Innovation and Global Competition Add Risk to Life Sciences Industry

Lee Farrow and Frank Goudsmit

CHUBB®

In an industry based on innovation, life science companies face ever-evolving risks. New technologies and treatments come to market every year, continually reshaping medicine and health care. Each new development and discovery, however, brings not only the potential to improve people's health and lives, but also new exposures, from cyber vulnerabilities to supply chain and regulatory risks. These exposures are amplified by the increasingly global nature of the life sciences industry.

As new drugs and devices transform the industry, the business landscape remains in a perpetual state of flux as start-ups develop new approaches and larger companies seek to acquire smaller firms with the most promise. Life sciences deals can reach into the tens of billions of dollars as companies position themselves to remain competitive in the multinational arena.

For companies that rely on suppliers in many countries, supply chain risks can prove formidable, while those that market and develop products internationally need to realize that their regulatory risks extend across borders. To protect themselves against exposures that can span the globe, life science companies should work with an insurer with worldwide experience in the industry, global relationships and a deep knowledge of how local regulations may compound their risks.

Cyber

The health sector in general has emerged as a prime target for cyber criminals seeking to steal patient records and personal information, and increasingly, for so-called "ransomware" attacks. While the data breaches at health care companies that have exposed tens of millions of patient records make headlines, pharmaceutical and medical device companies remain all too vulnerable. Along with personnel and patient records, life science companies hold highly valuable intellectual property involving drugs and devices that represent billions of dollars in potential or actual sales. The threats are growing more serious. Nearly two-thirds of pharmaceutical firms surveyed had experienced serious data breaches, according to a 2015 Crown Records Management survey[1]. A major cyberespionage group that has focused on government and government agencies has expanded into a variety of industries, including pharmaceuticals, security firm Symantec reported in 2016[2]. While corporate networks remain a favored target, mobile devices that may hold reams of valuable data have also come under attack.

Ever since the first computer bug emerged, cyber threats have kept pace with rapid technological change and even embraced social engineering to include phishing and spear-phishing schemes that seek to exploit human error. Recently, ransomware demands have multiplied rapidly. In such attacks, hackers break into a company's computer system and demand ransom paid in cyber currencies to either free up the system or to prevent the release of sensitive data. Ransomware attacks have quadrupled to a rate of roughly 4,000 a day, a U.S. Government interagency report estimated in 2016[3].

Besides holding data hostage, cyber criminals continually seek to break into corporate systems to steal personally identifiable information such as Social Security numbers and dates of birth. For all companies, the financial and reputational risks rise whenever customer and patient data is involved. If such information is exposed, many states require companies to notify those affected and provide monitoring services to help protect them against identity theft. Much of the expense of cyber claims involves first-party losses such as the costs to notify customers and provide credit monitoring services. The average cost of a data breach has risen to $4 million, up 29 percent since 2013, the Ponemon Institute reported in June 2016[4].

While sensitive and proprietary data is at risk, cyber-attacks can pose another, even more serious threat to companies, practitioners and patients.

Today, more Internet-connected devices store or transmit patient and medical data. Remote tampering with devices that monitor vital signs could seriously endanger a patient if that data is tampered with. Cyber vulnerabilities have been identified in some implantable heart devices[5], infusion pumps[6], and insulin pumps[7]. The risk stemming from Internet-connected devices was highlighted in the fall of 2016 by a massive attack mounted against the Internet infrastructure from a variety of devices, such as web cameras and baby monitors, known collectively as the Internet of Things[8].

For contract manufacturers, a cyber-attack might impact their ability to manufacture a product correctly for key customers. Such an attack could lead to business interruption exposures if the manufacturer cannot deliver the product, and errors and omission exposures for financial injury when unable to meet the terms of its contract. Cyber-attacks that lead to flaws in manufacturing could result in bodily injury or property damages that give rise to a product liability exposure. A hacking incident that compromises data in a clinical trial could jeopardize the results and cause costly delays and repetition of the trials.

