Hedge Fund Law Report
An Acuris company

Lowenstein Sandler

February 21, 2019

TECHNOLOGY

What Is Open-Source Software, and How Are Fund Managers Using It? (Part One of Three)

By Shaw Horton, *Hedge Fund Law Report*

Open-source software (OSS) is characterized by licensing arrangements wherein copyright holders grant licensees the ability to freely change and distribute that software. Pursuant to those licenses, however, licensees must meet certain requirements or follow certain restrictions. These obligations may be minimal, as is the case with permissive licenses, or onerous, as is the case with so-called "copyleft" licenses. OSS exists for virtually any application, including artificial intelligence, database management and system security. Its ubiquity means that fund managers can leverage OSS for all segments of their businesses.

This article, the first in a three-part series, discusses the basics of OSS, actions governments are taking to support it, relevant regulatory guidance and ways OSS is being used by fund managers. The second article will analyze the benefits of OSS, as well as the disadvantages and risks that it presents. The third article will evaluate actions fund managers can take to mitigate OSS risks, including policies, procedures and controls to adopt; ways to deal with third-party vendors; and due diligence.

See our three-part series on big data: "Its Acquisition and Proper Use" (Jan. 11, 2018); "MNPI, Web Scraping and Data Quality" (Jan. 18, 2018); and "Privacy Concerns, Third Parties and Drones" (Jan. 25, 2018).

What Is Open-Source Software?

OSS is defined by five major elements, explained Matt Savare and Bryan Sterba, partner and associate, respectively, at Lowenstein Sandler and members of its technology practice group. They are:

1. free redistribution;
2. source code availability and the integrity of that code;
3. allowance of derived works;
4. non-discrimination against persons, groups or fields of endeavor; and
5. the distribution of a technology-neutral license that is neither specific to a product nor restrictive of other software.

Open-source licenses come in two general forms: permissive and copyleft. "You usually do not have a choice between licensing software under a permissive license or copyleft license," said Ropes & Gray counsel Michael D. Kurzer, who represents clients on, among other things, intellectual property, data privacy and OSS matters. "The owner who makes the code available is the one who selects the license

for its application or library. There are a few examples of dual-licensing models – that is, where the owner of the code gives the licensee an option between the two – but that is much less common."

Permissive Licenses

Permissive licenses, such as the MIT License, the 2- and 3-Clause BSD Licenses and the Apache License, contain minimal requirements and restrictions. "For example, the MIT License simply requires licensees to include the copyright and permission notice," noted Savare. "The Apache License places limits on the use of trademarks and requires licensees to prominently disclose that they have modified files."

Kurzer added that it is fairly simple to comply with the obligations under permissive licenses. "In most cases, the requirement is just to include a copyright notice and a standard warranty and liability disclaimer. For instance, if the OSS copyright is held by Oracle, you would have to reflect that."

Copyleft Licenses

On the other hand, copyleft licenses, such as the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL), require licensees to distribute derivative works under the same license and release complete source code when making such distributions. The LGPL mainly applies to libraries. "Static linking refers to situations where the licensee uses the library to build its program. In those cases, the program is a derivative work of the library and must be redistributed under the LGPL," said Sterba. "Dynamic linking, on the other hand, refers to situations where the licensee builds its program independently and only uses the library to help run or execute the program. There, the licensee may distribute the work under different terms without the LGPL license applying to the derived work."

According to Sterba, because under the GPL mere interaction with a user through a computer network, with no transfer of a copy, is not viewed by the open-source community as a conveyance, many organizations use copyleft materials through a software-as-a-service (SaaS) model, so the GPL licensed code sits "behind the wall." Thus, organizations avoid subjecting their source code to copyleft requirements.

In response, however, GNU released the Affero General Public License (AGPL), which attempts to close the loophole by requiring licensees to "prominently offer all users interacting with [the program] remotely through a computer network . . . an opportunity to receive the [c]orresponding [s]ource" code. Code incorporated into a SaaS offering would still be subject to copyleft issues.

See "What Fund Managers Should Consider When Negotiating SaaS Agreements" (Dec. 20, 2018).

"A fair amount of OSS is licensed under one of the various GPL licenses," observed Kurzer. "I would say that the typical incidence of OSS being offered under one of the GPL licenses is likely 10-15 percent, maybe more. For most commercial applications, it may be best to avoid incorporating GPL into proprietary code if you are planning to distribute copies of the resulting software."

Offering software under a SaaS model reduces the risks relating to the use of GPL, but not entirely, Kurzer added. "There are OSS

licenses, such as the AGPL and Reciprocal Public License, for which the copyleft obligations are triggered even when used in the cloud, although these licenses are less common."

See "How Hedge Fund Managers Can Protect Their Trade Secrets in Light of Recent NY Appellate Ruling" (Mar. 9, 2017); and our two-part series on how hedge funds can protect their brands and IP: "Trademarks and Copyrights" (Feb. 23, 2017); and "Trade Secrets and Patents" (Mar. 9, 2017).

Governmental Support of OSS

Both the U.S. federal and state governments are making a push to utilize OSS, including blockchain, to a greater degree. "The federal government, pursuant to Federal Acquisition Regulation Part 12, aims to use 'commercial items' whenever possible," said Savare. "Whenever it is technically advantageous, they try to move away from software and systems that are applicable for only governmental purposes."

