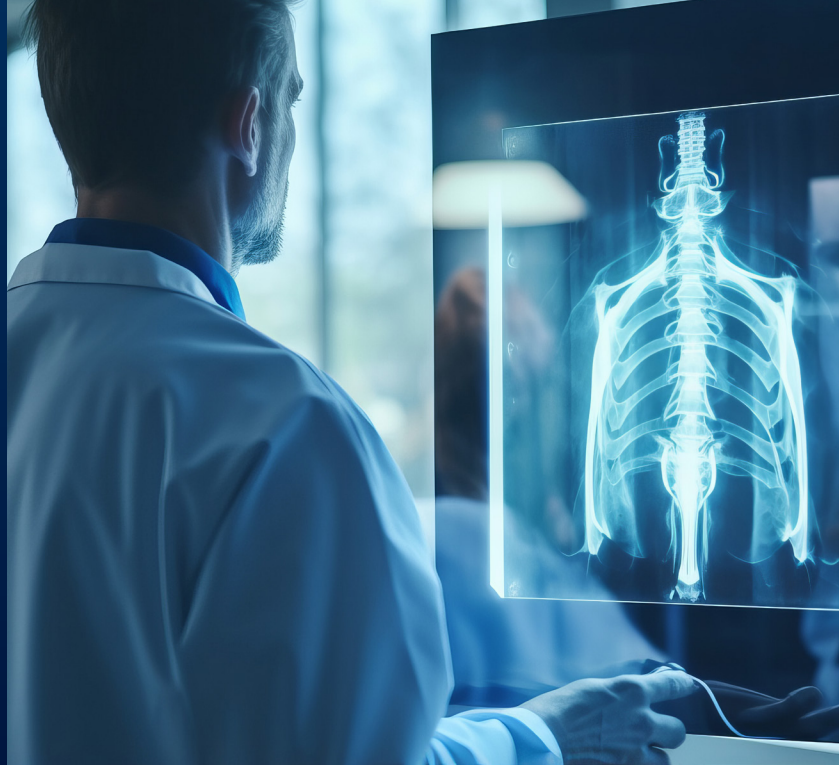
Brown & Brown

PROPERTY & CASUALTY

Cyber Coverage Handbook for Medical Devices

Risks, gaps in coverage and market availability

Authored by Christopher Keegan



Over the last 20 years, cyber insurance policies has evolved to provide a wide market for healthcare providers and technology companies supporting healthcare services, including medical device manufacturers and distributors. Today's cyber market covers the most critical cyber exposures, such as equipment failures, large-scale manufacturing outages and bodily injury claims. This handbook discusses insurance coverage for cyber risks arising from medical devices and related services and addresses opportunities to fill gaps in coverage.

Introduction to Insurance for Medical Devices: Existing Coverage Gaps and Market Availability

Companies that manufacture and distribute medical devices have a range of choices to insure risks that arise from cyberattacks and reliance on technology systems. Professional liability, medical malpractice, product liability, special crime and property insurance may provide some protection against cyber exposures. Cyber insurance policies have added cyber-caused property damage and bodily injury, as well as expanded with differences in conditions and limits umbrellas, to broaden coverage and ensure gaps are filled.

Medical devices that are internet and network-connected can potentially cause physical harm to patients. The most effective and protective type of insurance depends upon the organization seeking to be insured, its systems' configurations, its interactions and contracts with partners and to what extent outsourced vendors are used. All parties involved in providing medical services or products —hospitals, individual healthcare providers, manufacturers of devices, providers of software, etc. — might be held responsible for a breach or failure of a medical device. It is critical to implement a coordinated insurance program for all conceivable cyber risks with an understanding of the interactions between professional, product, property, cyber and other insurance policies.

Cyber Risks

Companies that supply or use medical devices face various cyber risks that can regularly change. The following discussion provides a brief overview of possible cyber risk scenarios.

Cyber Caused Bodily Harm to Patients

If an attacker can access devices and change settings remotely, they can physically harm patients.

Healthcare Provider

Medical professional coverage can help protect healthcare providers in cases of patient physical injury from failure of medical devices. A broad policy may not have exclusions for cyber related events. Although a cyber insurance policy can fill in gaps, adding bodily injury to forms is uncommon and must be specifically manuscripted. The necessary limits are likely unavailable.

Medical Device Manufacturers/Software, Services or Parts Providers

Patient physical harm caused by compromised or failed devices can be insured under a general liability and products liability (GL/products) policy. Technology errors and omissions (E&O) policies can be amended to provide contingent bodily injury coverage: bodily injury caused by digital events otherwise insured under the policy. Coverage under these policies should be aligned if they are purchased together.

