NOTICEBORED

Management briefing on

Social engineering metrics

Summary

This paper describes potential metrics for measuring and reporting on the organization's controls against social engineering attacks.

Introduction

Social engineers attack our people rather than our IT systems and networks. They aim to bypass or negate the technical and physical security controls by exploiting misplaced trust, naïveté and general inattention or lack of awareness by employees. In order to minimize our exposure to potential social engineering attacks, we therefore need a range of procedural and managerial controls to supplement the technical and physical controls. Measuring the effectiveness of those controls is important if we are to establish management confidence in them and systematically improve them. That in turn begs the question of how to measure what our people are doing, which is the object of this paper.

Social engineering control objectives (targets)

Complete immunity to social engineering attacks is unlikely to be achievable in practice but how much control is it reasonable to expect? It would be sensible for management to determine objectives or targets for the effectiveness of the controls against social engineering. The following points give an indication of how such targets might be framed and phrased – the specific values are for management to decide:

1. "**At least 80%** of general employees should be exposed to suitable security awareness, educational and training materials on the topic of social engineering";
2. "**At least 50%** of general employees surveyed at random should show a basic or better level of understanding of social engineering threats and controls";
3. "**At least 90%** of 'front-line' employees (*i.e*. those who routinely deal with callers or visitors, such as receptionists, telephone operators, Personal Assistants and secretaries, help-desk and other call center workers *etc*.) should be exposed to suitable security awareness, educational and training materials on the topic of social engineering, emphasizing their specific rôle in identifying and responding to potential social engineering attacks";
4. "**At least 75%** of front-line employees surveyed at random should show at least a basic understanding of social engineering threats and controls, and at least 50% should have a reasonably strong grasp of the concepts";
5. "On average, we expect that **at least one** actual or potential social engineering attack per month will be reported and investigated through the normal incident management processes."
6. "We anticipate **no more than one** serious social engineering attack to succeed in a year, and for the losses in such an event to be no more than $50,000."
7. "Total organizational expenditure on social engineering controls should be less than **$25,000 per year**."

Measuring social engineering controls (metrics)

Awareness, training and education coverage metrics

Target 1 above implies the need to measure 'exposure' to awareness, training and educational materials, in other words awareness campaign coverage. This can be achieved for example by counting the proportion of all employees who:

- Attend social engineering awareness briefings, seminars, presentations *etc*.;
- Receive social engineering awareness newsletters, briefing papers *etc*. distributed by email;
- Visit Information Security's intranet webpage on social engineering.

Metrics on understanding social engineering

Targets 2, 3 and 4 imply the need to survey employees' appreciation of social engineering. A generic survey form provided in the NoticeBored awareness module is intended for this kind of purpose and can be customized to suit the organization. Targets 3 and 4 might require additional survey questions or testing to identify whether front-line workers have sufficient grasp of their special rôle in relation to identifying and repelling social engineers.

Another way of measuring the strength of the social engineering controls is to see how employees respond to simulated social engineering attacks. A trustworthy independent and competent assessor (perhaps an IT auditor) might be commissioned by management to make random phone calls to solicit information from employees, or to undertake unannounced physical intrusion tests to check the physical and procedural controls relating to intruders on site. The output from such tests may include metrics (such as the proportion of staff who, when probed by an unknown caller over the telephone, provided valuable or sensitive information) and will almost certainly provide case study materials for reporting and awareness purposes.

Incident and output metrics

Target 5 implies the need to track the proportion of all incidents reported to the IT Help/Service Desk (or other incident reporting function) that relate to social engineering attacks. Naturally, it is likely to peak at the time that social engineering awareness materials are circulated but will probably fall away inside a month or two to a 'normal' level. This metric is therefore best reported annually, although it may be worth measuring more frequently, *e.g*. quarterly, so that there is time to take corrective action if the trend indicates the target may not be met.

Target 6 is an example of an information security process output or success measure. Measures of this kind are particularly difficult to determine objectively because of the complexities of relating particular information security risks and controls to business outcomes. However, it is certainly reasonable for management, having set their expectation, to request contemporaneous reports on serious information security incidents and end of year reports summarizing the incidents that have occurred during the period. The specific numbers (dollars lost *etc*.) are perhaps less important to report than the accompanying text which explains why the incidents occurred and (hopefully!) what has been done to prevent them recurring.

Expenditure metrics

Reporting against target 7 requires us to measure the costs of the associated significant control costs such as:

- Awareness, training and educational activities: costs of trainers, materials and staff time to attend briefings *etc*.;
- Routine and exceptional operating costs: estimated proportion of front-line staff time spent on dealing with social engineering matters, including man-hours spent investigating and resolving identified incidents.

Confidence metrics

Management's confidence in the controls against social engineering can be surveyed using continuous scales as follows:

How confident are you that our social engineering controls 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 social engineering 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 and could create interesting trends over time. The comments can provide useful feedback and quotations for use in management reports and other awareness materials.

Reporting on social engineering controls

The raw numbers obtained using the metrics noted above may simply be reported in relation to the corresponding targets, although it is probably more important for the Information Security Manager and/or CIO to provide some supporting text to help management appreciate the context and result. If the metrics are below target, management will expect to see some explanation of corrective actions planned or in progress. If the metrics are above target, it may (or may not) be appropriate to increase the targets.

If the organization uses an 'executive reporting dashboard', regular monthly/quarterly management reports *etc.*, there may be an opportunity to integrate the information security reporting with other "business" metrics, subtly making the point that information security is also a business imperative, not something that is simply done for its own sake.

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 about social engineering. Additional security awareness materials and advice on this topic are available on request from the Information Security Manager.