Indeed, the U.S. Chief Information Officer (CIO) and CIO Council published a source-code policy that covers federal use of OSS. Under a pilot program, all agencies must release at least 20 percent of their "custom-developed code" each year, prioritizing code that is "potentially useful to the broader community." When doing so, the CIO recommended that agencies, among other things, engage with existing communities, utilize open development practices, adopt a regular release schedule and adequately document source code (*e.g.*, by including information on the status of software, license details and "relevant technical details on how to build, make, install, or use the software, including dependencies"). These recommendations can also be helpful for fund managers that wish to contribute upstream to open-source projects, a practice that can provide several organizational benefits.

In addition, the European Commission (EC) published an OSS strategy in which it stated that it would place a "special emphasis on procurement, contribution to [OSS] projects and providing more of the software developed within the Commission as open source."

In a subsequent study carried out for the EC, entitled "The Economic and Social Impact of Software & Services on Competitiveness and Innovation," the authors recommended that the EC "[s]upport [OSS] in all sectors of the economy," including through the "exchange of best practices between private and public organizations." The study assigned EC support of OSS as having a "medium" economic impact. The authors of the study argued that EC support would "lower[ ] the risk of a vendor lock-in"; support co-innovation by creating "standards that are very important for the development of emerging technologies and that help lower the total cost of ownership"; and enhance interoperability. The study hypothesized that E.U. institutional use of OSS would "provide relevant use cases, ensure long-term support, and secure high-level quality control."

Government Guidance on OSS

Nevertheless, "there is very little guidance from the government or regulators on OSS," said Kurzer. "OSS is third-party software,

however, and there is plenty of regulatory guidance on the use of third-party vendors with respect to compliance. You cannot outsource compliance, and if you don't properly vet and diligence vendors, you will have compliance issues."

For example:

- In a 2016 IM Guidance Update on business continuity planning for registered investment companies, the SEC's Division of Investment Management noted that because "fund complexes . . . outsource critical functions to third parties, . . . they should consider conducting thorough initial and ongoing due diligence of those third parties, including due diligence of their service providers' business continuity and disaster recovery plans."
- In the 2015 Cybersecurity Examination Initiative Risk Alert issued by the SEC's Office of Compliance Inspections and Examinations (OCIE), the staff noted that "[s]ome of the largest data breaches . . . may have resulted from the hacking of third party vendor platforms." Therefore, SEC examination staff "may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms." In addition, in OCIE's 2018 National Exam Program Examination Priorities, SEC staff indicated that they would prioritize vendor management with respect to cybersecurity protection.
- In a 2016 NFA Interpretive Notice, the NFA stated that members should "perform due diligence on a critical service provider's security practices and avoid using third parties whose security standards are not comparable to the [m]ember's standards in a particular area or activity." Additionally, the interpretive notice explains that members should "consider adopting procedures to place appropriate access controls to their information systems and data upon third-party service providers, and procedures to restrict or remove, on a timely basis, a third-party service provider's access to their information systems once the service provider is no longer providing services."
- In the Financial Conduct Authority (FCA)'s Handbook, SYSC 8.1, the FCA noted that all Undertakings for Collective Investment in Transferable Securities investment firms "must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions or of any relevant services and activities."

See "Fund Managers Must Supervise Third-Party Service Providers or Risk Regulatory Action" (Nov. 16, 2017); "How Fund Managers Can Develop an Effective Third-Party Management Program" (Sep. 21, 2017); and "Study Reveals Weaknesses in Asset Managers' Third-Party and Vendor Risk Management Programs" (Mar. 9, 2017).

Ways Fund Managers Use OSS

"Open source is present in almost every single software package at this point," said Savare. "I don't know of any industry that doesn't use OSS. It may be a small component of a larger piece of software, or it may

comprise the entire software itself."

For example, a manager may license a third party's trading platform. The trading platform itself may be proprietary, but it may include open-source elements, such as the application program interface or connectors to the back-end. "Many financial services companies, however, are using pure open-source packages," added Savare. "Some, for instance, use Linux as their operating systems."

"One reason you may see OSS more in the hedge fund context is because they are more leanly staffed, without large information technology departments and often with few in-house software developers. They don't want to reinvent the wheel, and readymade solutions are attractive," said Kurzer. "They also don't necessarily have teams of lawyers to look through all the licenses and code, and some may view OSS as easier to deal with because the licenses seem simpler than full form commercial agreements. Additionally, there is no negotiating – you take the software or leave it."

Open-source applications can be used for, among other things:

- artificial intelligence and machine learning (*e.g.*, TensorFlow and scikit-learn);
- accounting (*e.g.*, SQL-Ledger and GnuCash);
- speech synthesis and recognition;
- database management (*e.g.*, MySQL and PostgreSQL);
- data mining (*e.g.*, Orange and Weka);
- enterprise search (*e.g.*, Elasticsearch);
- remote access (*e.g.*, OpenVPN and Synergy);
- file management (*e.g.*, 7-Zip);
- office suites (*e.g.*, Apache OpenOffice and LibreOffice);
- encryption (*e.g.*, GNU Privacy Guard and OpenSSL); and
- firewalls (*e.g.*, iptables and Shorewall).

