Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2016

A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden

Gunnar Wahlgren
Stockholm University, wahlgren@dsv.su.se

Stewart Kowalski
Norwegian University of Science and Technology, stewart.kowalski@ntnu.no

Follow this and additional works at: http://aisel.aisnet.org/wisp2016

Recommended Citation
Wahlgren, Gunnar and Kowalski, Stewart, "A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden" (2016). *WISP 2016 Proceedings*. 8.
http://aisel.aisnet.org/wisp2016/8

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2016 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Maturity Model for Measuring Organizations Escalation Capability of IT-related Security Incidents in Sweden

Completed Research Paper

Gunnar Wahlgren
Stockholm University, Sweden {wahlgren@dsv.su.se}

Stewart Kowalski
Norwegian University of Science and Technology, Norway {stewart.kowalski@ntnu.no}

ABSTRACT

Managing IT-related security incidents are a growing important issue facing the organizations in IT security risk management. We have used design science approach to develop an artifact to measure different organizations capabilities and maturity to handle IT-related security incidents. In this paper, we present how we have tested and will test the artifact on several different Swedish organizations. The participating organizations come from both the private and public sectors and all organizations handle critical infrastructure which can be damaged if an IT-related security incident occurs. Organizations had the opportunity to evaluating the actual model itself but also to test the model by calculating the organization's escalation capability using a query package for self-assessment. In this paper, we present the results of the self-assessment which indicate an overall low level of maturity in Sweden. The most remarkable result was only 20% of the participating organizations in the study had "Knowledge and Education" maturity above the lowest levels.

Keywords: Incident escalation, Maturity models, IT security risk management, Incident management.

INTRODUCTION

The Swedish National Audit office concludes in a recent report that for Government agencies the overall capacities to handle the consequences which can arise from serious information security incidents are largely unknown. Overall risk evaluation is currently lacking and instead there is uncertainty how strong the protection is and which incidents have taken place (NAO 2014). Managing IT-related security incidents are a growing important issue facing many organizations in Sweden and around the world. To manage escalation of incidents, organizations need established crisis teams with reporting channels and related report management tools that can handle incidents that do not require immediate action or escalation.

As part of a doctoral research program at the Department of Computer and Systems Sciences, Stockholm University we are carrying out a research projects in IT security risk management. The purpose of our research is providing a solution to this growing problem of managing IT related security incident. In our research, we have used design science approach to propose a mature model to be used by organizations and authorities to measure the capability to escalate IT related security incident both within and between organization and authorities. The advantage to use a maturity model is that it makes it possible to obtain a measurable result to compare and stepwise improve the organization capabilities. The maturity model could for example be used by organizations and regulators to understand where shortcomings exist and help define target and action to improve managing of information security.

We have divided the rest of the paper into 4 sections. In the first section, we present different related works. In the second section, we describe our research plans and our maturity model for escalation capability. In the next section, we present the background for and the result of the study. In the last section, we conclude the paper with a discussion of how our model is developed and tested.

BACKGROUND

IT Security Risk Management

The International Standard Organization (ISO) has established a standard for IT Security Risk Management; ISO/IEC 27005 (ISO 2013). The term IT Security Risk Management refers to approaches and methods that lead to cost effective security solutions and countermeasures. This is done by a process of measuring the security risk to IT systems and assuring adequate levels of protection. IT Security Risk Management is a continuous process and consists of the following steps (i) Risk monitoring, (ii) Risk Assessment/Risk Treatment, and (iii) Risk communication. The National Institute of Standard and Technology (NIST) has introduced a framework for Enterprise-wide Risk Management using three different levels or tiers where IT security risk management decisions are made: (i) Top management, (ii) Middle management, and (iii) Operation (NIST 2010).

For our research we have combined the ISO and NIST frameworks. The reason for this is that we assert that in practice each organizational level has its own individual Risk Assessment / Risk Treatment, Risk Monitoring, and Risk Communication processes. Since risk management decisions are made at different levels in an organization it is extremely important that the communication between the different organizational levels function efficiently work and that there are tools that can measure and monitor the efficiency of communication. Management of IT-related security incident is an area where communications between the different levels are critical. Our escalation Maturity Model represents an attempt to measures and help organizations improve the communication of risk decision between the levels within and between organizations.

