CASE STUDY

MAX for Purchasing Services Provider

Cooperative organization strengthens supply chain cyber risk management

SecurityScorecard delivers visibility and timely insights that drive decision-making

The Challenge: Manual and Unreliable Processes

The customer had an immature third-party risk management program that was heavily dependent on a manual, time-consuming process. The team would send out internal questionnaires to vendors during the initial onboarding and RFP process, which often took weeks to complete. With a small team and over 250 vendors, it was impossible to consistently perform these assessments and monitor risk beyond initial onboarding. This left them with limited visibility into their vendors' security posture after the initial vetting and no efficient way to respond to emerging cyber risks.

Key Benefits

- Increased visibility and actionable data
- Improved internal awareness and accountability
- Enhanced compliance adherence

About the Customer

The customer is a non-profit purchasing cooperative, owned by and providing services to franchisees of a fast-food brand in the United States and Canada. The company's mission is to negotiate the lowest costs for purchased goods and services while ensuring quality, improving competitiveness, and providing the best value to its franchisees and their customers.

> **SecurityScorecard moves the maturity of our supply chain cybersecurity program to another level."**
>
> Senior Cybersecurity Director

Customer Info

Industry

Purchasing and supply chain support

Headquarters

United States

Products

MAX Managed Services

SecurityScorecard.com
info@securityscorecard.com

The Solution: A Strategic Force Multiplier

Recognizing that their manual process for vendor risk was a "nonstarter," the customer's cybersecurity team gained executive support to invest in an automated solution. They chose SecurityScorecard over competitors due to its ability to provide quick, high-level risk data on a vendor's security posture. This speed was a critical factor for business stakeholders who needed to make decisions quickly before contracts are signed. Given their small team, the customer also adopted SecurityScorecard's MAX service, which handles the heavy lifting of continuous monitoring and engagement with their top 50 most critical vendors.

MAX is a technology-enabled service that incorporates people and processes to achieve operational excellence in supply chain cybersecurity. MAX operates a Vendor Risk Operations Center (VROC) which continuously analyses thousands of signals, findings, and indicators, using its expert insight to alert the customer of the most significant breach indicators and advise on trends across all vendors. When signs of escalating risk like exposure to known exploited vulnerabilities (KEVs), leaked credentials, and ransomware infections are detected, the MAX team will personally meet impacted vendors, explain the findings, and deliver remediation advice. This supply chain incident response capability ensures issue resolution, usually within 48 hours, and shields the customer from fire drills that are disruptive to the risk management team.

> **"SecurityScorecard expedites vendor outreach to remediate critical issues in our vendor ecosystem."**
>
> Senior Cybersecurity Director

The Result: Increased TPRM Program Maturity

The maturity of the customer's risk management program has evolved from solely performing basic due diligence and now they are working towards a standardized TPRM program. The customer's evolution is not merely an operational improvement; it is a strategic enhancement that has made their business more resilient, their internal processes more efficient, and their supply chain more secure.

> **SecurityScorecard delivers defensible, evidence-based content that helps us meet compliance requirements."**
>
> Security Compliance Analyst

Increased visibility and actionable data

The customer now has actionable data that allows them to have informed conversations with vendors and internal stakeholders, ultimately reducing risk. As a result, they have been able to identify and move away from some vendors with poor security postures. The customer is now working toward improving the security posture of its top 50 vendors and expects to see an upward trend over the next year.

Improved internal collaboration

The program has fostered a new level of partnership between the security team and business stakeholders. Business stakeholders have become more aware and involved in the vendor assessment process, often reaching out to the security team earlier in the procurement cycle. The business teams now understand working with the security doesn't have to come at the expense of meeting operating goals.

Enhanced compliance adherence

As a company that follows the NIST cybersecurity framework, the customer's vendor risk management program was previously a known gap. The implementation of SecurityScorecard has provided a clear path to improving their maturity in this area. Their TPRM program can now consistently perform due diligence and mitigate supply chain cyber risks.