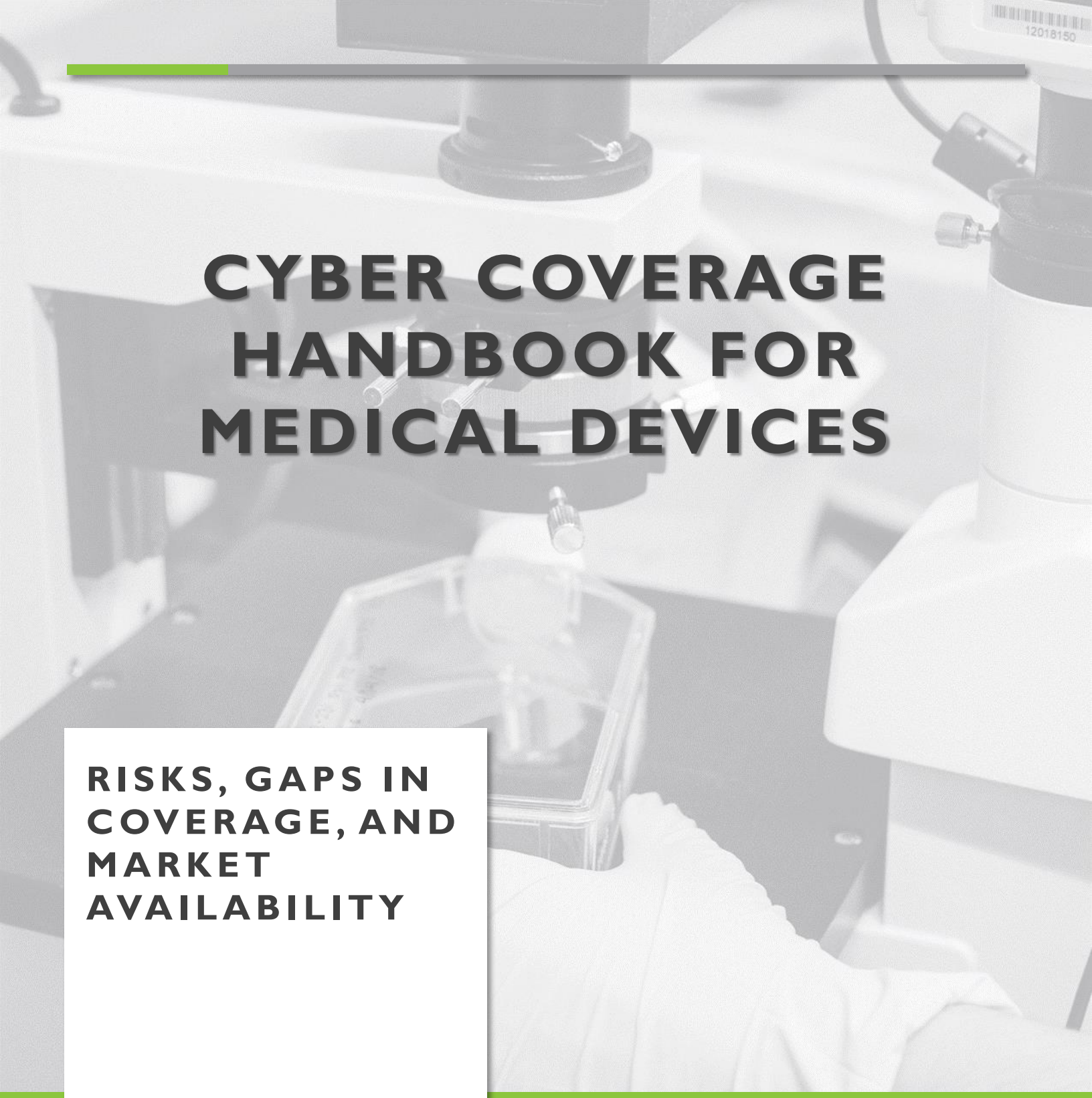


CYBER COVERAGE HANDBOOK FOR MEDICAL DEVICES

RISKS, GAPS IN COVERAGE, AND MARKET AVAILABILITY

BEECHER CARLSON

Cyber insurance policies have developed and expanded over the last 20 years to the point where there is a wide and deep market available for healthcare providers and technology companies supporting healthcare services including medical device manufacturers and distributors. Today's cyber market is now able to cover the most critical cyber exposures, ranging from equipment failures to large scale manufacturing outages to claims for bodily injury.

