10

Measurement

This chapter covers designing and interpreting measurements for information security management, both generated within the organisation and drawn from external sources. It forms part of Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.

Information security is a particularly challenging field for designing and interpreting measurements, as it deals with unknown circumstances and unexpected events, both of which are hard to measure.
This chapter uses the term measurement throughout, except where quoting other documents.

Many terms are used in the field of measurement, such as statistic, metric, and KPI. Find out what the rest of your organisation calls them, and use the same terms with the same meaning in your ISMS.

Key topics

- **Why measurements are worth using**
- **How to identify useful measurements, and evaluate the usefulness of the ones you are already using**
- **How to use measurements**

10.1 Why measure?

To manage anything you need to be able to measure it. As an ISMS is the tool for managing information risk, it must include the making and use of measurements (see clause 9 in ISO/IEC 27001).

Measurements' purposes may include:

- Judging the performance of the ISMS (and its controls) over time: which actions are taking the organisation closer to/further from its objectives?
- Checking that controls are operating as expected.
- Identification of opportunities for continual improvement (see Chapter 12, Continual improvement).
- Benchmarking/comparison against peer organisations.
- Some measurements (e.g. "success of ISMS"/"ROI") may be used for selling to top management (see Chapter 2, Information security governance).

10.2 What is a useful measurement?

Measurements are most useful to the management of information security if they measure practical aspects of information security, such as the organisation's level of preparedness, or the level of external threat.

As with many other aspects of an ISMS, measurements have a lifecycle – they are selected and implemented, they are used, and they are retired when they are no longer useful. Measurements should therefore be reviewed by management on a periodic basis.

All measurements must have an effect: either to support decision making, or to spark action.

10.3 How to design a useful measurement

In simple terms, an organisation can measure:

- its ISMS processes
- the controls managed by its ISMS
- external threats.

In addition to the above, some controls are based upon measurements (e.g. alerting following multiple failed attempts to access a secure room). These controls are sometimes known as detective controls (see Chapter 6, Controls).

It is important that measurements consider people and processes, as well as technology.

Risk cannot be measured directly, but can be determined indirectly. Measurements of threat and of control effectiveness, as well as information from detective controls, are used to inform risk assessment, one of the ISMS processes (see Chapter 5, Risk assessment). This produces information on actual and acceptable risk.

Measurements should include, in their definition, the following:

- what is to be measured
- how the measurement will be made
- the purpose for which the measurement is taken
- when and/or how often a measurement should take place
- which role is responsible for ensuring that the measurement takes place
- how a measurement is to be used (including reporting format)
- the intended audience for a measurement (e.g. top management, or technical specialists)
- the classification of the information obtained (see Chapter 7, Information management).

See SANS guidelines and ISO/IEC 27004 for more information on measurement definition.

10.3.1 Designing measurements of ISMS processes and controls

The organisation should identify the key processes of its existing ISMS and, for each process and each control, determine:

- how to demonstrate that it is in place
- how to demonstrate that it is operating as intended.

This approach will naturally lead to the definition of useful and relevant measurements.

10.3.2 Designing measurements of threat

The organisation should identify what threats it is currently concerned with. For each threat or threat source, the organisation should determine:

- whether the threat is capable of being meaningfully measured
- if so, what measurement will be useful.

10.4 Evaluating a measurement

Existing and proposed measurements should be evaluated to identify if they are suitable and effective. The organisation can assess the effectiveness of measurements using the table in the resources section for this chapter.

10.5 How to use measurements

Measurements should be used as defined in the organisation's ISMS to monitor its effectiveness, and to track threat levels.

Every measurement, if it has a purpose for being taken, must also have actions and/or decisions which it affects. The organisation should, when defining each measurement, in every case define how to use the information it will provide. Likely actions should be documented and agreed with top management as appropriate in advance, to prevent misunderstandings.