When it comes to pharmaceuticals and medical devices, consumer trust is crucial. That means that life science companies need to vigilantly safeguard their reputations from the lasting damage that can be caused by cyber-attacks or data breaches. For those reasons, firms often seek out cyber coverage not only for the risk transfer but also for pre- and post-incident services to help prevent or mitigate losses and to recover from a cyber event. That may include expert assessments of a company's cyber defenses and procedures and moves to strengthen them.

Mergers and Acquisitions

Product development complexity and patent cycles make mergers and acquisitions a permanent feature of the life sciences industry. Large companies are constantly looking for smaller firms with promising research projects to add to their pipelines, both to grow the business and to offset the impact of the loss of exclusivity when patents expire. While mergers and acquisitions are part of the fabric of the industry, they do represent a major cause of losses. Many life sciences companies have highly complex corporate structures that may include hundreds of subsidiaries, each with their own potential liabilities for an acquiring company.

Successor liabilities, for instance, can stem from how potential liabilities are apportioned in the purchase and sale agreements. Losses may arise from gaps in coverage when companies do not make sure that their insurance covers the liabilities they have acquired in a transaction. General liability policies do cover events that happen after a deal, but typically exclude coverage for events that occurred at an acquired company prior to the merger. Typical product liability policies also do not provide coverage for liabilities arising out of actions by the predecessor company. The seller's insurance policy is unlikely to provide coverage because the buyer will not be named as an insured party.

Even in transactions intended as asset-only purchases to limit such exposures, the acquirer may still be held liable for claims stemming from the now-defunct company. In addition, contract wording that seeks to guarantee protection from prior events may not withstand court challenges. For instance, problems with products that were manufactured prior to the acquisition but not sold until afterwards could lead to liabilities for the acquiring company.

To protect against these types of claims, companies should consider successor liability insurance, which responds to liabilities assumed by a new owner for claims made against them that emanate from a company's actions before the acquisition. Generally, such policies are not renewable, but provide for an injury

or offense period that extends for a certain number of years before and after the transaction date.

The representations and warranties made by the parties to the deal can also give rise to later difficulties. Representations and warranties insurance provides coverages against financial losses, including costs associated with defending claims, for unintentional and unknown breaches of the seller's representations and warranties. Such coverage can extend to the acquiring company as well as the target company.

To identify potential problems in a transaction, acquiring firms should seek to uncover any prior losses at the target firm and to understand its existing insurance arrangements. Points of concern include any activities that may have led to injuries or damages in the past, particularly for products with a long history. Products that are in the pipeline should be evaluated not only from a perspective of potential success but also for potential adverse events. Due diligence should include all of the company's outsourced manufacturers and component suppliers.

Supply Chain

Life sciences companies contract for services and products from suppliers, manufacturers and logistics facilities around the world, and often for research and sales as well. But supply chains that stretch across oceans and continents can prove fragile. Companies that rely on just-in-time supplies but do not keep sufficient back-up supplies on hand can experience an immediate and costly impact to their sales when a key supplier goes off line. For example, a fire in an Asian facility could destroy not only inventory but custom molds for a medical device maker, and it could take months to find a new subcontractor and to construct new molds. A cyber-attack could disrupt production at a key manufacturing partner by hacking into its customer list, or taking its advanced manufacturing device offline. Again, it could take months for the facility to recover its normal operations.

Optimally, companies would keep sufficient stores of all raw materials and finished products so that in the event of a supply disruption they could continue making sales out of inventory even if a supplier suffered a catastrophic loss. Where possible, companies should contract with back-up suppliers and vet them as thoroughly as their main suppliers to make sure that their manufacturing facilities, procedures and products meet all applicable standards.

Companies that have not taken the appropriate steps to mitigate the potential risks may face liabilities stemming from problems with the raw materials or components used by a supplier or contract manufacturer. In products that directly affect the physical health of customers, quality control is crucial. Before agreeing to do business with a supplier, a company should thoroughly validate the supplier's raw materials, production methods and business practices. Raw materials from a supplier should be regularly tested before they are incorporated into a final product. Should contaminated raw materials be incorporated into a product, all the contaminated batches would have to be recalled, discarded and replaced.

