A discussion-based on-line course in information security with minimal assessment

J.A. Koskinen
Lecturer
Tampere University of Technology
Tampere, Finland
E-mail: jukka.a.koskinen@tut.fi

Conference Key Areas: Open and Online Engineering Education, Engineering Education Research, Engineering Skills

Keywords: On-line course, Information security, Assessment

INTRODUCTION

Since 2006 we have given a biannual on-line course with very little assessment of learning outcome. Accomplishment of tasks is evaluated but not beyond judging whether students have written acceptable contributions. This judgment is done at fairly small units of student work – roughly 2 hours on average – and it is almost always approving. The course name *Daily InfoSec*, or DIS, refers both to the students' own information security and to those things students should know and be able to do about InfoSec of others, however excluding InfoSec work in organizations.

Already for years we have believed the course is good and worth deploying elsewhere, some of its ideas even outside the field of InfoSec. The belief has been based on seeing good solutions to the tasks, hearing good feedback from students, and using their critical feedback to guide adjustments. This paper was written as an attempt to support this belief and disseminate the ideas. The contribution is

- to document the didactics of DIS, Section 2
- to report evidence of the learning outcome from
  - self-evaluations by the students Section 3
  - the teacher's point of view Sections 1, 3 and 4

Section 1 reviews the role of assessment in asynchronous online-learning discussions using mainly the extensive literature research in [1]. In Section 2 the framework from [1] is used to characterize DIS didactics. At that point also the expected learning goals are outlined, with explanations how they fit in the InfoSec curriculum at Tampere University of Technology.

1 RESEARCH ON ASYNCHRONOUS ON-LINE DISCUSSIONS

1.1 Preliminaries and connection to DIS

We start the literature review by describing a framework through which we interpret the recent research and its relevance to DIS. The main characteristic of DIS is that the students engage in discussions by writing texts before and/or after reading each others' writings inside an internet service This sort of activity is termed asynchronous on-line discussion or AOD [1]. For DIS it also means that the discussions are restricted within groups of students and repeated on new topics every week. Most of the topics require some background work, with information or systems, before writing is possible. We use Moodle as our platform, more generally termed a learning management system, LMS. Each topic is discussed in a separate thread. There are also some other kinds of activities in DIS, but AOD with its background work accounts for nearly 70% of the course work.

In the context of learning outcome an AOD can be investigated with three approaches. The focus can be on

1. assessment of learning based on student's ordinary output within the AOD. A comparison to some other kind of assessment can be included or omitted in the study, but an important motivation for research lies in justifying the omission of any external assessment. Also, the student's AOD output being ordinary means that it is not made with the purpose of being assessed. The main tool is content analysis, which is a many-faceted collection of methods [1]. In simple terms it means understanding what the student has written and how that reflects his or her learning. This sort of analysis is a human activity but it can be facilitated by tools and methods of classification.
2. analytics, the indirect information that the LMS provides with its usage tracking tools, possibly with some extra quantitative data. This can even resemble content analysis when tracking e.g. sentence lengths, word classes, occurrence of keywords (*content* analy*tics* goes into this direction [2]). This information can be contrasted to the learning outcome that is measured through a different channel. A possible motivation, like in Approach 1, can be to avoid the other channel, which is likely to be more costly than the automatic analytics. It seems however that this approach has been used more to find early indicators of drop-out or other problems (incl. plagiarism) and not so much on assessment [3].
3. results that educators have reported from their experience, experiments and development work. Such results can be obtained at many levels of rigour: At a high level there would be experiments and comparisons between groups that have received different “treatment”, like AOD moderation, feedback etc. At a low level the reports can be based on teachers evaluating their experiences from a few instances of AOD usage, possibly using the approaches 1 and 2 to support their observations.

