Monitoring of Incident Response Management Performance

Maria B. Line[1], Eirik Albrechtsen[2, 3],
Stig Ole Johnsen[2], Odd Helge Longva[1], and Stefanie Hillen[4]

[1] SINTEF ICT, S P Andersens vei 15B, N-7465 Trondheim
{maria.b.line, odd.h.longva}@sintef.no
[2] SINTEF Technology and Society, S P Andersens vei 5, N-7465 Trondheim
{eirik.albrechtsen, stig.o.johnsen}@sintef.no
[3] Norwegian University of Science and Technology (NTNU), Department of Industrial Economics and Technological Management,
N-7465 Trondheim
[4] Agder University College, Grooseveien 36, N-4876 Grimstad
stefanie.a.hillen@hia.no

Abstract. Monitoring the performance of incident response (IR) management is important input for improving the IR management system. A set of performance indicators, which assists monitoring in a proper way, is described regarding: the incident response management system; information security culture; number of incidents responded to; average time spent on responding; consequences of incidents; number of incidents of high loss; downtime of SCADA systems; total costs of incident response; and learning. The entire set of proposed indicators is well suited for monitoring the total incident response management of an organisation as it covers all parts of incident response management.

1 Introduction

Monitoring the performance of information security incident response (IR) management is an important part of both the total incident response system as well as the general information security management system. Performance measures or indicators are well-suited for monitoring as they make incident response management visible for decision-making, communication, comparison, learning and competition. Indicators even play an important motivational role, both at higher management levels and among the workforce. Additionally, indicators are helpful in meeting public requests as given in e.g. the Sarbanes-Oxley act [USC02] which states requirements about mandatory reporting on incidents.

The purpose of this paper is to propose and evaluate a set of performance indicators monitoring incident response management. In addition, it is showed how the indicators might be utilized. The paper is written based on experiences of incident handling and general information security management in the Norwegian oil and gas industry. Information security aims at preserving confidentiality, integrity and availability [ISO05a]. In contrast, the oil and gas industry focuses mainly on preserving integrity and availability, particularly for SCADA systems, i.e. Supervisory Control and Data Acquisition (also denoted process control systems or production systems). Although the indicators are developed within the context of the oil and gas industry, they should be transferable to other organisational contexts as well.

Incident response management is a systematic approach for handling computer security incidents. An incident is an occurrence that compromises information security [ISO05a]. The ISO/IEC technical report 18044 'Information security incident management' [ISO04], is used as a framework for developing the performance indicators proposed in this paper. It describes incident response in four interrelated phases:

- *The plan and prepare phase* includes establishing and implementing an incident response management policy; performing risk analyses; training; and briefings.
- *The use phase* includes detection of, reporting of, and dealing with incidents. Forensic analysis is initiated when necessary.
- *The review phase* includes learning from the incident handling and identifying measures for improvement of the incident response management system. If necessary, further forensic analysis is performed.
- *The improve phase* includes implementing the improvements identified in the previous phase.

To make sure that the indicators are suitable for covering the total incident response management system, performance indicators have to be derived for all these four phases.

The paper is structured in the following way: In the next section, it is described how performance indicators support decision-making for improvement of incident response management. Thereafter, a set of performance indicators for an incident response management system is described. Subsequently, the quality of the indicators described is discussed.

2 Purpose and Use of Performance Indicators

Performance indicators have been utilized for monitoring a variety of different business processes [HC93], e.g. financial results; production efficiency; market reputation; quality management; and HSE (health, safety and environment) management. The field of safety management, particularly the oil and gas industry, has a tradition for using performance indicators for persistent feedback control [KJ00]. Both information security management and safety management aim at loss prevention, thus experiences of performance indicators within the safety field has been utilized as background information for developing indicators for incident response management.

Performance indicators are often used as input for feedback control, which is a regulating mechanism that produces corrective action. The performance of a control object (in this paper, an incident response management system) is monitored and compared to a norm, Fig. 1. Any difference between actual performance and the norm is used as input to decisions with respect to actions or improvements of the management system. In that sense, feedback control can be used in evaluating whether a given control subject works as intended or not. Consequently, performance indicators are important for the monitoring part of the feedback loop, and are thus the key input for decision-making.

