

message from partner in charge

In our final edition of the year, we feature stories about security threats from employees and how a strong management team can minimize the growing pains often experienced by emerging biotech companies.

It is the trust we place in our employees that is often the backbone of a strong company. But because in today's day and age so many employees have access to vital areas of a company's intellectual property designs or personnel information it is imperative that human resources departments make sure new and current employees can be trusted. Our lead article tackles this challenging business reality.

Considering that for every start-up biotech company that succeeds 15 to 20 fail, the question begs to be asked, "Why did the one make it?" More often than not, that answer is found on the roster of their management team. Seasoned executives will often be the difference to an emerging biotech company. Pepper partner Steve Mandell writes about veteran leadership in our second article.

As always, we welcome your feedback on our newsletter and your suggestions for future articles.

Happy Holidays!

Sharon R. Klein
949.567.3506
kleins@pepperlaw.com

in this issue

- 1 **What's Your Company's Biggest Potential Security Threat? Your Employees**
- 2 **Peppercast: Religious Discrimination in the Workplace**
- 3 **A Prescription for Emerging Biotech Companies: A Strong Management Team Helps Minimize Growing Pains**

What's Your Company's Biggest Potential Security Threat? Your Employees

A lost laptop with social security numbers for more than 50,000 people. A misplaced disk that contains account information for an entire state. Vital trade secrets and product formulas appropriated in an attempt to sell information to a company's biggest rival. Worrying about potential security threats like these are the stuff HR directors' nightmares are made of. Each of these examples have one thing in common – employees, whether by mistake, negligence or outright theft, led to the loss of vital company information.

For many companies, the greatest threat to security may not come from outside sources, but from its own employees. To protect themselves from such internal threats and loss of information or vital trade secrets, employers need to take specific measures to reduce their potential risks. Just checking an employee's background is not enough to ensure the safety of the company. Employers need to establish and enforce confidentiality policies or social contracts, and ensure that those policies can change with advancing technology. In addition, assuring good morale among employees also can help fend off potential security threats.

Detecting the Problem

In today's computer-driven world, information technology and accounting employees have access to many of a company's most vital records and information. Other risks stem from employees who habitually take computers or other confidential work to locations outside the office. Often the threat lurks in the form of employees who have hidden problems, which may include massive personal debt, or gambling, alcohol or drug addictions.

Among the possible security threats a company's own employees may pose are:

- **Information technology employees potentially represent the greatest security risk.** With companies increasingly reliant on technology, workers in the information technology department pose the greatest potential threat to compromising a company's systems. IT employees know all the 'sacred codes,' frequently work during hours when other employees are off, and are often located in restricted-access settings. If IT employees feel that their work is unappreciated or have an axe to grind with management, the company's IT systems may be at risk.
- **Financial and accounting employees also can be a potential security threat.** Employees in the financial functions have access to, and unique knowledge about, the company's money. Here again, bad morale among financial employees could cause them to want to hurt the company by misappropriating funds or information. Customer account information – including social security numbers, credit card accounts or other confidential information – is just as, if not more, vulnerable than the company checkbook.
- **Employees bringing work or work materials outside the office can be another possible security threat.** A company's secure data, such as client or consumer identification information, could be at risk if misplaced. Many security breaches have occurred when

laptops were misplaced or stolen. Although forbidding employees from taking work home may be counter-productive and ultimately impractical, restricting who can do this, for what purposes and for how long can decrease the loss of confidential data.

- **Employees with drug or gambling problems are another potential security threat.** Massive personal debt, drug, alcohol or gambling problems are not easily detected in the workplace. Workers with these problems may be tempted to steal to sustain their addictions or cover their losses.

Diminishing the Threat

Employers can diminish possible security breaches caused by their employees through a variety of methods.

- **Conduct background checks:** Before making a hire, companies should conduct an employee screening that includes prior references, a criminal background check and a credit check. Although screening will not necessarily pick up bad behaviors, it is a process that will provide employers with a better understanding of the people they are hiring.
- **Establish a social contract:** The social contract between employers and employees is quickly deteriorating.



Peppercast: Religious Discrimination in the Workplace

Few issues are as personal and potentially divisive as religion. In this podcast, **Robert Ludolph**, a partner in the Detroit office of Pepper Hamilton and chairman of the Detroit office's Labor and Employment Practice Group, discusses religious discrimination in the workplace, including how employers can deal with claims from employees that an employer did not accommodate their religious practices or beliefs and claims asserting religious harassment.

If you are interested in the latest updates in the world of labor and employment, e-mail podcasts@pepperlaw.com to subscribe to *Pepper@Work*. This is an electronic news alert that provides employers with advice on how recent labor judgments and opinions will affect their organization.