"Almost every new proprietary technology that is developed by the software community will – at a minimum – spawn a smaller open-source project that mirrors its functionality," said David St. John-Larkin, partner in Perkins Coie's intellectual property practice who regularly handles open source and proprietary software matters. "Some OSS is very mature – *i.e.*, the projects are regularly improved and have well-structured review boards that receive and issue revisions to the code. In particular, we see this where there is a lot to gain across many different industries, including the security, database technology and search functions."

"Blockchain is, by definition, open source, regardless of whether it is public or permission-based" said Savare. "More and more financial services companies are using blockchain within their own systems and processes, a phenomenon that is being aided by the fact that blockchain is an international protocol. It's a burgeoning industry, and I'm really bullish on it in the next five to ten years."

According to Savare, cross-border transfers of money are a particularly relevant use case, with financial services firms relying on Ripple. "It may take days or weeks for traditional international transactions to settle. Blockchain, however, facilitates this process in a fraction of the time," he noted.

In addition, entities are beginning to use blockchain in governance and voting matters, as well as with capitalization tables for

stock ownership. "The large banks are now members of consortia that are seeking to develop protocols and running beta trials on applications of the technology," Savare continued. Companies are also moving successful financial technology blockchain applications to other verticals. For example, NYIAX, developed in partnership with Nasdaq, uses a blockchain back-end for bid matching in advertising technology.

St. John-Larkin believes that the industry will also see more service-side development related to blockchain. "There are a lot of uses for blockchain outside of the virtual currency space. We are going to increasingly see open-source projects that integrate fundamental blockchain technologies not directly related to virtual currencies," he opined. "Database technology is an interesting area for this application. Blockchain proposes a solution for tracking transaction records that occur at a very high volume. Therefore, it may be very valuable in creating a history of someone's interaction with a database." This may have strong applications in the medical field, or in instances where consumer or client information is kept en masse and there is a need to audit search histories.

See "How Blockchain Will Continue to Revolutionize the Private Funds Sector in 2018" (Jan. 4, 2018); and our three-part series on blockchain and the private funds industry: "Basics of the Technology and How the Financial Sector Is Currently Employing It" (Jun. 1, 2017); "Potential Uses by Private Funds and Service Providers" (Jun. 8, 2017); and "Potential Impediments to Its Eventual Adoption" (Jun. 15, 2017).

Hedge Fund Law Report
An Acuris company

Lowenstein Sandler

February 28, 2019

TECHNOLOGY

What Are the Benefits and Risks of Using Open-Source Software? (Part Two of Three)

By Shaw Horton, *Hedge Fund Law Report*

Open-source software (OSS) can provide fund managers with several benefits, including cost savings, increased customization and access to a collaborative community that provides extensive support. In addition, participation in open-source communities can help managers attract talent and hone technical employees' skillsets.

Nevertheless, OSS does not come without risks. For example, under certain circumstances, a manager may need to release its own proprietary source code, or it could find itself subject to breach of contract or copyright infringement liability. OSS may also pose greater security risks than commercial software, which means that managers must carefully assess the areas in which they seek to utilize OSS.

This article, the second in a three-part series, analyzes the benefits of OSS, as well as the disadvantages and risks that it presents. The first article discussed the basics of OSS, actions governments are taking to support it, relevant regulatory guidance and ways OSS is being used by fund managers. The third article will evaluate actions fund managers can take to mitigate OSS risks, including what policies, procedures and controls to adopt; ways to deal with third-party vendors; and due diligence.

For a discussion of another growing technology, see our two-part series on implementing electronic signatures: Part One (Dec. 21, 2017); and Part Two (Jan. 4, 2018).

Benefits of OSS

Cost Savings

OSS is cheaper if used correctly, observed Matt Savare and Bryan Sterba, partner and associate, respectively, at Lowenstein Sandler and members of its technology practice group. "Like anything else, however, if you implement it incorrectly, you can fail miserably. This means looking at the entire lifecycle of the product," said Sterba.

Thus, managers must evaluate not only the licensing costs, but costs associated with customizing the software to their particular needs, as well as integration, maintenance, upgrade and support costs.

Customization and Development

Open-source applications also enable greater diversity, variety and customization. "Think of the Linux operating system. IBM has made that available as OSS, so numerous developers are building on it as a community," remarked Savare. "This can lead to continuous

improvements, and it means that the product exists past the lifespan of the original company or developer. Windows, on the other hand, can only be modified by Microsoft or one of its vendors."

Indeed, in *Jacobsen v. Katzer* (discussed below), the U.S. Court of Appeals for the Federal Circuit (Federal Circuit) noted that, through OSS collaboration, "software programs can often be written and debugged faster and at lower costs than if the copyright holder were required to do all of the work independently."

"OSS is available 24/7 and is free. As long as you are reasonably mindful of the fact that you have to do your own work vetting the software, the OSS community is collaborative and can offer wonderful crowd-sourced development work," said Ropes & Gray counsel Michael D. Kurzer.