Medical Device Seller

Patient physical harm caused by compromised or failed devices can also be insured under a GL/products policy for sellers of those devices. Such coverage can be selectively incorporated into cyber insurance programs with insufficient GL/products coverage, but customization is required. Sellers should also look to contract indemnifications from their distributors or manufacturers for protection.

Medical Device Exploit Causing Business Income Loss

Cyberattacks on devices are becoming increasingly common. Malware can include wiper viruses that “brick” equipment, which requires expensive replacements and lengthy outages that can result in income loss.

Healthcare Provider

For healthcare providers, traditional property programs can cover revenue loss due to devices compromised in cyberattacks; however, there are typically notable limitations and restrictions. Cyber insurance provides broader protection at higher limits and enhanced terms that can align with any available property coverage.

Medical Device Manufacturers/Software, Services or Parts Providers

Liability for financial losses caused by compromised or failed devices can be covered under E&O policies. Cyber policies can cover devices on the manufacturer’s network and the manufacturer’s direct losses. Contract terms will often provide protection.

Medical Device Seller

Liability for financial losses caused by compromised or failed devices can be covered under E&O policies. Contract terms can limit the ability to recover and provide further protection.

Medical Device as DDOS Platform

Distributed denial-of-service (DDoS) attacks can be launched from IOT and similar devices, causing outages at third-party networks.

Healthcare Provider

If devices on their network experience security failures, the responsible providers' only coverage option for the subsequent damages is a cyber policy.

Medical Device Manufacturers/Software, Services or Parts Providers

For this type of event, cyber and E&O policies can provide coverage for liability. It is best to incorporate both coverages in the same policy from the same insurer to avoid gaps or uncoordinated double coverage.

Medical Device Seller

A cyber policy is the only option that covers the harm that results from failures in security for devices that they are responsible for. Contract terms can limit the ability to recover and provide further protection.

Cyber Extortion

Threats to disclose exploits for devices, release confidential information or make data inaccessible are increasingly common. Companies with compromised or unadvanced backup systems may have to close operations for days or weeks.

Healthcare Provider

Cyber extortion costs can be covered under both special crime and cyber insurance policies. Resulting business interruption and liability may be covered under a property program with limitations or comprehensively in a cyber program.

Medical Device Manufacturers/Software, Services or Parts Providers

Both E&O and cyber policies can cover liability for failures at healthcare facilities caused by medical device manufacturers. To avoid gaps or crossovers in coverage, the recommended structure is a combined policy through the same insurer.

Medical Device Seller

A cyber policy is the only broad option that covers the damages that result from security failures on a network for which an insured is responsible. Contract terms can limit the ability to recover and provide further protection.

Breach of Patient Confidentiality

It is essential for businesses to have insurance for a potential failure to protect confidential healthcare information that may be collected from and on medical devices. If a breach occurs, there are direct costs for forensics, lawyers, lawsuit/regulatory action defense and more.

Healthcare Provider

A cyber policy is the only option for broad coverage of the consequences of failing to protect personal healthcare information. This can cover civil liability, response costs and regulatory fines and penalties.

Medical Device Manufacturers/Software, Services or Parts Providers

Cyber and E&O policies can provide coverage for liability, with cyber adding additional coverage for direct breach response costs. The recommended structure is a combined policy through the same insurer to avoid gaps or crossovers in coverage if both are purchased.

Medical Device Seller

A cyber policy is the only broad insurance coverage option for the harm done to others because of failures to protect personal healthcare information. Contract terms can limit the ability to recover and provide further protection.

Recall

If the security issues on the devices cannot be fixed remotely, companies face the possibility of a recall or removal of the device from the healthcare provider's premises and marketplace. Healthcare providers may face direct costs and income loss as a result. Manufacturers may be responsible for the cost of replacing and recalling devices and reimbursing the costs their clients may incur as a result. Companies in the medical device supply chain can be subject to the same liabilities as manufacturers. Insurers now offer targeted recall products to cover these types of exposures, but they have a limited appetite and coverage can vary markedly. Certain policies may cover first-party claims, while others will consider liability. Some may cover the cost of media and crisis management. Recalls are costly, and only some of these expenses may be mitigated by insurance.

Exposure	Healthcare Provider	Device Manufacturer	Software Provider	Supplier or Retailer
Bodily Injury				
Business Interruption (Healthcare Facility)				
Attack Devices				
Cyber Extortion				
Compromised Device (Liability)				
Device Recall (Direct Costs)				
Device Recall (Liability)				
Patient Confidentiality				

Key

- Medical and Products Liability
- Products Liability
- Cyber
- Technology E&O
- Property
- Special Crime
- Recall
- GL/Products

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com