NOTICEBORED

Management briefing on

Office information security metrics

Summary

This briefing outlines potential metrics for measuring and improving office information security.

Introduction

There are numerous information security considerations for a typical office or similar workplace, reflecting the variety of information security risks and the corresponding physical, logical and procedural controls. Offices can be viewed as 'information factories' where information security controls are essential to keep the factory, it's machine tools and production processes running smoothly, efficiently and profitably. Metrics can help by identifying constraints and potential disasters waiting to happen.

Office information security requirements (targets and limits)

As with other aspects of information security, it is technically impossible to negate all office security risks and completely prevent all incidents. Office security targets, then, are perhaps best developed in the form of year-on-year incident reductions (*i.e*. fewer and/or less damaging office security incidents) through systematically planned security improvements. If, for example, there have been twelve physical security incidents affecting corporate offices in the past year, and if that number is considered too high by management, then additional security guard patrols or other countermeasures may be implemented with the goal of reducing the number of incidents by one quarter this year and a further quarter next year. Simply setting the improvement targets without making the corresponding control improvements (which will often incur additional revenue expenses and perhaps capital investment) will achieve little.

Potential metrics for office information security

Office physical security metrics

- The number of physical security incidents affecting corporate offices, and perhaps other similar workplaces, measured monthly by Site Security and reported quarterly to the Information Security Manager and annually to the Security Committee
- The proportion of offices that have been security reviewed within the past three years [or according to policy and practice], along with the number of office physical security control improvements that have been identified as necessary but not yet fully implemented (potentially with a breakdown as to their nature and the costs involved if management support is needed for further investment)

Office logical security metrics

- The number of IT or information security incidents reported to the IT Help/Service Desk in which the incidents took place or affected corporate offices, measured and reported monthly by the Service Desk to the Information Security Manager, and reported annually to the Security Committee along with a breakdown by type and, ideally, consequences (both direct costs and other non-financial or indirect impacts)

Copyright © 2008 IsecT Ltd.

- 'Vulnerability scores' from automated desktop and laptop vulnerability scans that identify unpatched software and other technical vulnerabilities (*e.g.* using the Secunia PSI software)

Office procedural control metrics

- Proportion of office information security incidents that involve non-compliance with documented office security policies, procedures or guidelines
- Number of man-days expended on security awareness, training and educational activities relating to office security matters

Audit metrics

Comparative audits or management reviews of information security controls across all or a representative sample of offices will generate findings and management reports. While it is simple to report the absolute number of findings and corrective actions, it would be more informative to give a breakdown showing the types and gravity of the control issues noted.

Confidence metrics

It might make sense to survey office managers regarding their confidence in office information security controls, for example:

How confident are you that our level of office information 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.* are there any office security improvements you would recommend?

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.

Conclusion

Office information security is a more general topic than most, hence the metrics tend to be broad. However, it is possible to identify more specific metrics that can help drive improvements.

For more information

Please visit Information Security's intranet Security Zone for further information. Additional security awareness materials and advice on this topic are available from the Information Security Manager, Site Security or Facilities.

Copyright © 2008 IsecT Ltd.