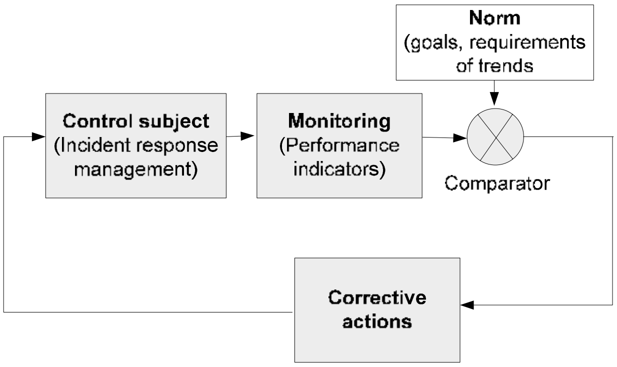

Fig. 1. System controlled through negative feedback (adapted from Kjellén [KJ00])

The principles for establishing norms for different indicators may vary. There might be a fixed goal established for a specific period of time, e.g. average time of response during a month should not be more than four hours. Another norm might be that an indicator must show continuous improvement from one period to the next. Furthermore, performance indicators might be used to evaluate whether a process is stable, by using control charts for several periods of time.

3 Performance Indicators for Incident Response Management

This section describes indicators for all the four phases of incident response management [ISO04]: 1) plan and prepare; 2) use; 3) review; and 4) improve. Each indicator is discussed with respect to how it could be measured and analysed and how it is expected to support decision-making processes. Table 1 summarizes the set of developed indicators. Before introducing a more detailed description of each indicator, an overview of how the indicators were developed is given.

Table 1. Set of indicators monitoring the performance of incident response (IR) management

Phase of IR management	Performance indicator
Plan and prepare	Rating system for the quality of the IR management system Assessment of information security culture w.r.t. to IR
Use	Number of incidents responded to during a period (d.a p.) Average time spent on responding pr incidents d.a p.
Review	Total consequences of incidents d.a p. Number of incidents of high loss d.a p. Downtime of SCADA systems due to incidents d.a p. Total costs related to incident response d.a p.
Improve	Average order of feedback d.a.p.

3.1 Method

Two main sources were used as inspiration for the development of the performance indicators of this paper: 1) representatives from the Norwegian oil and gas industry; and 2) related work on incident response; performance indicators; and information security in general.

Interviews and conversations with chief security officers in large Norwegian oil and gas enterprises have been performed, which have revealed relevant challenges and needs experienced by the industry itself. These interviews have shown that there is a lack of plans for monitoring and sets of indicators for incident response performance.

Indicators on information security in general have been identified in central standards and best practice guidances. The National Institute of Standards and Technology (NIST) has published two guides of relevance; *Security Metrics Guide for Information Technology Systems* [NI04a] and *Computer Security Incident Handling Guide* [NI04b] and ISO/IEC 17799 *Code of practice for information security* [ISO05a] is best practice on the area of administering information security in an organisation. One specific set of indicators are presented by Booker [Bo06]. US-CERT [USC05] and British Columbia Institute of Technology (BCIT) [BCI05] have taken a closer look to industrial security and control systems, and are therefore very interesting when selecting performance indicators for the scope of this paper.

Publications on safety management performance indicators [e.g. Kj00; Ti05] have also been used for inspiration. Although the field of safety management and information security are somewhat different, they are closely related in many ways. Safety performance indicators are far more explored than indicators within information security, and should thus be helpful for the purpose of this paper.

3.2 Indicators for the Plan and Prepare Phase

Indicator 1: Rating System for the Quality of the Incident Response Management Systems. Within the field of safety management results from audit-based rating systems for companies' safety management systems are used as a performance indicator [Kj00] for the quality of an incident response management system as it is planned and documented. This quality, i.e. how well-prepared the management structures are for handling incidents, is measured by looking at management elements such as feedback system, goals, documentation, management commitment, and education [Al99]. Regarding information security incidents it should also be considered to what extent necessary security mechanisms are in place. Audit-based rating systems resulting in performance indicators regarding the management structure are based on the following principles [Kj00]:

- An ideal model defining the elements of the management system and its contents.
- A scale is established for measurement of each element with respect to degree of compliance with the standard model.
- A set of criteria is used in evaluating actual performance in relation to the ideal model.
- The organisation compares actual performance with established goals.