This handbook provides an overview of insurance coverage for cyber risk arising from medical devices and related services and addresses opportunities to fill gaps in insurance coverage.

INTRODUCTION TO INSURANCE FOR MEDICAL DEVICES: EXISTING COVERAGE GAPS AND MARKET AVAILABILITY

Companies which manufacture and distribute medical devices have a range of choices with respect to how they insure new risks arising from cyber-attacks and reliance on technology systems. Professional liability, medical malpractice, product liability, special crime and property insurance each may provide some level of protection against cyber exposures. Cyber insurance has been adding coverage for events such as cyber-caused property damage and bodily injury and has expanded with difference in conditions and difference in limits umbrellas to allow companies to broaden their coverage and ensure gaps are filled.

Medical devices which are internet and network connected have significant potential to cause direct physical harm to patients. Recently pharmaceutical and healthcare companies were surprised by cyber-attacks resulted in large losses at levels which were not predicted. The property insurance market has largely been reducing coverage that has been available to cover such business interruption exposures while cyber insurance market has been developing new ways to provide protection with innovations such as zero hour waiting periods and broad contingent business interruption provisions to cover supplier downtime.

The type of insurance which will be effective to protect a company depends upon the type of organization seeking to be insured, the way in which they configure their systems, their interactions and contracts with their partners, and the level of use of outsourced vendors. All of the parties involved in providing medical services or products, whether it is a hospital, individual healthcare provider, manufacturer of devices or provider of software might be held responsible for a breach or failure of a medical device. Insuring each requires an individual analysis. Understanding the interaction between professional, product, property, cyber and other insurance policies and implementation of a coordinated insurance program for all conceivable cyber risks is critical to a leading strategy.

CYBER RISKS

Companies that supply or use medical devices face numerous and varied cyber risks which change every day. The following provides a brief snapshot of just some of the cyber risk scenarios possible.

CYBER CAUSED BODILY HARM TO PATIENTS

When an attacker is able to access devices and change settings on those devices remotely to be able to act to harm patients by changing settings.

HEALTHCARE PROVIDER

Healthcare providers should look primarily to their Medical Professional coverage to protect them against suits. Medical and Products Liability policies may not always be broad enough to cover failures in medical devices that rely upon software code, networks and computer technology to operate. Underwriters of those policies often indicate that they look to cyber or technology E&O programs for coverage. A broader interpretations of Medical policies would allow coverage because there are no specific exclusions. Cyber insurance policies can fill any gap but they must be specifically manuscripted to do so.

MEDICAL DEVICE MANUFACTURERS OR SOFTWARE, SERVICES OR PARTS PROVIDERS

Patient physical harm caused by devices being compromised or failing can be insured under a General Liability and Products Liability (GL/Products) policy. Such cover can be incorporated into cyber insurance programs where the GL/Products coverage is insufficient or not available but customization of the cyber policy is required. Technology E&O policies can be amended to provide "contingent bodily injury" coverage, that is, bodily injury caused by digital events otherwise insured under the policy.

MEDICAL DEVICE SELLER

Patient physical harm caused by devices being compromised or failing can be insured under a GL/Products policy for sellers of those devices. Such cover can also be incorporated into cyber insurance programs where GL/Products coverage is insufficient or not available but customization is required. Sellers should also be looking to contract indemnifications from their distributors or manufacturers for protection.

MEDICAL DEVICE EXPLOIT CAUSING BUSINESS INCOME LOSS

Cyber-attacks on devices are becoming an increasingly common occurrence. Recent malware has included wiper viruses which "brick" devices requiring expensive replacement and resulting income loss.

HEALTHCARE PROVIDER

Financial loss at hospitals or other providers caused by devices being compromised can be covered under traditional property programs but usually only to a limited degree and usually with restricted limits. Cyber insurance provides broader cover at higher limits which can be aligned with any property cover that is also available.

MEDICAL DEVICE MANUFACTURERS OR SOFTWARE, SERVICES OR PARTS PROVIDERS

Liability for financial loss at hospitals or other providers caused by devices being compromised or failing can be covered under an Errors and Omissions policy. Cyber policies can provide cover where the device is on the manufacturer's network and the loss is direct to the manufacturer.

MEDICAL DEVICE SELLER

Liability for financial loss at hospitals or other providers caused by devices being compromised or failing can be covered under an Errors and Omissions policy. The question is whether the seller can be held liable for the financial loss.