The current paper is a teacher's report that uses Approach 3. We stay at a low level but enhance it somewhat by referring to the long development of DIS using AOD, and our recent surveys, where students evaluated their own achievements. We use content analysis from Approach 1 only informally to make sense of some of the survey results. In a sense some of the LMS analytics is built-in in our approach: All successful students have gone through the sieve of sufficient contributions, and in the beginning there are often several interventions by the teacher. These interventions either help some students through their initial troubles or redirect some others to take DIS during a later term.

1.2 Results from literature, related to DIS

Klisc gives in her thesis [1] a comprehensive review of research literature concerning the use of AOD for education. We use the results of her review in subsection 2.4 to put DIS into the context of good AOD practices. Klisc's own research in the thesis addresses the question “How can student learning outcomes be enhanced in an AOD?” Her international survey among instructors means collecting results from teachers who used Approach 3. Her survey indicates that stating the purpose of an AOD task as well as assessment are among the most positively influencing factors. After this survey she continued the thesis by focusing in a local course on the effect of assessment on critical thinking skills. She found that assessment indeed is very important and it appears not to matter whether it is done on the outputs during the course or separately afterwards. These were the alternative ways of assessment used in the quasi-experiment she conducted. This part of her thesis uses Approach 3 at a relatively high level.

The Approaches 1 and 2 are evident in Klisc's literature survey. From more recent publications [4] deals with learning analytics, predicting learning outcome from LMS data. As was said above this sort of automatics is not intended to remove assessment but to help predict problems, and even the authors of [4] seem cautious to suggest such, although they reached very high accuracy in identifying low-achievers. The two suggestions from [4] for group based discussions are still useful for DIS: (1) support students' cognitive engagement from the beginning, (2) help students sustain consistent engagement.

One factor in [4] for the suggestion (1) is knowing your peers. There are always group members in DIS that do not know each other. One of the first AOD tasks in DIS requires everyone to (a) introduce oneself in free form, (b) declare one's own area of interest in the InfoSec field, (c) tentatively commit to pursue a certain level of skill and knowledge from the course, and finally (d) start choosing some topics for later tasks. The "level" in (c) is not about good or bad, but about *where* the students wishes to apply his or her InfoSec learning, e.g. ranging from membership of cyber society through other ICT professions to InfoSec professions. The tasks chosen in (d) also tell something to the peers about one's inclinations. For suggestion (2) from [4] DIS has a fairly tight schedule with bi-weekly deadlines, and so engagement is "guaranteed".

Some of the successfully predicting proxy variables from [4] would probably work well with DIS. The instructional design of DIS with clear-cut tasks and schedule, and the far-from-massive numbers of students makes such analytics less useful. The report [5] emphasizes the role of instructional design in tailoring LMS analytics, and gives the field of study almost equally high importance. Security certainly has very specific characteristics within engineering, and this shows already on the basic levels of study. (In what other discipline can a student get credit by "attacking" the LMS?)

From the point of the present paper [6] is an example of using assessment in AOD in a way that is complementary to Approach 1. The study investigates the use of AOD *as* assessment of learning that happens in other settings. This gives, however, good insight for checking whether learning on DIS has been good. The study in [6] used 14 assessment criteria. Without repeating them here we can say that all but two criteria are met by the contents of DIS discussions. Those that do not appear are the ones that give the highest score in the use of [6]: "Discussion refers to readings, literature review, theory, research to discuss position and insight." and "Discussion demonstrates timely and valuable online presence". These cannot be met by DIS discussions because each AOD task in DIS is so short. Of course not all the remaining 12 criteria are met by *every* DIS contribution.

When looking for signs of critical thinking with content analysis the study [7] used a set of criteria that mainly overlaps with that of [6]. Out of ten initial criteria eight turned out measurable, and three gave high scores. On the basis of our own informal content analysis we can quote from [7] (without the scores) also on the behalf of DIS: "outside knowledge was used a lot, justifications were regularly provided, and the posts were mostly critically assessed by fellow students”. Interestingly, possible teacher roles are mentioned in [7] and it is plausible that the teacher is just a “ghost in the wings” like in DIS.

