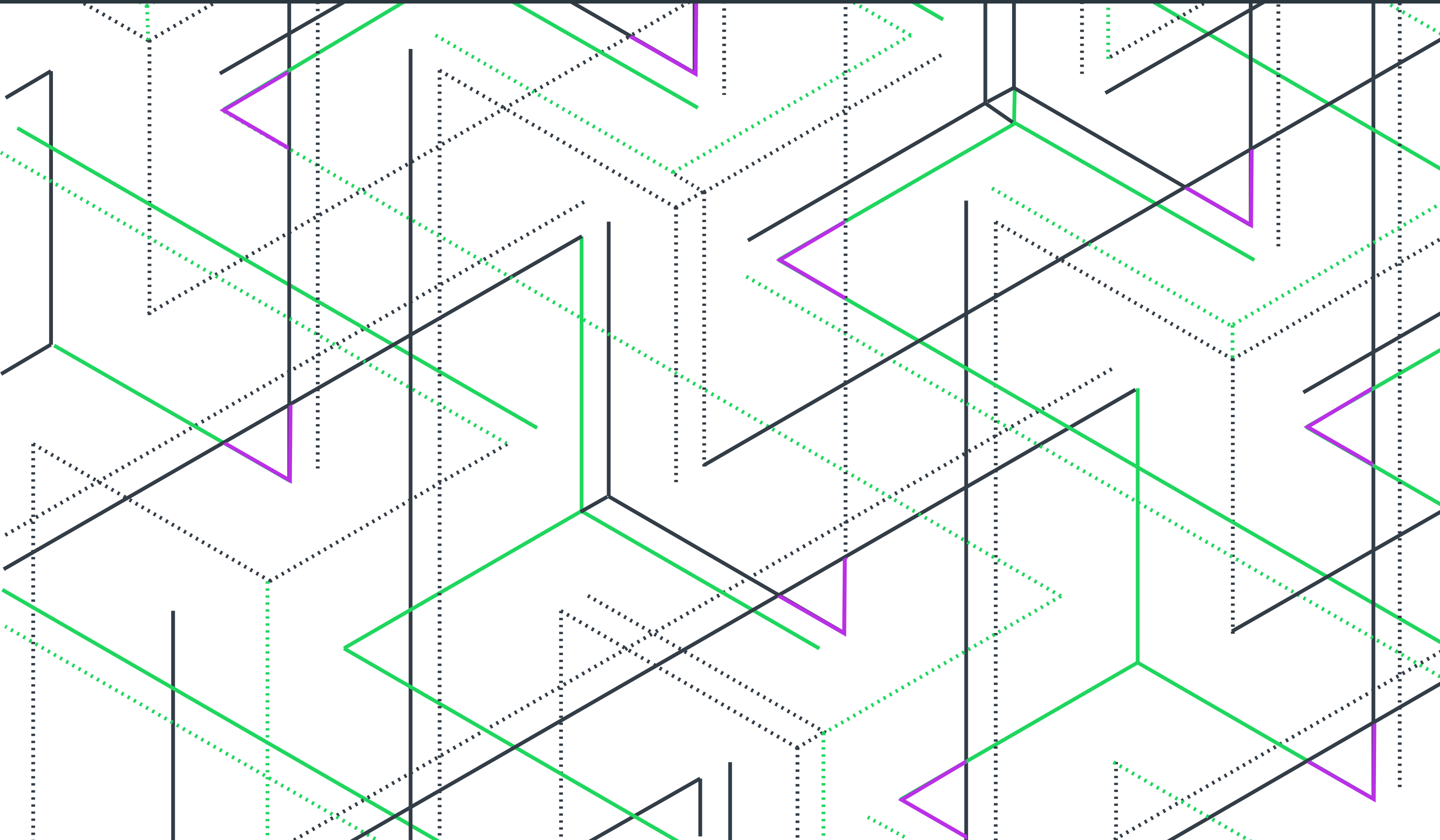
INDUSTRY REPORT

Open Source Risk

Fact or Fiction?



Open Source Risk

Many of today's hottest new enterprise technologies are centered around open-source technology. In the past 10 years, the impact of open source on how software is developed is enormous. The industry used to be one where almost every line of code was home grown. Today over half of a software product is open source—developed outside the organization.

The Big Process Gap

Open source software (OSS) has allowed organizations to become very nimble. But software developers should also take their processes to the next level and think about how they manage security and licensing risks.

No Process
No Protection

Most software engineers don't track open source use; Most software executives and devOps teams don't realize there's a gap and a security/compliance risk.

The Result

No remediation action and no protection for your clients and reputation.

Software suppliers (traditional software companies as well as IoT companies that are moving to software) often find themselves out of compliance with their open source licensing obligations. Suppliers miss or ignore known vulnerabilities because they're not tracking them or managing dependencies. The impact of not managing third party components creates security problems and legal issues that can put suppliers' business models at risk.