This indicator supports decision-making by specifying to what extent the planned incident response management system is appropriate for the context of the organisation. By rating the quality of different elements of the management system, the indicator gives input to what parts of the management system that are not adequate for the current context of the organisation. Consequently, the indicator makes it possible to identify and improve inadequate parts of the management system.

Indicator 2: Assessment of Information Security Culture with respect to Incident Response. It is difficult to provide one universal definition of information security culture. It can be said that the concept of information security culture deals with the shared values and beliefs of the members of an organisation, which states the members' commitment to the organisation's information security management systems and performance, including incident response. A performance indicator measuring information security culture with respect to incident response will, among other things, identify whether organisational members are well prepared regarding incident handling. This indicator may e.g. show that employees are not willing to report unwanted incidents. Consequently, it should be possible to develop measures such as training and awareness campaigns in order to increase the members' commitment to the planned incident response management system.

CheckIT [JND05] is an example of a tool measuring and improving information security culture. It consists of a questionnaire combined with group-based discussions and identification of improvements. The questionnaire contains 30 questions which are to be assessed on a scale from 1 to 5 by each respondent. The scale is based on Westrum's taxonomy of cultures ranging from a pathological, i.e. bad, culture to a generative, i.e. good, culture [We93]. By statistical analyses of the results from the questionnaire, a performance indicator regarding information security culture is produced. The questionnaire covers many dimensions of an information security culture. Regarding incident response, it includes questions on individual awareness and willingness to report and react on incidents. It is thus possible to produce a performance indicator regarding cultural aspects of incident handling. This is valuable input used for evaluating whether the organisation is sufficiently prepared and committed to incident handling.

CheckIT is both a questionnaire and a process involving key stakeholders to agree on remedial actions. The suggested actions or changes should be discussed and implemented to improve the trust between the participants, thus there must be a certain period between each time the method is used. An appropriate period could be once a year. The actions identified are carried out continuously.

3.3 Indicators for the Use Phase

Indicator 3: Number of Incidents Responded to during a Period. An incident is be responded to when it is discovered, the responsible party is informed, and some kind of action is taken to deal with the problem. When evaluating an organisation's ability to handle incidents, the number of incidents responded to is an important measure. However, this indicator must be considered with care. For example, a major decrease in this number from one period to the next does not necessarily mean that the quality of the incident response management has changed radically, but may be due to external factors such as a change in the overall risk picture, or a few serious incidents that required the highest priority over other, less serious incidents.

This indicator may be used for increasing awareness about the amount of incidents occurring, both internally in the organisation, and also among suppliers and contractors.

However, the main use of this indicator is as a basis for other indicators described in the following sections. It is most useful when presented in context with other parameters as well.

What is a reasonable period of time for measurement must be considered for different contexts. If the organisation typically experiences maximum one or two incidents per month, it may be more interesting to look at a longer period, like a quarter of a year. This consideration applies to all indicators looked at during a certain period.

Indicator 4: Average Time Spent on Responding pr Incidents during a Period. The time spent on responding to an incident says something about the efficiency of the incident response management. To obtain a number that is comparable from period to period, it is necessary to look at the average of this time spent pr incident. The time span goes from an incident is detected until the handling of the incident is finished. As an example, if the incident caused an abnormal situation for systems in operation, the handling of the incident is finished when the systems are recovered and again running in normal operation.

The average time should decrease as improved incident response is achieved, as long as the complexity of the incidents occurring or other factors of importance do not change dramatically. Earlier detection will occur due to increased understanding of abnormal situations, e.g. the time from a computer starts acting abnormal to one understands that it may be virus-infected will decrease. People will have a clearer view on what to react on, know how to respond, and know how to solve the problem as fast as possible. Furthermore, this indicator is valuable input to improve incident response, by e.g. training for more efficient response.

A trend analysis will show if this indicator significantly decreases or increases over time, which will give a more accurate picture of the efficiency of the incident response management, than just a comparison between two successive periods. The indicator should be derived from a reporting system, which also would account for the reporting required by the rules and regulations of the authorities.

3.4 Indicators for the Review Phase

Indicator 5: Total Consequences of Incidents during a Period. One of the ultimate goals of improving incident response management is to reduce the total consequences of all incidents. To compute the total consequences, one needs to sum up the consequences of every single incident one has responded to.

