whispir.

Increasing Business Confidence in Third Parties

ABOUT WHISPIR

Whispir is a communications intelligence company with a promise of the world's highest engagement rates that supports the delivery of more than two billion interactions worldwide. Whispir serves over 800 customers, and as any vendor with a significant portfolio knows, customer assessment requests can be a challenging, manual, and costly process.

THE CHALLENGE

Before Whispir joined CyberGRX, their security team struggled with four major challenges regarding both their status as a third party to their portfolio of customers, and also as a SaaS company with many third parties of their own.

© Copyright CyberGRX 2023

1 **Whispir couldn't effectively assess the security of all of the third parties in their ecosystem, resulting in a weakened TPCRM program.** They spent their limited resources chasing assessments, causing them to lack the bandwidth to conduct proper analysis and achieve a complete view of their third-party security posture. They weren't able to shine a light on the security posture of their full ecosystem and were lacking streamlined processes that would strengthen their TPCRM program.

2 **They had a limited ability to respond to all prospective customer assurance requests.** ISO certificates alone were not enough to provide prospective customers with confidence in Whispir's cybersecurity program. It was common for some customers to conduct extensive three-month audits. Often only one staff member was allocated to one of these comprehensive audits while juggling other tasks. Whispir's infosec team was spread thin, finding it impossible to allot the required capacity and resources needed for the quantity of comprehensive audits that were coming in. Additionally, several of Whispir's customer-facing teams, outside of just Infosecurity, were receiving custom questionnaires through multitudinous channels. Without audits funneling directly to the Infosec team, other frontline departments had the autonomy to provide inaccurate, outdated, and inconsistent responses to audit questions, all of which created an integrity risk. Whispir was in search of, and in need of, a standardized process.

3 **Meeting their customers' ongoing needs:** Whispir participated in third-party cyber risk management (TPCRM) audits by many of their customers, which was a hugely inefficient and costly process for them and their customers alike. As many SaaS companies can relate to, Whispir's customers would submit a myriad of bespoke security questionnaires and framework templates–thinking that theirs were unique–making it impossible for the infosec team to centrally control audits. At the time, 30% of the FTE's time was spent on customer-assurance work annually. Despite the bespoke questionnaires, Whispir's infosec team found that underlying controls remained the same regardless of the assessment questions or the frameworks. They were providing the same evidence again and again. Lastly, the bespoke process of custom assessments restricted them from having the ability to benchmark their security posture against the wider industry.

4 **Rapidly changing threat environment:** Whispir serves over 800 customers. The approach of an annual assessment control – updating their security posture once a year — wasn't enough for some of their most significant customers. Wait time became an issue when it came to projecting the control uplift achieved by the cybersecurity program.

THE SEARCH FOR A CRITERIA AND SOLUTION

Whispir needed a partner that was a leader in the TPCRM space, had a wide Exchange membership, had a cost, quality, and benefits match, and addressed their key pain pains.

That's where CyberGRX came in. The Exchange allowed Whispir to share its standardized assessment with more than 50 of its customers from the start. CyberGRX's latest capability, Predictive Risk Profiles, empower Whispir to harness the power of machine learning to view instant, predictive risk assessment results for every third party in their portfolio, even when a self-attested assessment doesn't exist. Predictive Risk Profiles enable their security team to meet third-party security review needs during the procurement and third-party onboarding process.

The Predictive Risk Profile feature provides analysis through machine learning that predicts how a given vendor will answer each assessment question based on firmographics, outside-in data, and similar completed assessments on the Exchange. These instant insights have allowed Whispir's security team to view inherent and residual risk to map against common and custom frameworks and provide control gap analysis using threat profiles and real-life cyber-attack analytics. Although this feature is a new component to the Exchange, Whispir is planning to embed it as part of proactive security assessments within procurement and supplier onboarding processes, and potentially even as a mandatory check.

© Copyright CyberGRX 2023

THE IMPACT OF CYBERGRX

Whispir is currently undergoing an expansion and by leveraging CyberGRX, their TPCRM process was able to respond and scale effortlessly to increased demand.

Whispir created a successful third-party security assessment process. Whispir is now able to assess all of the third parties in their ecosystem with ease, allowing them to analyze their third-party risk more efficiently through the lens that matters most to them, based on their custom framework. Within the first six months of using CyberGRX, they were able to go from essentially minimal-to-no TPRM over 10% of third parties, to having an advanced risk view of 95% of their third parties. Additionally, in December of 2021, the InfoSec/GRC team was able to take Whispir towards successful certification on the ISO/IEC-27018 standard. They were able to develop security standards, implement their organization-wide compliance program, and develop a database of additional security questions and standard responses in support of the sales process and customer-facing teams. By improving their assessment process, they've also seen a particularly positive impact on their sales process. Overall, by front-loading the CyberGRX security assessment results, also by making our assessment results self-serve for customers via the website, a major hurdle in the process was removed/made frictionless.

They can proactively share a detailed view of their cybersecurity program with prospective customers. Whispir has now shared its standardized assessment with more than 50 of its customers. By front-loading the CyberGRX security assessment results, and by making their assessment results self-serve for customers, they transformed their process to be frictionless.

They can benchmark data, improving customer relationships through confidence. Whispir was immediately able to benchmark its security posture against the wider industry which has allowed them to continue to meet its customers' ongoing needs. They use the benchmarking data to meet third-party security review needs during the procurement and third-party onboarding processes. They are able to share their validated assessment results with customers right out of the gate, providing them immediate value.

FUTURE VISION AND GOALS

In 2022, Whispir, like many organizations, is anticipating escalating supply chain cyber-attacks, highlighting the need for rapid visibility into degraded or compromised third-party security posture. As they look to the future, they view success as the ability of their customers to self-serve their assurance requirements. The third-party cyber security posture of their own suppliers was made into a responsive process that contributes to and translates into a better security posture of Whispir. They also intend to partner with suppliers to ensure their ecosystem security posture continues to meet the needs of their business and is showing continuous improvement.

> *We highly recommend CyberGRX to build a modern and effective risk-based TPCRM process at scale in your organization.*

For more information on how our platform can assist your company in assessing third parties like we did for Whispir, visit our website:

www.cybergrx.com

Cyber GRX