According to IRS guidance on the use of federal tax information in OSS, "it is important to understand the organization residing behind or supporting the continued development of the application under consideration. Depending on the application and the organization that stands behind it, there may be a tremendous amount of support for evaluating the software."

For more on tax issues affecting private fund managers, see "New Tax Law Carries Implications for Private Funds" (Feb. 1, 2018); and "The Effect of 2017 Tax Developments on Advisers to Private Funds: New Partnership Audit Rules, Tax Reform, Blockers, Discounted Gifting, Fee Waivers and State Nexus Issues" (Nov. 30, 2017).

Greater Security

"When thinking about security software in particular, you want a product that has been well-tested and well-vetted," commented Perkins Coie partner David St. John-Larkin. "That's exactly what you get with OSS. There is significant opportunity for people to test and debug the software across the world."

Talent Acquisition

Participating in open-source communities may also help managers attract the best talent. "Younger generations are more willing to work with open source than their predecessors," said Sterba.

"I don't know whether OSS is necessarily being used to recruit talent. Rather, I think that managers decide to use OSS because they understand that it can allow them to, among other things, scale faster and develop a competitive advantage," Sterba continued. Attracting younger developers, therefore, comes as an ancillary benefit, as managers can draw from a larger pool of candidates and demonstrate that they are using products with which developers are familiar.

"A lot of organizations find benefit – both in terms of supporting projects important to them and creating an outlet for engineers or developers to stay at the forefront of technological developments – in contributing upstream to open-source projects, rather than being raw consumers," remarked St. John-Larkin. "Some of the most prolific and important projects may offer a way to train and keep the skillset alive for their technical staff." St. John-Larkin added that upstream contributions can be difficult to trace back

to organizations due to individual engineers contributing under their own names or under the guise of a subsidiary company.

"It can be risky adopting certain OSS with no assurance the software will have the same longevity as the project or product on which you're working," noted St. John-Larkin. "Organizations that encourage their engineers to participate in the OSS community may help mitigate this risk by ensuring there are sufficient resources and interest behind projects of interest to the organization."

See "A Succession-Planning Roadmap for Fund Managers (Part Three of Three)" (Jun. 21, 2018); "Ways Fund Managers Can Compensate and Incentivize Partners and Top Performers" (Dec. 14, 2017); and "How Hedge Fund Managers Can Structure Deferred Compensation Plans to Retain Top Talent (Part One of Two)" (Jun. 22, 2017).

Disadvantages and Risks of OSS

License Restrictions

If a manager incorporates OSS into its own proprietary software, it may have a duty to release – or make open – that proprietary source code, cautioned Sterba. The issue only arises, however, under copyleft or viral licensing agreements and generally only in cases where an entity publicly distributes (*i.e.*, sells or licenses) the OSS.

"In general, the obligations under OSS licenses are only triggered upon a distribution of the software," remarked Kurzer. "For many OSS licenses, if you don't provide a copy of your software incorporating the OSS to someone else, then there has been no distribution and the licensee has no obligations." This is not the case for the Affero General Public License, Reciprocal Public License or similar licenses, which are triggered even without a distribution.

Distribution can include making a copy, making software accessible at a link, or sending the software out to third parties in any way (for example, by placing the code into a mobile phone app that can be downloaded). Copyleft licenses, like the GNU General Public License (GPL), impose the most onerous obligations on licensees who have incorporated that OSS into their proprietary code. "When you distribute your software, the GPL, GPLv2, and GPLv3 licenses include a requirement to share your source code and license it to the public under the same GPL license," stated Kurzer.

If a licensee refuses to comply with those obligations, then it no longer has a license and can be sued either under breach of contract or for copyright infringement. "The same is true if you do not, for example, include copyright attribution or a disclaimer under a permissive license. Permissive licenses are very easy to comply with, however, so you generally do not hear of those kinds of issues," noted Kurzer. "Managers must realize that OSS licenses are still legal agreements and that OSS is owned by someone – it is not public-domain software. Managers must comply with the licenses."

Hedge funds themselves are not generally distributing software incorporating OSS. "I haven't seen it, but that doesn't mean it doesn't happen," said Savare. "I've yet to have a hedge fund come back to me and say that it is using OSS to roll out its own product for distribution. Instead, fund managers typically use the software for internal purposes."

Therefore, whether the entire package, or just a component of the package, is open-source, managers typically will not run into this issue because they are not using OSS in a manner that would trigger some of these problematic provisions in the licenses. Even so, it is important for managers to understand this issue given the enormous risk associated with having to make proprietary code open-source.

When a manager licenses proprietary software, vendors will typically include restrictions on, among other things, reproduction, reverse-engineering and modification. There are limited circumstances under which licensors may allow modifications, such as the creation of front-end interfaces, for example, where the licensor does not provide any kind of developmental services, enhancements or other professional services. Nevertheless, according to Sterba, this is normally restricted given that vendors are eager to acquire additional work. "Not only will the vendor charge a fee for creating these components, but it will also often tell the licensee that the vendor owns any enhancements, even where those enhancements are specific to a particular client."