Escalation and escalation of IT-related security incident

The term escalation in the vernacular is used to describe how conflicts issues are handled by a higher level in the organization or society (Kahn 1965). We instead use the term when one level seeks assistance or informs a higher level about an issue it cannot handle. This means in both cases that you also pass the responsibility for dealing with the IT security risk to a higher level.

When defining IT-related security incident we have used the definition from Swedish Civil Contingencies Agency (MSB): “An IT incident is an undesired and unplanned IT related incident affecting the security of the organization's or society's information processing and that may cause a disruption of the organization's ability to conduct its operations" (MSB 2012). Examples of IT related incidents are disruption in software and hardware, loss of data, security vulnerabilities in products, external attacks, human errors in handling, interference in the operating environment, and external events.

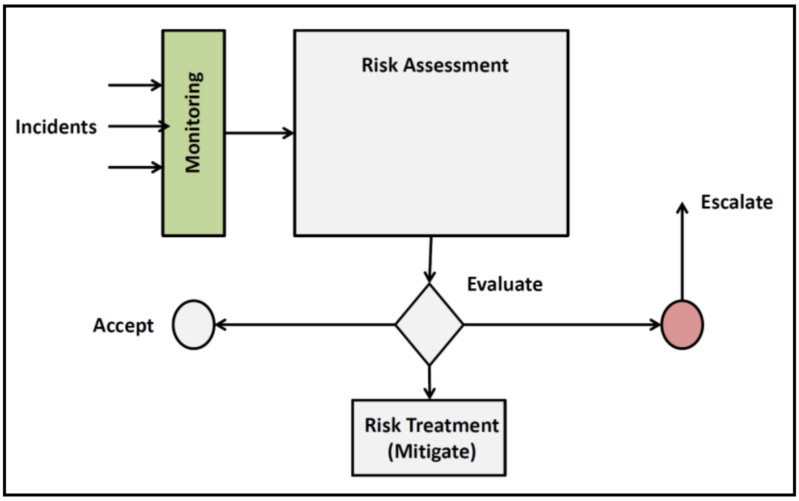


Figure 1. Handling of incidents

In Figure 1, we outline how different security incidents are analyzed with help of a given assessment process and depending on the outcome determine if the incident should be accepted, resolved or escalated. There could be many reasons to escalate. One reason could be budgetary considerations as it could be necessary to implement new expensive countermeasures. Another example is that the incident is so serious that help from a higher level is needed. Escalation of an IT-related security incident will probably lead to risk treatment of some kind. For example, if a crisis occurs, the organization must respond and recover from the damage the incident has caused. If the incident does not require immediate action, this could lead to that, in the future, new countermeasures to deter, prevent, and detect should be installed if similar incidents will reoccur.

Maturity models

The capability maturity model was first described by Humphrey who used maturity models for assessing software engineering capability of contractors (Humphrey et al. 1987). ISO discuss design principles of maturity models. There exist two types of process categories: Basic Process set and Extended Process set (ISO 2008). Pöppelbuβ describes three purposes for using maturity models: (i) Descriptive, (ii) Prescriptive, and (iii) Comparative (Pöppelbuβ et al. 2011). The Risk IT Framework from ISACA presents how maturity models could be used to recognize on what maturity levels different IT-security risk management processes are (ISACA 2009).