2 CHARACTERISTICS OF THE COURSE

This section describes DIS with very little attention to its contents, or even the topic area. Some details of these appear in Section 3.2.

2.1 Background

The main characteristics of DIS in its early form have been reported in 2009 in [8]. This includes how the course evolved from its very original form, which only contained discussion tasks in the years 2003–2005. They were a small optional extension of the basic course of InfoSec. The number of tasks was almost doubled in 2006 when DIS became a separate course. The new tasks were such concrete exercises that the students are able to do on their own equipment and software.

Students reported that their work load was often exceeding the nominal course size of 2 ECTS units. In 2013 the nominal size was doubled. Several new kinds of tasks were introduced, mainly outside the earlier weekly course routine. The course was given a more professional orientation, especially to serve its role as a compulsory part of the InfoSec curriculum. The course is still suitable for students majoring in other fields of information technology. Fewer than half of those who pass the course major in InfoSec. In addition the changes in 2013 gave more emphasis to soft skills in InfoSec engineering. Details on approaching them have been reported in [9].[1]

2.2 Learning objectives and assessment of DIS

As stated in the syllabus the objectives of DIS are:

- Development of awareness and attitude related to InfoSec, also in the ethical dimension.
- Adoption of InfoSec skills and good practices that are needed in everyday life.

The latter has some professional flavour, too, as evidenced in the declared content:

- How InfoSec and the lack of it appears in the daily life at the level of individuals and society. (The latter level is often termed cyber security)
- Arrangements of personal InfoSec at home, studies and work.
- A preliminary insight into the tasks of InfoSec professionals, and to scientific work with InfoSec surveys. Optionally also understanding of how the daily InfoSec is subject to innovations (and not only by criminals :)

The course is divided into dozens of small tasks, and passing the course requires doing nearly all of them. The assessment of the whole course is based on the belief that the learning objectives cannot be missed if the students have been sufficiently working with the wide spectrum of course contents. The assessment of the individual tasks is simply pass-or-fail. In practice it is a pass if the student has done the task, with very rare interventions by the teacher.

[1] The survey A (cf. Sec. 3) included questions related to soft skills. The answers mainly concentrated on the middle option which was “a little”, averaging only slightly above this. A significant exception is critical thinking, where the higher options “fairly much” and “noticeably” outnumbered the others. Putting the five options to a scale −2 .. 2, critical thinking averaged at 0.77. This result may be an indicator of DIS being successful, but it must be noted this was just a single item in a questionnaire and without explanation of the meaning of critical thinking.

Because the tasks are done on-line without supervision, there is an examination in the end: The teacher discusses for an hour with each student group and becomes assured that everyone has done their work themselves. Although a variety of awareness and skill levels becomes evident in the examination, the purpose is not to evaluate the level of learning outcome. Instead, part of the discussion is used to gather feedback from the students for improvement of the course. This part also has the examining ingredient in it, because a student cannot contribute if she or he did not participate in the activities.

2.3 Format and didactics

The bulk of DIS consists of a 7-week schedule of Discussions and Exercises. The Discussions are in the form of AOD. Each week has 3 topics of Discussion and each topic has 2 rounds. There are two Exercises per week and nearly all of them are reported on discussion forums, and most of them have a second round of reporting which is supposed to be responses to the first round of reports. The main difference between the two kinds of weekly tasks is that Discussions deal with information: the students contemplate, find and deal with it, whereas in Exercises the students deal with people, gadgets and systems.

The other course tasks have different scheduling: Averagely every other day the students must report published news and their own observations, in a tweet-like short contribution (‘tweet’ as in twitter.com). At a dedicated week each student writes a report on reading (in) a book and a summary of the discussions of that week in his or her group. At a suitable time the students write a report on a hacking experiment.