"In rare instances where the vendor does permit a hedge fund to modify the software – for example, where the hedge fund has a very specific or unique use – there will generally be further restrictions on the modifications," noted Savare. "The licensor will not want the licensee to disclose or sell those modifications."

Breach of Contract and Copyright Infringement

"Noncompliance with OSS license terms – whether copyleft or permissive – may lead to infringement of an OSS licensor's intellectual property rights," added Sterba.

In *Jacobsen v. Katzer*, appellant Jacobsen made certain computer code publicly available without a fee pursuant to an open-source license. Appellee Katzer allegedly incorporated some of the code into one of his software packages without following the terms of the license. Jacobsen sought a preliminary injunction.

According to the Federal Circuit, copyright owners who grant a "nonexclusive license to use . . . copyright material[s] waive[their] right to sue . . . licensee[s] for copyright infringement." On the other hand, if a license is "limited in scope and the licensee acts outside the scope, the licensor can bring an action for copyright infringement." The Federal Circuit found that the terms of the open-source license were conditions of, and not merely covenants to, the copyright license given that users who download the "copyright materials [are] authorized to make modifications and to distribute the materials 'provided that' [they] follow[ ] the restrictive terms of the [license]," including the inclusion of the copyright notice.

In the remanded case, the U.S. District Court for the Northern District of California (Northern District) ultimately held that the state law claim was preempted by the Copyright Act because the "breach of contract claim alleges violations of the exact same exclusive federal rights protected by Section 106 of the Copyright Act, the exclusive right to reproduce, distribute and make derivative copies." To avoid preemption, state law claims must have an "extra element" that changes the nature of the claim.

Later, in an April 25, 2017, order in *Artifex v. Hancom*, the Northern District denied

the defendant's motion to dismiss on the basis that the plaintiff's breach of contract claim was preempted by copyright law. Plaintiff Artifex developed Ghostscript, a PDF interpreter, and dually licensed it under the GPL and a commercial license. Defendant Hancom, a South Korean company, integrated Ghostscript's code into its own proprietary products and failed to purchase a commercial license or comply with the terms of the GPL (*i.e.*, it did not release the source code to its proprietary product). The court argued that the defendant failed to sufficiently explain why the "GPL's open-source requirement is not the required extra element."

The court also denied the defendant's motion to dismiss on the basis that the plaintiff failed to allege that the defendant committed a predicate act in the U.S. Hancom argued that "because it is a South Korean company the [c]ourt must draw the inference that all the predicate acts – the copying, integrating and incorporating of [p]laintiff's software – occurred in South Korea." The court, however, argued that "[t]here are no facts alleged . . . that would prohibit the inference that at least some infringement occurred in the [U.S.]"

In a subsequent order denying Hancom's motions for summary judgement, the court held that while it cannot "impose the terms of the commercial license" on the defendant, a jury can "use the value of the commercial license as a basis for any damages determination." The court also held that, under California law, plaintiffs may seek unjust enrichment or disgorgement as a measure of damages for free licenses. The court cited *Jacobsen*, noting that the "lack of money changing hands in open-source licensing [does not preclude] economic consideration." The *Jacobsen* court noted that there are "substantial benefits" that "range far beyond traditional license royalties," including generating market share by providing components free of charge and increasing international reputation.

The court also rejected the defendant's argument that the license terminated when Hancom "first released a product containing Ghostscript without complying with the open-source requirements." The court argued that "because the source code or offer of the source code is required each time a 'covered work' is conveyed, each time Defendant distributed a product using Ghostscript there was arguably an ensuing obligation to provide or offer to provide the source code." Moreover, Section 8 of the GPL provides, as long as certain conditions have been met, for "reinstatement of the license until notice of termination by the copyright holder."

Savare noted that the cases demonstrate the need for robust OSS compliance, along with customary regulatory compliance. "Open-source errors can lead to lawsuits, but it can also undermine the value of a manager's business," he explained. Fortunately, according to St. John-Larkin, "a cottage industry has developed, which helps organizations evaluate the source code and resolve copyright infringement or alleged copyright infringement."

Security Risk

In addition, OSS can lead to practical security risks. Heartbleed, an OpenSSL security bug, was a particularly infamous example of an open-source weakness. The bug was introduced into the software in 2012 and only publicly disclosed and patched in 2014.

According to heartbleed.com:

> This weakness allows [hackers to steal] information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. . . . The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

See "ACA Compliance Group Clarifies Misconceptions Commonly Held by Fund Managers With Respect to Cybersecurity" (Apr. 16, 2015).

"The security risk is greater with OSS because, by its very nature, the entire world can see and know some of the code you have in your software. Hackers do not have the same level of access to most commercially licensed software code," said Kurzer.

There are ways this risk can be mitigated before using OSS, Kurzer advised. Specifically, fund managers should look at whether there are known vulnerabilities that have already been exploited or shared on the internet and implement policies and procedures designating an individual to not only monitor for security issues, but to think through how the code will be used. "Will the code be used in a vulnerable area? You may not necessarily want to use it next to the crown jewels, but you may not be as concerned with less sensitive areas of your business," he said.

