NOTICEBORED

Management briefing on

# Network security metrics

## Summary

This paper outlines potential metrics that might be used to measure and improve network security.

## Introduction

"Network security", in the context of this paper, comprises a range of technical and procedural controls designed to prevent, detect and/or recover from security incidents affecting the corporate data networks – incidents such as unauthorized access (hacking), worms and other malware infections, and unplanned network downtime caused by accident or perhaps deliberately. The network is more than just a load of cables and equipment: it is, to a very large extent, the "glue" binding our information systems together, giving knowledge workers ready access to internal and external information resources, allowing rapid communications and facilitating many business processes including eBusiness. In other words, the network is a valuable corporate asset, hence the reason that network security is so important.

Management needs reliable information about the status of network security in order to align security controls with security risks, and to maintain that alignment in a dynamic business and IT environment. Network security threats originating from the Internet are a particular concern, especially given the growing involvement of organized criminals in hacking, extortion and industrial espionage activities. New network security threats and vulnerabilities emerge frequently, making this one of the most difficult aspects of security management to keep under control. On the upside, justified confidence in our network security permits us to initiate new business processes and take advantage of eBusiness opportunities that our competitors may fear to take. The network security metrics suggested below can help to build that 'justified confidence' and drive continuous security improvement.

## Network security requirements (targets and limits)

A policy of "zero tolerance" for network security incidents might sound vaguely attractive but the costs involved in such an approach would seriously restrict network usage and hence would undermine the business value of networking. The question is more one of "How much network insecurity can we safely accept?" which is really a risk management decision and as such part of corporate governance. At the highest level, corporate stakeholders needs to know broadly whether network security is under management control, whether there is sufficient investment in network security and whether that investment is being spent wisely.

Thinking this through, it is possible to determine targets or limits for network security incidents in various terms. We might, for example, say that:

- "We should suffer no more than X major worm outbreaks in a Y-year period" (similarly for other types of network security incident such as hacks, Denial of Service attacks, network overloads and network service outages *etc*.);
- "No single network security incident should cost more than X% of turnover, and all network security incidents should cost less than Y% of turnover in aggregate";
- "X, the total cost of network security measures, should be less than Y, the estimated total cost of security incidents that are prevented, avoided or mitigated by those security measures".

Those three bullet points all suggest possible metrics although the absolute values of X and Y in each case are arbitrary. Still, whatever values management feel are appropriate will act as targets or starting points for the continuous improvement that we seek.

## Measuring and reporting on network security (metrics)

### Incident metrics

We should be systematically measuring and recording network security incidents, provided the costs of record-keeping are minimal. The call logging and tracking systems used by IT Help/Service Desk provide a wealth of information on this topic (*e.g*. the number of various types of network security incident, and information on the impacts caused), along with supplemental information from post-incident reviews. One concern, though, on the reporting side is to avoid double-accounting: for instance, a network worm outbreak is both a network security and malware incident, although the business impacts occur once. Arbitrary allocations between certain categories of incident leads to the possibility of deliberate manipulation of the metrics, perhaps implying the need to audit the figures occasionally.

### Control metrics

One way to track network security control costs is to measure or estimate the investments in people, processes and technologies relating to network security. As with incident metrics, the possibility of double-accounting must be countered, perhaps using the cost accounting and allocation facilities in our finance systems, and periodic auditing. Conventional investment management processes will help, including the need for cost-benefit justification of network security control investments and tracking of the costs and benefits through the lifecycle of the controls.

### Risk metrics

Risk Management, IT Audit and/or Information Security professionals may be asked to report regularly on their assessment of the organization's network security status, relative to the previous report and/or relative to some external benchmarks or standards. A report identifying network security incidents, investments and status would probably be a worthwhile element of the Information Security Manager's management reports, showing trends over successive periods.

Network security reviews and audits provide another potential source of information and metrics. Benchmark reviews of network security conducted by competent consultants with knowledge of comparable organizations and industry standards typically deliver both relative positioning and improvement recommendations. In large organizations, individual business units may usefully be benchmarked against each other, and (with management support) good network security practices may be transferred from high-scoring units to their low-scoring peers.

### Compliance metrics

Compliance with corporate network security policies and other obligations (laws and regulations, contractual commitments, ethical considerations) can also be assessed by management reviews, internal/external audits and consultancy assignments. Compliance processes are required of organizations seeking certification against the international standard for information security management systems, ISO/IEC 27001. As with other metrics, the trick is to minimize the costs and maximize the benefits of measuring compliance. Good luck!

### Confidence and governance metrics

A different style of metric involves surveying people (managers, network security specialists and maybe others?) regarding their confidence in network security, for example:

*How confident are you that our network security meets 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?*

### Reporting

We have probably all seen the voluminous IT service metrics produced by some organizations – pages and pages full of busy tables and colorful graphs. They are often seen cynically as a defensive mechanism to conceal or gloss-over problem areas and justify claims that Service Level Agreements or contractual terms have been met. However some managers genuinely prefer this style of report. They like to check the details.

Others prefer high level summaries, red-amber-green 'traffic light reports' for example. These can either be written summaries with colored blobs identifying the status of each section, or graphical reports using the relevant colors. An effective reporting approach might be a 'heat-map' consisting figuratively of a background outline representation of the entire suite of key business processes, with transparent overlays for various aspects including network security. Various elements would be picked out on each layer in color, with annotations to explain the specific ratings and highlight particular improvements or outstanding issues. These might be presented on a web page with tabs for each overlay.

## 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 the experts present and discuss reports with management. The dialogue that ensues adds value to the written reports. 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 on network security, additional security awareness materials and advice. NIST's Special Publication 800-55, a 99-page "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics.