Safeguarding Software IP During And Beyond The Pandemic

By **Denise Mingrone** (August 31, 2020)

Denise Mingrone

Piracy has plagued software developers since the launch of the first software products decades ago.

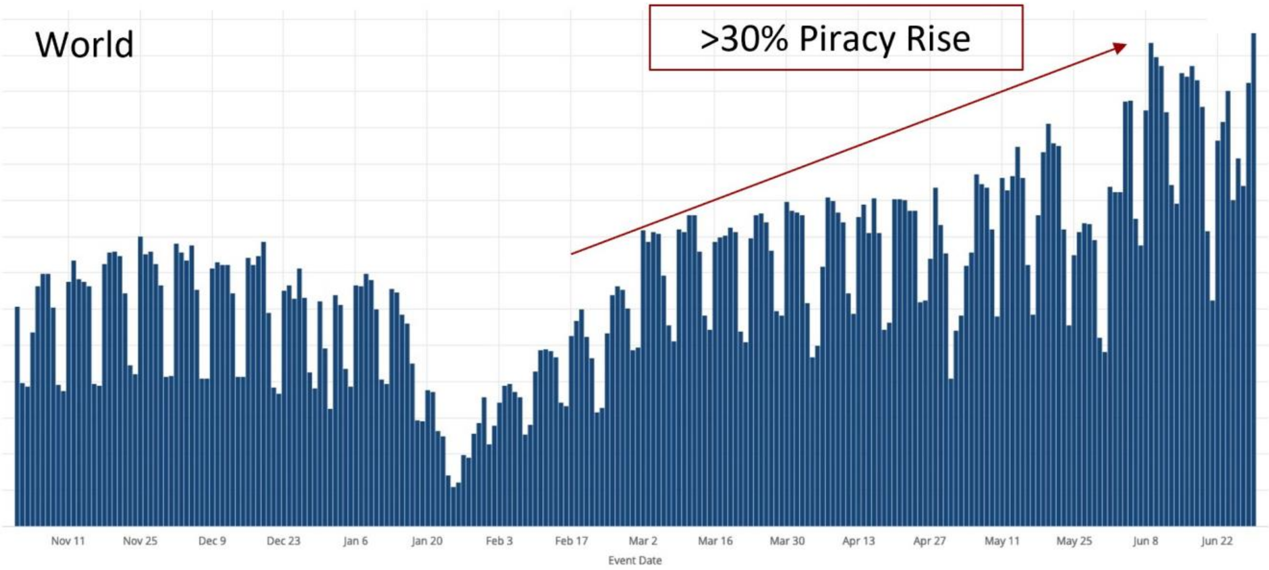
And piracy has continued to increase as enterprises expand their use of the cloud. Illegal software usage — software used without proper licensing, aka piracy — ranges from deliberate piracy involving making, using and selling illegal copies or cracking or circumventing license technology, to knowingly buying cheaper illegal copies online, to unknowingly over deploying or sharing licenses within a company.

Now the COVID-19 pandemic has posed a new threat. Software companies are reporting that piracy has increased 20%-30% since stay-at-home orders were issued in early 2020.

Such orders, coupled with increased remote working environments, have left the door open, literally, to allow sophisticated hackers to breach even the strongest online fortresses designed to protect companies' key intellectual property. Unemployed workers are buying pirated software over the internet to use in order to generate independent income and employees working from home are making illegal copies of software they need for their job that their company has not provided legally.

The chart below shows the uptick in illegal usage of several engineering software applications since stay-at-home orders were first imposed.

Global License Compliance Events



Source: Cylynt

How can companies best respond to ensure their crown jewels are safe while also protecting the health and safety of their employees? The keys to success lie in a data-driven analytical approach supported by anti-piracy technology and robust license compliance enforcement programs, which together enable companies to accurately identify, quantify and remediate illegal software use.

This article discusses how hearty compliance programs coupled with anti-piracy technology can protect software from piracy through a data-driven approach that uncovers illegal usage and permits compliance professionals and their counsel to shut down pirates, recover lost revenue and enhance the protection of their software.

Data Technology Versus On-Site Audits

Data technology and analytics are critical weapons in the software piracy environment for several reasons. First and foremost, it is nearly impossible to battle an enemy you do not know. Without collecting data on unlicensed usage, a company has only its suspicions as to who might be illegally accessing its software.

Second, traditional methods of ensuring compliance such as on-site audits may no longer be feasible in the post-COVID-19 world, where brick-and-mortar sites are closed, and users are working from home. Even assuming sites will eventually reopen and employees return, on-site audits are unlikely to uncover the full extent of preexisting piracy.

Why? Most servers, laptops and other devices that are typically reviewed during on-site audits only maintain record logs for short time frames, such as 60 to 90 days. In instances where lengthier logs might exist, they can be easily deleted or altered to mask piracy.

Additionally, most companies audit only certain areas rather than the complete site, trading off uncovering all piracy versus the expense of a full audit and the risk of jeopardizing the client relationship should the audit be too invasive and troublesome.

Anti-piracy technology coupled with license compliance programs, on the other hand, work seamlessly together to collect and analyze the usage details of unauthorized users accessing the software, regardless of physical location. Commonly known as phone-home technology, the anti-piracy software detects unauthorized use and then triggers communication between such user and the manufacturer.

