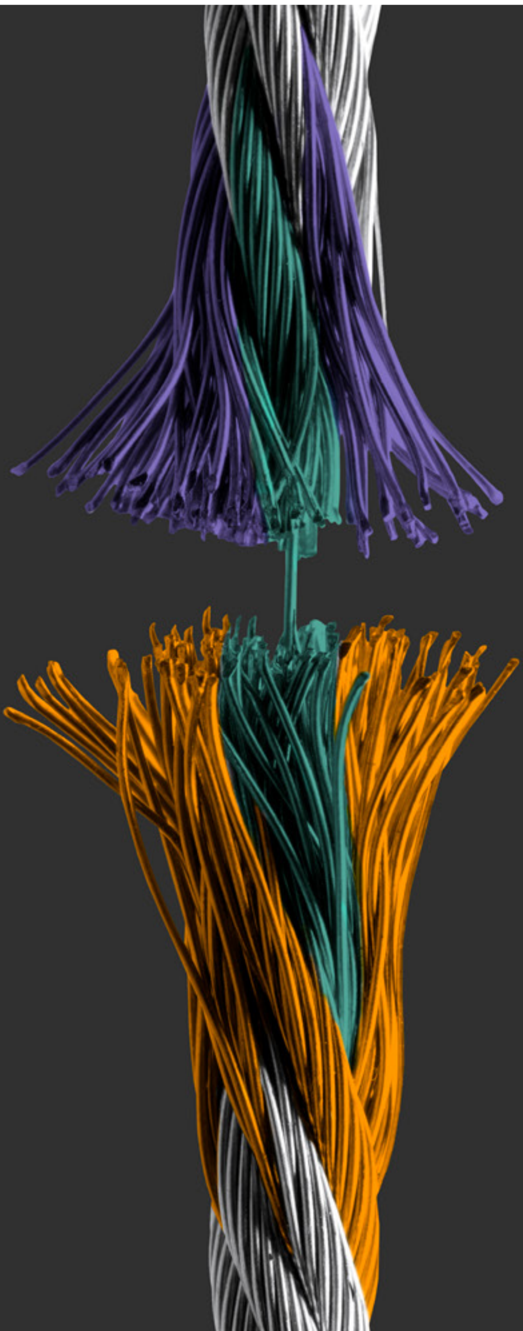
The CISO Circuit by
YL VENTURES

Top CISO Insights – Edition 7

# Third Party Risk Management



# About YL Ventures

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages over $300 million and exclusively invests in cybersecurity.

YL Ventures is uniquely focused on supporting the U.S. go-to-market of early-stage companies and leverages a vast network of industry experts, Chief Information Security Officers (CISOs) and U.S.-based technology companies as advisors, prospective customers and acquirers of its portfolio businesses. The firm's focused strategy allows it to conduct rapid and efficient evaluations for early-stage entrepreneurs and guide founders through their ideation processes pre-investment. The firm is also dedicated to providing unmatched, hands-on value-add support to each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

The firm's global network and footing in the U.S. have always counted among its most powerful assets: YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of YL Ventures' Venture Advisory Board.

YL Ventures' Venture Advisory Board is composed of over 100 security professionals from leading multinationals, including Microsoft, Intuit, Zscaler, Kraft Heinz, Walmart, Netflix, Nike, Spotify, Aetna and Optiv. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature. The advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from introductions to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

## Portfolio

**PiiANO**
PII Protection & Management
**www.piiano.com**

**valence**
Business Application Mesh Security
**www.valencesecurity.com**

**grip**
SaaS Security Management
**www.grip.security**

**enso**
Application Security Posture Management
**www.enso.security**

**satori**
DataSecOps
**www.satoricyber.com**

**cycode**
Software Supply Chain Security
**www.cycode.com**

**orca security**
Cloud Security
**www.orca.security**

**Hunters**
Open XDR
**www.hunters.ai**

**VULCAN**
Continuous Vulnerability Remediation
**www.vulcan.io**

**Karamba Security**
Embedded Security for Connected Systems
**www.karambasecurity.com**

**RIDEVISION**
Predictive Vision for Motorcycles
**www.ride.vision**

## Acquisitions

**MEDIGATE**
Acquired by
CLAROTY

**build.security**
Acquired by
elastic

**AXONIUS**
Exited to
late-stage investors

**Twistlock**
Acquired by
paloalto networks

**HEXADITE**
Acquired by
Microsoft

**FIRELAYER**
Acquired by
proofpoint

**Seculert**
Acquired by
radware

**BlazeMeter**
Acquired by
ca technologies

**Clicktale**
Exited to
Amadeus Capital Partners

**AcceloWeb** Click. You're there.
Acquired by
Limelight Networks

**UPSTREAM COMMERCE**
Acquired by
Walmart

# About the CISO Circuit

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions and cultivate portfolio company business development. As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities and opinions about the state of their organizational cybersecurity.

We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched "The CISO Circuit" (formerly "The CISO Current"), an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove useful to aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

# Table of Contents

# Introduction

In this report, our team set out to understand the cybersecurity challenges of Third-Party Risk Management (TPRM). Over the course of 40 interviews with distinguished survey participants hailing from a diverse spectrum of verticals and company sizes, we collected responses to a series of questions (see Appendix) about their most pressing TPRM concerns.

Whether they offer products or services, few organizations have the resources to plan, build and operate every facet of their workflows; offloading every possible function to third-parties enables organizations to focus their efforts on their most productive activities. The need to quickly digitize operations during the COVID-19 pandemic recently accelerated third-party reliance, as enterprises looked to outside services to support newly remote workforces. Today's market has grown increasingly integrated as a result. Different organizations now seek strategic access to each other's systems, networks and data in a race to maximize operational productivity and efficiency.