The teacher’s role is to act as a bookkeeper and give feedback. The feedback usually includes some criticism but this is most often done just by bookkeeping – a student loses some points from the initial score or has to do a compensating Exercise, and also the group sees who. The feedback is rather generic and encouraging. It tries to give a wider meaning to the student outputs in the finished weekly task. In some cases there is feedback in the middle of the week but this varies on the basis of the teacher’s other duties. A large part of the feedback would usually fit for the same task of a different course instance. In the recent years a habit has developed where in every feedback one or two students are praised for their contribution – if possible.

Dealing with student **attrition** directly is not included in the framework of the next section, whence we give a brief account on that here. DIS is peculiar in the sense that no one has ever failed the examination. Quite a few have failed to reach the examination, and dropping out usually happens in the beginning of the course. Most often the reason is an overbooked work schedule. Sometimes it is a change in the study plan, that makes DIS obsolete. The reported reason has never been that DIS would be too difficult or not rewarding enough. Some drop-out reports are very thin, though, and for those who drop out before the last threshold task the reason usually remains unknown. There are three thresholds inside DIS: (1) register to the Moodle platform by the 3rd day, (2) find and report on a security awareness application or quiz by the 4th day, (3) write the first tweet about news by the 7th day. In a way a fourth threshold is the prerequisite course. It is done with automated multiple choice questions and in urgent cases it is still passable during the first week of the course.

2.4 Good practices followed?

In this subsection we use Klisc’s literature review (cf. Section 1.2 above) as a framework to evaluate to what extent DIS is currently following the good practices.

Klisc identifies a general conclusion from the reviewed literature that high order thinking does not happen to any great extent in an AOD. Klisc notes that in response to this researchers have investigated factors that may improve high order thinking outcomes. We reproduce here as paragraph titles the factors Klisc distilled from 32 publications (among her nearly 400 references). These presumably represent the best practices of what can be done to enhance the learning outcome of an AOD, especially high-order thinking skills. In the paragraphs we state what DIS does in each dimension.

Stating the purpose for an AOD learning activity. The discussion tasks in DIS do not meet this requirement: They do not express what sort of learning is expected. Instead instructions for the discussions are just definitions of the task, usually in form of several related questions. However, the general instructions of DIS give the students a chance to understand the objectives. They are also sporadically recapitulated in teacher’s feedback. The general and task-specific instructions have been under constant development, and the biggest problem with them is that they tend to become too long.

Protocols used in AOD. In Discussions and in most Exercises the two contributions have deadlines on Thursday and Sunday. According to Klisc this scheduling is neither good nor bad, and the same holds for the fact that the length of postings is not set explicitly. Instead of exact rules the literature seems to suggest that the instructor should be aware what possible effects the choices can have and how they should serve the course. On DIS the teacher often gives reminders on the general features of contributions, and most commonly about some students writing too much in Discussions. Others find such contributions too exhaustive, both in the sense of already covering the topic, and making it difficult to keep focused with all the issues raised.

Different types of AOD design. Out of the different types DIS mainly uses debate and case studies which Klisc reports to have been doing well in contrast to several more involved designs. She notes that the results are mixed, though.

Supporting materials. In most tasks the students need to find new material, in some cases also software, from the internet, but nearly all tasks also have local materials, including examples. These materials are, however, more about the topic itself than about how to deal with the topic.

Group size. DIS starts with 8 or 9, which fits in the recommended range 8–10, but the target is actually to keep the number at least 6 after eventual late drop-outs.

Questions. DIS defines its tasks by questions and sub questions, but is not particularly attempting to stimulate thinking or create cognitive dissonance, and especially not with Socratic questions. The field of InfoSec seems to provide contrasting aspects by nature and student engagement has been deemed sufficient. Occasional lack of inspiration in the second discussion round has been observed and consequently remarks have been added in the questions about the possible content of the second round.

Message labelling. Students do not label their messages to indicate the level of learning and thinking they represent. However, they must self-evaluate their book review, and they must publish their best InfoSec observations. These and the book reviews are viewable by the world.