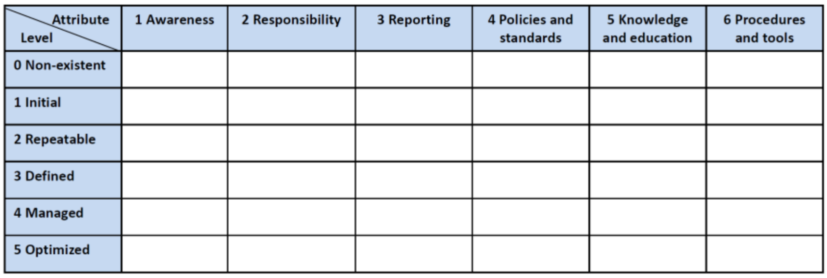
APPROACH

Introduction

The reason we have chosen a design science approach is that we need to develop an artifact where we can use different cases to validate our model. Design science research methodology consists of 5 steps (Vaishnavi and Kuechler 2004). First we gather information of the real-world problem. The next step is a tentative design. In the third step an artifact is developed. In the next step the artifact is evaluated with help of performance measures. In the last step the design processes are completed and conclusions are drawn. These steps are iterated until the real-world situation is improved. Our research is divided into three cycles. First we constructed the primary version which was evaluated with help of IT security specialist from both the private and public sector and also from the academic world. We made some improvement based on the evaluation. Version 2 of our model was ready late 2014 and was tested on different organization which is described later in this paper. In cycle 3 we will create test scenarios which will be used by a number of organizations with different self-evaluated maturity levels. A security specialist from these organizations will describe how the organization will handle these test scenarios judge by an independent observer, who is unaware of the organization establish maturity level. The result will hopefully result in enough empirical data to confirm or refute our hypothesis that there a correlation between how an organization could handle an incident more efficient way (e.g. time to solve the problem) and higher maturity level for the organization.

The escalation maturity model

As ISACA’s maturity model (ISACA 2009) our model consists of a matrix with different maturity levels as rows and different maturity attributes as columns as shown in Figure 2. We have used the same five maturity levels as Humphrey (Humphrey et al 1987). We have also, as ISACA, added a sixth level "Non-existent". Regarding the maturity attributes, we have used ISACA's maturity model as a starting point but adapted the attributes around the management of IT-related security incidents.



Attribute Level	1 Awareness	2 Responsibility	3 Reporting	4 Policies and standards	5 Knowledge and education	6 Procedures and tools
0 Non-existent						
1 Initial						
2 Repeatable						
3 Defined						
4 Managed						
5 Optimized						

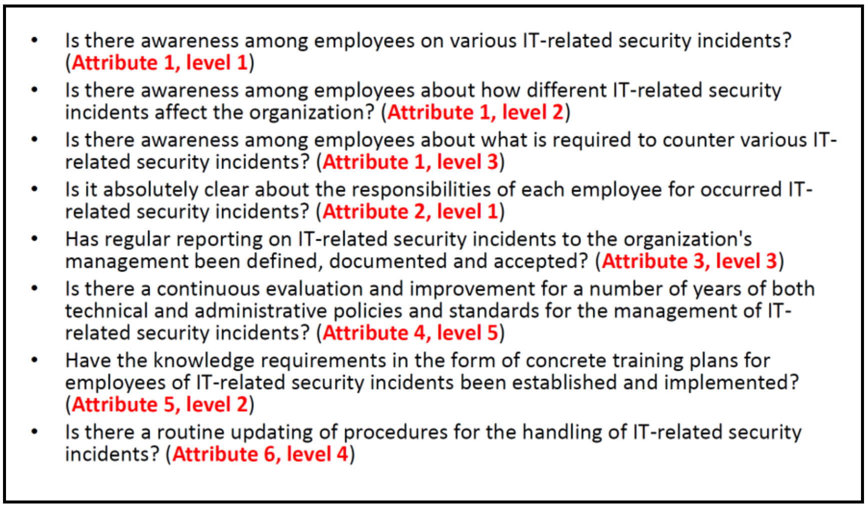
Figure 2. Escalation maturity model

The escalation maturity model has 6 different maturity levels. Level 0 “**Non-existent”** implies that different processes are not applied at all. Level 1 “**Initial”** is when the needs for measures have been identified and are initiated but the processes that are applied are ad- hoc and are often disorganized. Level 2 “**Repeatable”** is when measures are established and implemented and the various processes follow a regular pattern. Level 3 “**Defined”** is when measures are defined, documented and accepted within the organization. Level 4 “**Managed”** is when processes are monitored and routinely updated. Level 5 “**Optimized”** is when processes are continuously evaluated and improved using various performance and effective measures tailored to the organization's goals.

