NOTICEBORED

Management briefing on

Information security governance metrics

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

Clint Kreitner, SANS

Summary

It is not necessarily obvious how to measure information security governance. This paper describes potential metrics for measuring and improving information security governance. We are not suggesting that all of these metrics 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 governance framework.

Introduction

In its free booklet "Information security governance: guidance for boards of directors and executive management" (2nd edition), the IT Governance Institute (ITGI) describes information security governance in terms of the following key elements:

1) **Desired outcomes of information security governance** such as strategic alignment of information security with business strategy, risk management, resource management, performance measurement and value delivery;
2) **Knowledge and protection of information assets -** information and the knowledge based on it have increasingly become recognized as business-critical assets without which most organizations would simply cease to function. Knowledge is a business enabler, requiring organizations to provide adequate protection for this vital resource;
3) **Benefits of information security governance** such as increased share value, increased assurance by bringing information security under management control, better compliance and protection against liabilities; and
4) **Process integration -** integration of management assurance processes regarding security to improve overall security and operational efficiencies.

We'll use these four elements to derive more than four types of information security governance targets and metrics.

Information security governance metrics

If we accept that it is important to make our employees (and indeed those employed by third parties who work on our behalf) responsible for information security and especially if we intend to hold them personally accountable for their actions, so it makes sense for management to check how effective this process is and, where necessary, make adjustments to improve the governance of information security.

1. Desired outcome metrics

Clarity of expectations

If we are going to measure the organization against some desired outcomes, the requirements should be made clear. Some might for example claim that information security rôles and responsibilities must be "fully documented" if fulfilling such rôles and responsibilities is desirable but this is difficult if not impossible to achieve in practice. Job descriptions are inevitably quite generic and are not meant to define absolutely everything that employees are meant to do. Just like the laws of the land, information security policies, standards, procedures and guidelines also have to be interpreted to some extent depending on the particular circumstances. However, it is generally accepted good practice to document key information security rôles and responsibilities, policies, standards *etc*. This leads to the first group of metrics around the extent to which the requirements are defined and their suitability.

The organization's information security policy manual is an excellent place to start since (hopefully!) it defines a number of rôles and responsibilities and allocates them to the applicable departments, teams/functions or individual employees. It is feasible to work systematically through the policy manual, drawing up a rôles and responsibilities matrix along the following lines:

Information security policy manual section	**Department, team/function or person***					
	IT			**HR**		
	CIO	Network/system operators	Security admins	HR managers	HR admins	*Etc.*
5.1 Information security policy	R	R	R	R	R	
6.1 Internal organization	A	R	O	R		
6.2 External parties	A		O			
Etc.						

* A = Accountable. R = Responsible. O = Observer/advisor/auditor

Having drawn up the outline matrix, it is then possible for someone objective to work through the job/rôle descriptions, departmental objectives, 3rd party service contracts *etc*. to check and report on whether the corresponding roles and responsibilities are identified specifically and fully (100%), would be covered adequately by generic statements (>50%), are partially covered (<50%) or are entirely absent (0%). Significant gaps corresponding to extreme low values would naturally suggest improvement opportunities.

The level of detail in this process is optional. It might be sensible to start, for instance, at the level of whole sections of the policy manual, or to work down particular columns of the matrix (*e.g*. just within IT). The experience gained by this initial run should make a more detailed assessment slightly easier to stomach.

Fulfillment of expectations

A second group of metrics reflects the need to assess compliance with or fulfillment of the defined rôles and responsibilities. "Complete compliance" is an idealistic if naïve goal since limited noncompliance may be acceptable and even desirable under some circumstances, provided this is in the organization's best interests. This target is itself a policy matter that applies across all policies *etc*. It tends to be determined more by the organization's culture than by written edicts from management but, that said, management does set the tone from the top. The target seems likely to evolve as the measurement process matures – no bad thing.

Assuming that people have been told what they should or should not be doing in relation to information security, the next problem is to figure out how well they comply in practice. The key here is to focus on non-compliance since, for the most part, people tend to comply.

The 'number of non-compliance incidents in the previous period' seems relatively simple but ignores the importance of each incident. An alternative approach might be for someone to assign each non-compliance incident a 'score' (*e.g.* 0 meaning trivial or insignificant to 5 meaning extremely serious leading to dismissal or legal action) and present both the number of incidents and the mean score. Once the metrics bed down, management may well push back on the scoring process so it is probably worthwhile making the scoring process as open and well defined as possible, perhaps using examples of incidents at each level. You will of course need access to the source information about non-compliance incidents, ideally by close cooperation with HR and other management functions.