Participant role assignment. Each student acts as a chairman for one week’s discussion tasks, and summarizes the results for other groups to see. Otherwise there are no roles assigned. The variety of student background often “creates” various experts in the group, e.g. in programming, networking, and even InfoSec experience from organizations. It has not been possible to deploy this directly during assignment of students into groups, because groups are chosen by students based on the examination time. In practice there is always possibility to get in each group students from both Information Technology, and Information and Knowledge Management. These fields provide complementary experts to each group.

Assessment used in AOD. Very little assessment is used beyond approval and generic feedback (Sec. 2.2 and 2.3). Also the whole course is either pass or fail.

Moderation used in AOD. Moderation is hardly ever used in DIS. The first discussion round never seems to need it, but the second one would obviously benefit from it in some cases (see “questions” above). In general, Klisc notes, moderation can be important. It has many possible forms, however, and it seems that generic rules are hard to find.

Student characteristics. Different learning skills, styles and personalities are not taken into account in DIS. Although research has found differences based on such characteristics, Klisc does not report on any studies that would have found out how they could be taken into account.

Technology issues. Besides Moodle DIS uses two other platforms, which may be a little challenging to some students, especially as they are not designed to be used with smartphones. Some students have difficulties in finding all the instructions for DIS, even in Moodle.

2.5 The role of DIS in the curriculum of InfoSec

DIS follows the basic course that lays the ground with InfoSec concepts and principles. The basic course is just 2 ECTS units and it is completely self-study. It has automated exercises and its automated but supervised exam has a free schedule through the year. One of the DIS tasks is to make “better sense” of the materials and exam questions of the basic course. This happens in the form of an AOD with instructions of giving feedback to others, but this task is not scheduled.

Some of those DIS students who do not major in InfoSec, still take some other InfoSec courses that fit in their degree programs, like Network Security, Secure Programming, Cryptographic Engineering, or InfoSec Management. These are optional in the InfoSec degree program, and the course names show the wide spread of special InfoSec areas available. A compulsory element of the degree program is the Advanced Course in InfoSec. It has DIS as a corequisite and together with the basic course and DIS it is designed to form a tightly-coupled entirety with a wide spectrum. By coupling we mean that the students are provided with references backward and forward between these courses. It is important to note that the self-study basic course is actually not the first element. It has as a prerequisite a first-year lecture course that introduces networking and the essentials of InfoSec.

3 SURVEYS AMONG THE STUDENTS

3.1 Method

We have organized two slightly different kinds of surveys among DIS students with the purpose of investigating how much their InfoSec skills improved. The first kind was a single questionnaire, where the students had to estimate on scale 1–5, what their skill level had been before and after the course. The second kind consisted of similar questions but they were administered in the beginning and end of the course.

The first kind of survey was used for students of the academic year 2014–2015 and the second kind for the next year. *Table 1* shows basic data from the surveys, labels them with “A” and “B”, and gives numbers to the course instances. The column *Follow-up* shows, when an additional email questionnaire was given to the students, and how many responses there were. The main purpose of the follow-up was to let the students adjust their earlier evaluations as seen from several months’ distance from the course. A special theme in the follow-up was caused by the observation of “declining skills”: Although on average the post-evaluation was higher than the pre-evaluation, almost every respondent in survey B had a couple of items reversed. We will return to this in the analysis. At this point we note that the students were generally not able to give very useful evaluations in the follow-up. Together with thanks we sent some detailed personalized questions to each of those who had responded, but we received very few answers. And unfortunately only three students of the course instance #4 answered their follow-up regardless of several reminders.

