Security Scorecard

CASE STUDY

MAX in the Food Sector

Multi-national corporation protects brand and growth with SecurityScorecard

Global food retailer reduces the number of supply chain incidents by 75%

> **SecurityScorecard MAX provides us the opportunity to bolster our third-party cybersecurity posture quickly and efficiently through proactive, real-time risk monitoring and remediation.**
>
> Director of Technology Risk Management

Key Benefits

1. 25% reduction in number of supply chain security findings
2. 3x decrease in vendors with high incident likelihood
3. 100% remediation rate of zero-day vulnerability incidents

The Challenge

A global food retailer has operations in 105 markets and over 30,000 suppliers. To secure their brand and growth, they embarked on a journey to incorporate cyber security into their new global third-party risk management program that standardizes best practices across all markets. At that time, 67% of their security incidents were related to third-parties.

The existing TPRM strategy did not include cyber security and was reactive with processes that were fragmented across all markets. They were often responding to incidents instead of working towards preventing them. The company also had limited visibility of supply chain cybersecurity risk across all markets. They did not know who all their suppliers were or where all their data was stored. Their reactive nature and lack of visibility was surprising given their access to supply chain security data. Unfortunately the overwhelming amount of this data often paralyzed the operationalization of risk management strategies.

SecurityScorecard.com
info@securityscorecard.com

The Solution

The company had been working with security questionnaires and security ratings data for many years. These solutions were no longer viable since they often failed to provide the actionable information required to implement proactive strategies.

To make the shift from issue identification to issue resolution, they adopted MAX, SecurityScorecard's managed service for supply chain detection and response. MAX operationalized the company's supply chain cybersecurity program by driving the improvement of their supplier's security postures.

MAX performed all aspects of the company's third-party cyber risk management lifecycle. As the company was rolling out their global TPRM strategy, vendors onboarded into the new program were prioritized on the basis of incident risk and impact to the business. This was followed-up with an in-depth incident likelihood assessment that identified the necessary corrective actions needed to prevent unauthorized data access or disclosure. The MAX delivery had live interactions with the company's vendors where they explained the company's security expectations and how to remediate the issues that are creating concerns. After the vendor assessments are complete, SecurityScorecard's Vendor Risk Operations Center (VROC) continuously monitors every vendor. Anytime SecurityScorecard detects significant issues, the VROC reaches out to the impacted vendors to drive remediation. This service covers CVEs with critical CVSS scores, zero-day vulnerabilities, and known exploited vulnerabilities.

SecurityScorecard.com
info@securityscorecard.com

The Results

The company quickly and efficiently progressed through their supply chain cybersecurity maturity journey. They went from performing third-party risk management in an inconsistent and inefficient manner, to deploying a streamlined process for supply chain incident response. As a result, cyber risk management is now incorporated into every aspect of the vendor lifecycle, from contracting to offboarding.

The company has significantly reduced its supply chain cyber risk. They have prevented several supply chain breaches by working with their vendors to remediate issues before they are exploited. As the company's security teams and MAX delivery team monitor trends in the threat landscape, security thresholds are being refined to ensure that resources are used wisely and issues are remediated efficiently.

25% reduction in number of supply chain security findings

Continuous supply chain risk monitoring results across thousands of vendors creates a large volume of security findings that need to be triaged and responded to. Hundreds of thousands of ransomware infections, vendor breaches, instances of exposed information, suspicious activity and critical vulnerabilities were detected. With support from SecurityScorecard, the company was able to prioritize issue remediation efforts and focus on the vendors and issues that mattered the most, resulting in a 25% reduction in security findings.

3x decrease in vendors with high incident likelihood

In six months, the company has onboarded over two thousand vendors into their global supply chain cybersecurity program. SecurityScorecard independently evaluates the incident likelihood of every vendor and provides a high, medium, or low risk rating. At the start of services delivery, 136 vendors were rated as high risk. After driving remediation, SecurityScorecard was able to reduce the number of high risk vendors to only 32.

100% remediation rate of zero-day vulnerability incidents

Using its early warning and detection capabilities, SecurityScorecard alerted the company about vendors impacted by new and emerging potential zero-day vulnerabilities. 12 potential zero-day vulnerabilities were identified and 294 impacted vendors were identified. The detection of these issues immediately triggered outreach to vendors. SecurityScorecard explained to these vendors how we detected the issues and the importance of rapid remediation, resulting in all of them complying with the request to resolve issues on time.

> **MAX's ability to identify a wide range of cybersecurity concerns across our global vendor landscape, and in turn, partner with those vendors to improve, is a significant win for both our company and our vendors.**
>
> Director of Technology Risk Management

SecurityScorecard.com
info@securityscorecard.com