Panorays

The CISO's Guide to Third-Party Security Management

Demi Ben-Ari
CTO and Co-Founder, Panorays

Dov Goldman
Director of Risk & Compliance, Panorays

Introduction

In this guide, we provide the guidance you need to make your organization’s third-party security program effective and scalable.

In particular, we cover how to:

- Implement compensating internal controls when your suppliers don't have or won't reveal their own
- Collaborate with suppliers to ensure success in the remediation process
- Create KPIs to help manage, improve the process and demonstrate achievements

THE

Situation

Your organization's attack surface is growing continuously. As you outsource large portions of your IT systems to third parties, you are effectively adding their attack surface to your own. Moreover, you probably have people in your organization connecting with outside providers all the time, so often it's not even clear what is included in your attack surface.

Because you share data with third parties, you must stay informed about their security as much as your own. Managing the security of your third parties is even more important because of the following reasons:

1. **Increase in cloud apps.** According to a McAfee report, the average organization increased its usage of cloud services by 15% from last year. Moreover, the amount of sensitive data shared on the cloud increases 53% year over year. It's expected that within a decade, 90% of IT dollars will be spent outside of the IT organization.

2. **Remote working.** Many companies that have shifted to working from home face increased cybersecurity challenges, including technology and human risks. The same can be said for their third parties.

3. **Third-party data breaches.** According to a Ponemon report, 59% of organizations experienced a data breach caused by their third parties. The consequences of such breaches can be disastrous and can include lost consumer confidence and loyalty, as well as costly penalties that could even lead to bankruptcy.

4. **New regulations.** Data privacy regulations such as GDPR, CCPA and the NY SHIELD Act require companies to ensure that customer data remains private and secure. A breach through a third party could result in significant financial penalties for the organization to which it is connected.

For all of these reasons, having a comprehensive third-party security process is crucial.

THE

Problems

Most organizations use two tools to assess their third parties' security: Security questionnaires and security ratings services (SRSes). However, each method can be problematic on its own.

The Problems with Questionnaires

Questionnaires lack context. Often security questionnaires can contain hundreds of questions, and many are not relevant to every single third party. For example, a vendor that develops software should complete a different questionnaire than a third party which offers cloud-based infrastructure.

Questionnaire processes cannot scale. It's time-consuming to manually send relevant questionnaires to each third party. Following up with third parties to make sure they complete the questionnaire in a timely fashion and manually reviewing them can demand many resources. Such a lengthy process hampers business enablement and the ability to quickly onboard third parties.

Questionnaires are only good for a limited time. Answers to questionnaires may only be valid for the moment that they are completed. Because new technologies are introduced all the time, a third party may be fully secure one month and breached the next.

THE

Problems

The Problem with SRSes

SRSes provide a limited view of cyber posture. While they can do a good job of assessing the exterior attack surface of third parties, SRSes cannot make sure that a third party complies with internal security policies and practices. Essentially, using an SRS is looking at the tip of the iceberg: An organization cannot see the entire picture of cyber posture with just an exterior scan.

Both SRSes and Questionnaires Can Be Problematic for Third Parties

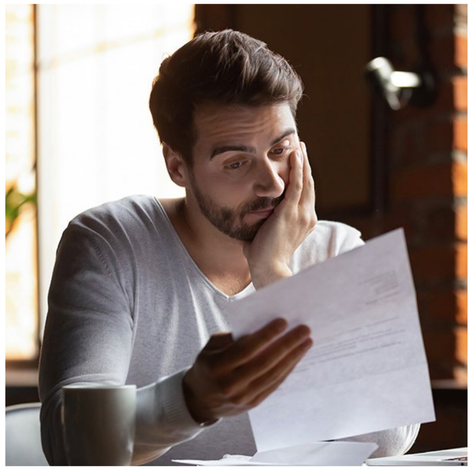
Your third parties want nothing more than to close the deal. A security check takes time and effort, and often requires third parties to remediate cyber gaps, which they may not have the resources to do. For these reasons, many third parties view security assessments as business blockers and can come up with excuses to avoid them. Some of those excuses, which stem from specific problems in the third-party security process, might even be like the ones on the next page.

