

## Vendor Security Management Programs

Written by Dave Hogan

### Issue

- Several organizations have been facing a challenge in assessing, improving and verifying the implementation of appropriate security controls at firms with whom they have network connections or data interactions. The requirements of several regulations also make this an urgent concern.
- Typically firms face four challenges when they approach the vendor management issue
  - What best practices to use as a basis for assessment and should these be customized based on size, and criticality (function and level of interaction)
  - Which assessing mechanism to use – rely on self reporting, use internal resources to assess or require a third party assessment
  - What actions should be mandated if controls are found to be deficient? As a corollary what penalties should be imposed and on what basis
  - Who will bear the expense of the assessment and how will this decision impact compliance and meeting deadlines
  - What happens if the vendor has a pre existing assessment

### Solutions

We can take the questions above in order:

#### **What best practices to use as a basis for assessment and should these be customized based on size, function or level of interaction?**

This can be addressed in three ways:

1. Segment the list of companies by criticality (level of interaction and function) and size and then create a custom set of security control benchmarks for each segment. Ideally the number of segments should not exceed three. This option will require resource commitment and expertise to research the various standards, evaluate applicability and to rank controls by criticality. The advantage of this approach is that there is an in context evaluation of controls.
2. Segment the list of companies by criticality and size and determine an uniform set of controls to evaluate against (either self created or adopting existing best practice), only prioritizing by segment criticality
3. Use experts (either internal or third party) to conduct evaluations that are customized at the time of assessment but use a general best practice guideline, for e.g. based on ISO17799, PCI, or GLBA.

**Which assessing mechanism to use? –Should you rely on self reporting, use internal resources to assess or require a third party assessment?**

Again there are various options for this.

1. A self reporting mechanism that uses a scoring algorithm to rank companies can be created and delivered either via the web or through paper, with only an external scan used for independent verification, regardless of segmentation above. Obviously, this approach lacks the rigor of verification.
2. A combination of self reporting and on site assessments, depending on segment, can be implemented with internal staff with expertise going on site. The disadvantage here is primarily that significant technology, people, training and money have to be committed to be successful
3. A third party with expertise can be contracted to go onsite for critical segments and asked to conduct less rigorous (possibly remote) assessments on less critical segments with self reporting used for the least critical segment. This reduces commitment to a financial decision
4. All segments can be required to undergo an onsite assessment. Again the key decision point here is related to budget.

*NOTE: Some Audit standards, such as PCI, categorize and lay out the mechanisms an organization must use to conduct a valid audit.*

**What actions should be mandated if controls are found to be deficient? As a corollary, what penalties should be imposed and on what basis?**

This is a particularly tough issue to deal with. Naturally most companies do not want critical vendors and partners to have inadequate security controls and if after going through the effort of conducting an assessment the controls are found to be deficient then insisting upon timely remediation is a challenge.

The ideal approach here is to use both carrot and stick. The carrot usually is in the form of assistance and expertise in the remediation process and the stick is the negative effect on the relationship. In severe cases one or the other can be enhanced. For e.g. if a particularly critical vendor of strategic value needs to improve security greater incentives can be offered with training, documentation, actual implementation help etc. On the other hand if a partner/vendor refuses to see the value in improving security, penalties in the form of fines, changes to contract increasing their liability, insurance requirements etc can be brought into play.

Ideally the assessing authority (internal or third party) will provide the necessary remediation assistance and most vendors are happy to have access to the expertise and are interested in improving their security posture. However, remediation assistance by internal staff tends to be a resource hog as the scope is unclear and the expertise has to be retained.

**Who will bear the expense of the assessment and how will this decision impact compliance and meeting deadlines?**

This is by far the most vexing concern in creating a vendor management program. This decision is naturally very context sensitive and depends on the kind of relationship that exists with the vendor/partner and the ease of substitution. If a choice is made to adopt self reporting or conducting assessments using internal staff, then the expense is automatically borne by the originating company. In the case of a third party vendor being used, there is an option to pass the expense on to the assessee. Assuming a third party scenario, most segments of

vendors/partners can be expected to bear the expense of the assessment with the proviso that they are directed to a assessing party that the originating company is familiar with and is comfortable with the prices charged. The drawback to this approach is that deadlines are now in the hands of the vendors and cannot be strictly enforced without seeming unreasonable at times. Also the third party assessment firm is faced with a minor conflict of interest, in that the paying party and the party interested in the report may have differing expectations. Proper management can mitigate these concerns. In cases where the vendor is critical and not easily substituted, the originating company finds it easier to ensure deadlines are met and compliance is satisfactorily achieved if they control the purse strings. In general, depending on the leverage available, getting the assessee to pay works up to a point, but ultimately several firms has had to pay for assessments on their own. It is important that all costs are taken into account including the increased cost of deciding to take on the payment responsibility later on which could result in budget concerns and time constraints. Ideally a decision should be made up front and followed through. Firms that decide to pay for the program on their own have naturally been able to exercise greater control on expense as well as timeline and quality.

### **What happens if the vendor has a pre existing assessment?**

If the vendor has a pre existing assessment, the standard used to conduct the assessment is relevant. If well-recognized and broad standards are used (for e.g. ISO 17799, PCI, COBIT, COBRA, BITS etc) then this assessment can be reviewed to ensure that essential controls are in place. However if the assessment is merely a scan result or a penetration test, then further evaluation is needed. In either case the costs of evaluating a vendor who has a pre existing assessment are lower than otherwise.