NOTICEBORED

Management briefing on

Metrics relating to the protection of trade secrets

Summary

This is a proposal for information security management metrics to measure the effectiveness of the controls protecting our trade secrets.

Introduction

Measuring and reporting on the information security controls protecting our trade secrets allows us to monitor their performance, identify control improvement opportunities and gain confidence that the controls are adequately addressing the associated risks. Metrics are a necessary part of any effective management system, providing facts to enable better management decisions.

In common with many other aspects of information security and risk management in general, if the controls protecting trade secrets are highly effective, we expect a negligible level of incidents. However, given that the 'baseline' level of trade secret incidents (*i.e.* the level before the information security management system was implemented) was relatively low and that such incidents were sporadic, it is difficult to measure the effect of the controls purely by the number and/or extent of incidents alone. Therefore, we propose additional metrics on the efficiency of the controls.

Requirements for the protection of trade secrets (targets and limits)

At a high level, the control requirement is to minimize the number and/or extent of losses through unauthorized or inappropriate disclosure of trade secrets, but without incurring excessive control costs (*i.e.* we are interested in the *net value of the controls*). Rather than set an absolute target, it may be more appropriate to think strategically in terms of a percentage annual improvement in the net value *e.g.*:

- A reduction in the gross costs of incidents arising from the unauthorized or inappropriate disclosure of trade secrets, taking account of number and severity of incidents, of at least X% year-on-year. The costs are likely to include estimates for lost business and customer defections arising from reputational damage, costs incurred in investigating and resolving incidents, legal action against perpetrators *etc*.
- Increasing the total cost of controls protecting trade secrets by no more than Y% year-on-year.

Management would need to define and periodically review the target values of X and Y, with advice from the Information Security Manager and other interested parties.

Be aware that measuring and accounting for the costs of incidents and controls is no simple matter, and that the costs of measurement will increase dramatically if too much precision is required – in other words, the 'law of diminishing returns' applies.

Measuring and reporting on protection of trade secrets (metrics)

Incident metrics

Many organizations track and report the number and severity of information security incidents, for example using statistics collected routinely by the IT Help/Service Desk from calls and incidents notified to them. So long as trade secret incidents are few and far between, corporate functions such as IT, Finance, Risk Management and Marketing should be able to review each one to determine or estimate the associated costs. At the very least, it is usually feasible to assign each incident to a simple category (*e.g.* high, medium or low impact), but it is always worth including a few words of explanation about each incident in the management reporting.

Metrics for physical security controls

Most physical access controls (perimeter walls and fences, door access control systems, security guards *etc.*) can be considered part of the corporate infrastructure with benefits in reducing many types of incident (such as theft and criminal damage to physical assets), not just theft of intellectual property. If physical security costs are tracked, management may allocate an arbitrary proportion of the total to the protection of trade secrets. Any physical control investments that are specifically related to the protection of trade secrets (*e.g.* safes, intruder alarm systems *etc.*) should be accounted for in full.

Metrics for legal and ethical controls

Again, the system of legal and ethical controls has value in reducing many types of incident, not just disclosure of trade secrets, so cost allocation is partly arbitrary. Specific legal costs relating to the investigation of trade secret incidents and prosecution of the offenders should be collated and reported, along with any identifiable costs incurred in negotiating non-disclosure agreements or contractual terms. Likewise the cost of specific ethical controls (such as awareness and training in ethical matters, creation and promotion of policies *etc.*) may be allocated appropriately by management.

Metrics for technical (IT security) controls

Aside from allocating some proportion of the general technical infrastructure security controls (such as intrusion detection and prevention systems), specific investments to protect trade secrets (*e.g.* encryption of the research and development systems and customer databases *etc.*) should be measured and reported.

Metrics for procedural and managerial controls

Compliance measures (such as the number and extent of non-compliances) may be used to measure the extent to which employees comply with corporate policies, standards, procedures and guidelines relating to the protection of trade secrets. In addition and especially when the information security management system is relatively immature, it may be worth measuring the extent to which trade secret controls are documented in policies, standards, procedures and guidelines.

Management confidence metrics

It is possible to survey management regarding their confidence in the system of controls protecting trade secrets. This form of metric has two key advantages: it is simple to perform (see example survey question below) and simultaneously acts as a means of raising awareness of the issues.

How confident are you that protection of trade secrets meets the business needs? Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

|----------+----------|

Not at all. Not quite enough | Just about enough Absolutely!

Comments *e.g.* what led you to this score? Have there been particular situations or incidents that influenced your decision?

Measure each response using the percentage scale to calculate a mean score. Provided enough survey forms are completed (ideally more than 30), the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials.

Reporting

We have probably all seen the voluminous IT service metrics produced by some organizations – pages and pages full of busy tables and colorful graphs. They are often seen cynically as a defensive mechanism to conceal or gloss-over problem areas and justify claims that Service Level Agreements or contractual terms have been met. However some managers genuinely prefer this style of report. They like to check the details.

Others prefer high level summaries, red-amber-green 'traffic light reports' for example. These can either be written summaries with colored blobs identifying the status of each section, or graphical reports using the relevant colors. An effective reporting approach might be a 'heat-map' consisting figuratively of a background outline representation of the entire suite of key business processes, with transparent overlays for various aspects including protection of trade secrets. Various elements would be picked out on each layer in color, with annotations to explain the specific ratings and highlight particular improvements or outstanding issues. These might be presented on a web page with tabs for each overlay.

For more information

Please visit the information security intranet website for further information. Additional security awareness materials and advice on this topic are available on request from the Information Security Manager. NIST's Special Publication 800-55, a 99-page "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics.