Management briefing on

Insider threat metrics

Summary

This paper suggests some metrics to measure and report on the level of insider threats to enable systematic improvement of our information security controls in this area.

Introduction

Information security incidents involving insiders (employees and pseudo-employees such as contracts and consultants) fall into two distinct types: accidental and deliberate acts. Deliberate acts by malicious insiders tend to be more serious, on the whole, but accidents are more frequent and, cumulatively, probably create greater losses. The metrics suggested in this paper cover both types with the aim of improving controls and thereby reducing the number and severity of incidents caused by insiders.

Control objectives (targets and limits)

The ultimate objective is not to completely prevent insider incidents but rather to limit the associated losses below the cost of the information security controls. Controls are costly to design, implement, operate and manage, therefore it would be counterproductive to implement excessive controls that did not earn their place by reducing the number and/or severity of insider incidents by a greater amount. This analysis begs further questions about how much the organization is losing through insider incidents and how much existing plus additional controls would cost. It is possible though not simple to measure both aspects, but an alternative approach is to accept that “we are where we are” and look instead at simply achieving improvements. This means making relatively small (and hence cheap) changes to processes and perhaps systems to reduce accidental and malicious acts by insiders, using selective measurements simply to confirm that we are moving in the right direction.

Measuring and reporting on insider threats (metrics)

Metrics on accidental incidents caused by insiders

Little accidents such as typos, small errors and omissions are so commonplace that it would be too costly to attempt to capture and measure them all. However, it would perhaps be possible to gather baseline statistics through surveying/sampling and observation, for example determining the most common types of mistake made by users during IT training or watching users interact with a new computer system. Employees might be surveyed on their opinions about the systems and business processes that they find the most difficult or complex to use, or on ‘inputs’ to their work that have the most errors and omissions. This kind of information is helpful in systems analysis and design.

More serious accidents that lead to significant information security incidents should be recorded by the organization’s normal incident management processes, such as IT Help/Service Desk call logs. Statistics about their number and nature should therefore be available, although incident costs are seldom recorded, unfortunately. With serious accidents occurring at a lower rate, the statistics should be monitored over a longer period (*e.g.* quarterly or annually) to even-out random changes.

Metrics on malicious acts by insiders

As with accidents, there is no doubt a 'background noise' of minor malicious insider incidents, punctuated by more serious events. Significant incidents are normally analyzed individually with follow-up actions being agreed by management to reduce the possibility of recurrence. Human Resources, Legal, Information Security and Internal Audit departments often get involved and management reports are written. These can be measured by their number and severity (*e.g.* if incidents are graded into minor / medium / major), and it helps to determine or at least estimate the total costs including direct losses and consequential costs (such as investigation and prosecution).

Confidence metrics

A rather different style of metric involves surveying managers regarding their confidence in our controls against insider threats, for example:

How confident are you that insider threats are under management control? 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 insider threat 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.

Conclusion

The generic suggestions in this paper have hopefully stimulated you to consider deriving useful metrics to measure and improve controls against insider threats in your organization. Insider information security threats have traditionally been overshadowed by outsider threats such as hackers and

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.