However, it is difficult to estimate the consequences of every incident, because there are different types of loss, and not all of them are easily translated into money value. Within the oil and gas industry, incidents can result in the following types of loss: direct financial loss. i.e. loss of production; injury to people; damage to the environment; loss or damage of assets; and immaterial loss, such as degrading of the organisation's reputation. One may rate the loss of each incident regarding these different types of losses using the following severity scale: negligible; marginal; serious; critical and catastrophic. To this scale one should add a money value scale, such as saying that for a consequence to be negligible the direct financial loss should be less than $10.000 or that injury to people should be limited to first-aid injuries. Each organisation must determine this scale as appropriate for them. The table below shows a way to structure the assessment of each incident.

Table 2. Matrix for evaluating the consequences of incidents; should be included in the reporting of each incident

	Direct financial loss	Injury to people	Damage to the environment	Loss or damage of assets	Immaterial loss
Catastrophic					
Critical					
Serious					
Marginal					
Negligible					

To estimate the total consequences of all incidents, one should sum up the matrices for each incident to see which types of losses have the highest occurrences. For simplicity, one may look only at the degree of loss. Improvement is indicated by a reduction in the possible loss of all incidents summed up.

A trend analysis will show if the consequences significantly decrease or increase over time, which will give a more accurate picture of the efficiency of the incident response management, than just a comparison between two successive periods.

This indicator may however be affected by other measures than just improvements to the incident response management system. It is still important to include it as an indicator because one of the goals of incident response is to reduce the consequences of incidents. Also, the requirements to an information security management system described in ISO/IEC 27001 [ISO05b] state that there should be mechanisms in place for quantifying and monitoring costs of information security incidents.

Indicator 6: Number of Incidents of High Loss during a Period. The incidents one wants to avoid the most are the ones resulting in the most severe loss. This indicator measures the number of incidents with the most sever losses, i.e. those incidents that are categorized as catastrophic or critical in the matrix in table 2 above. This indicator is closely related to the one on total consequences. The indicator of total consequences shows the loss of all incidents, while this indicator shows exactly how many incidents cause the most severe consequences.

This indicator should, according to chief security officers in the oil and gas industry, be very useful for risk communication to different stakeholders. Not least because it will draw attention to the need of high-quality incident response management among decisions-makers at higher levels in the organisation. Furthermore, the indicator is helpful in communicating the importance of awareness and willingness to react to incidents among all kinds of employees.

Indicator 7: Downtime of SCADA Systems due to Incidents during a Period. A SCADA system may be down due to an incident or due to planned maintenance. The former is relevant in connection to incident response. System downtime may result in loss of production, hence leading to financial loss. Irrespective of that, system downtime leads to frustration among employees because they are hindered from doing their regular work. Improved incident response should imply fewer incidents and faster recovery hence a reduction in system downtime should be achieved.

An incident does not necessarily result in downtime. This is why it is meaningful to use both this indicator and indicator 4 ‘time spent on responding to incidents’.

This indicator can be used to highlight the loss of incidents occurring, and it should be derived from a reporting system, which also would account for the reporting required by the rules and regulations of the authorities. The indicator gives input for improving the incident response management system as a too high indicator signifies that the efficiency of incident response is not good enough.

Indicator 8: Total Costs Related to Incident Response during a Period. Responding to incidents requires investments, both for preparations in advance and when incidents actually occur. The number of people involved and the amount of time and money they spend are parts of the total costs.

More efficient incident response should result in more efficient use of manpower and money and hence, the total cost related to incident response should decrease.

The total cost should be seen in connection with the total consequences of all incidents. A risk analysis must create the foundation for determining a reasonable balance between these two; so that investments on incident response are in proportion to the acceptable level of risk for consequences of incidents.

3.5 Indicators for the Improve Phase

Indicator 9: Average Order of Feedback during a Period. It is of outmost importance to communicate the lessons learned from each incident to all parts of the organisation – to management, employees, operators, suppliers, contractors, and others. The order of feedback is an indicator of the degree of learning from previous experience developed by Van Court Hare [Va67]. It also reflects what kinds of measures are taken after an incident. There are five orders of feedback ranging from no learning to long-term organisational learning, i.e. double-loop learning [AS96]:

- System order 0: No follow-up of incident.
- System order I: Correction of deviation without learning. The deviation may reoccur.
- System order II: Long-term storing of experience by means of changes in e.g. design or work procedures at the workplace of the incident. Lasting effects that may prevent reoccurrence, but of limited scope as it does not affect other workplaces.
- System order III: Long-term storing of experience by means of changes in the total technical and administrative systems at the functional department. Lasting effects that will affect other workplaces as well.
- System order IV: Long-term storing of experience by means of changes in the general management, the information security management system and the incident response management systems and norms. The changes will not only have lasting effects, but will also have a wide scope and affect many workplaces all over the organisation.

The indicator is measured be classifying the follow-up of each incident regarding the five orders of feedback. Then it is possible to quantify the average order of feedback during a period of time, which can be periodically compared. Learning should be aimed at the highest possible order of feedback, as this will have the best effect regarding time and scope of learning. The indicator will show to what extent an organisation learns from incidents. Is the organisation mainly doing fire fighting, i.e. correcting deviations, or is the whole organisation learning from the incident. By analysing the degree of learning it is possible to improve follow-up of incidents.

This indicator has been limited to learning within an organisation. At the same time, experience exchange to other organisations should happen as well. This inter-organisational learning can happen at all the orders of feedback presented above. For a more sophisticated analysis of learning, this inter-organisational learning can be monitored as well.

3.6 Combining Indicators

Combining two or more indicators will produce better support for decision-making as it increases the understanding of how incident response management functions and the effects of implementing new measures. By combining indicators, the credibility of monitoring incident response management increases. Merging different indicators makes it possible to create numerous combinations of indicators, e.g.:

- The ratio of number of incidents with high loss to total number of incidents. This combination gives an indication of the change in the overall loss of the incidents.
- Comparing the consequences of incidents and the costs of incident response management. This will show the elasticity of the resources used to minimize the consequences. This is important input for cost-utility analysis deciding the amount of incident response management efforts.
- Average loss per incident of high loss can be created by the ratio of the consequences of high loss incidents to the number of incidents with high loss. A rise in this ratio signals higher loss per incident and thus the need to improve incident handling in general and particularly for high loss incidents.

There are lots of possible combinations of indicators that can be utilized. The main reason for combining indicators is to perform a more sophisticated and detailed analysis of the results the other indicators provide. If one for example experiences a significant worsening of the indicator ‘average time spent on responding pr incident’, a possible way to react to this is to perform more detailed analysis by combining this indicator with e.g. consequences of incidents. This combination will answer if the increased response time originates from more severe incidents.

4 Evaluation of the Performance Indicators

Performance indicators can be evaluated by different approaches. One approach is a theoretically driven evaluation of the indicators. Another way is to apply them practically in the field as an exploratory approach. The proposed indicators in this paper have not been tested in the latter way, but are theoretically evaluated in this section. For further development and research, the indicators should be tested in practice.

4.1 Requirements for a Performance Indicator

Requirements for performance indicators are utilized in evaluating the indicators described in section 3. Kjellén’s [Kj00] requirements for HSE performance indicators are adapted for this purpose. A performance indicator should satisfy the following requirements:

- observable and quantifiable, i.e. it must be possible to observe and measure performance by applying a recognized method and scale of measurement
- valid, i.e. whether the indicator measures what is intended to measure

- sensitive to change, i.e. changes in the control subject and its' surroundings will be captured by the indicator
- compatible with other indicators, i.e. the indicators must not be contradicting for decision-makers
- easily understood, i.e. different users understand the meaning of the indicators

For the evaluation of the indicators it is asked whether the indicator satisfy each of the requirements above. This is summarized in table 3. The indicators are indexed Y (yes) if satisfying the given requirement and no (N) if not satisfying it. If an indicator is partly satisfying a requirement, the index Y/N is used.

As shown in table 3, all the proposed indicators for monitoring incident response management have weaknesses and strengths. It is thus important to have a set of indicators complementing each other. It can be assumed that the presented indicators match each other in a satisfying way. In the following, deviations from the requirements are explained.

