NOTICEBORED

Management briefing on

Integrity metrics ... and metrics integrity

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

Clint Kreitner, SANS

Summary

This is a management discussion paper outlining potential metrics for measuring and improving integrity controls. It also considers integrity issues relating to the measurement system.

Introduction

The dictionary definition of integrity - honesty (adherence to moral principles), soundness (the quality of being unimpaired) and wholeness (unity) – naturally suggests measurement targets for integrity. The greater problem is how to define relevant, measureable metrics but anyway we'll start with those targets before proposing suitable metrics.

In a departure from normal practice, this paper also considers the issue of integrity for the measurement/metrics system. A high-level assessment of the integrity issues typically associated with measurement systems creates a worked example for regular information security risk analysis techniques.

Integrity targets

Honesty targets

"Absolute 100% honesty and truth in everything" is a possible target but is it realistic, or even desirable in fact? Consider the many situations in which 'stretching the truth' or 'little white lies' are culturally acceptable and have little impact (sometimes being beneficial), whereas outright lies are generally harmful to the interests of those being lied to. Honesty is not a binary condition, therefore, since each event could be placed on an imaginary 'honesty' or 'truthfullness' scale:

0% 50% 100%

|----------+----------|

Downright lies	**Half-truths**	**Absolute truths**
At the bottom end of the scale are flagrant lies, statements that are patently and demonstrably false and, to varying extents, harmful to those being lied to.	The middle ground varies from lies containing an element of truth, through potentially misleading or neutral statements, up to 'little white lies' and stretched truths.	At the top end are totally accurate and open statements of truth. Unfortunately, these are not always beneficial, for example "No, your new expensive dress looks absolutely awful"!

If you accept the concept of the honesty scale, you can probably foresee potential problems if management sets a target for "absolute 100% honesty and truth in everything". Take advertising, for example. Many advertisements tread a fine line between telling lies and stretching the truth in order to promote a product's features. Similarly, many annual corporate reports display a fascinating combination of truths and half-truths: we all know the selection and presentation of statistics can be misleading, while the carefully-crafted prose does not always entirely reflect the situation shown by the tables and graphs. In situations such as these, it would hardly be in the organization's interests for management to mandate and enforce a policy of absolute honesty.

Risk is another aspect to this, specifically the risk of liars being discovered or caught out. Plain factual statements such as "our profits were up 23% on last year" can often be verified objectively, whereas many are more ambiguous and capable of interpretation (*e.g.* "We are the number one seller of widgets" – number one on which criterion? Value? Volume? Quality? …). Lies of the former type are unwise in any public forum, while the latter are often acceptable.

So, a more appropriate corporate honesty target might be "The highest possible levels of honesty and truth consistent with the organization's best long-term interests". Overtly social responsible organizations might wish to include the interests of society and/or employees. Such phrases can be enshrined in corporate policies and value statements but it is equally if not more important for managers to 'walk the talk'. This is typical of corporate cultural issues. The extent to which management is perceived to be open and honest with staff influences staff behaviors in this respect at least as much as corporate policies.

Soundness and wholeness targets

While truthfulness is important (*e.g.* in relation to governance and legal obligations for truthful financial reporting), data/information and systems integrity requirements fall largely in the area of soundness and wholeness. Here again the obvious target of being 'absolutely 100% sound and whole' may be counterproductive since this implies a high level of control that is likely to increase costs. Management is likely to accept lower levels of accuracy and completeness where this saves significant amounts of money, greater than the projected costs caused by the inaccuracy or incompleteness. In other words, this is also a risk issue.

One way to resolve this dilemma might be to designate certain important systems and data that must be as 'sound and whole' as possible, while leaving more leeway for others. This implies a prioritization based on management requirements. Integrity is likely to be highly important for SOX-relevant financial systems and data, for instance, whereas many other internal systems and data need not be so tightly controlled.

Integrity metrics

Honesty metrics

Measuring "honesty" is a difficult task for several reasons:

- Honesty is a sociological or human behavioral factor, making it inherently difficult to measure scientifically except by sampling and observation. Testing honesty may be socially unacceptable;
- Different people define 'absolute truth' and 'lies' differently. Where the criteria are factual and objective this may not be hard to resolve but in more subjective matters, the end points on the honesty scale may be disputed for good reason;
- Dishonest people often aim to conceal or gloss-over their dishonesty. Lies can also be overlooked, remaining undiscovered indefinitely, biasing the measurements.

Management needs to balance the effort and costs incurred in gathering, analyzing and presenting metrics against their value. Rather than spend a fortune on surveys, studies and discussions

around honesty, we suggest instead that you might collect and report 'case study' examples based on situations in which lies have been revealed or refuted. Situations such as frauds are inherently interesting to most people and fraud cases are valuable from an awareness and corporate learning perspective.