Some measurements can be used to monitor the progress of the organisation towards a mature information security management system. Examples of these include the speed and completeness of responses to notifications, for example of the availability of patches; the number of known vulnerabilities that are detected by routine scanning; or the number of the organisation's passwords that can be successfully cracked in a given time. On the non-technical front, the proportion of users who have received relevant training, and their scores on tests, are also very useful.

10.6 Reporting and interpretation

The results from monitoring and measurement should be evaluated and analysed (see ISO/IEC 27001 9.1 and 9.3), reported to a responsible management role or group, and appropriate actions taken to address any issues uncovered (see Chapter 11, Incidents and nonconformities).

The role of internal audit is key in ensuring that the organisation has, and maintains, an effective ISMS. Even if an organisation is not aiming for compliance with ISO/IEC 27001, its internal audit function can still undertake periodic reviews of different aspects of information security, especially to determine whether effective monitoring and controls are in place.

The presentation of measurements is critical to their usefulness, as appropriate presentation allows audiences to interpret the information easily. Reporting should be tailored to the audience. See Chapter 2, Information security governance, for suggestions on developing material for top management.

Reporting can also be used to highlight features of the information which the audience would otherwise not have noticed, or to explain subtleties in the measurement which can easily be misinterpreted.

An example of subtlety in measurement is where an organisation experiences an increase in reported incidents. While this increase might indicate that more security incidents are happening, industry surveys suggest that only a small percentage of incidents are noticed, so an increase is more likely to indicate improved detection. Users may also have become more confident that they can report them without being blamed.

The context of a measurement is also important; for example, if an organisation carries out an awareness campaign and subsequently sees an increase in reporting, this should normally be seen as a sign of increased awareness, rather than of decreased security.

Measurements gathered from other environments may not be directly comparable and may have been collected in different ways.

10.7 Examples of effective measurements

There are a number of sources of lists of measurements, including SANS, the US Office of Energy Delivery, and the Centre of Internet Security (see reading list for this chapter). In this chapter, a sample of metrics are given, divided into four categories:

- measurements of information risk
- measurements which aim to determine whether the ISMS is performing as expected
- measurements which aim to determine whether controls are performing as expected
- measurements which themselves are controls.

10.7.1 Measurements of information risk

These measurements can, by themselves, be monitored to identify whether information risk is increasing or decreasing. However, in order to tell whether there is a problem (see Chapter 11: Incidents and nonconformities), they should be evaluated to determine whether the actual risk related to them is acceptable to the organisation (see Chapter 5, Risk assessment). Examples of this type of measurement are:

- "opportunity window" between vulnerabilities being known and patches being installed
- number of unpatched systems at any given time
- percentage of sensitive data being handled in secure environments
- number of copyright complaints (which are correlated to the possibility of legal action, but not strongly correlated to the number of actual copyright violations)
- notifications to the Information Commissioner's Office (as for copyright complaints).

10.7.2 Measurements of ISMS effectiveness

The following measurements are examples of the types of measurement which can be used to determine if the organisation's ISMS is still performing as required.

- percentage attendance at management review meetings
- percentage of policies reviewed on or before their review dates
- percentage of controls whose effectiveness is being measured
- number of minor and major non-conformities found at last internal audit
- time to resolve non-conformities
- shortfall in resources.

10.7.3 Measurements of control effectiveness

The following examples are designed to show whether a control which the organisation has decided to implement is performing as required.

10.7.3.1 Types of incidents

It may be useful to measure the numbers of incidents of different types they handle, according to a standard categorisation. Changes in these numbers can indicate areas where more resources or skills are required, for example if the number of internal investigations increases or where current controls need to be reviewed, for example if there is an increase in malicious code incidents.

Normalising these values to incidents per 100 users creates statistics that can be compared between organisations: differences in the rates of occurrence, the proportions of different categories or the trends in their prevalence have prompted useful discussions of the impact of different security approaches.