Table 3. Evaluation of performance indicators for incident response management

	Observable and quantifiable?	Valid?	Sensitive to change?	Compatible with other indicators?	Easily understood for different users?
Rating system for the incident response management system	Y	Y/N	N	Y/N	N
Assessment of information security culture regarding incident response	Y/N	Y/N	N	Y/N	N
Number of incidents responded to d.a p.	Y	Y	Y	Y	Y
Average time spent on responding pr incidents d.a p.	Y	Y	Y	Y	N
Total consequences of incidents d. a p.	Y/N	Y/N	Y	Y	N
Number of incidents of high loss d. a p.	Y/N	Y/N	Y	Y	Y
Downtime of SCADA systems d. a p.	Y	Y/N	Y	Y	N
Total costs related to incident response d. a p.	Y	Y	Y	Y	Y
Average order of feedback d.a.p.	Y/N	Y	Y	Y	N

Neither the 'rating system for the incident response management system' nor the 'assessment of security culture' satisfy the requirement sensitive to change. For practical reasons, it is suggested that these two indicators are measured once a year. Nevertheless, the organisational culture, structure, and context are continuously changing dynamic risk contributing issues [Ra97]. Consequently, the suggested measuring strategy will only capture changes in conditions related to information security structures and cultures on a yearly basis. This might imply that important risk-related changes are not captured in time thus making the specific indicators insensitive to continuous change.

Planned, expected organisational and individual behaviour and actual organisational and individual behaviour are often contradictory [e.g.Br02]. The indicator 'rating system for the incident response management system' monitors the planned, expected behaviour, while the indicator 'assessment of information security culture' assesses actual organisational and individual behaviour. Consequently, these two indicators might be contradictory.

The indicator related to information security culture might have weak validity. It can be questioned whether it is culture, i.e. shared values and beliefs of organisational members, *or* individual attributes that are measured. To ensure that shared values are measured, it is suggested to discuss the questionnaire in a group setting. It can be argued that both characteristics are measured thus validity is dependent on the answer of the question above. Individual attributes are dissimilar to culture, as culture is not about single individual attributes but rather about how individuals interact [Ro02]. Furthermore, it can be questioned whether it is possible to quantify a culture. An interpretive/anthropological approach to culture will state that is hard to quantify culture [e.g. Ha01]. A functionalistic approach to culture on the other hand, claims that culture can be measured quantitatively [e.g. We93]. Consequently, whether culture is quantifiable or not is dependent on how one approaches observation of culture. Survey tools for assessing culture quantitatively are based on a functionalistic approach, and it is thus possible to assess information security culture quantitatively.

The performance indicators 'consequences of incidents' and 'number of reported incidents of high loss' have a common weakness regarding validity. This weakness is related to how consequences of incidents are categorized. The consequences of an incident might differ according to type of loss: direct financial loss; injury to people; damage to the environment; loss or damage of assets; and immaterial loss. The validity is dependent on the strength of this categorization. E.g. how can one ensure that a catastrophic consequence regarding material loss is the same as a catastrophic consequence for immaterial loss? It is easier to measure the consequences of incidents that are straightforwardly financially quantified. Longitudinal losses such as loss of reputation or delayed injuries to people make it even more complex to measure consequences of an incident. Following this argument, the indicator 'consequences of incidents' has a weakness regarding the requirement of quantification as well.

The indicator 'average downtime of SCADA systems' has weaknesses regarding the requirements on validity and sensitivity. Both incidents and planned maintenance might produce downtime of SCADA systems. Consequently, these two occurrences might create trouble when measuring downtime – is the downtime planned or is it unintentionally or intentionally produced? Are changes in the indicator created due to planned downtime or due to incidents?

The indicator 'average order of feedback' is somewhat difficult to quantify, as it might be difficult to differ the diverse orders of feedback.

Several of the indicators require a certain degree of knowledge on incident response management in order to fully understand them. Consequently, it might be difficult for lay people and top managers to understand some of the indicators. This can be an obstacle for risk communication in the organisation. For decision-makers without necessary knowledge to understand the meaning of some of the indicators, this might even lead to less optimal decisions.

4.2 Completeness of the Performance Indicators

Performance indicators can be categorised as leading or lagging indicators [Ph04], which sort out what improvements the indicators are used for. Leading indicators focus on removal or reduction of root causes; establishing and strengthening barriers; and improving the organisation before an incident occurs. Lagging indicators, on the other hand, focus on reducing the consequences of incidents.