The IRS, in its guidance on the use of federal tax information in OSS, noted additional security risks associated with the use of OSS, including that it may be difficult to ascertain whether the developers of open-source code follow security best practices or a "mature development methodology," or have sufficient "security programming skills and vulnerability testing expertise." Moreover, OSS developers "may be slow to respond to identified flaws," and OSS may not always integrate robust encryption modules.

See our three-part series on how fund managers should structure their cybersecurity programs: "Background and Best Practices" (Mar. 22, 2018); "CISO Hiring, Governance Structures and the Role of the CCO" (Apr. 5, 2018); and "Stakeholder Communication, Outsourcing, Co-Sourcing and Managing Third Parties" (Apr. 12, 2018).

Other Issues

Additionally, the IRS explained that OSS may not receive the same level of support as proprietary software because it "may not be backed by a vendor." Furthermore, it may be more difficult to train staff on the implementation and maintenance of OSS.

"Blindly adopting open source is a recipe for disaster. At some point, there will be legal conflicts, technical conflicts or both," said St. John-Larkin. Most large entities now have compliance officers who are tasked with collecting all the license information and version information, and with being the custodians. "Managers must take care to memorialize, in some form within the company, what OSS is being used, where it is being used and what version is being used," he added.

"It is also possible that someone could write OSS code that implicates privacy issues, but that typically hasn't been an issue that we've encountered," continued Kurzer. "Anyone who uses OSS has to realize that this doesn't absolve them of their own obligations to comply with privacy laws and data security laws."

See "How Fund Managers Can Navigate the E.U. General Data Protection Regulation and the Cayman Islands Data Protection Law" (Aug. 9, 2018); and "How the GDPR Will Affect Private Funds' Use of Alternative Data" (Jun. 14, 2018).

Hedge Fund Law Report
An Acuris company

Lowenstein Sandler

March 7, 2019

TECHNOLOGY

How Fund Managers Can Mitigate the Risks of Open-Source Software (Part Three of Three)

By Shaw Horton, *Hedge Fund Law Report*

Although open-source software (OSS) poses a number of risks, fund managers can take several steps to mitigate those risks. Managers should, for example, develop robust policies, procedures and controls regarding, among other things, the download and use of OSS, which may include the use of a committee to sign off on the introduction of new software. Additionally, managers should ensure they receive certain representations and warranties when dealing with software developers who integrate OSS into proprietary products. Finally, managers must conduct appropriate due diligence not only of OSS vendors, but of the software itself.

This article, the third in a three-part series, evaluates actions fund managers can take to mitigate OSS risks, including policies, procedures and controls to adopt; ways to deal with third-party vendors; and due diligence. The first article discussed the basics of OSS, actions governments are taking to support it, relevant regulatory guidance and ways OSS is being used by fund managers. The second article analyzed the benefits of OSS, as well as the disadvantages and risks that it presents.

For more on developing policies and procedures, see "A Checklist for Evaluating Employee Disciplinary Policies and Procedures of Private Fund Managers" (Mar. 22, 2018); and "Will Inadequate Policies and Procedures Be the Next Major Focus for SEC Enforcement Actions?" (Nov. 30, 2017).

Policies, Procedures and Controls

"Sometimes traders may get too eager and download software from the internet without reviewing all the terms and conditions," opined Bryan Sterba, associate in Lowenstein Sandler's technology practice group. "This software is free or cheap, and it is easily downloadable. This can come back to bite people because they don't know what they are signing up for. They don't realize that they are agreeing to a binding contract."

"In these cases, we may talk to the vendor and tell them that they are better off letting the manager out of the contract for a fee," explained Matt Savare, Lowenstein Sandler partner and member of its technology practice group. "Nevertheless, managers should have strict protocols in place to avoid these situations in the first place."

Unfortunately, many managers lack stringent practices surrounding the above scenario. "Everything should go through procurement or the legal department," Savare continued. "You

must have a lawyer who understands software licensing look at it – even those click-through agreements that may seem innocuous – or else there could be problems."

Managers should implement strict protocols even where no licensing fee exists, cautioned Savare. "Software can still have costs in, among other things, bugs, malware and poor interoperation. Thus, technical protocols should also be strict, with scans for viruses and malware."

OSS policies should also address developers' participation in OSS communities or development, noted Sterba. "These policies must be approached very carefully, however, given that developers may hesitate to join managers that have policies that appear overly hostile toward OSS."

"The decision to use OSS is sometimes made by the engineers out of habit," said Ropes & Gray counsel Michael D. Kurzer. "If there's no structure in place, then they utilize this software to make their job easier. There's often no interaction with lawyers before it used." Kurzer noted, however, that he does speak directly with companies and individuals who are seeking to start a company or fund about the risks that OSS presents. "Nevertheless, among all of the things that start-ups have to worry about – including limited resources and running out of money – this seems pretty low on the list."

"It is difficult to find an organization that isn't already using OSS in some capacity. Those that do must get on top of it as quickly as possible and adopt comprehensive policies," Kurzer continued. Managers must create an approval process within the organization, he added, which may include the designation of an individual or committee that signs off on the introduction of new software.

In addition, managers should delineate how new code is reviewed and vetted, and create specific stop signs, restricting the use of certain code entirely, for example in the form of a blacklist. "Managers may also want to mitigate risk by conducting a report on their existing code to get a firm grasp of where they already stand," Kurzer advised. "A manager may also choose to create a policy restricting the use of OSS altogether, but that is rare."