For example, if the software is modified or accessed via a counterfeit license, the manufacturer will be alerted and provided with detailed data about the geographic location of the machine using the software, such as the date, time and number of uses, as well as the machine's IP address.

The data generated can then be analyzed by license compliance professionals to discover the full extent of the piracy and contain it in advance of or in lieu of a physical audit. Concurrently, the data can be used to identify the perpetrators and ensure they are shut down and compensate the software owners.

Beyond simply providing raw evidence of piracy, data can also be collected and analyzed by counsel and experts to recognize patterns and develop the full story of misuse to effectively convey in legal proceedings.

License compliance professionals, counsel and experts can use precise telemetry data to protect their software and recover revenue lost to piracy in a number of ways, including through reports of piracy events showing dates, specific pirated software and detailed user activity.

Such analytics serve to assist companies and counsel in determining how best to manage their compliance programs by providing critical information such as regions and countries in which the highest amount of piracy is occurring so that personnel and assets can be deployed in high priority regions with the most promise to yield results.

Inadvertent Misuse

Software is pirated in both intentional and unintentional ways. In inadvertent misuse cases, employees typically share licenses by cloning their PC hardware or sharing license login credentials, or they make additional internal copies to install on a personal machine in order to work from home. Without data analytics and a robust compliance program, it is impossible for large global companies to keep track of all software usage and know who is and who is not using legal copies.

Cases of inadvertent misuse are common and uncovering and dealing with them can result in significant recovery of lost revenue, often without resorting to legal remedies. License compliance professionals can, for example, present such data before or during an audit to streamline, and possibly even eliminate, a full-blown on-site audit.

Even in instances in which legal remedies may initially be needed, such actions have proven extremely effective and are often short-lived and resolved amicably to the satisfaction of both users and manufacturers once the inadvertent users are made aware of the situation through the presentation of their usage data.

Deliberate Software Piracy

Deliberate piracy, on the other hand, typically consists of five main types, of which counterfeiting and internet piracy are the most high profile and well known. Counterfeiting involves making illegal copies of copyrighted software products for personal use or, more commonly, for distribution or sale.

Internet piracy occurs when counterfeited software is made available to download over the internet for free or sold at a much lower price. This kind of piracy is often highlighted in cases involving counterfeiting entertainment media such as music and movies, but, it is also the most common kind of piracy found in the software industry.

End-user piracy involves situations in which individuals make copies of software without authorization to install on multiple computers, take advantage of discounted upgrades without paying for the underlying legal version to be upgraded or acquire discounted educational licenses and use them for retail purposes.

Client-server misuse occurs when more users on a network are accessing the software than the license agreement permits, often called overuse. Sometimes end-user and client-server misuse occurs inadvertently, but often companies deliberately ignore their license agreements and overuse software in order to save money.

The final form of piracy is hard-disk loading, in which PC manufacturers or resellers deliberately load illegal copies of software on new computers to sell as an attractive bundle, thereby increasing their profit margins by not paying for legal licenses.

Using the detailed data provided through anti-piracy technology, compliance professionals, counsel and experts can accurately pinpoint illegal users to shut them down, as well as calculate and seek the recovery of revenue lost as a result of such piracy. Often illegal users, when confronted with precise metrics depicting each and every unauthorized access, agree to cease their illicit activity and negotiate appropriate licenses. Thus, pirates become legal users and loyal customers.

In instances in which users are unwilling to acknowledge the fact or extent of their misuse, counsel are able to use the data generated to seek injunctive relief to halt the piracy and ensure the owner's assets are protected. In such instances, litigation can be a highly effective tool to ensure the protection of critical IP, as well as to compensate software owners for the misuse that has occurred.

Remedies may include preliminary and permanent injunctive relief, actual or statutory damages and attorney fees and costs. Deterrence is also a critical goal that can be addressed via the use of data analytics to ensure that offenders do not repeat their prior piracy.

In addition to providing the evidence needed to prevail in a legal action, the data gathered can be analyzed and leveraged to protect company assets moving forward. Software can be better protected from future piracy by analyzing and understanding how the software is being pirated so that protective measures can be enhanced and fortified.

The analytics can also play a critical role in modifying future software deployments by allowing developers to gain insights into pirates' methods and devising countermeasures to combat such methods.

Conclusion

The Software Alliance, a leading advocate for the global software industry, estimates that the software industry loses nearly $46 billion in annual revenue due to piracy.[1] If usage trends continue this figure could increase by 30% or more by the year 2022. Piracy committed outside U.S. borders is increasing at an alarming rate, especially in the Asia-Pacific region and in China. However, based on the sheer size of the market, the U.S. is still the largest opportunity.

Fortunately, software companies can counteract the growing threat of piracy with a combination of innovation in analytics and technology and established IP legal protections. But in the current environment, it is crucial they do not delay — they should take action now to remain competitive and protect their valuable assets.

Denise Mingrone is a partner at Orrick Herrington & Sutcliffe LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] 2018 BSA Global Software Survey, conducted in partnership with IDC, June 2018.