MEDICAL DEVICE USED AS ATTACK DEVICES

Medical devices with deficient security can be taken over and used for Denial of Service attacks and Distributed Denial of Service attacks. Resulting downtime of computer systems of vendors, partners, customers and clients can result in liability for financial loss and possible theft or release of confidential information.

HEALTHCARE PROVIDER

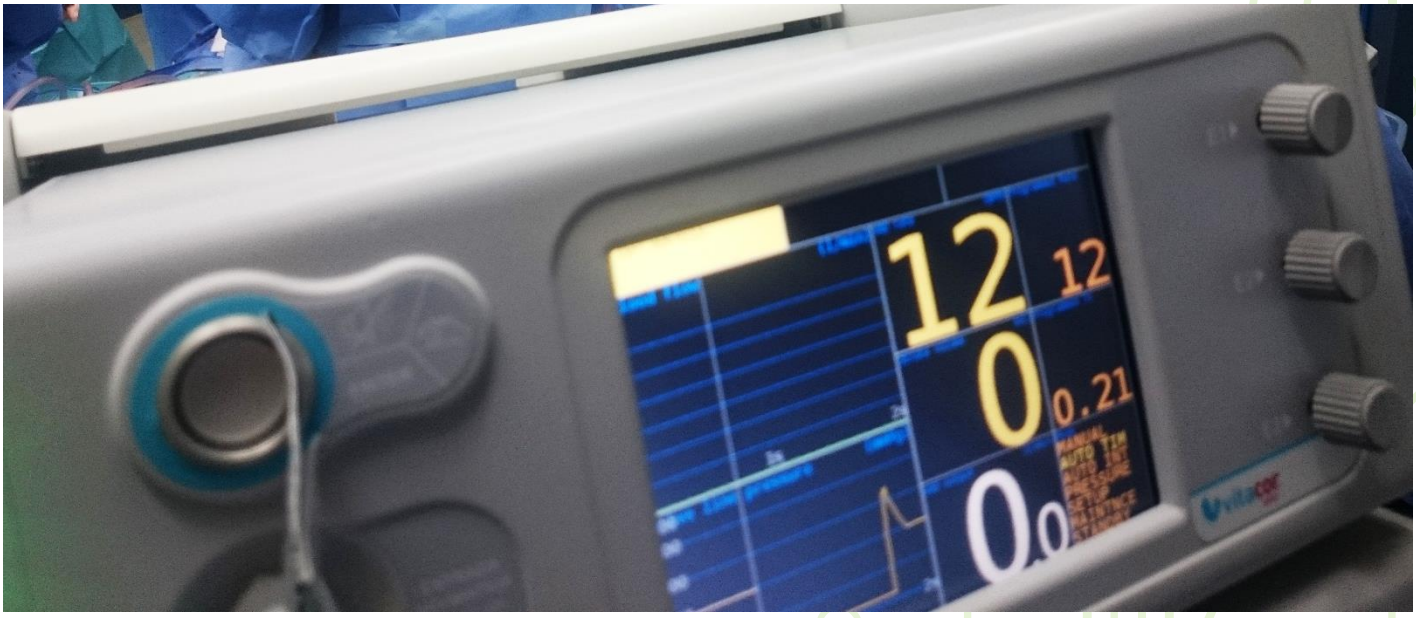
A cyber policy is the only real option for this coverage for the harm done to others as a result of failures in security for devices that they are responsible for.

MEDICAL DEVICE MANUFACTURERS OR SOFTWARE, SERVICES OR PARTS PROVIDERS

Cyber and E&O policies can provide coverage for liability as a result of this type of event. In order to avoid gaps or uncoordinated double coverage, it is best to incorporate both coverages in the same policy from the same insurer.

MEDICAL DEVICE SELLER

A cyber policy is the only real option which would encompass the harm done to others as a result of failures in security for devices that they are responsible for.



CYBER EXTORTION

Threats to disclose exploits for devices, release confidential information or make data inaccessible are becoming an increasingly common occurrence. Companies which do not have advanced backup systems or have had their backup systems compromised by the attacker may have to close down operations for days or weeks in order to repair their systems. Recent ransomware has included wiper viruses which "brick" systems requiring expensive replacement of hardware.

