Taking a proportionate approach to managing supplier risk reduces security exposure

Problem statement

External auditors had identified that a major insurance and pensions client was failing to meet key expectations in relation to third-party supplier security. The client was exposed to a high risk of compromise or data loss due to third-party access to its sensitive information, its network, and any externally procured software. Regulators and auditors hold organisations fully accountable for controls operated by suppliers on their behalf, and there is ever more focus on operational resilience within the financial sector.

The client had an incomplete picture of its suppliers, particularly in relation to their inherent security risk classification. This exacerbated the situation, as without a clear understanding of risk it was difficult to target assurance review activity. Assurance reviews determine how controls around the availability, transfer, storage, and processing of sensitive data are operated.

Auditors reported significant third-party security risks

Our approach

i-confidential's supplier profiling solution was deployed first, in order to determine the inherent security risk classification for the client's chosen suppliers.

We worked in conjunction with the client's IT Security team to acquire details of the suppliers to be profiled and their associated relationship managers, who were sent a straightforward questionnaire to fill in. Within three weeks, the returns were collected, validated, and rated to identify the client's highest-risk suppliers.

The output of the supplier profiling activity directly informed the scope of supplier assurance. The highest-risk suppliers received an assurance review, again via a questionnaire, to identify the scope and operation of their security controls. Based on the response, a site visit was undertaken.

> "i-confidential's supplier profiling solution identified where the client was most exposed…"

Following the visit, we produced a findings report, identifying non-compliances and rating these against the client organisation's risk appetite. Suggested remedial actions were also documented.

Management information, graphically describing the status and activity for each supplier, was delivered to the client throughout the assurance phase. This enabled accurate and timely reporting to key stakeholders in the organisation.

The outcome

i-confidential's supplier profiling solution identified where the client was most exposed to data loss and compromise from third-party suppliers by providing an updated view of their inherent security risk. Based on those results, assurance activities were carried out to identify non-compliance control gaps and remediation steps for the highest-risk suppliers.

Over time, the control gap tracker evolved to become the remediation tracker, allowing the client to monitor progress on various recommended risk mitigations.

The security team could then show evidence that third-party risk was moving back within risk appetite.

i-confidential
Cyber Security & Information Risk Specialists ®