Southpoint Business White Paper


SOUTHPOINT

# Southpoint Insurance Business White Paper:

## Workplace Practices, Cyber Liability, and Corporate Governance

TRUSTED 200 YEARS
THE HARTFORD

# Employ the Right Practices in the Workplace

If you're like most responsible employers, you have sound employment policies and procedures in place to help protect against a lawsuit. That's the good news. The bad news is that you can still be exposed to employment-related allegations that could cripple your organization.

Nearly every company is vulnerable: when terminating an employee, maintaining supervisor-employee relationships, making an employment decision that affects various groups differently – even when considering a contract worker. Companies today can easily get caught in the complicated web of federal and state statutes designed to prevent discrimination and harassment in the workplace. And it can be costly.

**Consider these facts:**

- The Equal Employment Opportunity Commission (EEOC) recorded nearly 76,000 employment-related charges in 2006.
- The average cost of such a suit exceeded $105,000.
- Employment-related harassment allegations alone reportedly cost the average Fortune 500 company $6.7 million a year in indirect costs.
- According to the EEOC, 40 percent of companies with 15 to 100 employees have been targets of claims.

The best way to protect your company from costly employment-related lawsuits is with Employment Practices Liability Insurance (EPLI). This coverage protects you and your employees in the event of claims of discrimination, sexual harassment, wrongful termination and retaliation. In addition, you can rely on your EPLI insurer to help you implement procedures designed to reduce the likelihood and costs of employment-related charges.

## Emerging Exposures

While race and gender-based discrimination have been the most common types of workplace-related lawsuits, charges of retaliation are on the rise and are on average the most expensive to defend. Even if a company wins a discrimination case on the merits, it can be held liable for retaliation if proven to have acted aversely against an employee, based on the underlying complaint.

### No Employees, No Lawsuit? Not So

A one-person consulting firm receives an unsolicited resume in the mail and tosses it out without thinking. Six months later, he receives notice of a discrimination charge brought by the resume-sender. Because the consultant has no record of the unsolicited resume and no formal procedure for handling such documents, he may have to defend himself against such an allegation.

Remember, you can be sued over employment practices by anyone who comes in contact with your business – and that includes your customers and vendors as well as your own leased workers and independent contractors.

Technology and life science companies – which some think provide a relatively benign place to work – are, in fact, facing ever-increasing exposure in the employment lawsuit arena. Why is that?

**Technology and life science companies:**

- Are becoming vulnerable to age discrimination charges since they are beginning to have more employees who are over 40 and who, therefore, are protected by the Age Discrimination in Employment Act (ADEA).
- May employ workers in science and engineering jobs that require experience, a very specific skill set, a high level of education and that pay a high salary. This demographic raises the number of potential cases that are prohibitively expensive to settle or litigate.

- Have struggled to hire women and minorities to fill science and engineering positions, creating a workforce that is skewed toward white males – a potential treasure trove for plaintiffs' attorneys.
- Are often in start-up environments where employee expectations are high.
- Can experience a high burnout rate because of the stressful and demanding workplace.

In addition, technology and life science companies – and, in fact, most companies – are relying more than ever on e-mail, text messaging and digital creation of content for communications. Because these communications create, in essence, an "electronic paper trail," they can be used as evidence in an employment-related lawsuit. The existence of e-mail, which is easily retrievable even after deletion, can embolden plaintiffs and encourage them to hold out for higher settlements.

## What You Can Do

There are specific steps an employer can take to decrease the likelihood of employment-related litigation. These include:

- Universal and consistent use of a fair and unbiased employment application
- A policy that calls for all applications for a position to be considered and jobs to be posted for a specific time period – preferably 30 days or more
- A formal, written employee handbook, including a written sexual harassment policy and all-forms harassment policy
- Ongoing training of managers and all employees on what constitutes sexual harassment and discrimination in the workplace
- Terminations based on performance and conduct, including a progressive discipline policy tied to well-written job descriptions
- Proper documentation maintained on all employees, including steps taken prior to termination
- Universal and consistent application of all policies and procedures to all employees

To help companies manage their employment practices exposures, The Hartford has launched ***www.hartfordhelp.com*** – an employment practices loss mitigation Web site available to all Hartford EPLI insureds. This site offers online training modules on sexual harassment, discrimination and other workplace behavior – modules that can be offered to employees at no additional cost. The site also contains model forms and policies that can help users create their own employment applications, employee handbooks and sexual harassment policies.

The Hartfordhelp Web site also provides a vast library of online material that addresses common workplace issues and offers tips on how to take the right actions.

As one of a handful of insurers to have continuously offered EPLI coverage since 1991, The Hartford is uniquely qualified to help companies with coverage and risk management guidance.

### Celebration Goes Sour

To celebrate the highly anticipated launch of a new software product, a techology company sponsors an employee happy hour at a local tavern. After a few hours of revelry, a project manager offers his co-worker a ride home. She refuses, but he persists until another co-worker intervenes. Having had a few too many drinks, the project manager quickly forgets the incident.