However, each point of third-party access introduces risk and a potential domino effect on connected nodes that can quickly expose stored data and critically hinder an organization's capacity to operate. Third-party vulnerabilities are responsible for a growing number of breaches that have taken place over the past two years. High-profile attacks of this nature, notably those of SolarWinds and Kaseya, underscore the mounting urgency to focus on third-party risk in cybersecurity posture. These developments prompted us to focus our research on how cybersecurity executives approach this issue and work with TPRM assessments.

Today's compliance requirements often feature TPRM despite their uncertain impact on security. Enterprises require TPRM solutions that are effective at mitigating—or at the very least, identifying—risk while promoting the need for efficiency at the root of engaging third-party vendors. At present, our surveyed experts warn that a lack of context, ongoing friction and lacking standardization largely hinder this among the current market of solutions. Instead, they offer, at best, point-in-time glimpses into cybersecurity posturing that are incomplete.

Moreover, their often binary approach to risk modeling fails to account for the more nuanced realities around true vendor vulnerabilities, such as vendor type, how buyers intend to use vendors and enterprise-specific risk prioritization. For example, demanding HIPPA requirements from a health care provider's outsourced landscaping company may verge on the unreasonable. Most importantly, they impose hard lines and rigid security expectations that fail to account for inherent software vulnerability.

Our experts are looking to other cybersecurity strategies to reinforce themselves against TPRM gaps. These primarily include the introduction of zero trust principles to third-party processes and technologies and enforcing a least-privilege process for vendors.

This document constitutes the seventh edition of the **CISO Circuit** report and contains data gathered from direct interviews with 40 cybersecurity executives at leading enterprises from YL Ventures' Venture Advisory Board. The surveys consisted of short-form questionnaires and longer-form discussions. In order to obtain the most candid data possible, and with respect to the sensitive nature of some of the information shared, we anonymized the names of our respondents and their associated organizations.

# TPRM

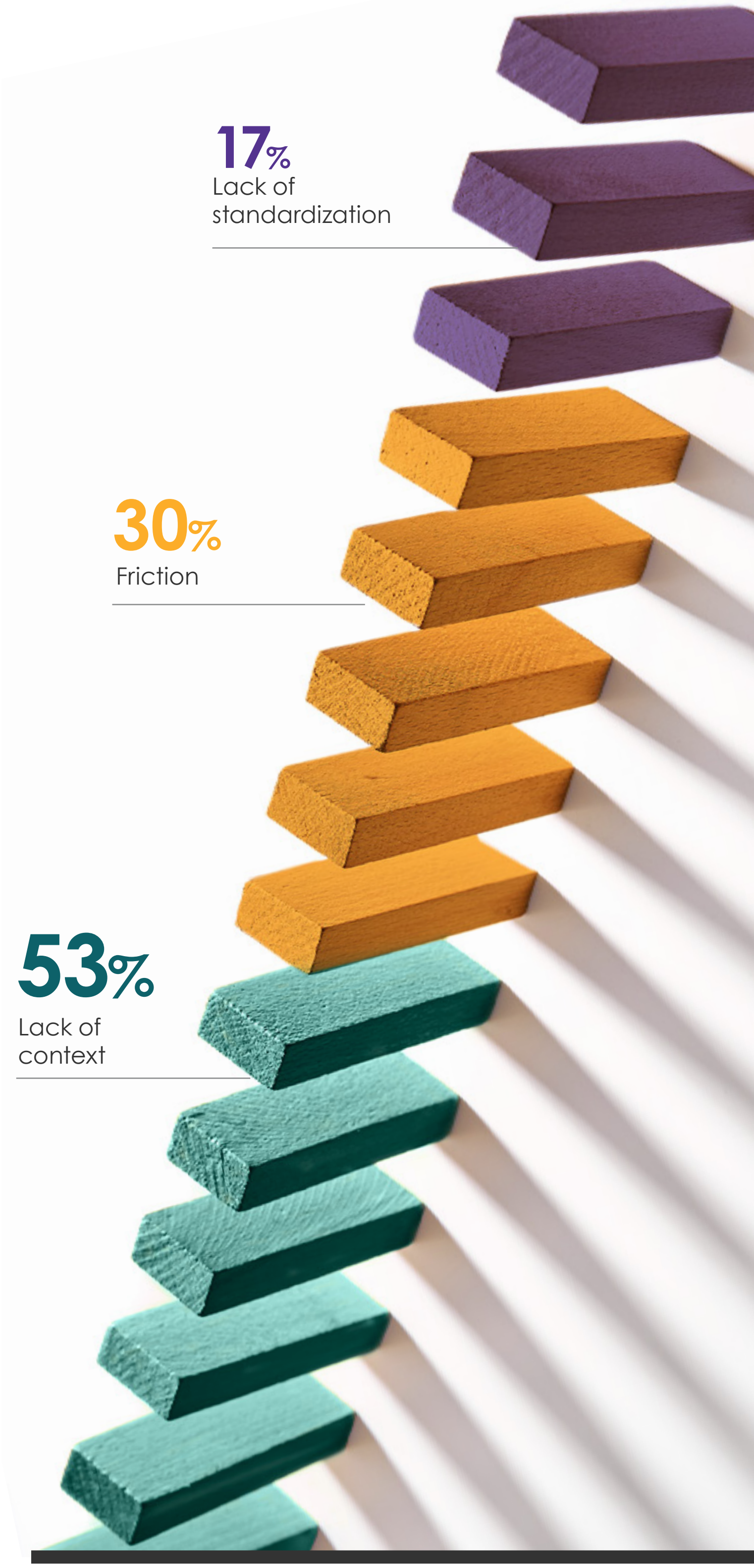
TPRM solutions ostensibly help assess and mitigate the potential risk introduced by third-party vendors throughout the customer-vendor relationship, which varies at every stage. Current TPRM solutions try to achieve this by investigating prospective and engaged third parties, tracking how they are used and ranking their cybersecurity posture. Broadly, some TPRM assessments scan a vendor's external attack surface to assess its security flaws. This is often carried out using public available information and does not require the evaluatee's participation or information disclosure. Others require vendors to complete questionnaires disclosing their ability to securely interact with a prospective customer requiring the TPRM process.