HEALTHCARE PROVIDER

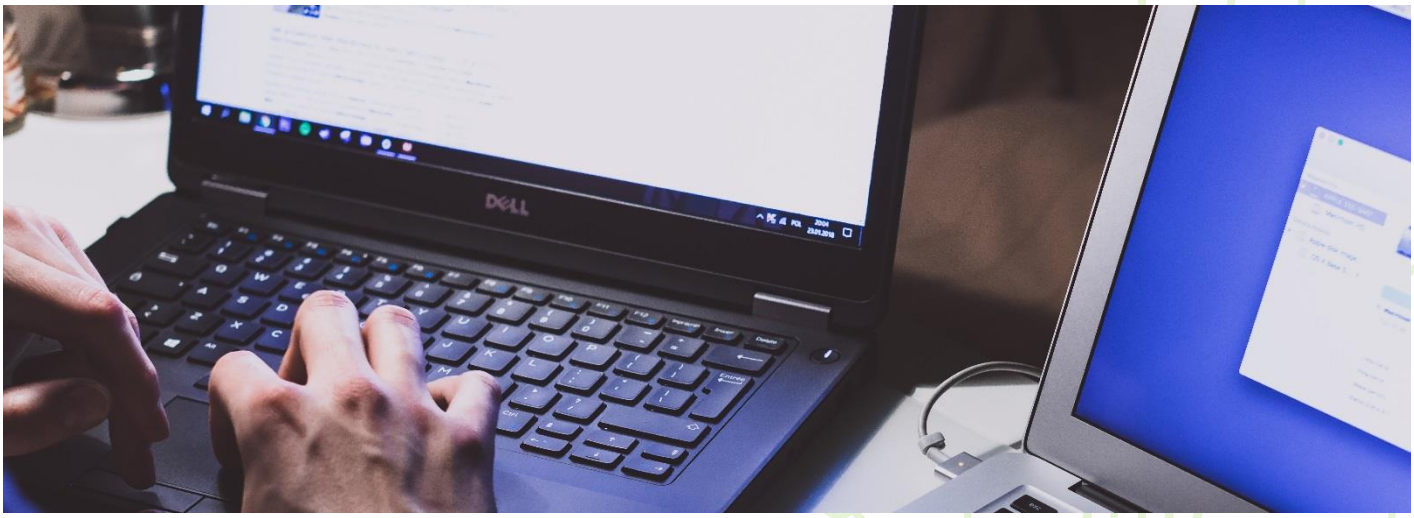
Cover for the costs of dealing with a cyber extortion can be covered under both special crime and cyber insurance policies. Resulting business interruption and liability may be covered under property and cyber programs respectively.

MEDICAL DEVICE MANUFACTURERS OR SOFTWARE, SERVICES OR PARTS PROVIDERS

Liability for failures at healthcare facilities could be covered under either an E&O or cyber policy. In order to avoid gaps or crossovers in coverage, they are usually covered in the same policy from the same insurer.

MEDICAL DEVICE SELLER

A cyber policy is the only real option for this coverage for the harm done to others as a result of failures in security for devices that they are responsible for.



BREACH OF PATIENT CONFIDENTIALITY

It is now considered critical for a business to have insurance for failing to protect private information that may, for example, be collected from medical devices. When a breach of confidential information occurs, there are direct costs for forensics, lawyers' fees and other response costs. Lawyers will often be needed to protect a company to take steps against the possibility of litigation and to negotiate with regulators who might be interested in pursuing fines and penalties.

HEALTHCARE PROVIDER

A cyber policy is the only real option for this coverage for the harm done to others as a result of failures in security for devices that they are responsible for.

MEDICAL DEVICE MANUFACTURERS OR SOFTWARE, SERVICES OR PARTS PROVIDERS

Cyber and E&O policies can provide coverage for liability as a result of this type of event. In order to avoid gaps or uncoordinated double coverage, they are usually in the same policy from the same insurer.