There are also six different maturity attributes which are fairly obvious when we want to assess an organization's escalation capability. It goes without saying, the employees must have "**Awareness"** of IT-related security incidents. There must be a clear allocation of **"Responsibilities"** for IT-related security incidents within the organization. "**Reporting"** channels of IT-related security incidents must be clearly defined. There must exist "**Polices and standards"** when escalation of IT-related security incidents should take place. "**Knowledge"** requirements for the different categories of employees of IT-related security incidents must be defined. There must be "**Procedures and tools"** how escalation of IT-related security incidents should be managed.

The query package.

The designed model artifact also includes a query package. The idea is that after the organizations have responded to the questions in the query package, it shall it be possible to determine the maturity level of the different maturity attributes. The number of questions in the current version is 37. The answer to each question (one or more) of the different maturity levels and attributes are "Yes" or "No". In this version we also have the response alternative "Do not know" which we in this context have interpreted as a "No" answer.



- Is there awareness among employees on various IT-related security incidents? (**Attribute 1, level 1**)
- Is there awareness among employees about how different IT-related security incidents affect the organization? (**Attribute 1, level 2**)
- Is there awareness among employees about what is required to counter various IT-related security incidents? (**Attribute 1, level 3**)
- Is it absolutely clear about the responsibilities of each employee for occurred IT-related security incidents? (**Attribute 2, level 1**)
- Has regular reporting on IT-related security incidents to the organization's management been defined, documented and accepted? (**Attribute 3, level 3**)
- Is there a continuous evaluation and improvement for a number of years of both technical and administrative policies and standards for the management of IT-related security incidents? (**Attribute 4, level 5**)
- Have the knowledge requirements in the form of concrete training plans for employees of IT-related security incidents been established and implemented? (**Attribute 5, level 2**)
- Is there a routine updating of procedures for the handling of IT-related security incidents? (**Attribute 6, level 4**)

Figure 3. Example of questions in the query package

Figure 3 shows examples of questions for the different attributes and to which maturity level each question belongs.

All of the maturity attributes in one maturity level must be satisfied before the next level can be obtained. It is important also to mention that the maturity level for various processes within one level, also apply for the next level. To find the current maturity level one needs take the maturity attribute that has the lowest value.

THE STUDY

Introduction

The Swedish Civil Contingencies Agency (MSB), together with the Department of Computer and Systems Sciences (DSV) at Stockholm University has conducted four seminars during April 2015. The participating organizations, who were invited by MSB, came from three sectors namely Trade and Industry, Governmental Agencies, and County Councils and Municipalities. Thirty three persons representing an information security function from the different organizations attended the seminars. The seminar was divided into two parts: (1) information classification of indicators and (2) a maturity model for measuring organizations escalation capability to handle IT-related security incidents. The first part was held by MSB. In the second part of the seminar individuals from the university presented the maturity model as well as the query package that was related to the model. An evaluation form where the participants were able to evaluate the maturity model was also presented. After the end of the seminar copies of the query package for self-assessment and the evaluation form were distributed the participants. The different organizations were expected to submit, at least the evaluation form, in a pre-paid letter to the university.

The organizations that responded belong to the following sectors: Trade and Industry (7 out of 8 possible), Governmental Agencies (4 out of possible 8), and County Councils or Municipalities (10 out of possible 17). The number of participating organizations that submitted the evaluation form was

21. The organizations that also sent in the query package were 16. This paper only describes the result from the self-assessment that the organizations have done with help of the query package. If we look at the person who answered the query package came from organizations with the following characteristics. The organization's size, in terms of number of employees, most organizations had more than 250 employees. All organizations had their own IT department. The majority of the organizations had an IT support department. Most of the organizations had their own IT operation department. All of the organizations handled critical infrastructure that can be damaged if an IT-related security incident occurs.

Result of the self-assessment

16 organizations submitted the query package. Many of these organizations had used the opportunity to respond "Do not know" to one or more of the questions in the query package. When we went through the answers we decided to not include those organizations that had answered "Do not know" to more than 25% of the questions. We concluded that in this case the representative who answered the questions has so poor knowledge of the organization in question that was not relevant to use the rest of the answers. After this review 10 organizations remained where the majority (7 of 10) had responded ”Do not know” to less than 10% of the questions. In the cases where the representative has responded "Do not know" to a question we interpreted this as a "No" answer. The results of each maturity attribute from the remaining 10 organizations are presented below and are summarized in Figure 4.