Two weeks later, the project manager is called to his manager's office to discuss a hostile workplace allegation brought by the co-worker. To make matters worse, the company is alleged to have contributed to the hostile workplace by sponsoring the event and furnishing alcohol. The allegation also accuses the company of negligent supervision of the project manager. The case is settled quietly for $250,000, and the project manager loses his job.

## For More Information

For more information on how to manage risks for your business, contact your local Hartford agent, or visit *www.thehartford.com*.

## *Best Practices for Your Business*

### About The Hartford's Technology Practice Group

For more than 25 years, The Hartford has insured technology and life science businesses of all sizes. Our products are flexible enough to grow with a business – from a startup or sole proprietorship to a large, publicly traded company. We also offer services that can help businesses lower their losses, like our series of Technology Best Practices.



TRUSTED 200 YEARS
THE HARTFORD

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.

TRUSTED 200 YEARS
THE HARTFORD

# Sarbanes-Oxley and Corporate Governance

***Businesses operating in the shadow of the Sarbanes-Oxley Act of 2002 and increased oversight of the Securities and Exchange Commission (SEC) are under the microscope to execute flawlessly when it comes to corporate governance – and the technology and life science industry is no exception.***

The technology and life science industry is characterized by intense mergers and acquisitions (M&A) activity, rapid technological innovation and product obsolescence, highly complex accounting issues, and the frequent need to access capital markets. These characteristics increase the chances of running afoul of federal regulation – a possibility that firms can't afford to ignore.

However, technology and life science firms of all sizes that embrace the new laws and the principles behind them are protecting themselves against possible litigation and enhancing their value to their investors, potential investors, acquirers, customers, and employees.

## The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 was developed and passed in response to the spate of corporate accounting and governance scandals that rocked the U.S. earlier this decade. The Act is intended to protect investors by improving the accuracy and reliability of corporate disclosure made pursuant to SEC laws, and for other purposes. The Act provides the SEC with greater enforcement powers over the activities of public companies by requiring increased corporate responsibility and enhanced financial disclosures. It also imposes more stringent corporate and criminal fraud accountability standards and greater white-collar crime penalties than before. *For more in-depth information about Sarbanes-Oxley, go to www.sec.gov and enter "Sarbanes-Oxley" in the search box in the upper right corner.*

## The Burden is on Business

These laws and regulations place the burden squarely on businesses to create a corporate culture that is focused on ethics and compliance. For technology and life science firms, this means increased scrutiny of company business practices. While it appears that Sarbanes-Oxley has done little to expand the rights of shareholders, it has helped to provide them with greater insight into the corporate governance and the adequacy of internal control structures of publicly traded companies, which could be used to support a civil action should shareholders choose to bring one.

In 2004, according to the PWC Securities Litigation study, the number of securities class action lawsuits was up 16%. This trend, coupled with a decline in the dismissal rates, is increasing defense costs for companies and their insurance carriers. As a result, the underwriters of Directors & Officers (D&O) liability insurance are

looking not only for adherence to the "letter of the law" but also the execution and enforcement of strong corporate governance policies and procedures that help to mitigate the risk of any negative surprises which can drive litigation or regulatory action.

## Sound Corporate Governance for All

The benefits of sound corporate governance are not just for large firms. They hold true for companies trading on the over-the-counter market, on the pink sheets, and even those that are privately held. By embracing the principles of good corporate governance, companies become less risky to investors, potential investors, acquirers, customers, employees (and more attractive to D&O insurers).

For example, a young company that needs to raise capital to finance development or market a new product may secure a higher valuation from investors and creditors when there is less perceived risk in its underlying business – particularly with respect to the quality of the financial reports and projections that are analyzed in the due diligence process.

The accuracy of financial books and records is also critical for firms that are looking to be sold. In order for a public company to even consider buying them, there needs to be near certainty that no accounting errors will surface post transaction that could lead to a restatement. Senior executives of the acquiring public company will have to personally certify the accuracy of the combined financial statements on the next filing date. A restatement subsequent to that certification could jeopardize the careers and net worth of those individuals as well as cause reputational harm to the acquiring company.

## Benefits Accrue

In addition to making companies better candidates to access the capital markets, sound corporate governance enhances their ability to attract talented and ethical employees and makes them less vulnerable to loss due to litigation, regulatory fines, and employee theft. Further more, statistical studies, such as those conducted by Paul Gompers of Harvard and Andrew Metrick of the University of Pennsylvania's Wharton School, and reported in their article, *"Corporate Governance and Equity Prices"* have found that "firms with stronger shareholder rights had higher firm value, higher profits, higher sales growth."

## Steps to Good Corporate Governance

As there is no one perfect model of corporate governance, your company's management and board of directors should seek the assistance of a law firm or an outside consultant to help design a system that is effective for your company based on its size and ownership structure.

Steps to good corporate governance may include:

- **A strong board of directors** – Build a board of directors with diverse backgrounds and areas of knowledge and independence.
- **Board of directors committees** – Form committees for audit, compensation and disclosure.
- **Compensation for directors and officers** – Align compensation with the long term interests of the company and its shareholders.
- **Codes of conduct** – Implement and enforce rigorous codes of conduct for all levels of employees.
- **Control policies and procedures** – Design control policies and procedures to ensure the accuracy and integrity of the company's financial books and records.
- **Disclosure** – Ensure the timely and accurate disclosure of material matters to shareholders.
- **Checks and balances** – Build a system of checks and balances to avoid any misuse or misappropriation of company assets by employees or outsiders.
- **Review of contracts** – Ensure strong legal (in-house or outside counsel) review of all contracts.
- **Adequate insurance** – Make sure your business has insurance coverage including D&O, EPL (Employment Practices Liability), Fiduciary Liability, Miscellaneous Professional Liability, and Crime/Fidelity coverage to go along with traditional property and casualty coverages such as workers' compensation, general liability, property, auto and umbrella.

Technology and life science firms of all sizes that embrace the new laws and the principles behind them are protecting themselves against possible litigation and enhancing their value to their investors, potential investors, acquirers, customers and employees.

## DIRECTORS & OFFICERS INSURANCE – WHAT IS IT AND WHY IS IT IMPORTANT

Directors and Officers (D&O) liability insurance found its roots in the 1960s when several landmark cases that clearly established the personal liability of directors and officers and class action suits were authorized. At the time, there were essentially no laws addressing the permissibility of indemnification by companies. And, it was uncertain if such indemnification would be considered to be against public policy. While case law eventually established that in many instances indemnification was permissible, the need quickly arose for a new insurance product to address the personal liability of directors and officers.

The first policies contained two basic insuring agreements. One protected directors and officers in the event their corporation could not indemnify them due to legal limitations on indemnification or the firm's financial insolvency. The other agreement protected the company from loss arising from its indemnification of directors and officers.

In 1995, the corporation was added as an insured "person" for claims by shareholders. This evolution in coverage was essential for publicly traded companies to address the problem of allocation of loss between the covered directors and officers and the uncovered corporation in shareholder litigation involving both parties. As a result of this entity coverage, the basic policy today contains a third insuring agreement that covers the corporation for claims by shareholders.

As coverage evolved for publicly traded companies, insurers also began to consider the needs of privately held companies. These companies saw less value in a D&O policy because the most significant exposure in D&O – shareholder suits – presented little or no threat. The largest threat to privately held firms – claims for wrongful employment practices – was usually addressed in a separate policy. Purchasing both policies was often too expensive for smaller companies. Today, insurers offer a combination D&O/Employment Practices Liability Insurance (EPLI) policy that addresses both exposures.

D&O is important because it provides balance sheet protection for your company should a claim be made, and protects the directors' and officers' personal assets should the corporate entity not be able to indemnify them. In addition, quality D&O coverage can help your corporation to attract and retain successful individuals to serve on your board of directors.

### For More Information

For more information on how to manage risks for your business, contact your local Hartford agent, or visit *www.thehartford.com*.

## *Best Practices for Your Business*

### About The Hartford's Technology Practice Group

For more than 25 years, The Hartford has insured technology and life science businesses of all sizes. Our products are flexible enough to grow with a business – from a startup or sole proprietorship to a large, publicly traded company. We also offer services that can help businesses lower their losses, like our series of Technology Best Practices.



TRUSTED 200 YEARS
THE HARTFORD

## Serving Businesses Of All Sizes

You've invested everything into growing your business, and Southpoint is here to help ensure you're insured from the unknown. Unexpected events such as natural disaster, employee injury, lawsuit, or death of a partner can devastate your business ruining years of hard work overnight.

Depending on your industry some types of insurance are required by law or business associations. These basic insurance requirements don't cover everything and is why you need coverage to protect all aspects of your business.

## About Southpoint

For 40 years, professionalism, hard work, and commitment to our clients have fueled our growth. Since our start, we've been independent. This allows us to respond to our clients and their service needs without internal bureaucracy or external shareholder pressures. An unrelenting commitment to superior client service fosters continuous improvements in our products and services.

SouthPoint is among the top 25 privately owned, independent insurance brokers in Illinois. Southpoint delivers world class insurance services to companies of all sizes as well as to individual clients. Southpoint has grown to become one of the largest Professional Liability insurance brokerage firms in Illinois.

## Our Resources

Southpoint's long-term relationships with underwriters around the world allow us to negotiate comprehensive coverage at the best price possible. We represent the top insurance companies in the country and will always place your coverage with the carrier that is most able to covers your needs.

## Our Commitment

Southpoint's private ownership means that each of our associates has a single-minded focus on serving our clients. Our independence from Wall Street keeps us focused on your needs, not the demands of analysts or stock price. We will never place your coverage with an insurance company based upon our own financial benefit.

## How Can We Help?

Questions about insurance and risk protection for your business?

Speak with a Southpoint Professional

708.478.3440

www.sthpoint.com

SOUTHPOINT