THE

Problems

Questionnaire Excuses

Irrelevant questions:
“The questionnaire was too long.”
Unclear questions:
“The questionnaire has nothing to do with my business.”
Communication gap:
“The questionnaire never got to the right person.”



SRS Excuses

Unclear report:
“I don’t know what you’re seeing.”
False positives:
“I disagree. This is not my asset.”
No remediation plan:
“You found an issue. What do we do?”

Panorays

THE

Solutions

Automation is key for a comprehensive third-party security program. It provides the ability to rapidly scale while considering the following:

Context: It's important for organizations to identify the risk-relevant characteristics of each of their third-party relationships. The business owner should provide context about what data the third party will be processing and how critical it is to the business, how the data flows and what it's being used for, who will have access, and whether the third party is doing business with subcontractors like cloud service providers.

Visibility: To effectively assess the security of their third parties, organizations should ideally combine an external cyber posture scan with questionnaires so that they can verify internal security policies. For example, if a company claims that it is PCI compliant but does not have encryption on communication in transit, that indicates a problem. In addition, third parties should be monitored continuously, with specific policies that include steps to be taken if a cyber issue is discovered.

Engagement: To enable business, it's important to partner with your third parties to make the security process as smooth as possible. Questionnaires should be tailored according to context, so that there is no need to respond to irrelevant questions. Findings and clear, actionable remediation plans should be provided to third parties, along with visibility about how cyber gaps were pinpointed. Organizations should set realistic deadlines and provide an intuitive method for communication. In short, the organization and third party should establish a collaborative business relationship.

Building Your Program

Organizations that need to create or wish to upgrade their third-party security program can get started by doing the following:

1. **Identify stakeholders.** It's important to understand who are your internal partners. They might include the business owner, legal and procurement teams and security subject matter expert.

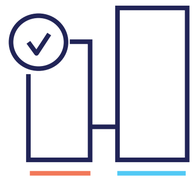
2. **Define tiers for the provider portfolio.** Have a comprehensive master list of all of your third parties and then tier it based on the inherent risk of each relationship. Inherent risk refers to risk based on criticality, meaning how long your organization can manage without that provider; combined with data risk, meaning how essential and/or sensitive is the data your organization shares with that provider.

3. **Define the standard of care for each tier.** Once you have identified the tiers of your third parties, you must establish a security policy for each tier. The policy should include how each level should be assessed, how often it should be reassessed, thresholds for continuous monitoring, an alert management process and your expectations regarding how a vendor should respond.

4. **Focus on providers that don't adhere.** Finally, it's important to establish a process for how to handle cyber issues that arise with third parties. Does your organization remediate, implement internal controls or terminate the business relationship? These are some of the issues that must be addressed.

Adding Intelligence

The most effective programs make use of cyber intelligence that helps support your decisions. Such intelligence may include:



Scanning a third party's attack surface

Detection of fourth parties

Business intelligence feeds

For example, if you know that your vendor is switching to remote work, a new security assessment might be appropriate. In addition, follow-up questionnaires and reviews might be considered at regular intervals, along with effective continuous monitoring. By implementing the right steps, you can take your third-party security program to the next level.

Panorays

Conclusion

As organizations continue to depend on third parties, the need for effective third-party security processes is growing. With these steps, organizations can be assured that their security process is scalable, efficient and comprehensive.