The result for the maturity attribute “**Awareness**” gives a somewhat mixed picture. One organization (of possible 10) did not understand the need for awareness among employees. The employees from 2 of the organizations seem to have at least some form of awareness of IT-related security incidents. For 2 of the organizations the employees also were aware how incident can affect the organization. Employees from 3 of the organizations also had good knowledge of different defined and documented IT-related security incidents. Two organizations had continuous evaluation and improvement of employees' awareness of IT-related security incidents.

The result for the maturity attribute "**Responsibility**" shows that a number of organizations (4 of possible 10) do not understand the need for accountability of IT-related security incidents. For 2 organizations the accountability for IT-related security incidents is established and implemented and it is clear which responsibilities that different employees have. For 2 of the organizations the accountability for IT-related are defined, documented and accepted by the organizations. Two of the organizations have ccontinuous evaluation and improvement of the accountability for both the technical and administrative management of IT-related security incidents.

The result for the maturity attribute "**Reporting**" shows that for the majority of the organizations (5 of possible 10), reporting of IT-related security incidents to the management has been identified and initiated. For 2 of the organizations reporting channels of IT-related security incidents are routine updated. For 3 of the organizations the reporting channels to the management of IT-related security incidents are also continuously evaluated.

The result for the maturity attribute "**Polices and standards**" also gives a somewhat mixed picture. Two of the organizations did not understand the need for policies and standards for IT-related security incidents at all, while for 1 organization polices and standards is at least identified and implemented. For 2 of the organizations policies and standards for IT-related security incidents are also establish and implemented. For 2 of the organizations both technical and administrative policies and standards for IT-related security incidents are defined, documented and accepted by the organization. For 1 organization both technical and administrative policies and standards for IT-related security incidents are routinely updated. Two of the organizations had continuous evaluation and improvement of both technical and administrative policies and standards for IT-related security incidents.

The most surprising results for the different maturity attributes were "**Knowledge and education**". A very large number of organizations (8 of possible 10) do not understand the need for employees' knowledge and training on IT-related security incidents. The implication of this is that these organizations among other things have not identified the knowledge requirements and training of employees on IT-related security incidents and that education plans are not defined and documented. Only 1 organization knowledge requirements and education plans for employees on IT-related security incidents have been established and implemented. For 1 organization both technical and administrative knowledge requirements and education plan for employees on IT-related security incidents are routinely updated.

The result for the maturity attribute "**Procedures and Tools**" shows that 1 organization seems to not understand the need for procedures and tools for management of IT-related security incidents. For 2 of the organizations procedures for managing IT-related security incidents have been identified and initiated. The majority of organizations (5 of possible 10) have procedures for managing IT-related security incidents that have been defined, documented and accepted. For 1 organization procedures for managing IT-related security incidents are automated and routinely updated. For 1 organization, these procedures are also continuously evaluated and improved.

When the responses from the participating organizations are analyzed, it turns out that only two organizations have reached the **total maturity level** "Repeatable" respectively "Initial". All other organizations have only reach the overall maturity level "Non-existent". The criterion for an organization to reach a total maturity level is that the organization has reached that level for all maturity attributes. If an organization, for example, shall reach the maturity level "Defined", all the individual maturity attributes, at least, must have reach the maturity level "Defined". Because of this, just two organizations have reached a total maturity level that is higher than the level "Non -existent". The main reason is that so many organizations only have obtained the maturity level "Non-existent", especially for the maturity attribute 'Knowledge and education' and the maturity attribute "Responsibility".