The indicators proposed in section 3 cover both leading and lagging indicators. The leading indicators are:

- administrative rating system; identifying root causes and strengthening operational barriers;
- assessment of culture; identifying root causes and strengthening operational barriers;
- number of incidents responded to pr. period; creating awareness and thus improving the information security organisation;
- number of incidents of high loss pr. period; highlighting the loss of the problem and gaining more support and funding and thus improving the information security organisation;
- downtime of SCADA systems during a period; highlighting the loss of the problem and gaining more support and funding and thus improving the information security organisation.

The lagging indicators are:

- average time of reaction during a period; improving incident handling and strengthening barriers;
- consequences of incidents; improving incident handling and strengthening barriers.

Furthermore, performance indicators can be either reactive or proactive [Ti05]. Reactive indicators measure what incidents result in, e.g. severity of loss. Proactive indicators, on the other hand, measure the effort made to prevent and reduce loss. The proposed indicators in section 3 are mainly proactive. Nevertheless there are two reactive indicators as well; consequences and number of high loss incidents.

Figure 2 shows the completeness of the performance indicators described in section 3 regarding an incident model. Altogether the indicators cover the whole sequence of an incident ranging from root causes to losses.

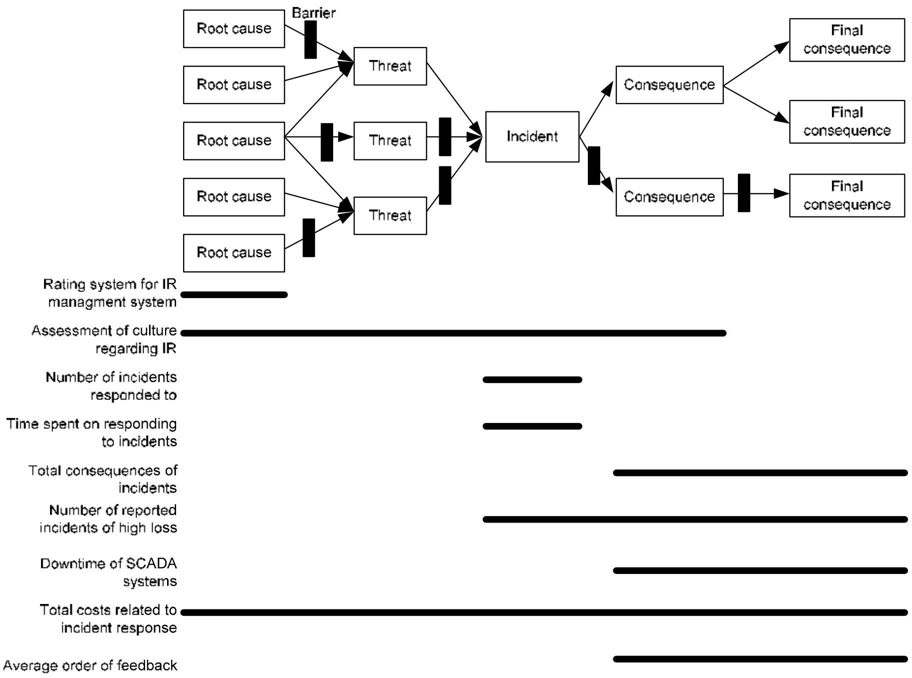
Barrier
Root cause
Root cause
Root cause
Root cause
Root cause
Threat
Threat
Threat
Incident
Consequence
Consequence
Final consequence
Final consequence
Final consequence
Rating system for IR managment system
Assessment of culture regarding IR
Number of incidents responded to
Time spent on responding to incidents
Total consequences of incidents
Number of reported incidents of high loss
Downtime of SCADA systems
Total costs related to incident response
Average order of feedback

Fig. 2. Performance indicators for incident response (IR) management and coverage of sequences of an incident.

The indicators are developed within the different phases of incident response management described in TR 18044 'Information security incident management' [ISO04] as a framework. The indicators are thus complete regarding all phases of incident response management as well.

Following the arguments in this section, it can be claimed that the proposed indicators of this paper creates adequate coverage regarding 1) type of improvement (leading and lagging indicators); 2) loss prevention and actual loss (proactive and reactive indicators); 3) incident sequences; and 4) phases of incident response management.