On the theme of frauds, simply counting the number of frauds discovered in a year is not very informative since they vary by impact. However it may be worth graphing the cumulative losses incurred in frauds with footnotes to expand on specific incidents of note, and probably caveats regarding accuracy of the figures presented (*e.g.* it is extremely difficult to assess and value the reputational damage that a serious fraud might have caused).

Soundness and wholeness metrics

Measuring data integrity is generally easier and cheaper than measuring the honesty of employees, especially if measurement functions are designed and built-in to systems, typically as a side-effect of data validation controls. Here are some possible data integrity metrics:

- Estimated proportions of data in a database that are inaccurate or incomplete – implying that someone with read access to all the data has the capability to identify inaccurate and incomplete entries. Automated data validation checking functions are likely to be cheaper to run and provide more accurate data but require additional specification, design, coding and testing of the functions;
- Number of data corrections made on a system during management review/approval activities (note: aggressively driving this metric down may encourage managers to be less diligent in their checking, an example of an unintended consequence of choosing an inappropriate metric);
- Trends in the number of items placed in 'hold files', exception reports *etc*. as a result of failing built-in data integrity checks, particularly around system interfaces. A relatively high number of data validation exceptions on inputs from a certain system probably indicates upstream integrity issues in the feeder system and/or its associated processes. Even crude measures such as the size of daily exception reports in kilobytes may be useful in identifying sudden changes requiring further investigation.

Confidence metrics

Management confidence in integrity controls can be surveyed through questions such as this:

How confident are you that data/system/personal integrity controls meet the business needs? Please mark the following percentage scale at the appropriate point, in respect of data/systems/people with which you are familiar:

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

IT service metrics produced by some organizations consist of pages and pages full of busy tables and graphs. They may be a defensive mechanism to conceal problems and justify claims that Service Level Agreements or contractual terms have been met. However some managers genuinely prefer such reports and like to drill down into the details.

Others prefer high level graphical summaries such as red-amber-green 'traffic light reports' or 'heat maps'.

Still others like to read the Information Security Manager or CIO's description and analysis of the current situation, particularly if there are action items or proposals.

You may be ambitious enough to combine high-level and detailed reporting methods through a 'dashboard' intranet site with summary statistics and commentary on the front page that can be clicked to reveal the supporting data beneath. Don't let the glossy presentation fool you though. The information value is limited by the quality of the chosen metrics, the data collected and the analysis. Given the choice, invest at least as much in those areas as in the dashboard itself.

Integrity of the system of measurements

Metrics, or rather the measurement system as a whole, can be analyzed like any other system to define information security objectives and control requirements to reduce or limit risks. Here are some common potential integrity issues worth considering, in addition to the confidentiality and availability aspects typically considered in an information security risk analysis:

- How are source data obtained? Are the sources themselves sufficiently trustworthy? Issues such as sample size for survey data can significantly affect their accuracy.
- Who is gathering, storing and processing measurements? Are they sufficiently competent, diligent and trustworthy? Are the criteria and processes for taking measurements sufficiently well defined so as to avoid ambiguity and to reduce the potential for abuse or fraud (*e.g*. selective use of 'beneficial' or positive data and disregard of negative values)?
- What about the computer systems supporting the measurement processes? Has anyone actually verified that spreadsheets and databases are correctly, accurately and completely processing measurement data? Are changes to the systems properly managed, for instance are code or design changes adequately tested before release?
- For trends analysis, it is clearly important that historical data can be relied upon, meaning that they must be suitably protected in storage. The problems that may arise if the basis or process for measurements change need to be taken into account when designing the measurements system: data from prior periods may need to be re-based or otherwise manipulated in order to remain valid for comparison with data from current and future periods.
- Do reporting processes accurately present 'the truth, the whole truth, and nothing but the truth'? What controls are in place to ensure the objectivity and accuracy of reported data (*e.g*. auditability or traceability)?

It is not appropriate for us to suggest specific integrity controls for your measurement system because it is highly context-dependent, hence the reason for suggesting that you analyze your information security risks in the normal way. The impacts of errors and omissions in the metrics may be quite different from one organization to the next – for instance, fraud might be a greater concern if managers' bonuses or promotion prospects are determined on the basis of certain metrics. The consequences of discovering mistakes or deliberately altered data might be worse (for the organization and/or the individuals concerned) in large, strongly hierarchical organizations, government departments and strongly-regulated industries than in small/medium-sized entities. Likewise the threats and vulnerabilities will differ from situation to situation.

Conclusion

The integrity metrics we have suggested are intended to help you consider and derive your own set. Similarly, we have discussed integrity controls for the measurement system to stimulate you to review your own requirements in this regard.

We will return to the topics of governance and ethics in future security awareness modules. Hopefully this paper has got you thinking along those lines.

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. 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.