"What you want to avoid is a procedure that requires everything to grind to a halt, for example by requiring a lawyer to be involved in every step. That gets very expensive, and firms do not typically have the resources for that," explained Kurzer. "I advocate for a risk-based approach – a manager should assess its areas of greatest concern and elevate resources accordingly. If we're talking about the crown jewels, then that's something that may require a high level of approval." On the other hand, low-risk areas should garner lower resource allocations. Kurzer noted that the same approach should apply to compliance with licenses or other regulatory issues. "The bottom line is that there is no 'one-size-fits-all' approach."

See "Key Elements of Electronic Communications Policies and Procedures for Hedge Fund Managers" (Nov. 12, 2010).

Representations and Warranties: Dealing With OSS in Proprietary Products

"Companies should set clear expectations about whether third-party developers may integrate OSS into proprietary products," suggested David St. John-Larkin, partner in Perkins Coie's intellectual property practice. "If a company permits OSS integration, the company should ask developers to clearly identify what OSS is used. Part of that conversation will center on the representations and warranties that the company will need." This conversation may govern whether a company utilizes OSS.

When licensing software, a manager should seek third-party representations, warranties and indemnities. "In a lot of contexts, however, software vendors will seek to provide software without a warranty or that is subject to the terms and conditions of other parties," said Sterba. "This can apply to any thirty-party plugin, and I always resist this. When I receive the contract, I ask them, 'How am I supposed to know what those terms and conditions are? I don't have a deal with them; I have a deal with you.'"

Instead, Sterba said he tells vendors that they must stand by their software and warrant any third-party components the same as they do their own. "This does not always work, however," opined Savare. "I've had clients who have walked away from using certain software because the other side was unreasonable in relation to third-party software. It doesn't happen often, but it is possible that OSS and third-party issues can blow up a deal."

A licensee-friendly provision with a proprietary software vendor may, for example, include the following language, said Savare:

> Schedule [A] lists all Open Source Materials used by [Vendor] in any way and the applicable license for each item, and describes the manner in which such Open Source Materials were used (such description shall include whether (and, if so, how) the Open Source Materials were modified and/or distributed by [Vendor]). [Vendor] is in compliance with the terms and conditions of all licenses for the Open Source Materials. Other than as specified on [Schedule to agreement,] [Vendor] has not (i) incorporated Open Source Materials into, or combined Open Source Materials with, any [Vendor] owned intellectual property or products; (ii) distributed Open Source Materials in conjunction with any [Vendor] owned intellectual property or products; or (iii) used Open Source Materials, in such a way that require, as a condition of use, modification and/or distribution of such Open Source Materials that other software incorporated into, derived from or distributed with such Open Source Materials be (A) disclosed or distributed in source code form; (B) be licensed for the purpose of making derivative works; or (C) be redistributable at no charge.
>
> "Open Source Materials" means software or other material that is distributed as "free software," "open-source software" or under a similar licensing or distribution terms (including, but not limited to, the GPL, LGPL, Apache License and MIT License).

All managers should also receive a representation that any software does not

include viruses and that the software does not infringe a third party's intellectual property, said Savare. "Getting hit with a demand letter can be a nightmare." For instance, Savare typically includes the following representation in licensing agreements:

> [Vendor] has and shall take all reasonable steps to test all software and work product for Disabling Devices (as defined below). [Vendor] shall not install into any computer, or include in any of the services, software, or work product, any software or computer code that (i) is designed to disrupt, disable, harm, or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation thereof, or any other associated software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"); (ii) would disable or impair in any way the operation thereof based on the elapsing of a period of time, the exceeding of an authorized number of users or copies, or the advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices); (iii) except as expressly approved in advance and in writing by customer, is typically designated as "open-source software" and/or distributed under any license approved by the Open Source Initiative as set forth in www.opensource.org or similar licensing or distribution terms; or (iv) would permit access by vendor or any third party to cause such disablement or impairment (sometimes referred to as "traps," "access codes," or "trap door" devices), or any other similar harmful, malicious, or hidden procedures, routines, or mechanisms that would cause the services, software, or work product to malfunction or to damage or corrupt data, storage media, programs, equipment, or communications, or otherwise interfere with operations (all of the above collectively Disabling Devices). [Vendor] shall remove any such Disabling Devices, and make any corrections necessary to fix any problems directly caused by any such Disabling Devices, at no additional cost to customer.

"I often ask for approval rights over open source," said Sterba. "If they aren't willing to give that, I include language requiring the licensor to represent and warrant that any licensed materials don't contain any open-source code obligating the licensee to make code available to others or otherwise subject the licensee to obligations not expressly set forth in the agreement."

Due Diligence of OSS Vendors

"Some software products are dual-licensed," said St. John-Larkin. "That is, a vendor may offer – for substantially the same software – either a free license on an as-is basis with no representations or warranties, or a commercial license where the vendor stands behind certain representations and warranties."

Regardless, "due diligence of OSS vendors is necessary," observed Savare. "No one should license an open-source program that he or she has never heard of. Similarly, a manager should not license an open-source program until it has conducted a deep dive into the code."