Supplier contracts should provide the necessary indemnifications to ensure that the supplier assumes the appropriate liabilities for their products and that their insurance policies provide adequate financial protection. For U.S.-based companies, that should include U.S. jurisdiction product liability insurance. Suppliers may only have local liability insurance limited to their home country, meaning that any legal action would have to be taken in local courts, whereas worldwide jurisdiction insurance would provide coverage for legal claims wherever they occur.

When it comes to suppliers, financial strength is another important consideration. Faced with a potentially costly claim, a smaller supplier might decide to go out of business. That could force a company that does not have sufficient inventories or other suppliers to halt production.

Like many technology firms, some life science companies are "virtual" businesses that outsource most of their operations, from research to manufacturing and sales. For those companies and others that rely on outside suppliers and manufacturers, business interruption risks can be considerable. In addition to making sure that the supplier has a solid business interruption and/or disaster recovery plan in place, contingent business interruption coverage can protect a company against the risk that an incident or problem with a crucial supplier may cause a severe disruption to its own sales. Besides coverage, companies often look for an insurance carrier that can provide risk mitigation and engineering services to help identify vulnerabilities in their supply chain.

Regulatory Risk

Regulations are often challenging enough in just one country, but global businesses must deal with layers of complexity arising from what can be very different legal and regulatory environments in each country where they do business. Domestically, companies are highly focused on the U.S. Food and Drug Administration, because they will need the agency's eventual approval to sell a product. In Europe, they will need the approval of the European Medicines Agency. Of course, many other countries have their own agencies and own regulatory requirements that must be understood and addressed.

To develop new drugs and devices, life science companies need to conduct clinical trials in a variety of countries, whether for economic, research or regulatory reasons. Each country, however, has its own laws regarding insurance in general along with specific regulations for clinical trials and coverage requirements for those trials. In many countries, a U.S.-based policy may not legally provide coverage, and a company must purchase coverage from an insurer that is licensed, or "admitted," to do business in that country. The regulatory challenges include not only the insurance coverage for the trial but also the agreements between and among the trial sponsor and the contract research organization, the investigators and the site. The requirements for clinical trials differ greatly from country to country, even within the European Union.

Potential problems can be easily overlooked. For instance, in a contract between a U.S. biotech start-up and state-run Russian hospital where the trial investigator is a hospital employee, that investigator may be considered a Russian government employee. This could cause the company to run afoul of the Foreign Corrupt Practices Act. For smaller companies, in-house counsel is unlikely to be admitted to practice law in foreign countries which means that they will be unable to represent the company's interests there. Companies considering clinical trials abroad need to make sure they have access to the right legal expertise so that their agreements do not violate local laws, regulations or customs in that country - which can lead to problems at home.

While the eventual success or failure of a product is not an insurable risk, companies can obtain coverage for financial injury stemming from errors or omissions that require a trial to be repeated, which can cost millions or even tens of millions of dollars. For instance, if a contract research organization's (CRO) software fails to properly randomize trial participants, the data from the completed trial could be rendered unusable, forcing the sponsor to spend millions of dollars more to repeat the trial. The CRO's failure to: meet test subject recruitment goals; set up the appropriate amount of sites; or not contract with enough investigators could all jeopardize a trial.

While the eventual success or failure of a product is not an insurable risk, companies can obtain coverage for financial injury stemming from errors or omissions that require a trial to be repeated, which can cost millions or even tens of millions of dollars.

Choosing the right CRO is crucial. The appropriate CRO will be able to help a company avoid regulatory pitfalls and to get a trial up and running in the most appropriate country or countries for the drug or device being tested. A country may be chosen as a trial site, because it has the proper patient population, the right medical expertise, or because the company will want an eventual approval in that market. CROs help companies to negotiate the regulatory risk, to prequalify vendors and to make sure that trial sponsors are obtaining the proper contractual language to protect themselves against the potential risks. That same caution should extend to the contractual agreements that a trial sponsor reaches with a CRO.

