M&A Cybersecurity Due Diligence — Executive Summary

TARGET: B2B SaaS Company (Approximately 400 Employees)
ASSESSMENT SCOPE: Documentation Review, Management Interviews, and External Security Posture Assessment
ASSESSMENT PERIOD: Three Weeks | Pre-Signing

1. Transaction Overview and Assessment Scope

A pre-signing cybersecurity due diligence assessment was conducted to evaluate the target company's security posture, identify material cybersecurity risks, and assess potential implications for the proposed acquisition.

The assessment included a review of security policies, audit reports, system architecture documentation, and other materials provided through the transaction data room. Four management interviews were conducted to evaluate security governance, operational practices, and the maturity of key security controls. An external security posture assessment supplemented the documentation and interview findings.

The assessment was performed under the transaction's confidentiality agreement and was limited to information made available during the three-week diligence period. Internal vulnerability assessments, penetration testing, and direct validation of production security controls were outside the authorized scope. Accordingly, findings reflect the evidence reviewed and should not be interpreted as comprehensive technical assurance.

2. Overall Cybersecurity Posture

The target demonstrates an uneven level of cybersecurity maturity, with stronger security practices within its product engineering environment than across its corporate IT operations.

The product engineering function exhibits evidence of established security practices, including structured code reviews, dependency management, and cloud architecture controls. These capabilities indicate deliberate investment in securing the company's core technology platform.

However, opportunities for improvement were identified in enterprise identity and access management, privileged access governance, security monitoring, and third-party risk management. These gaps introduce operational and compliance considerations that should be addressed through confirmatory diligence and post-acquisition integration planning.

No evidence of a material historical cybersecurity incident was identified in the documentation provided. However, limitations in security monitoring, detection coverage, and historical log availability restrict the ability to independently validate the absence of prior compromise.

Overall Assessment: The target has a developing cybersecurity program with a comparatively mature product security function. Identified deficiencies appear addressable through targeted remediation and integration activities; however, certain risks warrant additional validation before closing or integration.

3. Material Cybersecurity Findings and Transaction Implications

HIGH Customer Security Commitments Not Fully Substantiated

ESTIMATED REMEDIATION EFFORT: MODERATE

A review of selected enterprise customer agreements identified contractual security obligations relating to encryption and access governance that could not be fully substantiated by the control documentation provided.

The discrepancy between documented contractual commitments and available evidence creates potential compliance and contractual exposure. Additional validation is necessary to determine whether the required controls are operationally implemented or whether substantive remediation is needed.

Transaction Implication: Potential contractual liabilities and customer assurance obligations may transfer to the acquiring organization. Confirmatory diligence should establish the extent of any control deficiencies, evaluate potential exposure, and determine whether specific remediation commitments or transaction protections are warranted.

HIGH Concentration of Privileged Production Access

ESTIMATED REMEDIATION EFFORT: LOW TO MODERATE

Privileged access to production infrastructure and critical credentials is concentrated among two senior engineering personnel. A formally documented emergency access mechanism and alternative administrative access procedures were not identified in the evidence reviewed.

This concentration creates key-person dependency and increases operational continuity risk, particularly during employee transitions or post-acquisition organizational restructuring.

Transaction Implication: The acquiring organization should consider this dependency when developing employee retention, knowledge transfer, and integration plans. Priority remediation should include documented privileged access procedures, appropriately controlled emergency access, and reduced reliance on individual personnel.

MEDIUM

Incomplete Security Monitoring and Detection Capabilities

ESTIMATED REMEDIATION EFFORT: MODERATE

The target maintains security logging capabilities; however, alerting coverage across the production environment is limited, and the available historical security telemetry does not provide sufficient visibility to support a comprehensive retrospective assessment.

These limitations may delay the identification of malicious activity and reduce the organization's ability to investigate historical security events.

Transaction Implication: A targeted compromise assessment is recommended before connecting the target's production environment to the acquiring organization's systems or networks. Post-acquisition priorities should include expanded detection coverage, centralized security monitoring, and improved log retention and investigative capabilities.

MEDIUM

Inconsistent Third-Party Risk Management

ESTIMATED REMEDIATION EFFORT: LOW

The target has identified material third-party service providers and subprocessors; however, the documentation reviewed did not demonstrate an established process for periodic vendor security assessments, ongoing monitoring, or formal risk reassessment.

This gap limits management's ability to consistently evaluate cybersecurity risks arising from external service dependencies.

Transaction Implication: The acquiring organization should incorporate the target's critical vendors into its third-party risk management framework. Initial activities should prioritize vendor inventory validation, risk classification, and assessment of material service providers.

4. Recommended Post-Acquisition Security Priorities — First 100 Days

A risk-based remediation and integration plan is recommended to address the identified deficiencies while maintaining operational continuity and minimizing disruption to the target's business.

The initial 100-day program should prioritize the following activities:

1. **Privileged Access and Operational Resilience:** Reduce key-person dependencies, establish controlled emergency access procedures, and strengthen privileged access governance.
2. **Security Compromise Assessment:** Conduct a targeted assessment of the production environment to evaluate indicators of compromise before initiating network or infrastructure integration.
3. **Contractual and Compliance Alignment:** Validate customer security obligations against implemented controls, document identified gaps, and establish remediation plans for outstanding commitments.
4. **Security Monitoring Enhancement:** Expand production detection capabilities, improve centralized logging and alerting, and establish appropriate monitoring and incident response procedures.
5. **Third-Party Risk Governance:** Implement a structured vendor review process aligned with the acquiring organization's security and compliance requirements.

The full diligence report assigns accountable owner roles, remediation priorities, and target completion windows to each recommended activity. Progress should be tracked through the acquisition integration governance process, with unresolved material risks escalated to the appropriate leadership stakeholders.

5. Executive Conclusion

The assessment identified a cybersecurity program with established product engineering security practices but less mature corporate security governance and operational controls. The most significant areas of concern relate to unverified customer security commitments, concentration of privileged access, and limited visibility into potential historical security incidents.

Based on the evidence reviewed, the identified findings do not independently establish a need to discontinue the proposed transaction. They do, however, justify targeted confirmatory diligence, documented remediation commitments, and risk-informed integration planning.

Recommended Transaction Position: Proceed with targeted confirmatory cybersecurity diligence, prioritize validation of contractual security obligations and production security exposure, and incorporate the identified remediation activities into the first 100 days of post-acquisition integration. Final risk acceptance should remain subject to satisfactory validation of material findings and review by the appropriate transaction stakeholders.

Disclaimer. This report is a fictional example prepared for illustrative purposes. All company characteristics, assessment activities, observations, findings, and conclusions are hypothetical and do not relate to an actual transaction. Related: M&A Cybersecurity · Private Equity & Portfolio Companies.