Table 1. The surveys

Survey	Course instance	Course Time	Survey Time	Stud-ents	Res-ponses	Follow-up time: resp’s	InfoSec majors
A	#1	2014 autumn	2015 summer	26	18	---	7
	#2	2015 spring		23	17	---	6
B	#3	2015 autumn	Beginning and end of course	15	15	March 2016: 12	8
	#4	2016 spring		12	12	May 2016: 3	3

3.2 Results

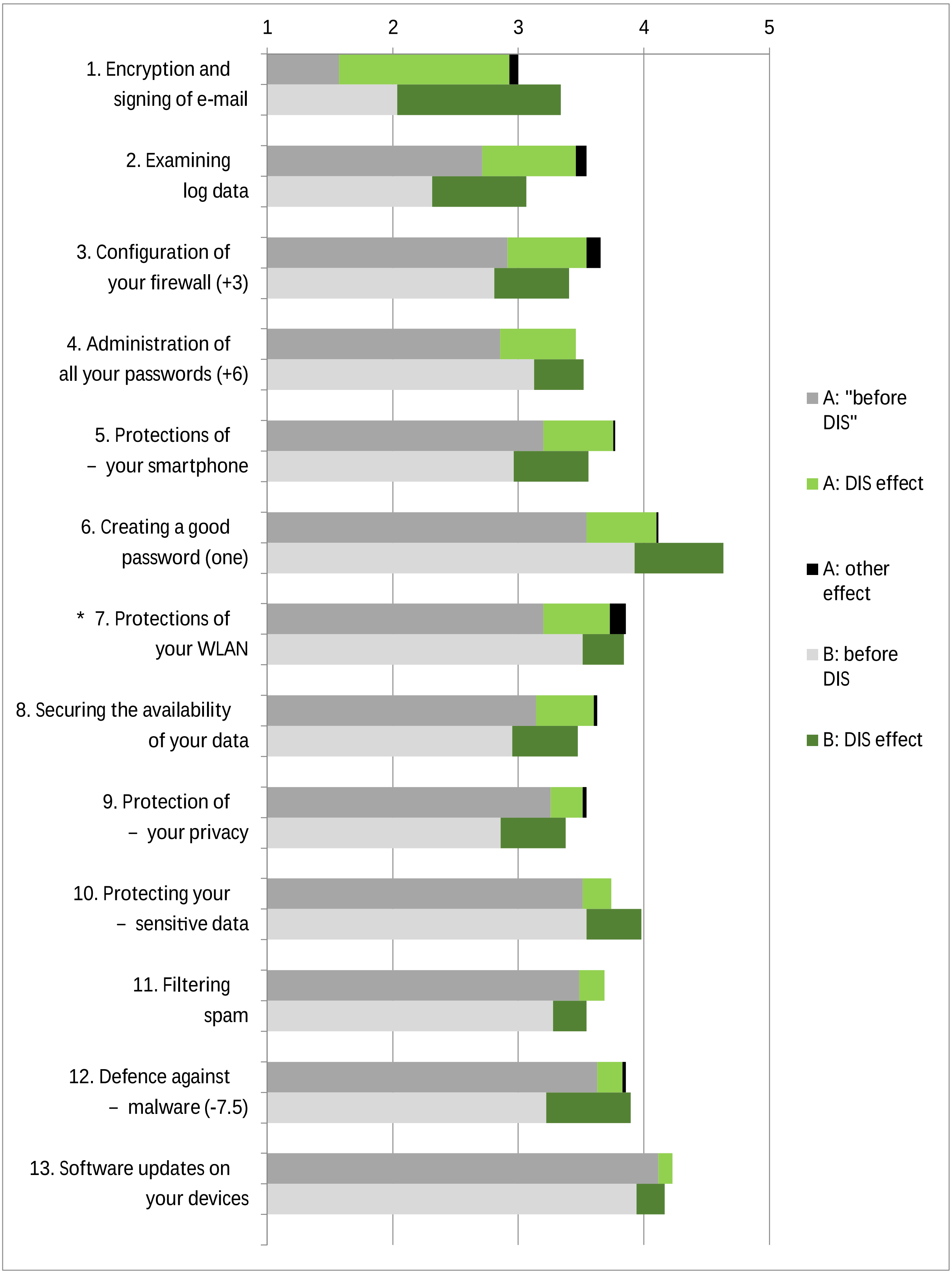
3.2.1 Display

The core of the surveys was a questionnaire with 35 items representing desirable InfoSec skills and loosely corresponding to the topics of DIS. Each of the *Tables 2–4* shows one category of skills: The first category is about ability to deploy useful countermeasures. The second one, awareness, includes knowledge, observing ability and sometimes also behaviour, but this is more about thinking than doing. Thirdly “practices” is more about activity and attitude than skill or awareness.