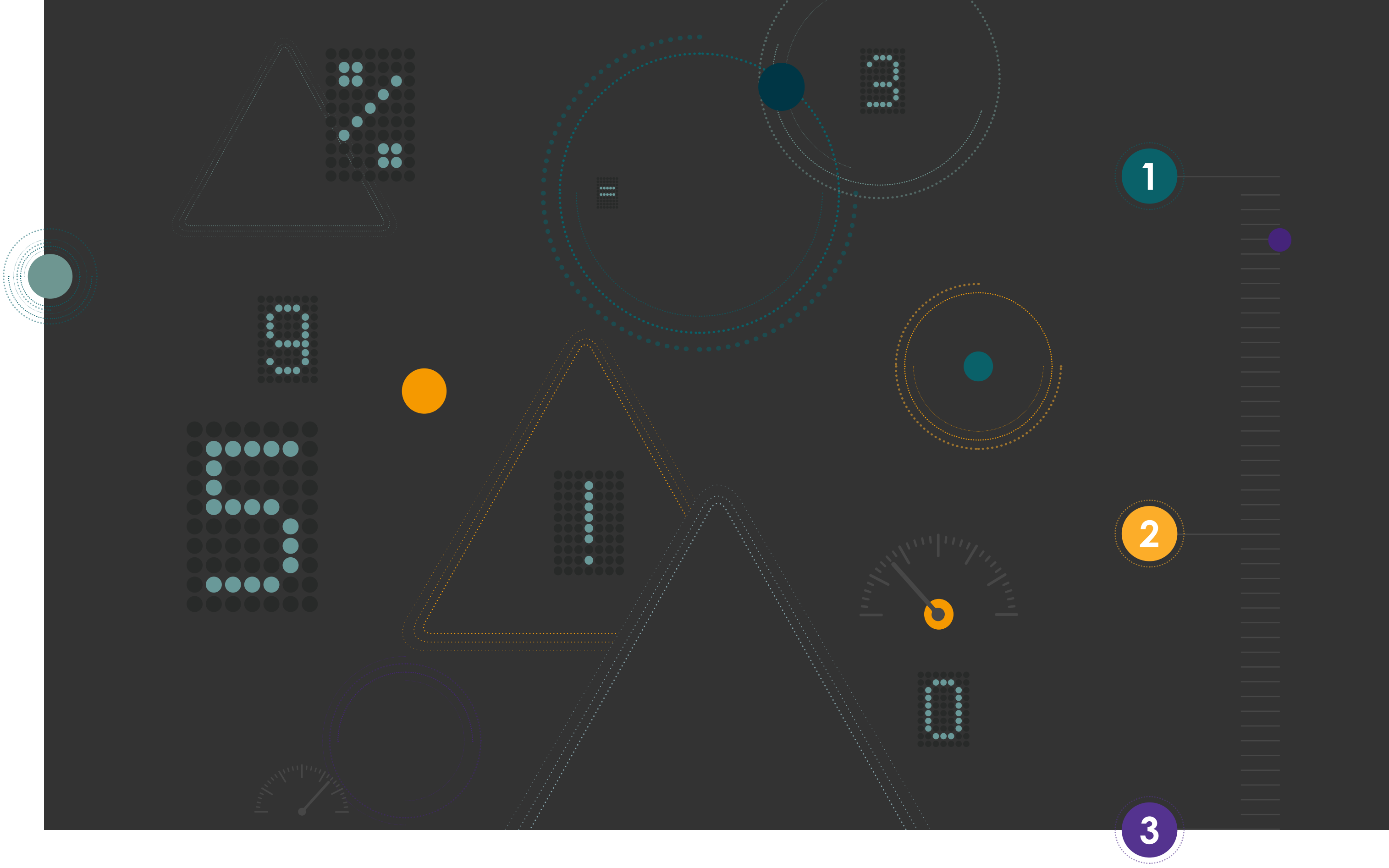
# TPRM Concerns

TPRMs offer limited visibility into a vendor's cybersecurity posture and are often plagued by a lack of lead time. This results in many incomplete or unactionable assessments that provide little insight into the real supply chain risk a vendor poses to potential customers. Many security leaders challenge the objective nature of scoring systems for such a subjective domain. Further, questionnaires are not legally binding and risk dishonest or incomplete disclosures.

When directly surveyed about their concerns over TPRM processes and assessments, 53% of our surveyed experts cited lack of context, 30% complained of friction and 17% specified lack of standardization.

**What are the problems with how TPRM is conducted today?**





## Lacking Context in Score-Based Systems

The cybersecurity leaders surveyed for this report argue that current score-based solutions fail to adequately account for the contextual data necessary for producing accurate cybersecurity posture assessments. Many rely on publicly available data to infer or surmise a security posture without enough flexibility to account for risk-based approaches and prioritization.

