Safe and sound

Brady Huggett

How should you go about protecting the assets in your business?

Most security coverage in the biotech sector centers around patent protection. But securing intellectual property (IP) isn't the only type of protection you'll need to worry about when launching a startup. There are all kinds of assets associated with your business—computers, data, biological specimens, reagents, even employees—that you need to safeguard.

The good news is that all elements of your company can usually be identified and protected under one security program.

Taking stock

To begin thinking about protecting your company, you should ask some simple questions about your firm, starting with: What are the threats to your business? Once you've identified these threats, you should move to: What is the probability of these threats occurring? And lastly: What would be the consequences if these threats did occur?

If you're a greenhorn CEO, you probably have put more thought into building assets than into protecting existing ones. From day one, however, there are several tenets you should keep in mind (**Box 1**). Another way to educate yourself is to examine the risks of a 'like' company—a public firm similar in size and/or focus to the one you are running or hoping to build. Sift through the other company's annual reports for its identified risks, says Anthony Patillo, associate vice president of security in North America at Sanofi-aventis, based in Paris. Compare what you find there with your own company, and you should get a basic idea of what you'll be up against.

That might be enough to put you on the right path to protecting your company, especially if it is small and contained in an academic setting or incubator. But as your firm grows in size and importance (meaning you develop actual products and your IP becomes more valuable), the best thing to do is an official risk assessment, which will help you determine your company's weaknesses. There are several organizations that can help with this, including the International Security Management Association (ISMA), based in Buffalo, Iowa, and the American Society for Industrial Security (ASIS), located in Alexandria, Virginia.

Brady Huggett is Business Editor at Nature Biotechnology.

Box 1 Five dos to consider in safeguarding company assets

There's a legion of potential areas of concern when safeguarding the assets of a complex business, such as a biotech startup, so where does one start in addressing these issues? Five key starting points when thinking about security for your company are listed below.

Recognize that security encompasses much more than locks and lights. For example, security programs should include efforts to protect colleagues when they travel (**Box 2**), the supply chain, the information technology environment, intellectual property and your proprietary information.

Realize that a good security team allows you, as CEO, the freedom to focus on the business, enabling you to assume some risks while avoiding others. A security team can provide you with a competitive advantage in the marketplace.

Define the security culture you wish to develop at your firm. By default, this definition takes into account the risk appetite of the business.

Ask yourself what you think will be your security risks next year and five years from now. This will help define the overarching security strategy.

Ensure that your security team is closely aligned with the business's goals and objectives. The security profession has matured and developed exponentially within the past 15 years and is being viewed more than ever before as a trusted business partner.

—Richard E. Widup is senior director of corporate security at Purdue Pharma, Stamford, Connecticut, USA.

Box 2 On the road

Protection is needed away from the office, too. Although that means personal safety, most companies (of any size) already have kidnapping and ransom insurance, even if that's an unlikely scenario, says Hamilton Mixon, senior director of risk and global security at Vertex, in Cambridge, Massachusetts. What's more important is protecting intellectual property.

This starts with your legal representation working with your security professional (though this can be done through the communications manager or perhaps a public relations firm, if it's in the contract). If you're on a road show for investors or partners, you'll need to make sure your PowerPoint presentations do not give away sensitive information because you never know who's in the room. For closed meetings, you might want someone ensuring a competitor isn't outside putting a glass to the door while you disclose trade secrets. You'll need a person in charge of collecting or destroying any handouts not taken from the room.

There are other small concerns: shielding screens for laptops and not leaving sensitive information in hotel trash cans, for example. Even more egregious—making sure a laptop itself isn't left on a table somewhere. As CEO, you'll need to consider these things until the tasks are designated to someone else—a hired security person—and it's up to you to decide when that is. *BH*

Box 3 When to pay

When incubated within academia or an accelerator, it's likely your security needs are taken care of, but eventually you'll need to consider it yourself. At first, you might be able to get by with a facilities manager, working in tandem with the local security agency.

But should the company be talented (and lucky) enough to mature to 25–200 people and beyond, you'll need a security manager, and that hire will mean an additional salary you must cover. Depending on the area and the cost of living, that salary will differ. Expect to pay around $100,000 yearly to hire a good security head on the East Coast, though you might be able to get one in the middle of the country for something like $55,000, says Hamilton Mixon, senior director of risk and global security at Vertex, in Cambridge, Massachusetts. As a rule of thumb, you should assume that a security person with 5–10 years of experience should earn as much as the director of facilities.

