A McCann Investigations White Paper
www.mccanninvestigations.com
(800) 713-7670

Digital Intellectual Property Theft: Protecting Your Organization from Potential Attacks

April 2, 2013

Summary:
This paper explores the complexities of digital intellectual property. The sophistication of cyber assaults has increased at alarming rate allowing hackers to steal intellectual property from individuals and small companies, to large companies with a significant global presence. Threats come from not only state-sponsored cybercriminals, but also from internal employees. Companies must look at securing their data from the view point of a hacker, rather than a company trying to protect its assets.

Digital Intellectual Property Theft: Protecting Your Organization from Potential Attacks

As digital technology continues to advance, so do the tactics used by cyber criminals. Many experts agree that digital intellectual property (IP) theft is on the rise – the United States Department of Commerce recently estimated that stolen IP could cost companies a combined $250 billion every single year. That dollar amount doesn't even include unnoticed or unreported instances of IP theft and other cybercrimes.

It's not just the technologies and tactics that these hackers are using to accomplish their crimes – the organization and coordination of these cyber assaults has also become far more sophisticated. In fact, many officials believe that state-sponsored cybercrimes against the United States government are among the most common forms of cybercrime.

Businesses are particularly vulnerable to cybercrime. As companies increase their scope and begin to collaborate with business partners on a global scale, their exposure to criminals and foreign governments also increases. This makes the risk of a cyber assault even more palpable. Competing companies will do anything they can to get a leg up in their industry, even if it means resorting to illegal or unethical means to do so.

Therefore, it is extremely important for businesses, organizations and other entities to thoroughly manage the risks of cybercrime. The best way to do this is not to simply treat the threat of hacking like any other security risk. Instead, you must take a counterintelligence mindset and *always* assume that someone is coming after your data.

A famous example of this mindset is the anti-hacker approach taken by Facebook. There are well-known stories of Facebook founder Mark Zuckerburg hosting all-night "Hack-a-thons" at Facebook headquarters in Palo Alto. The purpose of these events is to have self-professed hackers attempt to break into Facebook's system. If nobody succeeds, then great – Facebook remains secure. If they *do* manage to succeed, then that's also great – Facebook becomes aware of potential weaknesses in their security.

If your company approaches the risk of IP theft and cybercrime with the mindset of a hacker rather than a company simply hoping to cover its assets, your information will be significantly safer.

What types of organizations are susceptible to IP theft?

Any company or individual that has intellectual property stored in a digital format has at least a small risk of IP theft. However, the seriousness of this threat ranges based on the type of information stored and how well-defended that information is. Some of the organizations that have the highest potential IP theft risk include:

- Large organizations that operate on a global scale or work with foreign partners
- Small and midsize businesses that operate in a particular niche market
- Military of government organizations that delegate work to contractors
- Telecommunications companies that run national infrastructure
- Any organization without sufficient monitoring or enforcement of online security

Note that it's not only high-profile targets that face the risk of intellectual property theft. Simply put, if your business or organization has information online or stored digitally, then there is always the risk of IP theft. Though large, global organizations face a greater chance of cybercrime and a much more sophisticated cybercriminal network, every organization needs to do its due diligence in protecting itself from these types of crimes.

Who is looking to steal my information?

While the threat of state-sponsored and other types of external attacks is very real, and though these potential attacks pose a variety of challenges, the more common threat facing the average business is an internal breach. As we would say, it's not China that wants your information – it's Bob the Employee who is looking to start his own competing company.

McCann Investigations handles a significant number of cases that deal with intellectual property theft stemming from within the company itself. The perpetrator could be a dissatisfied employee

looking to branch off and start his own business, a former employee who either resigned or was fired and is attempting to start his own business, an untrustworthy current employee hoarding protected information or any number of other potential possibilities.

Higher profile companies, therefore, need to be particularly careful with their information, as they have many more employees, partners and insiders that could potentially steal their intellectual property. Organizations need to consider risks posed by in-house employees to employees who connect to their system from a home office, or from other external networks.

How can I keep my organization's intellectual property secure?

There are a variety of means available for organizations to protect their intellectual property, but the first step is to determine exactly what that intellectual property is. Just because you have a particular idea of what the most valuable pieces of information stored on your company's databases are, doesn't mean that cyber criminals share the same opinion.

To identify what information could be particularly valuable to hackers, first consider what information you have that could help a competing business get ahead of your company in the market, or help a foreign company gain ground in its own market. Asking these sorts of questions is a good type of self-reflection that forces you to think in a different way about the state of your digital security.

Next, you need to figure out exactly how much money and effort you want to spend on protecting this information. What exactly *is* the value of the information that you are trying to store? You must way the costs and benefits of your potential IP security system before you put a system in place. The greater potential you have for theft or loss, the more you should invest in security.

The most common security tools used by organizations to combat IP theft include sturdy firewalls, antivirus and antimalware software, digital forensics tools and other forms of intrusion detection tools. However, as previously mentioned, it behooves organizations to use these tools with a counterintelligence mindset, as opposed to a passive defense mindset. Search for potential weaknesses before a cyber criminal can exploit them.

There are also far more advanced security tactics available. These deeper cyber defense strategies typically have multiple layers of different types of protection. In addition to antivirus and antimalware software and all of the other standard fare for defense, the security system could also contain segmented networks with tighter security for their information, more advanced detection systems, and various portions of the network that are “demilitarized” to allow access for public data.

In the end, there is no way that your organization can ever guarantee that all of its information is completely, 100% secure. But there are ways to cover your bases and ensure that you are at least prepared in the event that a security breach actually occurs.

What happens if a security breach occurs?

Many people who work in IT departments have the mindset that it is important to get the servers back up and running as quickly as possible after an attack, but this is not always the most prudent course of action. Before you even think about getting the information back up, consider the importance of the contents at risk, whether the network intruders got a hold of any of that information and whether the attack was actually meant as a diversionary assault to distract you from a much greater threat.

If the threat level appears to be high and there could be a significant impact of the incident, then it may be a good time to get law enforcement involved and increase security of other company systems.

Also, it is important to keep communication channels open during security breach situations. Work with your public relations advisers to determine whether it’s best to inform partners, vendors and the public of the breach, and if so, how it should be done.

After the situation is resolved, it is also important to reflect on how the breach happened and what could have been done to prevent the situation. Which data did the hackers go for? Which tools and methods did the hacker use to reach the data? How did you react to the breach, and

how did you go about solving the problem? Assess every single facet of the entire incident, so that you are even better prepared if and when another incident occurs.

Call us when a security breach occurs

When your organization or company falls victim to a security breach, contact the team at McCann Investigations for assistance. Our digital investigators locate the cybercriminal and uncover evidence that proves their guilt. Contact us for more information about our services and how we can protect you when your intellectual property is at risk.