



5 insights on cyberattacks and intellectual property

An interview with Don Fancher, principal, Deloitte Financial Advisory Services LLP

Business leaders know that a cyberattack can severely damage and disrupt their company. Yet they may underestimate the scope and depth of the threat. The expected costs, such as notification and protection of affected customers, potential litigation, and necessary cybersecurity improvements, can pale next to other possibly longer-term impacts lurking beneath the surface.

Consider these five factors when assessing the security of your company's intellectual property:



Beyond the theft of customer data and potential regulatory issues and reputational damage following a cyberattack, it is imperative to understand other less-obvious costs, such as theft of intellectual property (IP).

IP is the lifeblood of many organizations. It fuels innovation, growth and differentiation. As discussed in the Deloitte white paper "Beneath the surface of a cyberattack: A deeper look at business impacts," IP loss is among the hidden or less visible costs of an attack, along with lost contract revenue, potential devaluation of

your company's trade name, and damaged or lost customer relationships. IP theft differs from customer information theft in that your company owns the IP, whether trade secrets, drawings and plans, or proprietary know-how. Because of this, your company may very well have an obligation to shareholders and stakeholders to identify what has been stolen, assess potential impact and loss, and seek potential recovery of the IP as soon as possible.



Speed is crucial when investigating IP cyber theft.

A pernicious trait of malware and other types of cyberattack software used now is the difficulty of detection. Cyber theft can go on for an extended period of time and companies often fail to realize that their information is being siphoned off. Moreover, competitive advantage can evaporate if significant IP is stolen. So it is important that you rapidly determine what has been taken and assess the damage to your organization, customers, and others affected, as well as look for other viruses or malware that may be lurking in your systems.

Taking these steps sets the stage for two responses. The first is to pursue the thieves and try to either recover your data or block them from using it in a way that potentially damages your company.

The second action, as discussed in the "Beneath the surface" paper, is to quickly determine how the stolen IP can potentially be modified—or new IP developed—to regain the competitive separation originally sought between your organization and other players in the market. The more time passes, the more opportunity the organization behind the cyberattack has to use the stolen IP against your company, whether directly or by selling it to your competitors. Quick identification of the theft can accelerate your process of strengthening security around your IP and, if possible, developing other innovations to regain and maintain your company's competitive advantage.



Forensic investigation is vital when IP or trade secret theft has occurred.

Forensics can be important to several aspects of the investigation. The first is tracking the cyberattack to determine what happened, how it happened, and what, in fact, was stolen or taken. Forensics can help identify the data involved, its sources, and where malware or other destructive capabilities infiltrated the system.

Understanding these factors provides the basis to quantify the impacts of the theft, including ripple effects such as damaged customer relationships, lost contract revenue, and trade name devaluation; pursue and identify the theft perpetrators; and build a defensible chain of custody around the data. If the data is unrecoverable, the investigation can support efforts to pursue legal action aimed at mitigating your organization's losses.

Encouragingly, this past spring the US Congress passed and the president signed the Defend Trade Secret Acts of 2016, which for the first time provides federal criminal penalties for trade secret theft. Previously state laws governed trade secrets. The act expands prosecutorial, damages, and recovery aspects of enforcing trade secret law, which should help improve a company's response to such issues.



Forensic investigation relies on specialized talent and methods.

Data analytics specialists can pull data off of compromised systems and run queries to identify patterns, isolate security breaches, and determine whether data has changed or gone missing. These professionals also help establish the chain of custody for data, including what was taken, as well as when and how. They understand the signatures, hallmarks of and distinctions between internal and external actors. Utilizing person-to-person interviews and analysis of computer systems and network traffic, investigative teams can determine whether the attack was the work of internal or external actors.

Forensic financial and accounting specialists who understand IP and its value are also essential. Along with their technical expertise, they can bring perspective on business processes and the competitive marketplace to quantifying damages associated with theft or infringement. They also often serve as expert witnesses in subsequent court cases, testifying about the theft of the IP or trade secrets, their value, and financial impacts of the theft.



Beyond cybersecurity, there are important preventive steps to take.

When a company pursues litigation against someone it claims has stolen IP, the defense's first move is typically an effort to prove that the plaintiff didn't do enough to protect it. How can something be IP if every employee had access to the compromised database and information?

Readiness means not only having secure systems, but also that your company's trade secrets are maintained such that they can rightly be deemed IP. Take, for example, if one of your employees steals documents and drawings and sells them to a competitor. Your company should be able to show that while the employee had access to the data, very few other people did. This can support your case for prosecuting the employee.

Proving this level of security requires proper policies and procedures, employee protections, and systems in place. To accomplish this, top executives from the CEO down need to be on the same page in understanding how to deal with a cyber threat. War-gaming scenarios involving these players can be invaluable.

Our take: Protecting IP requires understanding its vulnerabilities and a comprehensive approach to thwarting cyber threats.

Some business leaders are simply not aware of the risks to their company's IP, or the opportunities available to protect it. Taking these threats seriously and fighting back, both as a matter of preparation and of response, is imperative. Otherwise, the bad actors will continue to perpetrate their crimes, because there's no reason not to. Manage and mitigate risk, but in a way that enables you to create and protect value, and to power your performance.

Contact

Don Fancher

**Principal | Deloitte Advisory
Forensics & Investigations**

Deloitte Financial Advisory Services LLP

+1 404 220 1204

dfancher@deloitte.com

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.