NOTICEBORED

Management briefing on

Information security and risk management metrics

"A few well-chosen metrics can be a huge help in monitoring controls and measuring their effectiveness"

Clint Kreitner, SANS

Summary

This paper discusses a range of potential targets and metrics to improve the management of information security controls and risks. We are not suggesting that all of these are necessary or appropriate for any organization, rather that management should consider the suggestions and then select 'a few good metrics' to use as part of the overall corporate management framework for information security.

Introduction

Information Security Management can be viewed as just another function or department to which the standard range of management practices and activities apply. Certainly budgeting, man-management, planning and general management reporting are common issues that are not considered much further in this paper. Conventional operational metrics regarding proper management of financial and human resources, for example, apply to Information Security Management and Risk Management just as much as they do for any other corporate department or function.

This paper concentrates more on metrics that are unique to Information Security Management and Risk Management functions. [Furthermore, metrics relating to the governance of information security (including aspects such as measuring Returns on Security Investment) will be discussed next month rather than here.]

As usual, we start by considering the kinds of targets that might be appropriate to the management of information security risks, and then discuss the corresponding metrics. Remember that this is a discussion piece: if you would prefer to set other targets and metrics in this area, feel free to discuss them with the Information Security Manager, Chief (Information) Security Officer and your peers. Creative ideas and suggestions based on your experiences are particularly welcome.

Information security and risk management targets and metrics

In order to propose a set of targets for information security and risk management, we'll examine some of the function's key rôles and responsibilities.

Business enablement

Information security can be a business enabler. This goes beyond the obvious but rather negative target of security not 'getting in the way of business' into the more positive realm of security 'facilitating the exploitation of new business opportunities'. It is vaguely conceivable that an organization's strengths in information security might encourage management to launch a new product or attack a new market segment. More likely however is the situation that new business

development proceeds with minimal concerns from management about security of the IT infrastructure and processes that underpin it, in full knowledge of the risks (ignorance is not an effective control measure!).

This line of thought suggests targets and metrics such as:

- Close involvement and alignment between information security and business departments when planning new IT systems, business processes *etc*., particularly in connection with new products or new markets (metric: survey of project managers);
- Completion of business impact analysis no more than a month after all business case approvals (metric: compare dates on BIA reports to dates on the corresponding business cases).

Information security as a business differentiator

Taking the view of security as a differentiator between comparable organizations suggests targets such as 'being perceived as more secure than our peers and competitors'. In some cases, information security is an important quality or component of the organization's products (goods and/or services), not just for companies selling overt "security" products such as antivirus software. Confidentiality, integrity and/or availability of customer information, for example, may be vital aspects of the customer experience and hence customer perceptions about the organization's security stance may affect the brand. This is borne out to some extent by the experiences of organizations that have suffered serious security breaches affecting customer credit card numbers, Social Security Numbers, health records *etc*. [Note the explicit use of 'perceptions' in this target. Whether or not they match reality, the *perceptions* of customers and other stakeholders may have a major influence on the organization's image and hence success. This applies equally in the government and not-for-profit arenas as in commerce, and implies that 'perceptions management' should be part of the contingency plans, hence the need to maintain a professional Public Relations function even in a disaster scenario.]

Potential targets and metrics include:

- Customer/stakeholder perceptions that the organization is no less secure than peers and competitors (metric: customer/stakeholder survey);
- Incremental year-on-year improvements in customer/stakeholder perceptions about the organization's security status (metric: customer/stakeholder survey).

Controlling business processes

Information security has a rôle in helping to control business processes, for example limiting or preventing unauthorized access, or providing reliable and complete audit trails. This leads to the concept of information security and risk management providing 'services' to the rest of the organization, and managing its internal customer-supplier relationships.

Potential targets and metrics:

- Positive and ideally increasing 'internal customer feedback' on the performance, approachability, professionalism and general quality of interactions with Information Security and Risk Management (metric: internal survey results);
- Decreasing number of identified information security risks relating to inadequately controlled business processes (metric: analysis of risk inventory).

Compliance

Information security supports compliance with a range of laws, regulations, standards and policies. Some explicitly mandate security controls (*e.g*. privacy and data protection laws) while others imply the need for adequate security measures in the context of corporate governance, ethics and propriety (*e.g*. Sarbanes-Oxley and finance/corporation acts). While noncompliance with technical standards and corporate policies in relation to information security is discretionary and therefore

unlikely to lead to sanctions as severe as fines or jail terms for executives, noncompliance still devalues and discredits standards and policies.

Potential targets and metrics:

- No substantiated compliance issues raised by external auditors, regulators, prosecutors *etc*. in relation to mandatory information security obligations (metric: management review);
- Downward trend in the number of exemptions or exceptions to corporate policies, standards *etc*. authorized by management (metric: analysis of the security exemption/exceptions database).

Confidence and assurance targets

This is a tough one. Information security and risk management functions are generally expected to keep risks under control, to the extent that management does not lose sleep over the possibility of security incidents. The problem is that there this objective can be met in two ways, by:

1) Understanding and controlling all relevant information security risks; or
2) Failing to appreciate (or even worse hiding) information security risks from management.

To a large extent, the way things work depends on the quality and integrity of the information security and risk management professionals but management's attitude towards information security is equally important. Management support is crucial in terms of 'not shooting the messenger' (reacting badly to news of security risks and issues), dealing positively with identified risks and investing appropriately in information security.

Potential targets and metrics:

- Increasing management confidence in the information security and risk management function/s (metric: internal management survey);
- No nasty surprises in relation to information security, such as totally unanticipated security incidents (metric: management review).

Management confidence in the assurance rôle performed by information security and risk management can be surveyed through questions such as this:

How confident are you that our information security and risk management arrangements meet 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 simple 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 provide useful feedback and quotations for management reports and other awareness materials.

Using security targets and metrics

Firstly, there is the above-mentioned issue of determining which (if any!) of these targets and metrics are applicable to the organization. If we assume that management has discussed and chosen 'a few good metrics', the next issue is how best to use them in practice.

There is an argument for assigning the work involved in gathering, analyzing and reporting information security metrics to an independent function. While this will probably increase costs, it also reduces the possibility of fraudulent or accidental errors in the statistics (although if this is a genuine concern in relation to such a trusted area as information security and risk management, the organization evidently has serious issues that metrics alone will not solve! Allowing management to 'drill down' to the details also reduces the risk). More importantly, though, it allows the use of specialists, for example in statistical analysis and survey design. A compromise might involve relying on the Information Security and/or Risk Managers to self-report but encouraging them to use commercial statistical analysis/survey services or tools.

These days, management reporting frequently involves some form of balanced scorecard or dashboard, typically on the corporate intranet or as part of an executive information system. Information security metrics should ideally be integrated alongside other metrics.

One more thing to consider carefully is the use of targets and metrics as personal goals, perhaps linked to annual bonuses for information security and risk management professionals. Such an approach brings home the need to design metrics very carefully to avoid unintended consequences from employees unintentionally or even deliberately 'gaming the system'. [The classic paper "Metrics: you are what you measure" is highly recommended here.]

Conclusion

The suggested metrics are intended to help you derive creative and useful measures for your own situation. Do not underestimate the value of presenting and discussing targets and metrics among management. The dialogue can be very effective at teasing out any underlying issues and concerns on both sides, and it promotes adequate investment in information security. It's all part of management-level security awareness.

For more information

Please visit Information Security's intranet Security Zone for further information on information security and risk management. Additional security awareness materials and advice on this topic are available from the Information Security Manager. NIST's Special Publication 800-55 "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics. Andrew Jaquith's book "Security Metrics" is a more pragmatic guide.