The often binary model of TPRM assessments, in which vendors are either deemed 'secure' or 'insecure', also fails to account for how much progress a company has made towards achieving specific security goals. For example, a vendor that has nearly achieved SOC2 might be rated in the same manner as one that has not started their SOC2 process at all. Finally, most assessments do not provide insight into specific products by specific vendors, which are often the biggest points of risk.

Moreover, today's TPRMs often fail to account for non-technical considerations—such as the risk posed to business viability—as well as for interdepartmental relationships and workflows. Taking these latter points into consideration can generate completely different results. Ironically, the limited scope of TPRMs also fails to contextualize an evaluated vendor's own supply chain security. The SolarWinds breach serves as an excellent example of the long chain of risk that can reach fourth, fifth and even sixth parties.

Further criticism extends to TPRM scoring frameworks that offer little context around its results—rendering them unactionable. Whether offered in binary or numerical format, few understand how to utilize their scores. Many scoring frameworks use "best-in-class" models regardless of their actual relevance to the vendor under investigation. Moreover, assessments, even when carried out on a regular basis, only provide point-in-time glimpses into the potential risk profile of an organization. They can be rendered moot by different ongoing organizational changes, including the dynamic quantity and sensitivity of data shared with third parties.

## Friction with Questionnaires

Our respondents also highlighted issues with friction in both the TPRM questionnaire process and limitations around persuading vendors to change their practices. TPRM deployments and maintenance can quickly spiral into large projects that take up too much time with far too much overhead; the need to verify or follow up with more tests can run up both labor and costs.

Oftentimes, it is the responsibility of TPRM consumers to aggregate assessment data themselves—an arduous task lacking automation. Because they cannot even provide continuous insight, this demand on resources is antithetical to the efficiency promise of engaging third parties at all. In some cases, large organizations dedicate entire teams towards administering TPRM questionnaires, an expensive operation often focused on escalating "failed questions" as priorities, regardless of their relevance to actual business needs. In other cases, poorer scores can reflect a lack of means or resources to work with questionnaires rather than the true state of a vendor's security posture.

Final scores meant to support or warn against a partnership carry little sway on their own. Many feel that the questionnaires are incentivized to poke holes in their stature to demonstrate value, rather than actualize it. TPRM assessments are often rendered further unactionable by their unenforceability—especially in the case of large evaluated vendors and small prospective accounts.

## Lacking Standardization

TPRM is not practiced consistently across all organizations, nor are the evaluation processes and assessment results based on an official body of standards. Our surveyed experts argue for a single source of truth that can dictate the safety standard for sharing information with vendors based on standardized sensitive data classification. The qualitative nature of the assessments, despite an objective approach, only further contributes to their unenforceability. Moreover, the absence of organized information exchange in the TPRM community further hinders its effectiveness.

The safety standard for sharing information with companies, according to our surveyed experts, must begin with data classification. Many organizations have yet to accomplish this, despite its fundamental role in data protection best practices. Further, our advisors contest models that arbitrarily assign higher trust to highly regulated industries. For example, the premise that we must automatically place trust in financial or healthcare vendors. Moreover, at present, TPRM vendors conduct questionnaires and scoring with bespoke methodologies that lack consistency.

However, our experts also warn against a one-size-fits-all approach; different standards are required for different types of enterprise and organization verticals, as different organizations face different third-party risks.

**The qualitative nature of the assessments, despite an objective approach, only further contributes to their unenforceability.**

# Accuracy and Reliability of TPRMs

## Actual TPRM Use

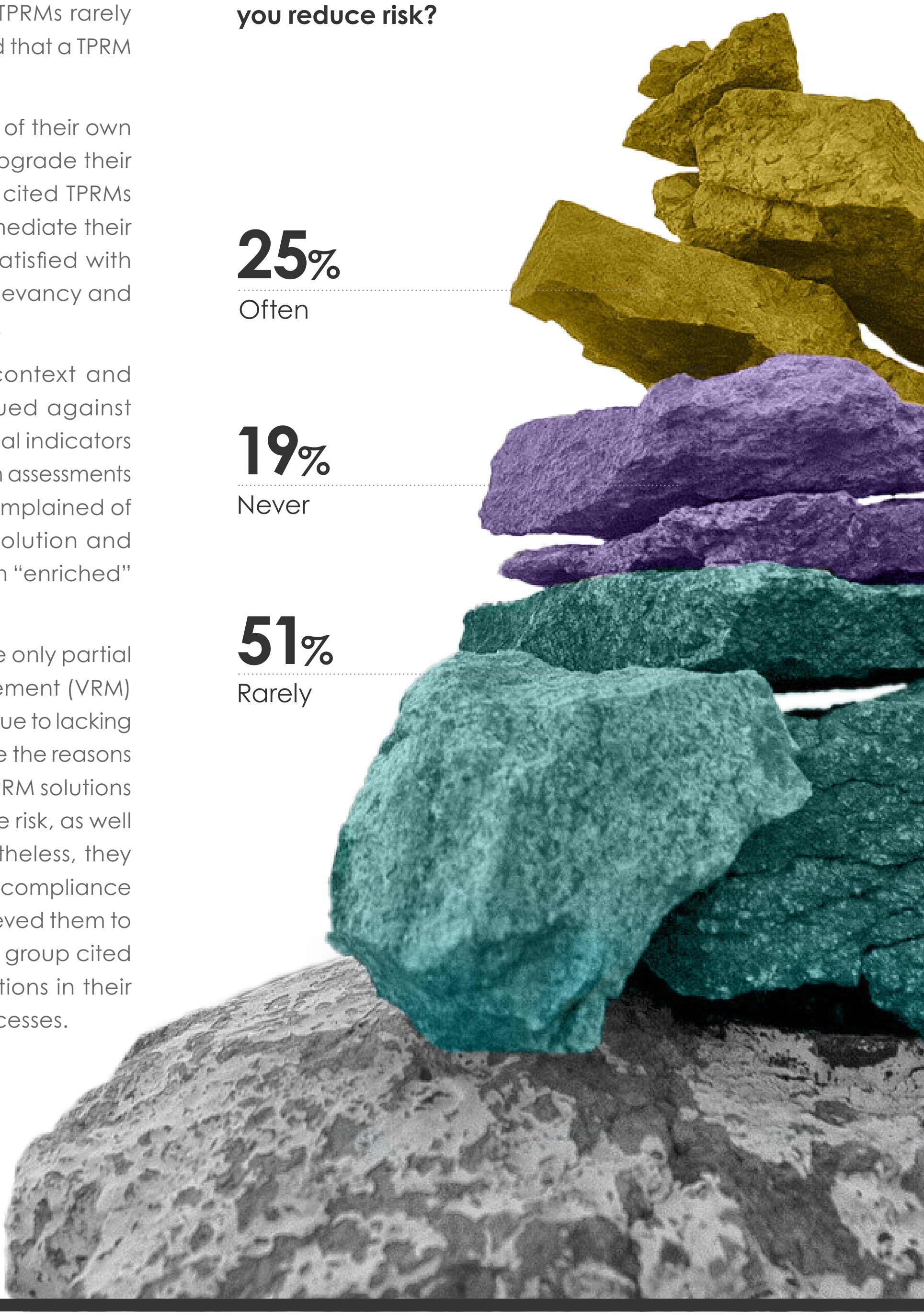
Of the cybersecurity experts surveyed for this report, 19% mentioned that TPRM solutions never helped them reduce risk. Conversely, 51% reported that TPRMs rarely helped them reduce risk, while 25% mentioned that a TPRM solution often helped them reduce risk.