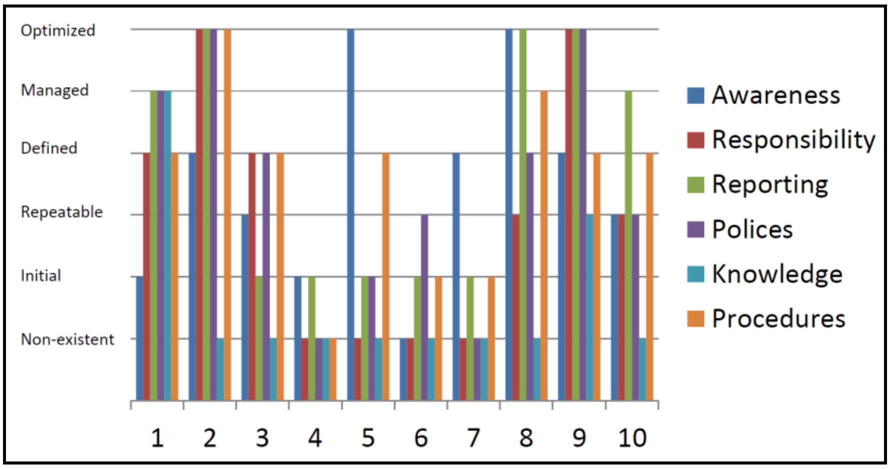
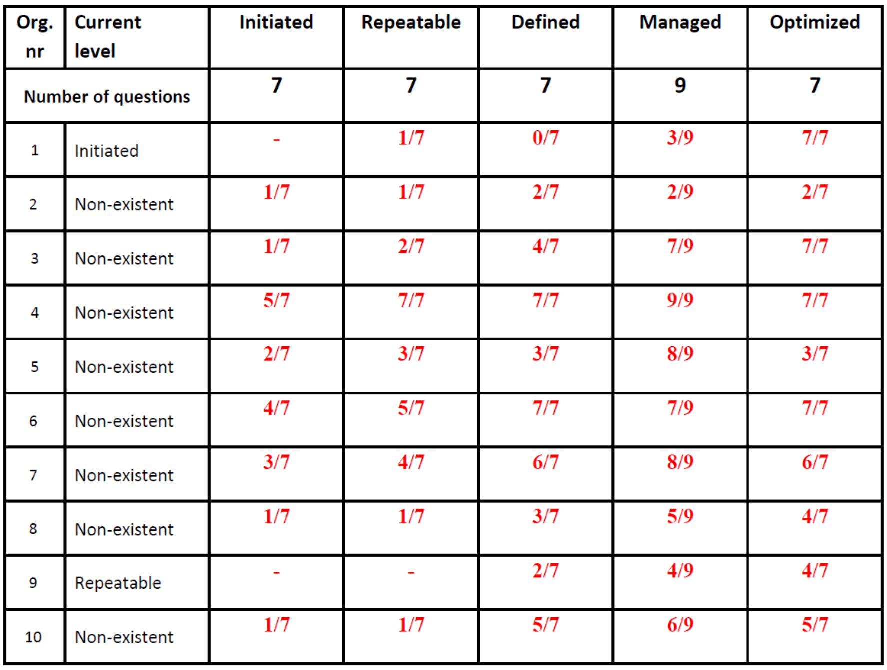


Figure 4. Maturity levels for all maturity attributes

To get an idea of the extent of actions that each organization must perform to reach the next maturity level, we have introduced the concept of "**Alignment efforts**". If an organization has answered "No" to a question in the query package, this will lead to that at least one action must be performed if the organization wishes to reach the next maturity level. We realize of course that the actions needed to meet the requirements that a question suggest can vary strongly but still think that "Alignment efforts" gives a pretty good idea of the amount of work that an organization must perform in order to reach the next maturity level. We define "Alignment efforts" for a specific maturity level is the sum of the questions with the answer "No" to all of maturity attributes of that maturity level, divided by the total number of questions for all maturity attributes of that maturity level. We define the "Total alignment efforts" to reach the highest maturity level (Optimized) as the sum of questions with the answer "No" for all maturity attributes, divided by the total number of questions for all maturity attribute. Figure 5 shows the "Alignment efforts" (Number of actions) that the organizations in the study must perform to reach the different maturity levels.