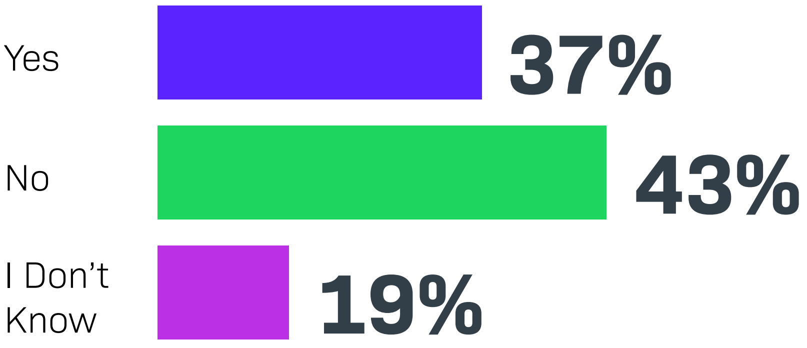
Is this exposure fact or fiction?

Revenera surveyed more than 400 commercial software suppliers and in-house software development teams within enterprises about their open source practices. For the first time, Revenera shines a light on open source security and compliance practices and their impact in a series of reports.

Are You OSS Savvy?

Revenera asked respondents about their open source acquisition and usage policy, and the responses were alarming. Only 37% said their companies had open source acquisition or usage policies in place. 43% said they did not. And 19% did not know.

Does Your Company Have a Formal Open Source Software (OSS) Acquistion and Usage Policy?



Answered: 437, Skipped: 1

Why Does This Matter?

Remember Heartbleed?

When Heartbleed hit, did you know how many components you needed to remediate in your code? Failing to keep track of open source components could result in embedding within the entire software supply chain a critical vulnerability that hackers can exploit.

Think GPL

For a legal document, the General Public License is surprisingly easy to read and understand—*if code licensed under GPL is included in your commercial product, your obligation includes open sourcing your entire product.*

Bottom line

Reducing open source risk can only happen if software suppliers have policies in place and enforce them. They have to communicate these policies to all the development teams that are writing code and incorporating open source components into that code.

Who Owns the Problem? Depends on Who You Ask!

Not surprisingly, based on the response to the first question, we found there is no industry-wide standard as to who owns open source security and compliance. We asked software suppliers about the specifics of their open source acquisition and use policies.

We have an Open Source Review Board (OSRB) that governs our Open Source Software and intellectual property compliance	**12%**
Our legal councel is responsible for Open Source Software and intellectual property compliance	**12%**
Our engineering team is responsible for Open Source Software and intellectual property compliance	**28%**
Another team is responsible for Open Source Software and intellectual property compliance	**9%**
No one within our company is responsible for Open Source Software and intellectual property compliance	**18%**
I don't know	**21%**

Only 28 percent of respondents said that the engineering team is responsible for OSS. Other respondents said this job fell to an open source review board (12 percent), legal counsel (12 percent) or some "other" team (9 percent).

Alarmingly, 39 percent of respondents said that either no one within their company is responsible for open source compliance—or they do not know who is.

Why Does This Matter?

There's a wide disconnect within the industry as to "who's in charge" when it comes to open source security and compliance. Most C-level executives and general counsel are unaware of the open source components in use and their impact on the company.

Open Source Review Board

In many companies, a small team of subject-matter experts across many disciplines comes together to form an Open Source Review Board (OSRB). This team often includes Engineering, Legal, IT, DevOps, Security Experts and Management sponsors. The OSRB will help set policies and responds to license compliance and security events. They also provide open source training and education to the rest of the company. The group can be ad hoc or more tightly structured, depending on a company's maturity and size.

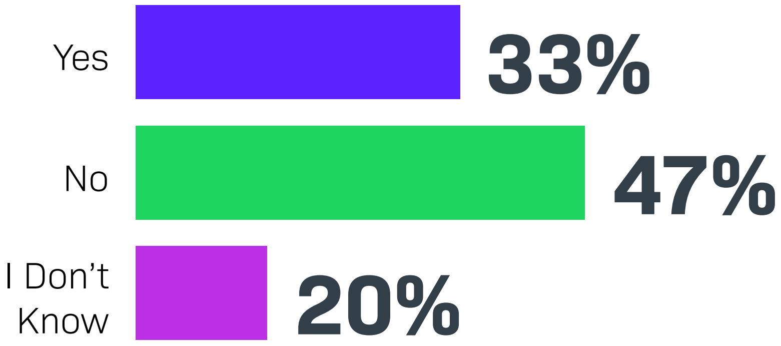
Crowd Sourcing Risk

Widespread contributions to open source projects mean more valuable components are available to application developers. But, if contributors have poor internal processes for managing open source compliance and security, they're likely putting others at risk when they contribute to open source projects.