Some advisors view them as an integral part of their own cybersecurity posture and enthusiastically upgrade their practices where necessary to comply. They cited TPRMs as major contributors to helping find and remediate their vulnerabilities. Those partially and fully unsatisfied with their scores contested their accuracy and relevancy and complained of the difficulty of altering them.

Citing the aforementioned concerns of context and actionability, dissatisfied respondents argued against assessments exclusively carried out on external indicators and for the need to include inside information in assessments to truly contextualize risk. Finally, they also complained of poor communication between the TPRM solution and evaluated vendor, as well as TPRM reliance on "enriched" data.

Many respondents feel that TPRM solutions are only partial components of a larger Vendor Risk Management (VRM) process and are too often rendered irrelevant due to lacking contextualization and enforceability. These are the reasons cited by the surveyed experts who felt that TPRM solutions have rarely helped their organizations reduce risk, as well as those who felt that they never did. Nonetheless, they continue to use them to meet regulatory and compliance standards. Those that felt more positively believed them to help reduce risk often. Many within this latter group cited successful outcomes of involving TPRM solutions in their vulnerability detection and remediation processes.

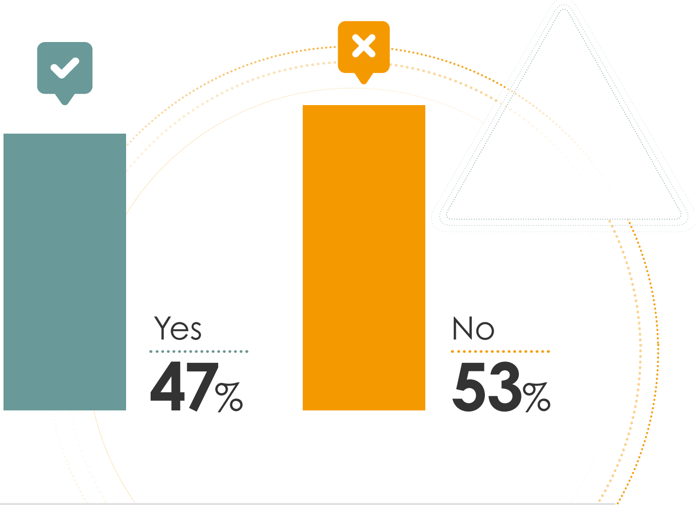
**How often has a TPRM solution/platform helped you reduce risk?**

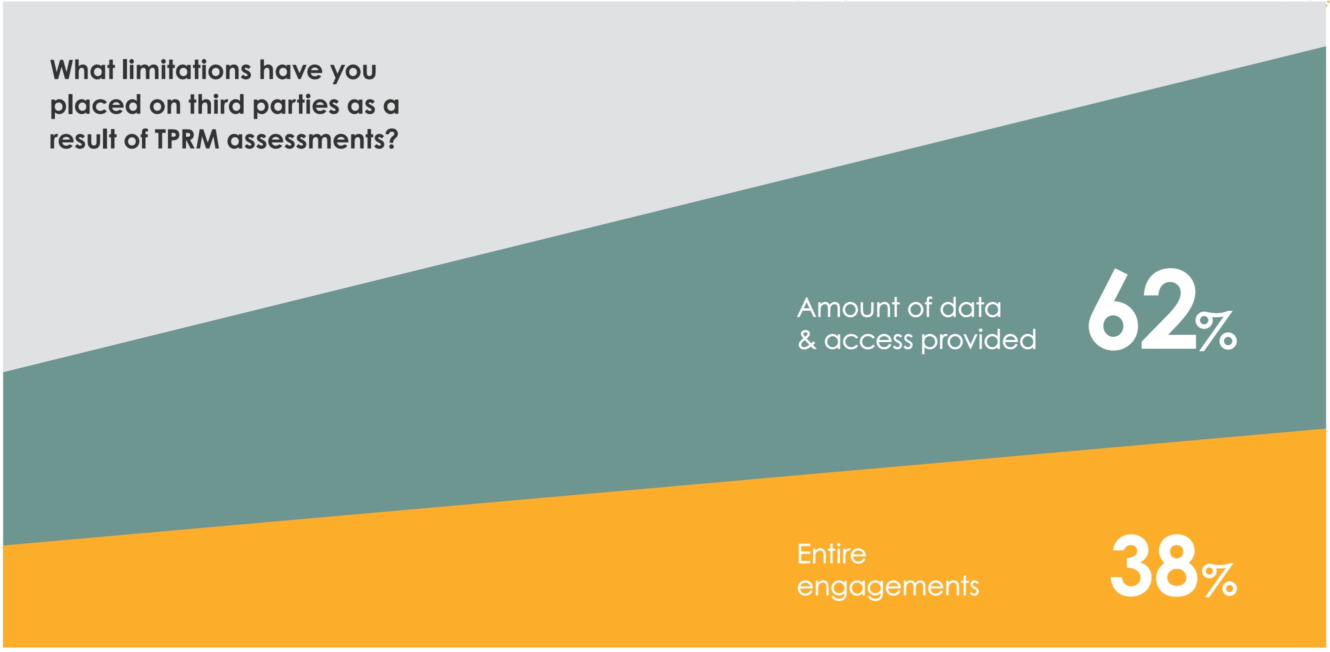


## TPRM Influence on Vendor Assessments

The results of whether CISOs actually ended vendor relationships over TPRM scores are less varied. 47% of surveyed respondents have declined a vendor due to indications from a TPRM. Of the 47% that were influenced, many cited flagrant discompliance as the main reason for declining a vendor. Those who did not decline vendors due to TPRM scores cite their lack of relevancy to their specific use-case or working relationship with the vendor in question. Many still use TPRMs to simply further contextualize their own final assessment.

**Have you ever declined a vendor due to indications from a TPRM solution?**





## TPRM Influence on Risk Mitigation

Of those whose TPRM assessments help reduce risk, 62% were persuaded to limit the amount of data provided to third parties as well as limit third-party vendor access through technologies such as SSO. This is largely enforced through TPRM-based service-level agreements and other legally enforceable contracts, including NDAs and liability coverage. 38% were influenced to limit entire existing engagements with third parties.

# The Future of TPRM

According to the data above and further qualitative insight provided by our experts, better TPRMs must account for more context around product and vendor obligations. At the very minimum, many respondents argue that TPRM vendors must better familiarize themselves with the workflows and services of the company verticals they evaluate. True third-party risk management can vary from one industry vertical to the next according to specific operational needs. Moreover, they recommend including frameworks, security controls and organizational structures.

A considerable number of respondents wish to see TPRM service-level improvement with automation—specifically timeliness and expediency around the exchange of information and continuous monitoring with the option for real-time assessments. Some wish for more flexibility around the scoring process and decreased friction with the help of automation. Finally, surveyed experts voiced considerable demand for assessments to transparently reflect the status of vendor security programs, rather than assign arbitrary scores that are difficult to understand.

**Surveyed respondents highlighted the close relationship between TPRMs and Compliance Management. However, the current landscape is rife with often overlapping—and sometimes even contradicting—compliance standards.**

## The Software Development Lifecycle

In light of the SolarWinds attacks, our respondents distinguished the role of securing software development lifecycles for averting supply chain attacks. This remains top of mind for security leaders in the process of building security into the architecture of their environments, as software development is notoriously and increasingly reliant on third-party vendors. With the introduction of a software bill of materials (SBOM), a list of software components in a piece of software, CISOs are keen to find better source code protection against the risk of contractors' access and deploying third-party software.

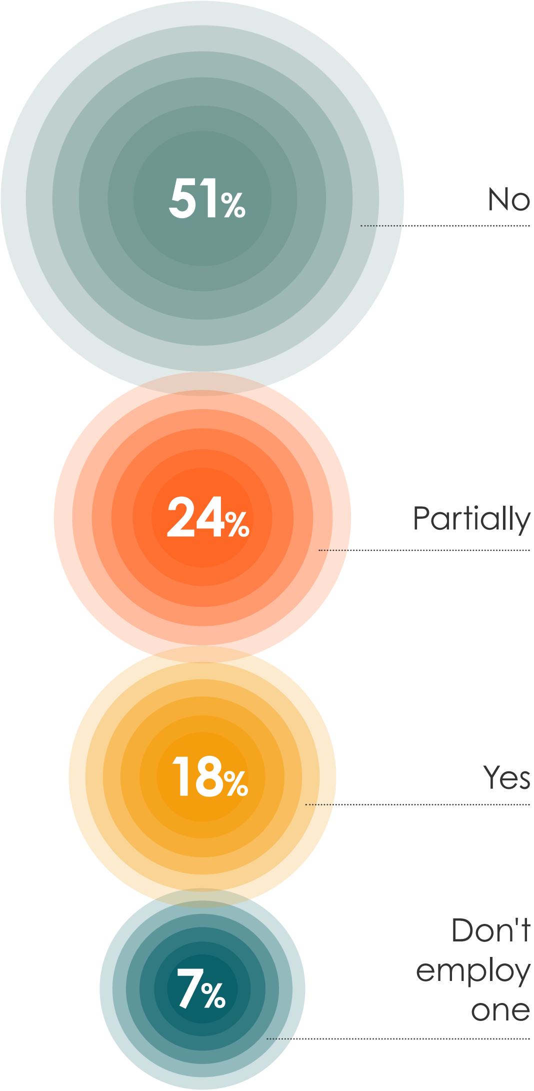
## Bespoke Business Workflows

Every enterprise follows its own unique procurement process with varying degrees of complexity. It is important to understand this workflow beyond the technology involved and investigate individual legal and business constraints. Our experts suggest that TPRM vendors invest more time in understanding the true importance of the data they have access to, and to offer the flexibility required by their findings.

