NOTICEBORED

Management briefing on

Security compliance metrics

Summary

The metrics described below can help improve the organization's compliance with information security obligations embodied in laws, regulations, standards, contracts and policies.

Introduction

Given the ever-increasing range of security-related obligations enshrined in laws and regulations, coupled with internal/commercial pressures to achieve compliance with best practice standards, policies *etc*., compliance activities can consume a significant amount of effort and yet still represent risks to the organization due to the residual level of non-compliance. The organization's stakeholders might ask "How compliant are we?", a deceptively simplistic question that is extremely difficult to answer definitively.

Security compliance requirements (targets and limits)

100% compliance with all security obligations might at first seem like a sensible target but is almost certainly unachievable in practice and is likely to be unreasonably costly. 100% compliance with *mandatory* security obligations is a bit closer to the mark but even that is a tough target, and what target would you set for discretionary obligations – 50%? 80%? It's an arbitrary figure that may not get the respect it deserves.

Instead of absolute targets, consider setting relative targets (improvement goals), such as "Ten percent fewer non-compliances than in the previous reporting period". Here, the percentage value is still arbitrary but sets an expectation for improvement whose magnitude reflects the gap between the current compliance level and 100% (*i.e*. it is asymptotic).

Another option is to set benchmark targets *e.g*. "We will be in the top quartile of organizations in our industry for legal and regulatory compliance", although these imply the need for comparative data on other organizations that may be difficult and costly to obtain since very limited compliance information is ever published.

Measuring and reporting on security compliance (metrics)

Metrics relating to noncompliance

- Number of security noncompliance incidents in the period, reported as a number, trend or proportions by significance (*e.g*. divided into serious, important or trivial categories, with commentary on the worst cases and/or common causative/contributory factors).
- "Security compliance status" measured across the organization by management reviews and audits and compared to the previous reporting period and/or targets set by management.

Metrics relating to meeting compliance obligations

- Time, effort and money spent on achieving compliance, perhaps reported by the nature of the obligations (*e.g*. legal/regulatory/contractual/internal) or ranked by the risks of noncompliance (to focus attention and effort on the most significant obligations)

- "Compliance lag" *i.e.* the total number of days that compliance activities are overdue, analyzed across the business or by type of obligation or by risk

Metrics relating to compliance processes

- Time, effort and money spent on compliance-related activities such as compliance reviews/audits, disciplinary action, legal and other enforcement actions.
- Efficiency metrics such as the proportion of employee time spent on compliance assessment, improvement and enforcement versus other more productive business activities.

Confidence metrics*

A rather different style of metric involves surveying management regarding their confidence in security compliance, for example:

How confident are you that the level of security compliance 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 noncompliance situations or incidents that influenced your decision?

Confidence metrics like this give a guide to the level of compliance effort that management feel is appropriate, and hence can help set priorities, but obviously they depend on managers understanding their compliance status and giving honest responses. [Some would call this an indicator not a metric]. The comments can be just as useful as the statistics, however.

Reporting

Compliance reporting includes two aspects: the statistics and the commentary. The statistics give a guide to the compliance status relative to absolute or comparative targets and previous performance (trends), whereas the comments help put noncompliance incidents and compliance activities in a business context. These are complementary, mutually supporting approaches. You should put just as much effort into both to ensure that managers understand the priorities and support additional effort (and perhaps investment in automated controls) where necessary.

Conclusion

The metrics and reporting methods noted in this paper have hopefully stimulated you to derive creative and useful measures for your own situation. Do not neglect the value of having someone present and discuss reports with management. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides. Why not present and discuss these ideas with your management and seek their opinions, bringing to the table some prototype reports

* It is possible to automate this kind of survey on the intranet *e.g.* see www.2ask.de (German language)

in one or more formats to stimulate discussion and clarify their objectives? Better that than to prepare your reports blindly with no idea whether it is even read, let alone useful for management.

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 and Andrew Jaquith's book "Security metrics: replacing fear, uncertainty and doubt" sets out a robust case for scientific measurement disciplines in information security.