NOTICEBORED

Management briefing on

Database security metrics

Summary

This paper explains a range of metrics that can help management measure and assess the general status of database security.

Introduction

Potential metrics for database security encompass general information security measures as well as those specifically concerned with database security since databases are central to the organization's applications and IT infrastructure. In this briefing, we will consider only the more specific database security metrics for the sake of brevity.

Database security requirements (targets and limits)

The main purpose of database security controls is to minimize the costs associated with database security breaches, costs that arise from loss of confidentiality, integrity and/or availability. The target here is simple enough to express ("Minimal net losses due to database security breaches") although measuring it is not quite so straightforward (see below).

If the organization has an effective set of management controls to track and assess the costs arising from database security incidents, it may be feasible for management to set realistic target limits on the costs, or the number and extent of breaches. For example, "Management expects database security incidents to cost less than $1m in total in any one fiscal year with no individual incident expected to exceed $100k in direct and indirect losses". This kind of explicit target can help set parameters for risk analysis and investment purposes, but needs to be accompanied by clear accountabilities (*e.g.* "Nominal database system owners are accountable for losses to their own and other business departments that are caused by security failures on those systems").

A secondary purpose of the controls is to maximize the intangible benefits of database security, such as management's confidence in the controls. Again, the target is obvious but measuring it reliably can be awkward. The confidence metric shown below is one possible solution.

Measuring and reporting on database security (metrics)

Metrics for losses arising from database security incidents

It is generally worth tracking and accounting for losses from all types of security incident in order to establish a suitable basis for management decisions. Costs including direct losses, investigative and corrective actions, legal action *etc.* may be measured or estimated, and although indirect losses arising from reduced customer confidence or loss of market share are much harder to assess, they might at least be broadly classified (nil, low, medium, high).

Database security incidents are a subset of all security incidents where the primary issue is a failure of the confidentiality, integrity or availability of a database system. Take for example a network worm incident that causes widespread disruption of network systems. Costs associated with unplanned outages of vital database systems to clean up the worm's damage can be accounted for as database security failures as well as part of the cost of malware incidents.

Metrics for the costs of database security controls

Database security controls include controls that are specific to databases (*e.g.* database user authentication and encryption software) and general security controls (*e.g.* physical protection of servers in the data center). It might be possible to allocate the IT department's costs to security, operations, development and other categories, and within security to identify database security costs. In practice, however, this is likely to turn into a rather pointless exercise because there are so many arbitrary decisions to be made (*e.g.* what proportion of a DBA's time is spent on security processes?). High level/summary metrics are perhaps the best than can be expected.

Confidence metrics

Managers and perhaps other stakeholders may be surveyed regarding their confidence in database security, for example:

How confident are you that our database security 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 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.

Confidence metrics are likely to take a knock after serious security incidents so there is value in repeating the surveys throughout the year to even out the variations and look for trends.

Reporting

The metrics numbers themselves provide some interest but the most value comes from the information that metrics reveal about the state of the organization's controls. Graphing the accumulated database security losses over the course of a year, for instance, should highlight the peaks caused by serious incidents and provide opportunities to discuss the actions taken to prevent a recurrence.

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 Information Security's 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.