## Setting Industry Standards

Surveyed respondents highlighted the close relationship between TPRMs and Compliance Management. However, the current landscape is rife with often overlapping—and sometimes even contradicting—compliance standards. In the security sector, where demand for individualized context is on the rise, are universal industry standards possible? Our experts believe that true TPRM is only possible with compromise.

**Are you satisfied with the TPRM solutions you are using?**



## New Frontiers of TPRM

33% of surveyed respondents believe that zero trust principles can remedy several of the gaps left by existing TPRM solutions. This offers more actionable measures, such as the employment of APIs and technological solutions enabling granular visibility of third-party access into their systems and data.

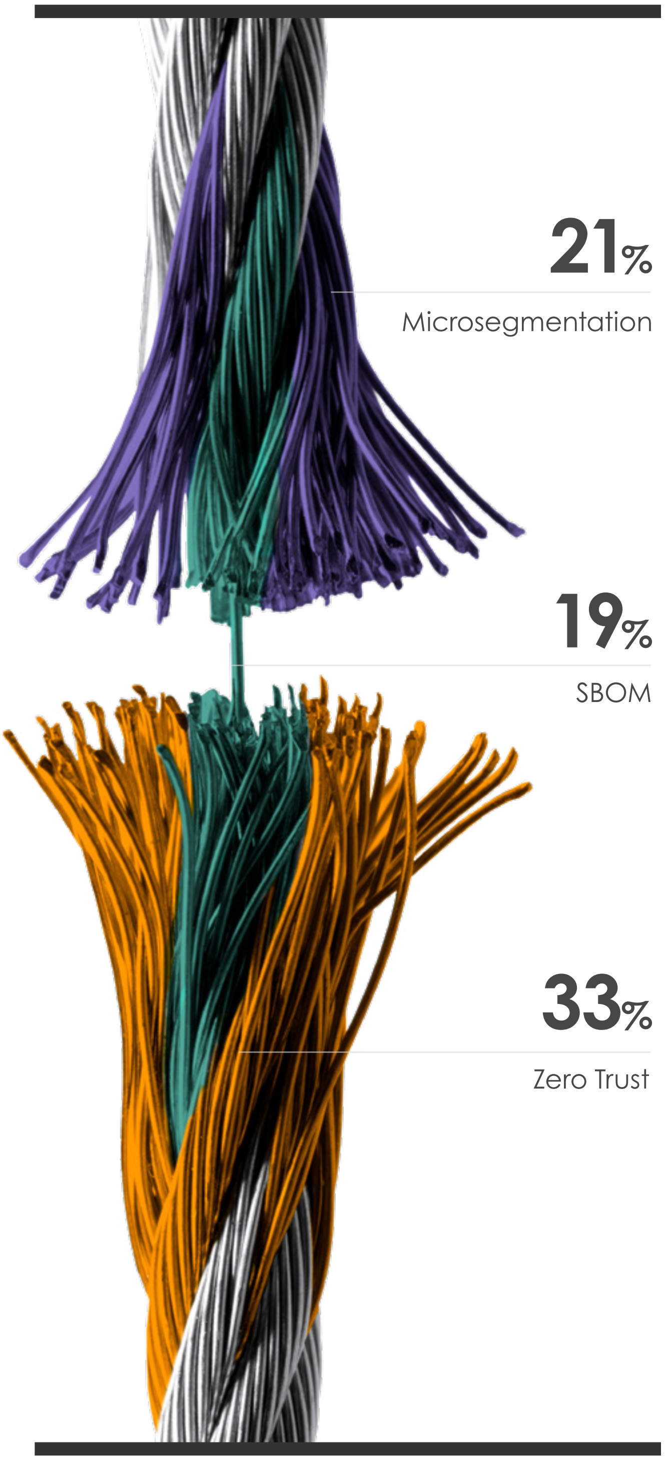
Cybersecurity leaders are looking to rely more heavily on zero trust principles and least privilege processes for vendors in the absence of satisfactory TPRM solutions. In a true zero trust scenario, access ought to be delayed by default and only permitted by exception. These exceptions might be decided by baselining the behavior of a third-party, understanding exactly what third-parties require access to and generating corresponding policies.

Our experts underscored the importance of applying these principles to inbound traffic or inbound communications from third-party vendors to their customers. Conversely, they expressed little optimism in controlling outbound traffic. To date, only large-scale organizations and governments have successfully restricted outbound traffic to strictly necessary functions. This may be possible in the future if IT teams can generate policies enabling IT management vendors to strictly access update servers, but not the internet.

21% believe that microsegmentation should be the attained approach. This includes defining access policies for a specific network or infrastructure segment of which access is requested. 19% rely on SBOM, which specifically addresses how software vendors often assemble a variety of open source and commercial software components to write applications. In effect, it encourages TPRM solutions to streamline their processes. Others similarly rely on Google's Supply Chain Levels for Software Artifacts, or "SLSA", an end-to-end framework for ensuring the integrity of software artifacts throughout the software supply chain (which, in turn, requires SBOM as a prerequisite for the usage guidelines).