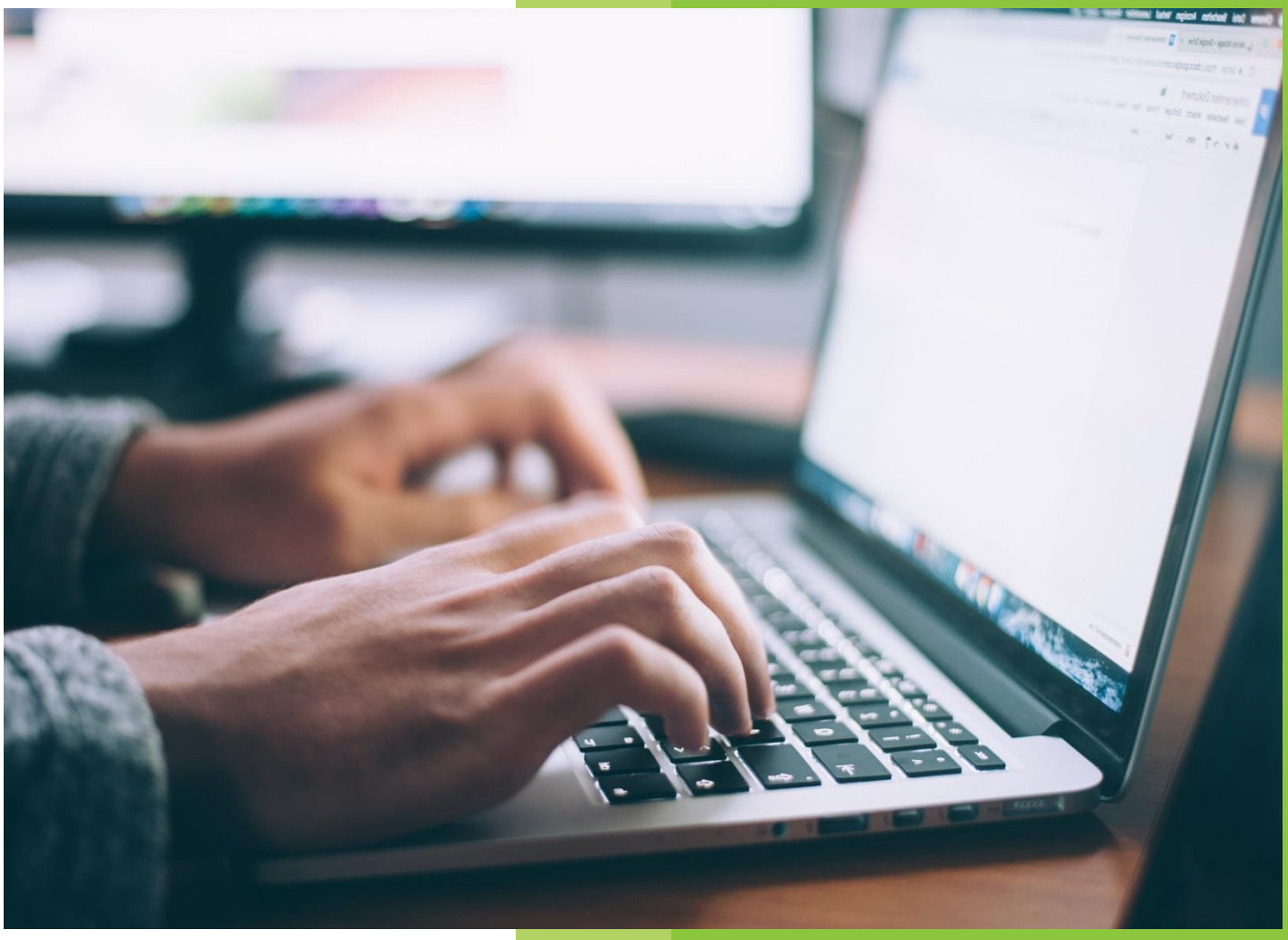
MEDICAL DEVICE SELLER

A cyber policy is the only real option for this coverage for the harm done to others as a result of failures in security for devices that they are responsible for.

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 face the cost of replacing and recalling those devices and also reimbursing the costs their clients may incur as a result of the recall. Companies in the medical device supply chain can be subject to the same liabilities as manufactures.

Insurers have begun offering targeted recall products to cover these types of exposures but they have a limited appetite and coverage can vary markedly from one insurer to the next. Some policies only cover first-party claims while other underwriters only will consider third-party risks. Some, but not all, will cover the cost of media and crisis management. The trigger for coverage in the insurance policies can vary significantly. Recalls are expensive and only some of these costs may be mitigated by insurance.



IN COVERAGES POTENTIALLY TRIGGERED BY MEDICAL DEVICE EXPOSURES

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

PLEASE CONTACT US FOR MORE INFORMATION

CHRISTOPHER KEEGAN

Senior Managing Director

Cyber and Technology Practice Leader

646.358.8530

ckeegan@beechercarlson.com