Panorays can help you create and improve your third-party security process. Using Panorays, you can:

Get a 360° view of your suppliers

Eliminate manual questionnaires

Comply with regulations

Benefit from contextual ratings

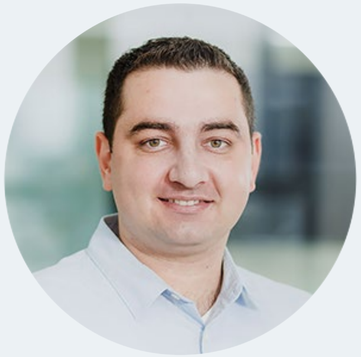
Engage effortlessly with suppliers

Remediate cyber gaps

Receive continuous visibility

Detect third and fourth parties

About the Authors



Demi Ben-Ari
CTO and Co-Founder, Panorays

Ben-Ari is an expert at building communities and networks—both online and offline. His technical background enables him to provide visibility into companies' seemingly blind spots and build large systems to empower users through insight-sharing. Ben-Ari is a recognized Google Developers Expert, co-founder of "Big Things"—one of the largest big data communities—and of the local Google Developer Group Cloud. He is a renowned international speaker, presenting big data solutions and distributed and scalable systems to both technical and management teams

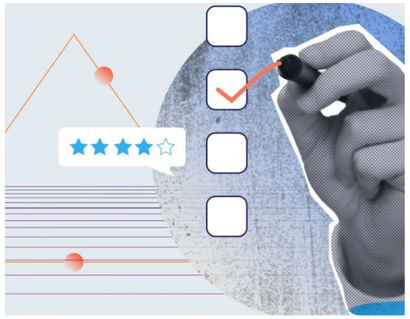
Dov Goldman
Director of Risk & Compliance, Panorays

Goldman has years of experience in the third-party risk and compliance field, as well as a long history as a serial entrepreneur, software and network engineer. He focuses on the evolving best practices and industry standards in third-party management and regulatory compliance. Previously, Goldman was VP of innovation at Opus, director of product marketing at Navigant, and founder and CEO of Cognet Corp and Dynalog Technologies. He has spoken at industry events around the world and has been quoted in numerous industry press articles, as well as *The Wall Street Journal*, about information security and privacy.

Get Educated!

Take a look at these resources for helpful third-party security tips and insights:

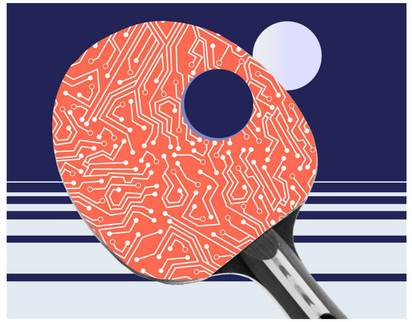
The Impact of EBA Guidelines on Third-Party Risk Management



3 Key Tips for Making Your Security Questionnaires More Effective

4 Ways to See if You Are at Risk of a Vendor Breach

The 4 Most Important Features to Look for in a Third-Party Security Risk Platform



5 Ways to Prevent Third-Party Data Breaches

How Panorays Can Help

Panorays quickly and easily automates third-party security risk evaluation and management — handling the whole process from inherent to residual risk, remediation and ongoing monitoring.

Unlike other solution providers, Panorays combines automated, dynamic security questionnaires with external attack surface assessments and business context to provide organizations with a rapid, accurate view of supplier cyber risk. It is the only such platform that automates, accelerates and scales customers' third-party security evaluation and management process, enabling easy collaboration and communication between companies and suppliers, resulting in efficient and effective risk remediation in alignment with a company's security policies and risk appetite.

Panorays is a SaaS-based platform, with no installation needed, and is the missing link that creates an out-of-the-box process and security plan, which also easily integrates into existing organizational workflows and systems. It is trusted by organizations worldwide in industries such as financial services, banking, insurance and healthcare, among others.

About Panorays

Panorays is a rapidly growing provider of third-party security risk management software, offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK and the EU, and has been adopted by leading banking, insurance, financial services and healthcare organizations, among others. Headquartered in New York and Israel, with offices around the world, Panorays is funded by numerous international investors, including Aleph VC, Oak HC/FT, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess. Visit us at www.panorays.com

Panorays

Want to learn more about how Panorays' automated questionnaires can help your third-party security process?
Request a demo today!