Be aware of the iceberg problem: you are very unlikely to find out about all non-compliances, primarily those that result in significant incidents and are clearly visible. There will always be a larger hidden body of non-compliances, but the hope is that they are insignificant so really don't matter to the organization.

2. Knowledge and protection of information asset metrics

Potential metrics in this category are described in the metrics discussion papers provided every month as part of the awareness program. There is a huge array of things that could be measured but it is far more difficult to pick out 'a few good metrics'.

A key metric that strikes a chord with some is based on the old "Days since a lost time accident" display boards common outside factories in the 1970s and 80s. The modern-day equivalent is "Days since a significant security incident", typically displayed on the corporate intranet. Clicking on the headline number pulls up details on the breakdown of incidents by type, significance and/or business unit/department. The lowest level of detail may include brief descriptions of actual incidents, ideally accompanied by explanations of the controls that were fixed or improved to prevent recurrence.

3. Benefits of information security governance metrics

Here we seek to measure the financial control elements of governance as they apply to information security management. Information security raises legitimate management questions such as:

- How much is 'enough' information security? Are we investing too much or too little in managing our information security risks (and by the way, do we even track all the costs)?
- Are our information security investments being applied wisely, achieving both efficiency and effectiveness?

Financial controls are commonly measured so the metric ideas in this section are also just brief suggestions:

- Matching expenditure to budget, accounting for any under or over-spend;
- Annual expenditure on information security, expressed as a simple value (with caveats around the distributed nature of information security controls), a proportion of income or of some other major expense (*e.g*. proportion of the IT budget), or a trend;
- Matching risk and reward, achieved by measuring the recovery of procurement or development and implementation costs for information security controls through reduced impacts and risks (*i.e.* increased assurance and confidence). Business cases for significant security control investments should contain metrics.

4. Information security process integration metrics

It may seem counterintuitive but "the inverse of the number of people employed in information security management" is potentially a metric for this governance goal – the idea being that most information security activities should ideally be performed by people working in other corporate functions. Many organizations that are mature enough to understand and adopt the "information security" rather than "IT security" approach take the line that information security is a distributed function, spread throughout the organization, albeit one led/directed by a specialist advisory function ("Information Security Management") which requires a certain number of competent and experienced workers in order to be effective. As information security knowledge and skills permeate the organization, there is potentially less and less need for a large core team of dedicated information security managers in a centralized function, but conversely someone needs to maintain the policies, compliance activities, awareness programs and so forth on behalf of the entire organization.

A more pragmatic metric, therefore, might measure the proportion of information security man-days expended within *versus* without the Information Security Management department. This is not an easy metric to measure since accounting for information security management man-days outside the ISM function requires the cooperation of all departments doing ISM work.

5. Confidence metrics

A rather different style of metric involves surveying managers, for example:

How confident are you our information security governance meet the organization's 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? Are you aware of information security governance failures or issues, or conversely what makes you think we are world-class?

It is simple to measure percentage values from each response and calculate the mean score (indicating the perceived level of confidence) and variance (showing the range of opinions). Provided sufficient survey forms are completed and measured, the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials, as well as worthwhile ideas for improvement. The mere fact that people are being asked their opinions in this manner itself supports greater awareness of, if not interest in, information security governance.

Management reporting

The numbers themselves are generally less important than what they mean or imply about the organization's information security governance. It is worthwhile analyzing and explaining the numbers – for instance, a written management report and executive summary with key recommendations for governance improvements, backed up with appendices containing the actual numbers. Consider repeating the measurements periodically (*e.g.* every year or two) to assess progress towards your governance objectives. Consider also preparing an interim 'status report' a few months before the full presentation to senior management, giving middle managers and staff an opportunity to address the worst metrics before it's too late.

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 metrics and reporting with management, especially on a topic such as governance. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides.

For more information

Please visit Information Security's intranet Security Zone for more on information security governance. Additional awareness materials and advice on this topic are available from the CISO or Information Security Manager.

NIST SP 800-55 (Rev 1, July 2008) *Performance Measurement Guide for Information Security* (new title - formerly *Security Metrics Guide for Information Technology Systems*) is "a guide to assist in the development, selection, and implementation of measures be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs.*"* Take a look also at SP 800-80 (DRAFT, May 2006) *Guide for Developing Performance Metrics for Information Security.* This is a more useful than the original SP 800-55 but still rather over the top for most organizations (it is intended for large US government departments subject to FISMA).

Andrew Jaquith's book Security Metrics is a pragmatic guide and the classic 1998 paper by Hauser and Katz "Metrics: You Are What You Measure is also highly recommended.