NOTICEBORED

Management briefing on

Physical information security metrics

Summary

This paper outlines the design/selection of metrics relating specifically to physical aspects of information security.

Introduction

Physical protection of information assets is every bit as important as the protection afforded to computer data by logical controls, given that there are significant threats (such as fires, floods and thefts), vulnerabilities (*e.g*. the sensitivity of electronic devices to power glitches and overheating, and the flammability of paper records) and impacts (severely damaged or destroyed systems and data may be impossible to recover economically, and unauthorized disclosure of information on stolen systems or papers may cause legal, regulatory and commercial repercussions). Measuring and reporting on them is an important element of tracking risks and promoting control improvements.

Physical information security targets and metrics

Incident-related

Working backwards from the end-goal, it is possible to set targets relating to the maximum number of information security incidents with a physical cause *e.g*. how many fires, floods or thefts occur in the year. The absolute number of incidents is only part of the story, however: their severity is also of concern. If statistics are gathered routinely on the total costs of information security incidents, these may make better targets either in absolute or relative terms (*e.g*. "No individual losses above $50k", "Cumulative losses below $200k" or "Total losses below the level experienced in the previous year").

Control effectiveness/efficiency

It is quite easy to spend a small fortune on physical security controls in a glorious but ultimately vain attempt to minimize or eliminate physical incidents but the 'law of diminishing returns' needs to be taken into account. Control costs can usefully be tracked in categories such as:

- Specification and design of physical controls including periodic reviews and re-design work
- Implementation costs including procurement and installation/commissioning costs
- Ongoing operational costs including management overheads, support *etc*.

There is a risk of double-accounting unless care is taken to differentiate physical control measures whose primary purpose is to protect information assets, from other physical controls protecting fixed assets *etc*.

Management confidence metrics

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

How confident are you that physical security 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?

It is a simple matter to measure percentage values from each response and calculate the 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

Depending on the size of the organization and the amount of information available (*e.g.* the number of incidents and the extent of financial data on incident and control costs), it may be appropriate for the Information Security and Site Security/Facilities Managers to collectively monitor and respond to the metrics throughout the year, reporting summary statistics and progress to management every three, six or twelve months. If annual reporting is deemed appropriate, it remains valuable for those responsible and accountable to track the accumulating figures continuously in order to spot and respond to adverse trends before reporting day.

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 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.