NOTICEBORED

Management briefing on

Privacy and data protection metrics

Summary

This paper discusses the selection of information security metrics to measure the status of privacy and data protection-related controls.

Introduction

Unauthorized disclosure of personal information is the main concern with privacy and data protection. Privacy lapses can affect employees as well as customers *etc*., since the organization holds personal data on staff. Disclosures can occur through breaches at the organization (*e.g.* database hacks or accidental 'leakage' of information) or at third parties (such as IT outsourcers, communications providers *etc*.). Legal or regulatory enforcement action stemming from complaints by data subjects can lead to the organization being prosecuted, fined and forced to undertake corrective actions, increasing the organization's costs and creating adverse publicity/brand damage.

Privacy and data protection requirements (targets and limits)

Privacy and data protection controls essentially fall into two camps: those required for legal and regulatory reasons, and those required for commercial and ethical reasons. The former imply the need for compliance measures against external standards, while the latter require compliance to internal security, risk management and control requirements.

Legal and regulatory compliance

Legal and regulatory compliance is far more than simply a matter of management asking "Do we comply with the privacy and data protection laws (yes/no)?" Multinational corporations and those which routinely transfer personal data between countries have to comply with a complex and often confusing mesh of laws and regulations. For further details, consult corporate counsel! In short, the obvious target of achieving "Full compliance with our legal and regulatory obligations on privacy and data protection" may be practically unattainable, at least without incurring excessive control costs. A more reasonable target, then, might be "Full compliance with our legal and regulatory obligations on privacy and data protection, where cost-justified on the basis of risk". Partial or complete non-compliance with the privacy laws in, say, Rarotonga might be commercially acceptable whereas non-compliance with the European data protection laws or HIPAA might lead to commercial suicide.

Compliance to corporate privacy and data protection requirements

Compliance to internally-defined privacy requirements involves policies and ethical matters, neither of which is easy to measure. The issue of control costs again perhaps implies the need to specify targets in terms of their cost-effectiveness and risk mitigation (*e.g.* "Full compliance with our policies and ethical stance on privacy and data protection issues, where cost-justified on the basis of risk").

An alternative approach might be to look purely at the commercial aspects, leading to targets such as "No privacy or data protection incidents costing more than $X in aggregate in a single financial

year, or more than $Y in any single event" where the values of X and Y are determined by management in relation to other similar potential losses.

Potential privacy and data protection metrics

Control-related metrics

The potential targets noted above are intended to ensure that privacy and data protection controls are cost-effective, meaning of course that we ought to be measuring the control costs and their effectiveness. This line of thinking leads to the following types of metric:

- Aggregate costs for privacy and data protection controls in any financial year, including specification, design, testing, implementation, operation and management costs. In practice since many such information security controls will be generic rather than specifically related to privacy and data protection, it might be more sensible to consider specific privacy costs (such as encryption of customer and employee databases) plus an allocation of the 'infrastructure security' costs,
- Control effectiveness can be measured by the number and severity of incidents but this is of course a lagging indicator. A leading indicator might be the number and severity of privacy and data protection-related issues raised by audits, management reviews *etc*.

Compliance metrics

- Relative proportions of jurisdictions in which we operate for which our privacy and data protection obligations have been (a) formally identified or determined by assessing local laws and regulations; (b) made fully compliant; (c) independently certified or assessed as compliant by qualified auditors, certification bodies, regulators *etc*.
- Number of legal and regulatory non-compliance warnings or notifications received in the current calendar or financial year.
- Number of privacy and data-protection complaints received in the current calendar or financial year, perhaps differentiated by their status (full upheld/justified, partially upheld/justified, rejected/unjustified).

Confidence metrics

Since privacy is a serious issue for data subjects (*i.e*. the individuals whose personal data we process) as well as for the organization, it may be worth surveying their confidence in our privacy and data protection, for example:

How confident are you that our privacy and data protection arrangements meet your personal 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 privacy-related 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

Annual statistics are best reported by graphing the cumulative value by month or quarter, starting from the origin at zero. Compare actual data against the annual target, shown as a straight line increase through the year, to project whether the organization will fall short, meet or exceed the targets. If you have the data, another way to present the information is to compare last year's figures with this – an approach that naturally promoted year-on-year relative security improvements.

Proportional statistics are effectively reported using pie charts where the whole pie (360°) equals 100% and each component is represented by a slice (3.6° per percent). Luckily, spreadsheet or presentation software makes short work of the mathematics!

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.