In survey A there were two particular questions that let the student attribute the eventual improvements correctly: The student had to pick those items from the 35 where the improvement was mainly from other sources than DIS – in case she or he had reported some other sources. Work, other studies and own interest had been such sources and 26% had taken at least one further InfoSec course. Furthermore the student was asked to similarly pick items where there had been other influence but also DIS had had a clear effect. These attributions were used in the following way: if the main effect was from elsewhere then the reported change was zeroed. If the effect was shared, then the change was halved. Similar attribution was asked in the follow-up questionnaires for survey B, but the results were so small that they are not displayed.

Each upper bar gives data from survey A and the lower bar from survey B. The total length of each bar describes the average level of the students' current skill, knowledge or activity as self-evaluated on scale 1–5. The left part (grey) of each bar

Table 2. Practical measures



shows the starting level. To the right of this is the effect of change. For survey A it is distributed in two parts. The middle part is the DIS share, and the rightmost (black) part comes from elsewhere.

The items are sorted and numbered according to descending DIS effect in survey A. The label of each item is followed in parenthesis by an indication how much different the rank of that item was in the ordering for DIS effect in survey B. For example −4 means the item would belong four steps closer to the top of the table. Only differences bigger than 2 are shown, because some variation in the order already follows from different, and small, populations.

3.2.2 Analysis

The DIS effects for survey B remain less clear than for survey A, because of a shortcoming in the measuring tool. The pre- and post-measurements in survey B were about the same skills but not by the “same person”. The students had changed during the learning process, whence they saw their skills differently. This became evident, when almost all students evaluated some items (averagely 4,2) lower in the end than in the beginning. This phenomenon of “declining skills” was partly corrected by the numeric answers in the follow-up questionnaire for course instance #3. The free-form comments in that questionnaire support the InfoSec-related explanation that “You are more comfortable if you don't know something.” In other words, students thought they were secured but learned that things were not that simple. The results of survey B still contain several cases of “declining skills” from course instance #4, because none were corrected in the follow-up. Assuming they were all at least zeroed, the DIS effect in whole survey B would rise averagely by 0.065 for each item. *Tables 2–4* include an indication of which items exhibited the highest effect of “declining skills” before any corrections: the 11 items where at least 5 students showed this effect have been marked with a minus sign before the second line of the label.

As seen in *Tables 2–4* there is only one area which was earlier in poor condition and in which the students’ performance gets substantially better because of DIS. It is the protection of emails – using PGP (1st in *Table 2*). The tasks related to this are divided to three weeks, which helps to increase the effect. Unfortunately this is not the most important or even very useful skill, unless the students can teach it to their communication partners. This explains why the final level of this item remains so low especially in survey A[2].

