Make IP a priority

Why you must diligently enforce policies that protect valuable data

INTERVIEWED BY MARK SCOTT

MICHAEL CRAIG
Attorney
Intellectual Property Group
Brouse McDowell
(330) 434-6273
mgcraig@brouse.com

WEBSITE: To learn more about how to protect your company's valuable Intellectual Property, visit www.brouse.com.

When most people think of cybersecurity issues, they think about loss of personal information such as bank and credit card data or usernames and passwords which may lead to identify theft and potential financial loss.

But the loss of intellectual property (IP) and IP rights can often create more lasting damage, says Michael Craig, an attorney in the Intellectual Property Group at Brouse McDowell.

Patents, trademarks, copyrights and even trade secrets are all tools used by companies to protect their IP rights. The problem is some companies get so busy that they don't take the time to formally apply for these protections.

"You'll find companies that put it off and leave openings for their invention to be disclosed publicly," Craig says. "One of the things about patents is there has to be absolute novelty, meaning no public disclosure. It doesn't matter if it's inadvertent or purposeful. If it's publicly disclosed, you may not be able to get a patent on it."

Smart Business spoke with Craig about how to protect your IP from being exposed through social media.

What can a company do to protect its IP from being leaked?

If you have new discoveries, inventions or processes that you want to protect with a patent, don't wait. The law recently changed with patents so that it is the first person to file that gets the patent. It used to be the first to invent, but now it's the first to file. So the first person to the patent office with their application is the one who gets the patent.

In the U.S., there is a one-year grace period from public disclosure, but most other countries do not have that in place. So the lesson here is once you've vetted something for a patent, pursue it as quickly and securely as possible.

Trademarks are a little different in that once you file a trademark, it becomes publicly available. If you're Cedar Point and you're coming out with a new roller coaster, you might not mind the publicity when you file the trademark. But if you're rolling out a new branding strategy, you may want to wait to file until the day you are coming out with it so as not to alert others until you're ready.

Trademarks, copyrights and patents are all protected by federal law. This is not the case for trade secrets. But if you have a design, process, procedure, formula or some method that you derive some kind of economic value from not being known by others, you are protected in Ohio. As long as you're making an effort to protect that information as a trade secret, you can do it perpetually.

What's the key to protecting IP as it is being developed?

Information loss often comes by way of current and former employees and vendors. Most often it is a crime of opportunity, and is not always malicious. It's unlikely that your company will fall victim to an act of corporate espionage involving an unknown infiltrator trying to expose your new ideas.

But events occur, and companies often live by the 'patch and pray' method of protecting IP. An incident occurs and you throw a patch on it hoping it never happens again. Obviously, this is not a very reliable security strategy.

The best approach is to begin with a top down review of how information is managed in your company both internally and externally. Everything is on the cloud now, providing countless access points to valuable information. Get a policy in place to protect you and enforce that policy. Make sure all employees, vendors and anyone else who might come across sensitive information sign nondisclosure agreements that provide a remedy if something is disclosed. You also need a policy for online behavior. Any place you go, you have people on their mobile devices accessing a variety of information online. Unfortunately, that's where these compromised bits of code and things are introduced onto the devices.

They return to the office, link back to your system and that code gets uploaded which can allow access to sensitive information.

You may need to limit user access to websites or the email they can send and receive, if you have information you're serious about protecting. ●