Introduction

Purpose

Classify the vendor based on:

- Likelihood of the vendor providing inadequate service levels.
- Likelihood of the vendor compromising the organization's data
- Impact of the vendor not meeting the organization's requirements.
- The criticality of the vendor's services or products to the organization.

Identify missing or inadequate security controls, policies, and processes for maintaining agreed-upon service levels and protecting the privacy of the organization's data.

Collect and archive important vendor information:

- General information about the vendor and the services/products they provide.
- Vendor contacts.
- Contracts/Agreements.
- Evidence of implemented security controls.

Measure and communicate the added risk the vendor imposes on the organization.

Scope

There are multiple areas where vendor deficiencies can threaten service levels and privacy. The following areas were evaluated.

- Policies and processes
- Regulatory compliance
- Security and privacy controls
- Business continuity and recovery plans
- Breach disclosure
- Service level agreements
- Financial stability
- Vendor location

Mission

This assessment was conducted using VendorWatch, a third-party risk assessment tool that identifies gaps in the vendor's existing controls, policies, and processes that could negatively impact the organization's business delivery, reputation, and competitiveness. Using defined standards for the organization's vendors as a benchmark goal, this assessment is part of an ongoing process to gauge the vendor's current state and its progress toward meeting that goal and ensure that it adheres to the defined standards once that goal is reached. This risk management process aims to reduce the probability of loss or significant reduction of the availability of critical services/products to the organization and the unauthorized disclosure of personal data (employee or customer) or trade secrets. This is accomplished by providing evidence-based information and analysis to stakeholders to make informed decisions regarding vendor options.

Approach

The evaluation, the roadmap to improvement, and the sustained adherence to standards are managed using RiskWatch's VendorWatch application. Management is based on the ISO 31000 risk management process consisting of six cyclical phases.

Phase 1 – Establish Context: The organization identified a vendor that required assessment. Vendor contacts with knowledge of the vendor's existing security controls, policies, and processes were included in phase 2 to provide information about the vendor.

Phase 2 – Risk Identification: Checklist surveys designed to identify if all required controls are in place by the vendor were distributed by the VendorWatch application to the contacts selected in Phase 1. These vendor contacts answered the survey questions and provided additional information as comments, documentation, and visual evidence in screenshots, diagrams, or charts.

Phase 3 – Analysis: The data gathered from the completed surveys are processed using VendorWatch for analysis. Survey question weighting is used to measure the impact of responses deemed non-compliant with the organization's defined security standards.

Phase 4 – Evaluation: VendorWatch identifies any security and compliance gaps based on the survey results and computes a Vendor Risk Score based on these factors:

- Criticality of this type of vendor to the organization's business functions.
- Potential consequence of this vendor's services or products being unavailable.
- Likelihood of threat actors targeting the vendor.
- General level of reliability that this type of vendor has provided historically.
- The vulnerability level of the organization's operations due to the vendor not meeting standards.

The organization can compare the Risk Score against a predetermined risk tolerance level to determine what remedial action the vendor should take to do business with the organization. The organization can also compare the Risk Score with competing vendors to help rank them based on risk.

Phase 5 – Treatment: The organization prescribes remedial recommendations for the vendor, and an action plan is developed and managed through VendorWatch.

Phase 6 – Monitor: The organization conducts periodic reassessments to monitor the continued adherence to the organization's standards and the maintenance of an acceptable level of compliance.