

CASE STUDY

PayPoint

Third-Party Risk Management Program Transformed

How PayPoint Streamlined Third-Party Cyber Risk Monitoring with SecurityScorecard

Using the SecurityScorecard platform, PayPoint transformed its third-party risk management program from manual spreadsheets to automated, real-time visibility, enabling the IT Risk Team to better prioritize risk, support audits, and strengthen supplier accountability across the business.

Use Case



Cyber Due Diligence



Third Party Risk Management



Vendor Risk Monitoring

About PayPoint

PayPoint is a leading provider of in-store payment services and digital commerce solutions in the UK. They have over 30,000 convenience stores and multiple retailers as well as around 400 suppliers across the Group of which 100 are key to helping provide services to clients and consumers.

PayPoint facilitates essential consumer transactions across energy, parcel delivery, and financial services. Operating in one of the most targeted sectors for third-party breaches, PayPoint recognized the growing importance of managing cybersecurity across its supply chain.



Monitoring supplier cyber risk is so much easier with SecurityScorecard. It gives us real-time insight into the cybersecurity posture of our vendors, helping us focus on what matters most. We're able to direct resources where they're needed, respond quickly to emerging threats, and demonstrate our commitment to robust risk management during audits. It's not just a tool—it's become a core part of how we manage cyber risk across the business.

Paul Rogers
Head of IT Risk
PayPoint

Key Benefits

1. Automated monitoring of top 100 suppliers and expanded watchlist oversight
2. Real-time alerts and reports enable faster incident response
3. Improved focus on suppliers exceeding acceptable risk thresholds
4. Enhanced audit support for ISO27001, PCI DSS, and Cyber Essentials
5. Cultural shift in how IT and procurement teams engage with cybersecurity insights

The Challenge

Third-party risk is one of the most significant threats faced by PayPoint's cybersecurity team. Previously, the firm's third-party risk management relied on direct communication with suppliers and manual tracking through spreadsheets, making it time-consuming and difficult to scale. As PayPoint's vendor ecosystem grew, the team found it increasingly challenging to maintain regular engagement and visibility across all critical suppliers.

SecurityScorecard's 2025 Global Third-Party Breach Report found that **35.5% of all data breaches originate from third parties**, with many organizations unaware of the true origin of their incidents.

The Solution

PayPoint selected SecurityScorecard in 2024 after a competitive tender process to automate and enhance its third-party risk oversight. The IT Risk Team now uses the platform to continuously monitor the cybersecurity posture of its top 100 critical suppliers, while maintaining broader visibility with a watchlist.

Real-time alerts now allow the team to respond quickly to incidents and escalate them to relevant stakeholders when needed. The platform's reporting features also feed directly into management discussions, supporting operational decisions and resource prioritization based on evolving risk levels. With breach likelihood analytics showing that vendors rated "C" are 5.4x more likely to be breached than those rated "A", this insight has proven invaluable for targeting resources effectively.

The Results

Targeted Risk Management

SecurityScorecard enables PayPoint to identify which suppliers exceed acceptable risk thresholds, allowing the team to allocate resources more strategically and work with vendors to reduce exposure.

Stronger Cyber Governance

Insights from the platform are now embedded into regular reports shared with the Cyber Security Management Team. This integration has shifted the company's operational model toward more proactive risk management.

Audit and Compliance Support

SecurityScorecard has played a vital role in demonstrating PayPoint's third-party risk management maturity during ISO27001, PCI DSS, and Cyber Essentials audits. One of the key requirements of standards such as ISO27001 & PCI DSS is monitoring the risk inherent with the use of third-party suppliers.

SecurityScorecard has made it easier to demonstrate effective control in this area. Having automated alerts for breaches and drops in security scores provides much better and faster information for us to assess risk and take any necessary mitigating action.

Stakeholder Engagement and Culture Change

Senior leaders in Procurement and IT now use SecurityScorecard data when assessing vendors, fostering a more collaborative and security-conscious culture.

Looking to the Future

PayPoint sees major potential in expanding use of features like breach likelihood analytics and questionnaire workflows. The platform is also driving greater attention to PayPoint's internal cybersecurity posture, and reinforcing a broader culture of cybersecurity accountability across the company.