10.7.3.2 Successful attacks vs attempted attacks

Where successful attacks can be measured using technical means – for example a phishing attack that directs victims to a unique website – a measurement looking at the proportion of recipients who became victims may be a useful guide to areas of the organisation where additional measures (e.g. awareness raising) are required. Through an employee phishing campaign, Caputo et al (see reading list for this chapter) demonstrate human factor considerations around the measurement of behaviour in organisations.

10.7.3.3 Measuring time to patch

Where patching is considered to be a suitable control, the obvious associated measurement would appear to be how long it takes to patch after an update is available. In fact, the correct measurement is the difference between the agreed appropriate time to patch and the actual time to patch. Where the two are identical, then the control "patching our servers" is operating as expected. Where patching takes a longer or shorter time than required, then the organisation is not managing its risk as it has decided to, and there is a problem.

10.7.4 Measurements which are controls

The following measurements are direct measurements of components of the organisation's environment and activities; their results can be used to determine if an incident is occurring, for example. They are also called "detective controls" (see Chapter 6, Controls).

- number of virus alerts
- unexpected changes in key database files
- loss of a heartbeat signal from a logging system
- alerts from an intrusion detection system.

10.8 Examples of measurements which may be less helpful

10.8.1 Level of information security

A simple measure of organisational information security is unlikely to be achievable and would, in any case, provide little clues regarding how information security can be improved.

10.8.2 Number of incidents handled

An often cited measurement is the number of incidents handled by an organisation's security team – for example, the number of copyright infringement notices. Typically this combines individual measures with many of the problems discussed above: some incidents will be triggered by user reports, others by technical detection of attacks. And as noted earlier in the chapter, the interpretation of this statistic is very ambiguous.

As a result it is unlikely to be a useful measure of the organisation's security, threat or preparedness. It is best seen simply as a measure of how busy the incident responders are – a measurement which can be used to manage service delivery, but which has a very indirect bearing on the actual level of risk or threat to the organisation. A better measurement may be the historical trend in incidents.

Summary

- Measurements may be used to measure the performance of an ISMS, the effectiveness of controls, to track threat levels, and as part of controls themselves
- Every measurement must have a purpose: to direct action, and/or to support decision making
- Suitable presentation of measures is critical to their effectiveness

Resources

How to evaluate a measurement

Reading list

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
www.ucisa.ac.uk/ismt39

http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

CIS Consensus Information Security Metrics
www.ucisa.ac.uk/ismt40

http://benchmarks.cisecurity.org/downloads/metrics/

SANS Guide to Security Metrics
www.ucisa.ac.uk/ismt41

http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

Jaquith, Security Metrics, 2007

Vaughn, Henning, Siraj, Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy, HICSS'03, 2002

Villarubia, Fernandez-Medina, Piattini, Towards a Classification of Security Metrics, WOSIS '04, 2004

Jansen, Research Directions in Security Metrics, Discourses in Security Assurance and Privacy, 2009

Hecker, On System Security Metrics and the Definition Approaches, SECUREWARE '08, 2008

Ouedraogo, Mouratidis, Khadraoui, Dubois, Security Assurance Metrics and Aggregation Techniques for IT Systems, ICIMP '09, 2009

Savola, On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems, IJCSNS, 2010

Wang, Wulf, Towards A Framework For Security Measurement, NISSC '97, 1997

Debra S. Herrmann, Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI, Auerbach Publications, 2007.

IATAC Cyber Security Report, Measuring Cyber Security and Information Assurance State-of-the-Art Report (SOAR)", IATAC, 2009

Atzeni and Leoy, Why to adopt a security metric?, 1st Workshop on Quality of Protection, 2005

Julisch, A Unifying Theory of Security Metrics with Applications, IBM RZ3758, 2009

Jonsson and Pirzadeh, A Framework for Security Metrics Based on Operational System Attributes, International workshop on Security Measurements and Metrics - MetriSec2011

Chapin and Akridge, How Can Security Be Measured?, ISACA, 2005

D. Caputo et al, Going Spear Phishing: Exploring Embedded Training and Awareness, IEEE Security and Privacy, 2014