Listen today by visiting the Labor and Employment section of www.pepperpodcasts.com.

People are not as loyal to their employers as they once were. But, more important, employees generally do not feel as valued and appreciated. Employers need to pay more attention to the way they treat their employees on a daily basis, and establish a comfortable and loyal work force. Such attention goes a long way toward boosting employee morale, which is an important factor in diminishing security threats.

- **Make employees aware of confidentiality policies:** Problems can arise in the transfer of trade secrets or other confidential information to someone outside the company. Employees should be informed of a company's general confidentiality policies, especially with regard to e-mail. Often these clauses are buried in an employee handbook, even though they are essential to maintaining a company's key assets. Make it a point to train employees in confidentiality policies, and send out policy reminders on a regular basis.
- **Adapt company policies to new technologies:** As technology continues to evolve, businesses need to be informed and adapt their policies accordingly. Now that cell phones can take pictures and external hard drives can easily download a computer's entire content, there are more ways a company's sensitive information can be compromised.

Authors:

*Sharon R. Klein
949.567.3506
215.981.4172
kleins@pepperlaw.com*

*Jonathan Kane
610.640.7803
kanej@pepperlaw.com*

RSS on www.pepperlaw.com

Subscribe to the latest Pepper articles via RSS feeds. Visit www.pepperlaw.com today and click on the RSS button to subscribe to our latest articles in your news reader.

A Prescription for Emerging Biotech Companies: A Strong Management Team Helps Minimize Growing Pains

The biotechnology industry has grown substantially in the last two decades and is more than halfway toward \$1 trillion in annual revenue. The issuance of more than 7,700 biotechnology patents each year is testimony to the vibrancy of the industry. But at the same time, biotech companies frequently fail – by one estimate, for every start-up that succeeds, 15 to 20 fail.

What do the successful companies have in common? Seasoned, flexible and responsive executives who can weather the biotech lifecycle and grow successful, profitable, businesses while minimizing the growing pains inherent in the drug discovery and development process. Here are a few traits biotech companies – and their investors – should look for in a management team.

Managers of biotech companies must have a knowledge of science and disease processes, an understanding of the IT tools used to research and develop their products, a grasp of national and international policies for drug discovery, and insight into the ethics involved in using evolving technologies. They must be willing to work to create new collaborative arrangements, and to manage those collaborations. An ability to tap potential investment sources – governmental and private – is important. And it wouldn't hurt to know the intricacies of university tech transfer offices and how to work with academia and other research organizations.

Unlike many types of companies, biotech companies frequently shift missions as they move from research to product based, commercialized organizations. To maximize company strength and unique product knowledge, the biotech management team must include leaders with practical management, marketing, administrative and production skills, who are capable of anticipating change and creating well-planned and targeted strategies for growth. At the same time, the management team must meet specific scientific milestones, which may slow the company's development.

Building a commercial infrastructure demands competence in such varied business skills as finance, accounting, HR, facilities management, distribution, the regulatory process, market access strategies, and knowing the competition. The ability to recognize opportunities to merge, strategically ally, and to buy, sell or license (and protect) intellectual property are essential to biotech success. Sufficient capital and a pool of highly qualified and capable workers also are critical to minimizing biotech growing pains.

Another important biotech management skill is knowing how to use outside resources. Excellent accountants, staffing specialists, legal counsel, specialized facilities agents, CROs and others are key elements to early and continuing success.

Legal counsel can address important issues and help prevent mistakes that can stop sustained growth. Significant legal issues confronting emerging biotech companies concern entity organization and corporate governance, HR matters (including non-disclosure, non-compete and assignment of IP rights), venture capital and corporate finance, benefits and incentives, tax, facility leasing, strategic alliances, M&A and other corporate transactions, and maximizing the value of and protecting intellectual property.

The selection of counsel should be based on the attorney's abilities to help the company grow. Selection criteria include knowledge of the applicable law and the biotech industry, a commitment to become familiar with the company's operations and goals, attorney accessibility and responsiveness, contacts that may help the company grow, and bench strength of the attorney's law firm. Just as important are the ability to communicate with and on behalf of the client, and "likeability" – confidence that the client will enjoy working with the lawyer. Fees – and the knowledge that legal work will be performed cost effectively – also are important, of course. Since the attorney, once becoming counsel for the biotech, may continue in that role for years to come, it is wise to take time upfront before deciding on the right person. If the decision in this regard is made well, the attorney could become a valuable asset for the long run.

Author:

*Steve A. Mandell
202.220.1201
mandells@pepperlaw.com*

Pepper Hamilton LLP Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County
Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2007 Pepper Hamilton LLP. All Rights Reserved.
This publication may contain attorney advertising.