With that in mind, we asked respondents if they contribute to open source projects.

A third said they do. Nearly half said they do not. And 20 percent said they do not know.

Does Your Company Contribute to Open Source Software Projects?



FOLLOW-UP CORRELATION

Do the companies of the contributors have a formal open source acquisition and usage policy? Of the 62% of respondents without a policy or who do not know if a policy exists, 43% contribute to open source projects.

Many individuals and companies contributing to open source projects lack their own internal open source acquisition and usage policies. 43% of developers contributing to OSS are not aware of a formal OSS usage policy.

Why Does This Matter?

Open Source Risk Management benefits everyone.

When you're working with open source code but you're not managing vulnerabilities and compliance, you put your products and customers at risk. You're also hurting the community instead of helping it.

Ultimately, the customer pays the price, running software or devices that contain potentially risky source code.

Open Source Risk—It's a Fact!

In the coming years, open source will unlock new technologies in the Cloud and IoT space—creating billions in value. The need of the hour is visibility and compliance without burden. Discovering issues earlier in the DevOps cycle means less impact on development and meeting business deadlines. Equate finding licensing irregularities or potential security vulnerabilities to finding a bug in a software application. The earlier it's discovered, the less expensive and impactful it is to correct.

Start Managing Open Source Risk

Educate

The basics of open source license compliance management should be taught at all levels in the organization. Senior management needs to understand license compliance requirements, and the value of periodically update products to remediate vulnerable open source components.

Set Up an Open Source Review Board

The OSRB sets policies, responds to license compliance and security events and provides training and knowledge to the rest of the company. It can be ad hoc or more tightly structured depending on a company's maturity and size.

Implement Processes and Policies

The development/devOps teams can implement OSRB policies. They should first emphasize compliance with all open source licenses being used. Then they should focus on creating a process to discover vulnerable components and release updates as needed.

Automate

Software Composition Analysis (SCA) tools will help discover and manage the open source and third-party content being used. These tools can alert companies to vulnerabilities and licensing issues.

Track and Report

An SCA solution allows you to track and report on open source use throughout your organization. Streamlined reporting and security alerts benefit software teams and executive management. Customers also win because they'll get accurate third-party notices and Bill of Materials for compliance and license obligations.

Most importantly, you protect your clients, your company and your reputation.