It might take, literally, a decade or more before your startup requires a person dedicated full time to security. Mixon says that it was 19 years before Vertex was "strategically ready" to need a full-time professional, meaning the company had progressed to a point at which it had plenty to lose if something went wrong. Upgrading can be done in stages, but a typical time line for a company of 200 people is about 3 years with a cost of up to $500,000 to provide full protection, which includes closed-circuit television and entry access. *BH*

Have discussions with several security experts before deciding whom to hire. Also, use your networking skills—ask other biotech executives whom they have worked with and gauge their level of satisfaction with the results.

The risk assessment will determine the current needs for your company. How you address those varied needs is up to you—you'll have to determine the risk appetite for your particular company, and you'll need to decide what you must absolutely take care of (and pay for) now. As CEO, you'll need to keep in mind that a "big lawsuit might wipe you out," says Patillo, and balance that against the probabilities of any particular risk actually occurring.

Once the gaps are identified and the company's appetite for risk established, close the gaps with a strategic plan. It should be specific to your company and its goals, but there are two basic aspects that require protection at every company: human and nonhuman assets.

Nonhuman assets

To protect the nonhuman aspects of your company, you'll need to keep track of the *humans* entering and leaving your building. At the very least, this keeps simple things like chairs from being stolen, but it also means unauthorized people don't enter your lab or access the computers. There's no reason to put at risk valuable data or patent information.

The most effective way of achieving this is by controlling access. If you're in a space leased from an academic institution, or in an accelerator, it's likely this is already taken care of. But if your firm has moved out on its own and has people coming and going, you'll want an identification badge system and/or a closed-circuit television system to monitor the exits. There are dozens of places to turn to online for help, but a good starting point would again be ASIS. (There is a membership fee to join the site, but it's fairly low at less than $200 annually.)

Perhaps you need more than door security—perhaps you need a fence to protect valuable reagents or equipment or biological materials, or maybe you have a pilot plant for producing second-generation biofuels. Either way, the risk assessment will help you identify your needs, and you can make your decisions from there.

The human factor

The most important part of any company is the employees, so protecting them is paramount, both at the office and when they travel (**Box 2**). Although there are reports of animal rights extremists attacking biotech companies (perhaps most infamously the two pipe bombs that were detonated at Chiron, of Emeryville, California, in 2003, although there were no injuries), history suggests these types of activities are quite rare. Instead, most employees simply need to be protected from their own behavior, says Hamilton Mixon, senior director of risk and global security at Vertex, in Cambridge, Massachusetts.

Partly, this means preventing theft of IP or proprietary information by your employees. How this is actually done, and the systems put in place, will be company specific and generated by your risk assessment.

But there is more to consider here, as employees are also people, leading complex lives and having emotional desires and goals that vary widely. They will interact with each other; it's possible they will have differences of opinions and sometimes even strong dislike for one another. As a founder or executive, you'd do well to consider a program for monitoring and preparing for violence in the workplace. Mixon says the most common occurrence is simple assault. A good program will aim to detect early warning signs of a disgruntled or potentially violent employee, and it will also lay out a plan of appropriate response. It is crucial to stop these types of occurrences before they happen, not only to prevent injury but also because it takes just one violent incident to make others feel unsafe on the job for years to come.

Hired help

Even after programs have been put in place, the issue of oversight remains: Who will monitor all this? The point at which your startup needs a dedicated security person will mostly depend on you and the rest of leadership. You'll need to discuss this with the board and decide if it's time to allocate the resources to the new position. Also, there has to be enough work to keep that new hire busy, so if you're a three-person company in a university space that has its own security, then it's not the time to fill that position.

When the hire is made, that person will work closely with both the human resources department and your legal representation. The job of human resources is to take policies and issues to the staff, hopefully smoothing over any inconveniences caused by implementation. The legal department helps ensure that those involved in any infraction do not have their rights violated and covers your company in terms of liabilities.

All of this comes at a cost, of course, and as a company you'll need to decide what you can spend (**Box 3**). But once it's in place, it simply needs tweaking to reflect growth. "A small firm with 100 employees will have the same components as a billion-dollar, multinational company," says Mixon, "but it has to be done to scale."

Conclusions

Biotech is not crime fighting, and running a small business is not espionage for the government, but you'll need to take certain steps to protect the valuable assets of your company. That begins with a gap/risk assessment that will help you define what type of security program you'll need to put in place.

ACKNOWLEDGMENTS

The author is grateful to Hamilton Mixon, Anthony Patillo and Richard E. Widup for insights in drafting this article.

To discuss the contents of this article, join the Bioentrepreneur forum on Nature Network:
http://network.nature.com/groups/bioentrepreneur/forum/topics