Bloomberg BNA

Privacy and Security Law Report®

IP Theft

In the digital age valuable intellectual property isn't just secret formulas but also source code used by tech providers and high frequency trading models of financial companies, the author writes, detailing measures companies can take to reduce their vulnerability to IP theft.

Addressing the Increasing Challenges of Digital IP Theft

BY EVAN BUNDSCHUH

Intellectual property is more than just a valuable asset. For many companies it is their financial backbone. Remove it and they may crumble. A testament proven by the numerous layers of security controls secretly guarding the vault housing the Coca-Cola Co. recipe. Criminals would have an easier time stealing a painting from the Louvre.

In today's digital age, valuable IP is not solely restricted to unique recipes of Fortune 500 companies. An increasing number of companies rely on their IP, from tech providers and their source code to financial firms and their high frequency trading models to gaming companies and their physics engines. And with ''constant connectivity'' that IP, if stored in a digital environment, is at risk.

Evan Bundschuh is vice president and commercial lines head at GB&A, an independent insurance brokerage located in New York focused on insurance programs and risk management solutions for tech companies, financial and professional services, manufacturers and product-based businesses.

We are all familiar with the varying types of IP. However, less familiar, is the many forms IP theft can inhabit. IP theft can masquerade itself in the form of gifts or may appear as a ''standard'' data breach. With all of the risks threatening intellectual property however, cyber espionage is regularly cited as the single biggest risk to digital IP—particularly cyber espionage by China, with some estimates calculating 40-80 percent of IP theft having ties to actors in China.

The recent breach against ThyssenKrupp Services AG clearly demonstrates both of these points. In this case, the breach was carried out with intent, as a targeted hack seeking their industrial trade secrets and seems to have been executed from Southeast Asia. Luckily it was discovered by the company fairly early in the intrusion, allowing them to limit the damages and prevent any further exposure. These types of hacks though, even if discovered early can pose significant challenges, as it is often very difficult to determine how much of the company's IP has been exposed and what the hackers motivations and intentions are in utilizing any trade secrets or source code that may have been obtained.

In this case, ThyssenKrupp believes fragmented IP had in fact been accessed or stolen but quantifying that can be difficult. While cyber espionage continues to be a leading risk to intellectual property, the second greatest risk may come as a surprise—your own executives and employees. Exiting executives who feel as though they have an ownership stake and executives breaking off to form competing organizations may attempt to take the IP with them. Corrupted or poached employees and those that are let go are also likely to steal. Without

strong internal controls, employee theft can be extremely difficult to detect and near impossible to prevent.

When it comes to implementing controls, there is a wide range of software and policies/procedures companies can implement in order to protect against theft—digital/cybersecurity controls being the most obvious. Organizations with valuable IP should begin with implementing standard protections, such as firewalls, dual-factor authentication and strong encryption, working their way out to more advanced controls such as installing specialized software to identify code exfiltration and fragmentation of source code (when able).

Cyber espionage is regularly cited as the single biggest risk to digital intellectual property; the second greatest risk are your own employees.

The entire security environment should be white-hat stressed tested on a regular basis for vulnerabilities, establishing (and tracking) any key risk indicators and improving any weak links in the process. Implementing strong ''Internal practices'' is equally important. These practices should incorporate employee training programs to identify and report suspicious behavior and published policies against storing or transmitting IP on any mobile devices, cloud services and/or unsecured third-party platforms. Organizations with particularly valuable IP/source code can also consider ''slotless'' workstations (that contain no media ports) and physical security/tracking controls in an effort to prevent theft from employees.

When discussing theft of IP, a strong defense is often the best offense. For some companies this may require operational changes. For example, shortening supply/development chains and reducing the number of outside vendors effectively reduces the number of potential breach points. While not always an option, avoidance of high risk countries altogether can also significantly reduce exposure.

If and when IP is stolen, legal recourse is technically available through administrative and judicial channels however the processes are costly and lengthy and pose a number of challenges. Foreign laws differ, and in many countries, do not provide the same level of protection afforded by U.S. laws. Pursuing claims against foreign actors can be extremely difficult. Resulting judgements also seem to yield limited results. With many attorneys and investigators still familiarizing themselves with e-forensics, establishing proof of theft alone may prove challenging. Criminals could also attempt to mask their theft through ''silent'' intrusions and by slightly altering the IP.

Needless to say, pursuit of foreign infringers will very often not provide sufficient indemnification post-loss. With such limited recourse, some reports have gone so far to recommend taking aggressive (and controversial) measures including retaliatory cyber intrusions and social engineering attacks overseen by counsel.

Organizations particularly concerned about IP theft, will often look to insurance with the hopes of mitigating any remaining risk. Those companies will almost always come up short in their searches for ''true'' IP coverage. Simply put, there are no policies that provide protection against theft of source code or IP.

Opinions may differ on whether or not such coverage belongs under a cybersecurity insurance policy or a crime/fidelity insurance policy but I would consider the risk to fall under the latter due to the fact that such crimes do not solely arise out of cybersecurity breaches. The underlying problem is a matter of semantics and poses many challenges. Many insurers only provide coverage for theft of ''tangible property,'' and intellectual property, by its own definition, is not tangible. Even the term ''theft'' itself is problematic—how can something be stolen that is not tangible? And this dilemma is not an isolated problem for insurance companies. Courts have an equally difficult time arriving at a determination, as demonstrated by the Goldman Sachs case which was overturned a few years ago, then successfully re-pursued last year.

The fact that such property is also inherently difficult to value, poses an additional challenge to insurers. Any insured IP will almost certainly be viewed (by the buyer) as being worth more than determined by the insurer at time of loss. The challenge of calculating lost revenues resulting from such a theft is yet an entirely separate hurdle. Insurance companies have created specialized policies in the past in order to test the waters, only to quickly retreat. The only current solution for insuring against IP theft would be via a specially developed captive program. However these programs often require the buyer to create their own program, and act more as an asset management tool than true risk mitigation vehicle. There are however insurance products available to protect the c-suite and any residual damage resulting from outside intrusions targeting your IP.

Shortening supply/development chains and reducing the number of outside vendors effectively reduces the number of potential breach points.

Though cybersecurity insurance policies provide no protection against direct financial loss of IP theft, the theft itself does not have to be successful to inflict damage. In their quest for IP, cyber thieves may also steal confidential information for additional monetary gain. Security intrusions can also cause collateral damage by corrupting data and disrupting networks in the process, which often result in lost income from downtime and restoration costs to the organization. Depending on the specifics of the breach, these intrusions may also trigger disclosure obligations under breach notification laws.

This residual damage can (and should be) insured against through the placement of a well-structured cybersecurity insurance policy. The residual risk to directors and officers is even greater. Due to the tremendous value of an organizations' intellectual property, theft of that IP can often result in catastrophic damages—from shareholder claims triggered by stock drops (asserting that the company failed to take proper precautions) to creditor/bankruptcy claims when the organization can-

  PVLR ISSN 1538-3423

not financially recover. When employee stock option plans suffer and/or large layoffs are triggered, employment liability claims may also follow. The last line of defense against such claims is a well-structured director and officer liability (D&O) insurance policy. With some insurers slowly incorporating cybersecurity-related exclusions on their D&O policy forms, buyers should be extra diligent to avoid any such exclusionary clauses.

For companies unfamiliar with management liability policies, please see the GB&A guide to data breach insurance.