Steps an Organization Should Take to Protect Confidential Information

Confidential information defines organizations and is what sets them apart from their competitors, whether it is business plans, personnel records, trade secrets, patent applications, or consumer research. In a world that is only getting more competitive, it has never been more important to protect that information by any means necessary.

Of course, guarding confidential information is not a novel concept, but that being said, keeping papers locked in a safe behind a picture frame does not cut it anymore. Companies working with secure information today face enormous challenges to protecting their secrets—virtually every person has the means to record information and send it anywhere in the world, causing irreparable harm with the touch of a button. Those challenges have only been exacerbated by the need for many organizations to permit remote working, which has forced companies to communicate about and work with sensitive information outside of the office, opening a pandora's box of opportunities for mishaps—unintentional or not.

Luckily, there are a number of steps companies can take to be proactive about securing their confidential information—the modern day equivalents to a lock and key, but potentially even safer. The best starting point is to conduct a full analysis of secure information protocols and ensure that best practices are applied throughout and apply the same level of scrutiny to employees who are departing.

Unfortunately, there will always be the reality that no protocols are bulletproof, and information will slip through the cracks. In that case, it is critical for organizations to have protected themselves legally to the extent possible.

In short, a company should have a robust mixture of technological and legal based safeguards in place, each mutually reinforcing the other.

Security Protocols

Going back to basics is the first step to securing any piece of information. Oftentimes in high-level discussions about information theft, people portray the theft of confidential information as if it were the storyline of a James Bond film. Make no mistake, such threats are out there and should be taken seriously, but the reality is that a majority of confidential information leaks come from a lack of basic security measures.

A thorough assessment of information storage is essential for companies that keep confidential information of any value. Secret documents and materials should be labeled as such both physically and digitally and be subject to restricted electronic access and password protection. They should be kept on separate servers from general documents and if possible, only be accessible via secured networks.

With the connectivity of the world only increasing, companies should not trust anyone with their information and should put strict limits on how the information can be shared. Many companies have invested in software and platforms exclusively for such information, wholly taking away the risk that a PDF can simply be attached to an email. For those that continue to use paperwork and other confidential physical assets, storing the files in a separate location from others and allowing only heavily restricted, supervised access are responsible

measures. When materials need to be shared in boardrooms and the C-Suite, even the most senior officials should turn in their phones and all paperwork should be collected after the meeting to limit leaks.

Training any staff who handle confidential information is another simple but important step that companies can take to protect secrets from being shared unintentionally or otherwise. Such training can help people identify what is confidential and when they are handling it, and also help them understand the damage that could be done to the company if it is made public. Thorough training also covers protocols for taking company property and materials off site and how to establish secure remote connections at home or otherwise—a critical additional step in the age of enhanced remote working.

When employees leave an organization

The same level of scrutiny must be applied to employees who part ways with the company. One of the biggest concerns in any industry that relies heavily on confidential information is the threat of their employees being recruited and poached by competitors. The practice is becoming more commonplace in many industries, and when it happens, it comes with the risk of the former employees using prior knowledge to another company's advantage.

The immediate solution to this is inserting a noncompete clause in contracts, but in a job market that favors workers, sometimes that is not feasible when recruiting talent. If that is the case, companies should have strict protocols in place for departing employees to take every step possible to protect confidential information and trade secrets.

Regardless of the subsequent employer, upon notice of departure a company should be intentional about reminding the employee of any confidentiality agreements that were signed during their tenure. Most agreements are legally binding for the lifespan of both parties and do not expire when the relationship ends and departing employees should be reminded of that and also be asked to acknowledge it in writing. While these precautions may seem extreme in the moment, especially if the separation was on good terms, they serve as an opportunity to manage the risk of confidential information being used improperly. It also shifts legal liability away from the information owners in the case that action must be taken and creates a clear expectation of legal ramifications if an agreement is breached.

Finally, companies need to be sure they do their due diligence with regard to confidential information when employees leave. Be sure that they are locked out of all IT servers and platforms, and ask for all confidential physical assets to be returned, including sensitive documents, laptops, phones, and identification cards. It is worth noting here that private servers with restricted access and sharing permissions, as mentioned before, make this process significantly simpler. If confidential information is secured electronically, it mitigates many of the risks that come with keeping things on paper.

Trade secrets

Not only do basic security protocols make confidential information more secure on its face, but it also allows it to be enshrined by the legal protections that come with being trade secrets.

Like patents and trademarks, trade secrets are protected under U.S. Code and violations can be prosecuted. State law protection is also available. Both federal and state trade secret laws offer significant protections for owners of confidential information. But unlike patents, a company need not apply for a trade secret, as telling someone (even the government) would make the title of "secret" null and void. Instead, information must meet the following criteria to be a trade secret:

1) Have actual or potential independent economic value by virtue of not being generally known
2) Have value to others who cannot legitimately obtain the information
3) Be subject to reasonable efforts to maintain its secrecy

While the first two rules are straightforward, the latter is worth scrutinizing: to legally protect confidential information, the information itself must meet the threshold of being reasonably protected. The caveat: what is "reasonable" is not well defined in many cases. Each court applies its own standard of what is reasonable to trade secret cases, so in order to be able to apply the legal protections it is critical companies take extra steps to meet the standard. Although the threshold could vary with each court, by seeking out precedent from prior cases companies can have comfort that secrets will be protected by trade secret law should they ever need to take legal action.

Perhaps the most applicable precedent is that confidential information needs to be secured beyond that of normal information within a company. For example, every company today puts documents on a secure server. In order to be a trade secret, confidential materials need to be put on a more secured server than the rest. Taking the steps outlined in prior sections would be strides toward meeting that threshold.

Nondisclosure agreements (NDAs)

It goes without saying that the best way to protect confidential information is to share it with as few people as possible. But that being said, it is unrealistic to think that individuals and companies can bring ideas and products to market without enlisting help from employees, manufacturers, third parties, and countless others — all of which require that some secrets be shared. When that happens, one of the most popular prescriptions for keeping information safe is a nondisclosure agreement.

By nature, NDAs immediately create a confidential relationship between the owner of the information and another party. It allows secrets to be shared more openly and forms a more productive dialogue. Furthermore, the risk involved in information sharing decreases markedly, and while there is still potential for a breach of trust, the owner has a clear legal path for retribution.

However, companies should continue to be cautious with confidential information even if a nondisclosure agreement exists between people or businesses. While an NDA does protect information, it does not always prove ownership, and as such leaves open the possibility that another party could use the information themselves, even without being in violation of the agreement. To protect their information and liability, companies should strongly consider laying a contractual claim to ownership when transferring confidential information.

Confidential information is the lifeblood of organizations, and they should be intentional about protecting it. While the steps outlined here do come with costs, a helpful exercise is to think about the costs that would come if the most significant piece of information was stolen from the company and used against it. The harm would be irreparable, and legal retribution difficult, which begs the question, why wouldn't companies take the steps necessary to protect themselves? Basic security protocols, nondisclosure agreements, meeting the threshold of trade secrets, and properly offboarding employees are low-cost steps that pay high dividends in protecting the confidential information that businesses rely on.