In many ways, licensing OSS is no different than licensing proprietary code – after all, a developer can place bugs into either.

Therefore, when using any third-party code, Savare recommended that managers understand who the licensor is; properly scan the code; and – before deploying the code in a live environment – reasonably ascertain that no malware, viruses, trapdoors or backdoors exist. This means examining the code in a test environment before installing it onto a production environment, he continued.

"The biggest risk for hedge funds, which are governed by the Gramm-Leach-Bliley Act and Regulation S-P, is preserving privacy and data security. These regulations require managers to implement commercially reasonable physical administrative and technical safeguards for nonpublic financial or personal information," continued Savare.

Thus, when licensing OSS – whether that software is physically installed on a manager's hardware or used as a service on the cloud – it is critical that a manager investigate whether the vendor conducts background checks on its employees, whether there is oversight over who has access to data and whether the vendor scans software before installation. "It is really easy to infect a network," opined Sterba. "Vendors can plant security holes and gain access to highly sensitive data." In addition, managers should ask about a vendor's data protection policies; ask for references; and interview its chief technology and chief privacy officers. These policies are particularly important because many security testing tools do not detect open-source security vulnerabilities, remarked Savare.

The IRS recommended that federal agencies wishing to utilize OSS pursue a "conservative approach" – that is, "seek organizations that . . . provide assurance[s] that a secure development lifecycle is employed and that software support for the application . . . is available. This may include the use of a third-party vendor that specializes in supporting this application but is separate from the primary development organization." Managers that intend to pursue the adoption or further integration of OSS more cautiously may also wish to follow that approach.

See "Current Trends in Operational Due Diligence and Background Checks" (Nov. 3, 2016). See also our two-part series "Key Considerations for Hedge Fund Managers in Evaluating the Use of Cloud Computing Solutions": Part One (Oct. 18, 2012); and Part Two (Oct. 25, 2012).

Although larger entities and quantitative fund managers will have chief technology officers and a host of other technology personnel involved in the process, smaller managers will likely have to engage third-party consultants to assist in evaluating vendors. Very few fund managers have large information technology staffs and instead only have one or two experts in-house.

"Open source is in almost everything, and it can be easily addressed, including through scans from vendors like Black Duck," Sterba said. "It's rare for managers to ask law firms for technical advice, but they do ask if we've dealt with certain vendors before – either for software or for professional services. Chances are that we have and we'll know about not just their quality, but the terms that they would accept."

See our three-part series on quantitative investing: "Dispelling Myths and Misconceptions" (Aug. 9, 2018); "Regulatory Action, Guidance and Risk" (Aug. 23, 2018); and "Special Risks and Considerations" (Sep. 6, 2018).

Due Diligence of OSS

How can an organization evaluate the quality of OSS itself? Kurzer recommended that managers look at, among other things:

- message boards or other public forums to see whether others have pointed out issues;
- release logs;
- the number of commits;
- the number of bugs fixed per version, as well as the amount and severity of open bugs per version;
- the vitality of the community; and
- the frequency of updates.

"In addition, companies have normal check-in processes when installing code to the code base, so they should be doing this on open-source code like they would do with any new code," added Kurzer. "There is no easy way to tell if code infringes on some other third-party software. So, the engineers have to be honest about where the code is taken from and consider the risks."

Ultimately, some of the process is simply intuition- or judgement-based, Kurzer opined. "People who create software will have a sense for whether the code looks well-written or poorly written. If it's poorly written, it may contain more vulnerabilities or bugs, and it may require additional work. As a result, it is more of a technical diligence than legal diligence."

"Unfortunately, I don't think smaller funds are engaging in much of this diligence at all. When they start to develop their own proprietary platforms, they may lean heavily on open-source code," noted Kurzer. "Issues arise, not when they use the software internally, but when they try to commercialize that software, *i.e.*, by offering it to third parties to gain an extra stream of revenue."

See "The Importance of Exercising Due Diligence When Hiring Auditors and Other Vendors" (Jun. 21, 2018); and "Perspectives on Operational Due Diligence From an Investor, Consultant and Manager" (Nov. 9, 2017).

Portfolio Companies

"Issues also arise when private equity firms buy or sell portfolio companies. That is a typical scenario when a company finds out about all of its open-source problems," said Kurzer.

"A private equity firm may buy a three- or four-year-old company with a proprietary software platform," Kurzer explained. "One of the reasons that company was able to grow so quickly was because it relied so heavily on open-source code to build the platform. It may not have complied with many of the licenses, however."

Kurzer recommended that firms conduct a scan and figure out the risks piece by piece. "We may advise that the firm see whether the problematic open-source code can be replaced and how many distributions have been made. It can then figure out what can be done to remediate past distributions."

For more on private equity funds, see "Anatomy of a Private Equity Fund Startup" (Jun. 22, 2017); "Private Equity in 2017: How to Seize Upon Rising Opportunity While Minimizing Compliance and Market Risk" (Jun. 8, 2017); and "SEC Enforcement Director Highlights Increased Focus on Undisclosed Private Equity Fees and Expenses" (May 19, 2016).