eSENTIRE

DATA SHEET

Vendor Risk Assessment

Identify Your Risk of a Third-Party Breach

CUSTOMIZED QUESTIONNAIRE DEVELOPMENT

Using industry standard frameworks, our security experts develop customized questionnaires designed to measure vendor risk unique to your business environment.

RAPID THIRD-PARTY DATA COLLECTION

Alleviating resource constraints, our security experts conduct third-party data collection on your behalf accelerating the evaluation process and ensuring response accuracy.

COMPREHENSIVE EVALUATION OF VENDOR RISK PROFILES

Illuminating areas of greatest risk, our security experts perform careful examination of responses and corrective actions against your organization's level of risk tolerance.

44% revealed that they had experienced a Third-Party-related data breach in the last year[1]

33% of organizations cited lack of internal resources as a challenge in evaluating Third-Party vendors[1]

48% of organizations that experienced a third-party breach reported significant business consequences (reputational damage, discontinued business, financial loss)[1]

As ever-expanding digital networks necessitate expansion of third-party and vendor access to sensitive data, the old adage that a chain is only as strong as its weakest link has never been more relevant from a security perspective. In an unfortunate tradeoff, business enablement from third parties and vendors in turn present business risk from a security perspective. Lack of visibility and end-to-end control of vendor security practices increase the potential attack surface for which organizations must account. Unfortunately the scale and expertise required to assess potential third-party risk presents challenges for most organizations with resource constraints.

Based on the eSentire Security Framework that is built on the foundations of NIST, eSentire Vendor Risk Assessment is designed to help resource constrained organizations:

- Determine risk identification and measurement criteria
- Categorize assessment data access against risk appetite
- Develop questionnaires for assessment
- Conduct comprehensive assessments
- Analyze data with comparisons against risk categorizations
- Define corrective actions for risky third parties and vendors
- Determine defensive adjustments to mitigate risk

[1] *eSentire/Spiceworks Third-Party Third-PartyRisk Research, January 2019*

FACTORS REQUIRING A VENDOR RISK ASSESSMENT:

- Exploration of acquisition or mergers
- Regulatory requirements
- Risk measurement of new partnerships, vendors or third parties
- Increased risk profile of existing vendors due to additional data access, public breach or Nth party access

WHAT DOES IT HELP YOU ANSWER?

- What should my criteria be for assessing my third parties and vendors against?
- What questions do I ask to gather the right level of information?
- How do I categorize my third parties and vendors against their potential to disrupt business?
- Do my third parties and vendors meet requisite security standards?
- How effective is my current third-party risk policies and controls to mitigate against risk?
- Who are my third parties and vendors sharing my data with?
- What measures do I require my third parties and vendors to put in place that is balanced with their risk profile?
- How do we track progress and improvement?
- What controls should we put in place based on the assessment?

HOW DOES IT WORK?

4-6 WEEKS

DEFINE

- Identify and scope the third parties to assess.
- Build out Vendor Risk questionnaire.

CONDUCT

- Facilitate the entire data collection process from distributing questionnaire, interaction with the third party, collection and assessment of responses.

MEASURE

- Compare findings against client-specific risks, industry standards, and the eSentire Security Framework.

ASSESS

- Executive summary on findings
- Recommendations on how to implement change

DELIVERABLES

- Measurement criteria and questionnaire development
- Execution of risk assessments on identified vendors and third parties
- All vendor interactions and necessary follow-ups handled by eSentire on behalf of the client
- Measurement of risk assessment data against client-specific risks, industry standards, and the eSentire Security Framework
- Assessments completed within a predictable 4-6 week timeframe
- Executive summary on findings
- Recommendations for programmatic improvement and progress measurement

MAKE THE CASE FOR AN ESENTIRE VENDOR RISK ASSESSMENT:

- Comprehensive third-party and vendor risk visibility
- Risk identification and categorization criteria unique to your business operations
- Satisfies third-party risk compliance mandates
- Frees up time and resources from compliance, risk, IT, and cross-functional teams
- Tracks, measures, and holds your third parties and vendors accountable for the risk they pose
- Guidance for continued improvement in third-party and vendor risk mitigation strategy and controls

eSENTIRE®

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.