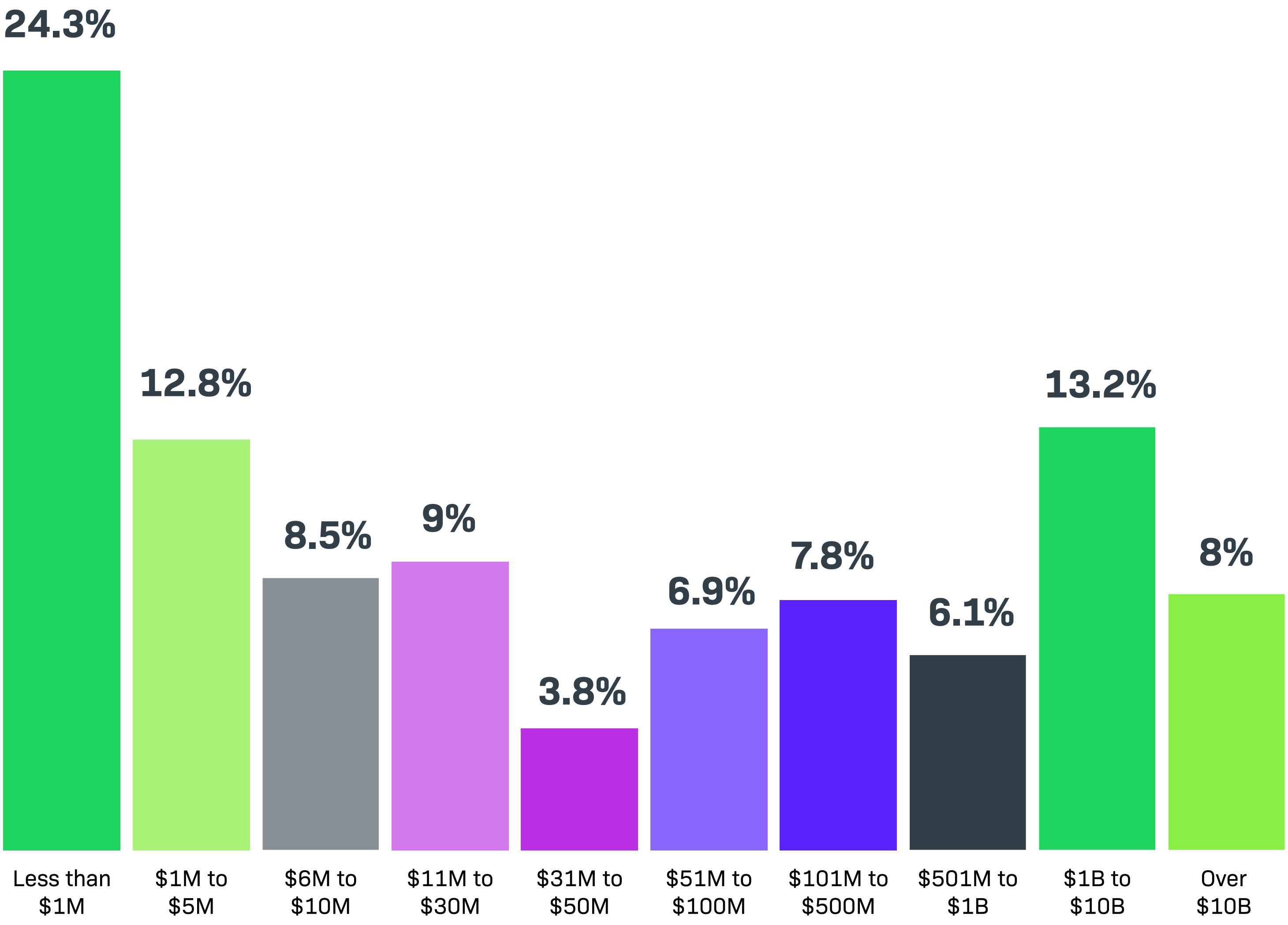
Survey Background

This survey was conducted by Revenera, the leader in open source compliance and security solutions. The survey reaches out to executives at IoT and software companies as well as in-house development teams within enterprises.

In total, 438 respondents participated in the survey in 2017. The functional roles of the respondents within their organizations include software developers, DevOps, IT, engineering, legal and security.

Respondent Demographics: Revenues

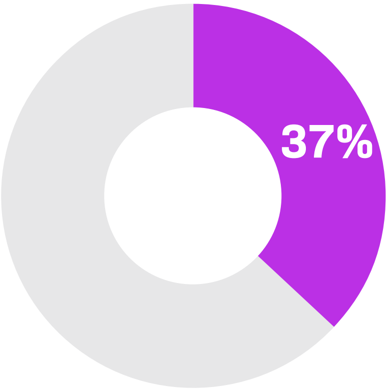
Which of the Following Represents Your Annual Revenues?



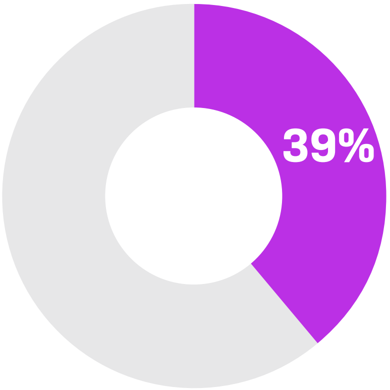
Respondent Demographics: Software Type

As a software developer, what category of software do you develop?	
Software developer for in-house applications	**19%**
CAD/CAM	**2%**
Security	**4%**
Infrastructure	**6%**
Educational	**4%**
Embedded software (software for hardware and/or Internet of Things Devices)	**7%**
Scientific	**4%**
Gaming	**1%**
Consumer	**4%**
Financial/Accounting	**4%**
eCommerce	**4%**
Supply chain automation	**4%**
CRM	**1%**
Healthcare	**6%**
Industrial	**7%**
Networking	**4%**
Oil & Gas	**2%**
Retail	**1%**
Banking	**2%**
Other	**16%**

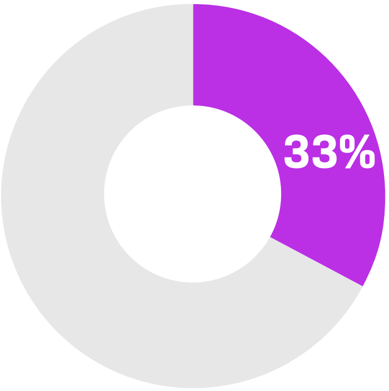
Open Source Risk



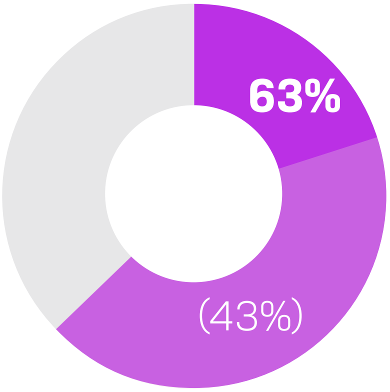
Only 37% of companies have an open source acquisition or usage policy.



39% said that either no one within their company is responsible for open source compliance—or that they don't know who is.



33% say their companies contribute to open source projects.



Of the 63% of respondents without a policy or who do not know if a policy exists, 43% contribute to open source projects.

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**