5 Conclusion

Monitoring incident response management is important support for decision-making aiming at improved incident response. Performance indicators are well suited for this purpose as they in a comprehensible way make it possible to measure processes, communicate results, and make decisions. This paper proposes and evaluates a set of performance indicators that support monitoring of the performance of incident response management. Each indicator has its weaknesses and strengths, it is thus important to use the full set of indicators as they overlap each other's weaknesses. Combining indicators in order to produce new ones is also recommended in order to get deeper insight of the incident response management performance. The sum of all the proposed indicators covers the total performance of incident response management in an organisation.

The proposed performance indicators are not tested empirically. This should be done in order to evaluate the practical quality of them. Testing must be performed over a period of time. A practical utilization of them should even prove to be helpful in identifying the need for other indicators than the ones proposed in this paper.

Acknowledgements

This paper is developed within the research projects IRMA [Jo04] – Incident Response Management and AMBASEC – A Model-Based Approach to Security Culture, financially supported by the Research Council of Norway and the Norwegian Oil Industry Association. We offer thanks to the Norwegian oil company Hydro for contributing with a pilot for a case study in the projects.

Martin Gilje Jaatun and Lillian R□stad (SINTEF ICT); Jose Gonzales (Agder University College) have contributed with well-formulated and constructive input.

References

[Al99] Alteren, B. Implementation and evaluation of the Safety Element Method at four mining sites. In Safety Science vol 3 (1999), pp.231-264

[AS96] Argyris, C and Schön, D. Organizational Learning II. Addison Wesley, New York (1996)

[BCI05] British Columbia Institute of Technology (BCIT): Industrial Security Incident Database Reporting Form. www.bcit.ca/appliedresearch/security/services.shtml#9 (2005)

[Bo06] Booker R.: Re-engineering enterprise security. Computers & Security (2006) 13-17.

[Br02] Brunsson, N. The organization of Hypocrisy. Talk, Decisions and Actions in Organizations. Abstrakt forlag, Oslo (2002)

[Ha01] Haukelid, K. Oljekultur og sikkerhetskultur. [In Norwegian. Oil culture and safety culture] (2001) Available at: www.risikoforsk.no/Publikasjoner/Oljekultur%20og%20sikkerhetskultur.pdf

[HC93] Hammer, M., Champy, J.A.: Re-engineering the Corporation: A Manifesto for Business Revolution. Harper Collins, New York, NY. (1993)

[IS04] ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management.

[IS05a] ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.

[IS05b] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

[JND05] Johnsen S.O., Hansen C.W., Nordby Y., Dahl M.B.: Measurement and improvement of information security culture, HKARMS Asia-Pacific Conference on Risk Management and Safety, ISBN 962-442-279-6. (2005) www.checkit.sintef.no

[Jo04] Johnsen, S., R□stad, L., Haugset, B. and Dahl, M.B.: From Incident Response to Incident Response Management. Proceedings from Probabilistic Safety Assessment and Management (2004)

[Kj00] Kjellén, U.; Prevention of accidents through experience feedback, Taylor and Francis. (2000)

[NI04a] NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems. http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf (2004)

[NI04b] NIST Special Publication 800-61: Computer Security Incident Handling Guide. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (2004)

[Ph04] Phimister J. et al: Accident precursor analysis and management Reducing Technological Risk Through Diligence. The national academies press (2004)

[Ra97] Rasmussen, J. Risk management in a dynamic society: a modeling problem. In Safety Science vol 27, no.2/3 (1997) pp:183-213

[Ro02] Rosness, R. Safety Culture: Yet another buzzword to hide our confusion? (2002) Available at: www.risikoforsk.no/Publikasjoner/Safety%20culture.pdf

[Ti05] Tinmannsvik, R.K. Ytelsesindikatorer for flysikkerhet. [In Norwegian: Performance indicators for air transport safety] SINTEF report (2005)

[USC02] US Congress: Sarbanes-Oxley act of 2002. Available at: http://files.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

[USC05] United States Computer Emergency Readiness Team (US-CERT): Control Systems Cyber Security Awareness. US-CERT Informational Focus Paper, July 7th 2005, Available at: www.us-cert.gov/reading_room/Control_System_Security.pdf

[Va67] Van Court Hare: System Analysis: A Diagnostic Approach. Harcourt Brace & World, New York (1967)

[WE93] Westrum, R. J.: Cultures with Requisite Imagination. Wise, Stager and Hopkin (Eds.) Verification and Validation of Complex Systems: Human Factors Issues, Springer, Heidelberg. (1993)