Security Scorecard

CASE STUDY

MAX in the Automotive Industry

Automobile Parts Manufacturer Operationalizes Third-Party Cyber Risk Management

SecurityScorecard drives continuous visibility and vendor risk reduction

The Challenge: TPRM Program Gaps

The customer's third-party risk management program was a manual, point-in-time process that relied on questionnaires which were often not completed by all vendors. The existing program was primarily focused on performing assessments at the time of onboarding. This approach led to a significant backlog of vendor reviews and left the company exposed to unmonitored risks, especially with its increasing reliance on a cloud-first strategy. The team needed a solution to move from a reactive to a proactive security stance.

Key Benefits

- Reduced supply chain cyber risk
- Improved vendor engagement
- Increased operational resilience

About the Customer

The customer is a global leader in designing, manufacturing, and selling components for the automotive industry. Their third-party risk management program's initial focus was on IT-centric vendors to protect critical data and systems. The team is now working to operationalize this program and expand its scope to include direct, non-IT suppliers by collaborating with departments like purchasing.

> "I don't have to worry about our third party risk management at this point."
>
> Senior IT Manager, Cyber Security & IT Compliance

Customer Info

Industry

Automobile Parts Manufacturing

Headquarters

United States

Products

MAX Managed Services

SecurityScorecard.com
info@securityscorecard.com

The Solution: Operationalized TPRM Program

The customer chose MAX, SecurityScorecard's managed service, to operationalize its third-party cyber risk management program. MAX is a technology-enabled service that incorporates people and processes to automate assessments, continuously monitor threats, and engage vendors to remediate issues.

MAX Incident Likelihood Assessments pinpoint breach potential and trigger response workflows by surfacing active information security indicators that vendors should investigate and remediate. In addition, MAX creates, delivers, and analyzes security questionnaires to gain insights on risks that cannot be analyzed without direct input from vendors. MAX operates a 24x7 Vendor Risk Operations Center (VROC) which continuously analyses thousands of signals, using its expert insight to alert the customer to 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 automatically meet impacted vendors, explain the findings, and deliver remediation advice. This supply chain incident response capability ensures issue resolution and shields the customer from fire drills that are disruptive to the cybersecurity team.

> **"SecurityScorecard provides a continuous view of risk, which is a significant change from our previous point-in-time assessments."**
>
> Senior IT Manager, Cyber Security & IT Compliance

The Result: Increased Risk Awareness and Reduction

By implementing MAX, the customer achieved a proactive risk management model without increasing the staff needed to operate its program. This allows their team to reduce its assessments backlog and focus on other critical initiatives, such as expanding their program to analyze evolving risks like vendors' use of artificial intelligence. Continuous monitoring of vendor risks provides a sense of security and trust that was previously missing from their manual processes.

> **We can track a vendor's security posture as they address vulnerabilities, which provides a clear and demonstrable path to risk reduction."**
>
> Senior IT Manager, Cyber Security & IT Compliance

Reduced supply chain cyber risk

SecurityScorecard performs vendor escalation engagements whenever a vendor shows signs of increased breach likelihood. During these engagements, SecurityScorecard advises vendors on how to improve their information security program. These collaborative engagements have led to 23% of vendors improving their security posture. The number of vendors with a low cyber risk rating has increased by 18%, including one vendor that improved their security rating grade from an "F" to an "A" in less than one month.

Improved vendor engagement

MAX delivers value directly to vendors instead of creating noise or unwanted tasks. Vendors receive timely alerts about threats that may lead to breaches. Escalation calls focus on communicating findings and best practices. The MAX outreach methodology emphasizes building win-win relationships with vendors as opposed to auditing them for security gaps. As a result, 57% of vendors are actively managing their external attack surface which outpaces the industry benchmark of 6%.

Increased operational resilience

The customer expanded its TPRM program beyond just IT-centric vendors to gain visibility into the threats impacting suppliers that are critical to its manufacturing and production. This strategy directly addresses the risk of a supplier incident having a downstream impact on their ability to operate and serve its own customers. Working with its purchasing organization to integrate assessments data, they are identifying and mitigating risks with these key partners.