Risk Management to Meet the Challenge of Constant Change

Discovery, technology and competition are driving continual change in the increasingly global life sciences industry. As new technology is adopted in the business and embedded in its products, new cyber threats emerge, targeting not just valuable corporate and personal data but also Internet-connected medical devices. Industry consolidation and mergers add risks even as they improve a company's overall competitive position. Global supply chains bring advantages but also create vulnerabilities. Both existing and changing regulations can ensnare unwary companies. Clinical trials, in particular, present a complex set of regulatory risks.

As life science companies grow they are likely to find themselves in the international arena. The same global viewpoint that embraces development, suppliers, products and sales should extend to insurance as well. As businesses expand across borders, they should seek an insurer that can provide the coverage and services that help make sure their risk management strategy responds to the current and emerging risks they're likely to face. A financially strong insurer that has the industry expertise, experience and relationships around the world can help companies make sure that as they grow, their risk management strategy grows as well.

About the Authors

Frank Goudsmit, CPCU, is Senior Vice President and a 28-year veteran with Chubb Life Sciences, who has several decades of experience in developing global clinical trial liability insurance solutions for Life Sciences companies. Mr. Goudsmit has collaborated on the development of insurance policy wordings, and has helped clinical trial sponsors benchmark themselves against, and implement, best practice risk management controls. He has been a frequent speaker on clinical trial insurance issues such as clinical trial risk mitigation, compensation guidelines and compulsory insurance requirements.

Lee W. Farrow is an Executive Vice President and leads the Chubb Life Sciences Industry Practice. The Practice oversees the strategy, operations, and underwriting of life sciences, pharmaceutical, supplement and medical device companies, life science support and service companies, and human clinical trials. Chubb Life Sciences insures companies for their world-wide exposures, and specializes in the placing of local admitted clinical trial policies around the world. As a part of the underwriting process, in addition to evaluating the exposures, Mr. Farrow examines many contracts including informed consent language and hold-harmless and indemnity agreements. Mr. Farrow is an attorney admitted to practice law in New York and New Jersey, and has spoken about clinical trial, litigation, insurance, and risk management issues

at BIO, various ACI Conferences, and American Bar Association seminars, among other events. He is the past and founding Co-Chairperson of the ABA Product Liability Committee's Biotech Subcommittee, and was on a steering committee that organized a summit on ethics and human research at Fordham University.

Mr. Farrow has been in the insurance industry for over 20 years, and he has held various positions from claims to in house counsel to underwriting. Mr. Farrow earned his undergraduate degree in Business Management from Hartwick College, and his J.D. from CUNY School of Law.

Endnotes

[1] Cybercrime still hitting the pharmaceutical sector, Crown Records Management, July 22, 2016, https://www.crownrms.com/en-us/article/cybercrime-still-hitting-the-pharmaceutical-sector-

[2] Patchwork cyberespionage group expands targets from governments to wide range of industries, Symantec, July 25, 2016, http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

[3] How to protect your networks from ransomware, U.S. Department of Justice, https://www.justice.gov/criminal-ccips/file/872771/download

[4] Press Release, IBM & Ponemon Institute, June 15, 2016. See :http://www.prnewswire.com/news-releases/ibm--ponemon-institute-study-data-breach-costs-rising-now-4-million-per-incident-300284792.html

[5] U.S. Food and Drug Administration, Press Release, Jan. 9, 2017, http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

[6] U.S. Food and Drug Administration, Press Release, July 31, 2015, http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

[7] "J&J warns insulin pumps could be hacked," Financial Times, Oct. 4, 2016,

[8] "DDOS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, Oct. 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

As businesses expand across borders, they should seek an insurer that can provide the coverage and services that help make sure their risk management strategy responds to the current and emerging risks they're likely to face.

Contact Us

Frank F. Goudsmit
Senior Vice President
O 314 889 4408
E Frank.Goudsmit@chubb.com

Lee Farrow
Executive Vice President
O 908 572 4697
E Lee.Farrow@chubb.com

About Chubb

Chubb is the world's largest publicly traded property and casualty insurance group. With operations in 54 countries, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. Chubb Limited, the parent company of Chubb, is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at new.chubb.com. Insurance provided by ACE American Insurance Company and its U.S. based Chubb underwriting company a liates.

Chubb. Insured.[SM]