Org. nr	Current level	Initiated	Repeatable	Defined	Managed	Optimized
Number of questions		7	7	7	9	7
1	Initiated	-	1/7	0/7	3/9	7/7
2	Non-existent	1/7	1/7	2/7	2/9	2/7
3	Non-existent	1/7	2/7	4/7	7/9	7/7
4	Non-existent	5/7	7/7	7/7	9/9	7/7
5	Non-existent	2/7	3/7	3/7	8/9	3/7
6	Non-existent	4/7	5/7	7/7	7/9	7/7
7	Non-existent	3/7	4/7	6/7	8/9	6/7
8	Non-existent	1/7	1/7	3/7	5/9	4/7
9	Repeatable	-	-	2/7	4/9	4/7
10	Non-existent	1/7	1/7	5/7	6/9	5/7

Figure 5. Alignment efforts to reach next maturity level

CONCLUSIONS

It appears from the study that the overall maturity to handle the consequences which can arise from serious information security incidents is low. However, before you can know and compare these levels among organizations a calibration and deepening of the questions seems to be necessary if organizations should be able to use the maturity model as a tool for self-assessment. Several terms also need to be better defined. This could be the reason that many organizations responded "Do not know" to many of the questions. If the respondent had more time to examine a particular factual situation the answer to the question may have been different. Other reasons could be that the requirement for different maturity attribute that the organizations should achieve could be inaccurate or unclear. The query package in its current state is probably more suitable in an interview situation. In parallel with this study some students at DSV have used to the questions in the query package when they interviewed two organizations in the financial sector (Wahlgren et al. 2016) and they had not the slightest problem getting answers to all questions because at any ambiguities with a question they could provide the respondent with additional information.

We will therefore make several changes to our maturity model, and then we will develop a web-based tool, including a Help function, to assist organizations in the self-assessment process. The tool will be used by organizations to enter answers to the questions in the query packet and then automatically calculate the total level of maturity as well as the maturity level of the individual attributes. The tool will also calculate the Alignment efforts and suggest what action the organization could take to achieve the desired level of maturity. We will use English when we define our new maturity model so that it is possible to use our web-based tool internationally. To verify our new maturity model and the web-based tool we will use the tool on some organizations both in and outside Sweden. We will then continue with cycle 3 of our research where we will create a number of test scenarios that involve IT-related security incidents. We will select a number of organizations with different self-evaluated maturity levels. Then a security specialist from these organizations will describe how they will handle the test scenarios. The result will be judge by an independent observer. The result of cycle 3 will then establish the predictive ability of our maturity model.

REFERENCES

Humphrey, W., Edwards, R., LaCroix, G., Owens, M., and Schulz, H. 1987. “A Method for Assessing the Software Engineering Capability of Contractors”, Technical Report, Software Engineering Institute, Carnegie Mellon.

ISACA 2009. “The Risk IT Framework”, ISACA Rolling Meadows, IL, 60008 USA.

ISO 2008. ISO/IEC Technical Report “Information technology – Process assessment Part 7: Assessment of organization maturity”, ISO/IEC TR 15504-7, International Standard Organization.

ISO 2013. ISO/IEC 27005:2013 “Information security risk management”, International Standard Organization.

Kahn, K. 1965. *On Escalation: Metaphors and Scenarios*, Praeger.

MSB 2012, Swedish Civil Contingencies Agency (MSB). ”Nationellt system för it-incidentrapportering (in Swedish)”, Myndigheten för samhällsskydd och beredskap.

NAO 2014, Swedish National Audit Office. “Information security in the civil public administration”, Riksrevisionen, RiR 2014:23, 2014

NIST 2010. “Guide for Applying Risk Management Framework to Federal Information Systems”, NIST Special Publication 800-37 Revision 1, National Institute of Standard and Technology, U.S. Department of Commerce.

Pöppelbuβ, J., and Röglinger, M. 2011. ”What makes a useful Maturity Model? A Framework of general design principles for Maturity Models and its demonstration in Business Process Management”, Proceedings of the Nineteenth European Conference on Information Systems (ECIS 2011), Association for Information Systems (AIS).

Vaishnavi, V., and Kuechler, W. 2004. “Design research information systems” [Retrieved from: http://desrist.org/design-research-in-information-systems/, last accessed March 2016].

Wahlgren, G., Fedotova, A., Musaeva, A., and Kowalski, S. 2016. ”IT Security Incidents Escalation in the Swedish financial sector. A Maturity Model Study”, Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), pp 45-55.