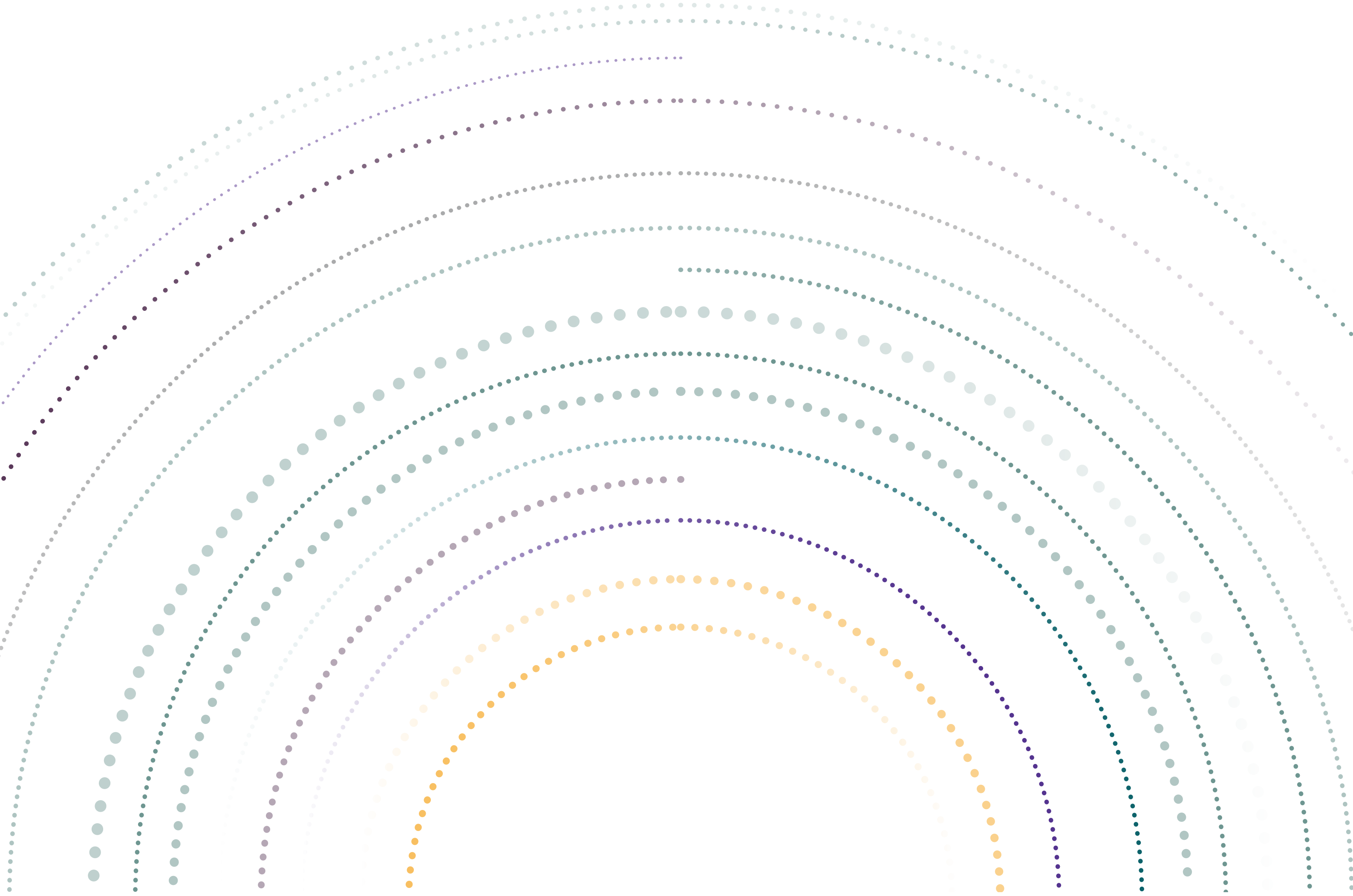
In a perfect world, our experts would wish for an alert mechanism for when third parties deviate from baselined behavior paired with more aggressive control—especially blocking—functions.

**What technological approaches can help offset third party risk?**



# Final Observations

Despite its perceived limitations, our respondents argue that the criticality of supply chain risk leaves no option but to continue employing TPRM solutions. However, cybersecurity leaders are concerned by the lack of contextualized assessments, their lack of means to truly validate and confirm scores due to an absence of TPRM standardization and the greater risk acceptance involved in working with solutions involving such high friction. Many evaluated vendors feel as though the scoring system potentially causes unfair business loss by imposing "objective" measurements on a "subjective" topic. The difficulty in changing a rating further exacerbates this feeling of tension with TPRM providers. Finally, lacking legal authority or any true enforcing power, many continue to raise questions over TPRM validity and seek alternative solutions.



# Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based startup looking for guidance for seed-stage funding, we invite you to contact **Ofer Schreiber, YL Ventures Partner & Head of Israel Office**, at **ofer@ylventures.com**. We also invite you to direct any questions relating to this report to this address.

We would like to sincerely thank all of the CISOs who participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Circuit, please contact **John Brennan, YL Ventures Partner**, at **john@ylventures.com**.

# Appendix

## Survey Questions

1. Are you satisfied with the TPRM solutions you are using?

2. Are third-party cybersecurity ratings reliable? (TPRMs that deliver assessments to their customers' vendors)

3. Have you ever declined a vendor due to indications from a TPRM?

4. Do you believe that your organization's TPRM score aligns with your security program? Do you agree with your score?

5. How often has a TPRM helped you reduce risk?

6. What proactive, risk-reducing measures have TPRM assessments prompted you to take?

7. How can entrepreneurs build better TPRMs?