THE HARTFORD

"I'VE HAD A DATA BREACH! AM I AT RISK?"

Understanding Cyber Liability for Technology Companies

by Joseph Coray, VP, Technology & Life Science Practice and Marine Practice at The Hartford Financial Services Group

Recently, a large healthcare provider reported that, due to a data breach, it would be providing credit monitoring and identity theft services to over 600,000 individuals for two years. In addition, the same provider settled class action lawsuits in several states with payments to each individual. The total costs to the provider were in the tens of millions – all as a result of a network security failure. This scenario illustrates the economics of cyber risk and liability, an area of growing concern for life science companies.

What is cyber risk and how do medical technology and pharmaceutical companies manage this potential for financial loss?

Cyber Exposure

Simply stated, cyber exposures are directly connected to the responsibility companies have to protect their electronic information. Cyber risk refers to the potential consequences associated with this information being compromised or misused.

In broad terms, breaches to computer networks and the ramifications of unauthorized access to sensitive data are the key elements of cyber risk. These risks include personal injury, intellectual property infringement, and financial injury from allegations of negligence, as well as fines, costs and obligations associated with Consumer Protection and Data Privacy Regulations. These exposures to financial loss are everywhere as they arise from the operations and use of information and telecommunications networks. Information, today, is ubiquitous, traveling over private and public wired and wireless networks. When the security of the network is compromised, information which should be private may be made public. This is the essence of a data breach event.

Exposures to financial loss from data breach generally fall into two categories:

- **Third Party Liability** – the risk of a third party filing a suit or making a claim against your business. Typically, this is associated with your company's responsibility to protect private, sensitive or confidential information, to prevent the transmission of virus through your network, or to avoid causing or contributing to the network breach.
- **First Party Expenses** – expenses your company may incur as a result of a cyber event, like a security breach or misappropriate of information. Expenses could include notification, credit monitoring, cyber investigation, crisis management, data privacy regulatory expenses.

Today, forty-six states have laws which require "reasonable" data security and specific actions. Many laws outline standards that require an entity which maintains either personally identifiable information (PII) or personal health information (PHI) to implement a comprehensive, written information security program. Further, the laws often specify obligations of the entity to report any data breach and offer credit monitoring or other protection to affected individuals.

Medical technology companies may have greater exposure to this risk as medical devices become more integrated with data and telecommunications networks of healthcare providers. PHI data stored on these devices – from imaging to mobile computing telemetry – can be vulnerable to security breaches. If the medical device's operation contributes to a network data breach event, the manufacture of the device may be liable for their customer's cyber risk costs.

Life science companies may have data that qualifies as PII or PHI from human research, clinical trials or biological specimen repositories. With increasing awareness and evolving regulations, device and drug companies must consider whether they have cyber risk – and how to manage this exposure to loss. The degree of risk depends on the products and services offered, as well as the type and amount of private, sensitive, and confidential information they manage, control, store, transfer, and maintain.

Evaluating the Exposure

To assess your exposure, it can be helpful to answer some basic questions about your products, services, customers, vendors, and communication and information networks:

- What types of products or services do you provide? Who are your direct and indirect customers?
- What type of sensitive information (confidential, personal, intellectual property) is associated with the product or service you sell to your customers?
- Do any of your vendors or suppliers have access to or control of this sensitive information at any time? If so, when? How often? How long? How much? Where?
- How is sensitive information protected while in your possession or control? Do you utilize access restrictions, encryption, segregated storage, usage monitoring, password protection, etc.? What policies are in place to ensure proper handling procedures are followed by all employees?
- Do you collect or manage personal information of individuals other than your own employees? If so, what personal information is involved (full name with social security number, medical information, financial account information, driver's license number, credit card information, etc.)?
- Could this information qualify as nonpublic personal or personally identifiable information under a Data Privacy Regulation?
- What are the costs of the obligations imposed by data privacy laws of the states in which you are conducting business?

Reducing Cyber Risk Exposure

As medical technology and life science companies evaluate their cyber risks, one key action they can take is the elimination of any unnecessary data. Many companies collect or maintain sensitive data without having a specific purpose for such information, increasing their cyber risks without a viable business benefit.

Other areas to consider include: the tracking of sensitive information, verification information security controls, assessment and monitoring of access privileges for users including remote access, web applications review/testing, and computer systems event log monitoring. Some additional best practices for helping to prevent data breach and protecting your network include using security software and maintaining the updates, deploying encryption of databases including data that is sent through e-mails or stored in offsite or cloud environments.

In addition, employing basic common sense behaviors may be helpful in preventing data breaches: never share passwords, lock or shut down computers when not in use, remove unnecessary programs, do not open e-mails from unknown sources, and avoid downloading unapproved software from the internet. Finally, maintaining physical security of portable computing and data storage devices is also very important. Some data breach events have begun with lost or stolen laptops, flash drives and CD-ROMs.

Protecting against the Financial Loss from Cyber Risk

The cost of a data breach event could be significant, including both direct costs as well as litigation costs from claims of negligence and damages. Life science companies may need to review their insurance coverage since most Commercial General Liability policies do not cover the costs of these actions or damages, nor offer defense for these types of claims. Many insurers now offer options to help companies manage this risk; however, each coverage form is unique. Cyber risk or cyber liability insurance policies generally cover the first party costs of a data breach and may offer defense and indemnity coverage for third party claims. Often these coverages may be offered as part of a professional liability insurance program. Since there are many types of cyber insurance policies available, it is very important that companies who purchase this insurance understand the coverages and the exclusions in their policy. Speaking with an insurance advisor may be helpful in this regard.

The Hartford's FailSafe® suite offers variable coverage solutions for most technology and life science companies' professional liability exposures including the capability to address both third party liability and first party expenses related to cyber risk. At The Hartford, we've been insuring innovation in the technology and life science industry for more than 25 years. We understand the rapidly changing environment in which this business operates. For more information on best practices for cyber risk management, please visit The Hartford's Technology and Life Science website, www.thehartford.com/info/technology or contact The Hartford at medtech-lifesci@thehartford.com.

Joe Coray is the Vice President, The Hartford's Technology & Life Science Practice and the Marine Practice. In this capacity, he is responsible for all execution activities of the group, including overseeing field sales, underwriting and strategy for the practice, including Life Sciences & Medical Technology. Combining Middle Market, Small Commercial and Professional Liability, the Technology Practice has over $400 Million in written premiums and is growing as an industry vertical and leader in insurance and risk management for technology and life science companies. The Marine Practice focuses on Construction, Transportation, Renewable Energy, Inland and Ocean Marine coverages for a variety of industries.