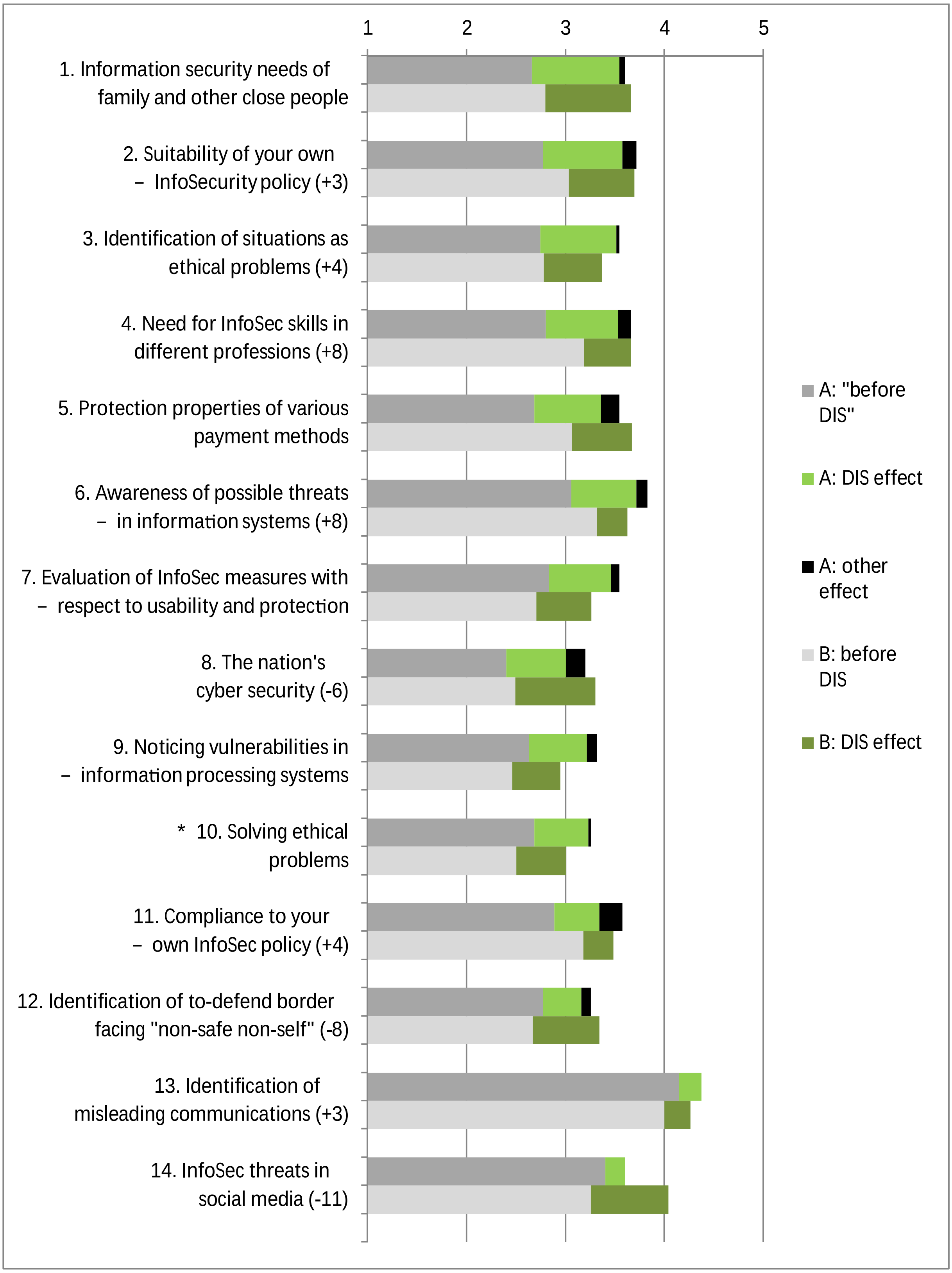
“Programming” at the bottom of *Table 4* serves as partial support for the validity of the measurements, for both surveys. It shows a very small DIS effect, which is correct because DIS does not teach programming. It has a task where students try to find vulnerabilities in PHP code, and this may be the reason why the effect is not zero. A little larger effect of that task appears in *Table 4* at “7. Inspecting program code”. This is still a very small effect (0.2 for both surveys) and judging from the student output in the AOD this item could not indeed be labelled as having a good learning outcome. Many used the offered option to pass this exercise without actually inspecting code.

The top items in each table also give support to the validity, because they all correspond to tasks that are clearly new to students and some learning is granted:

[2] The first skill category in survey A included an evaluation of the level also during DIS, and email protections was the only item where there was a drop from the middle of the course to the end. In the follow-up of course instance #3 this item also suffered a small loss: two students corrected their post-evaluations downwards.

besides email protections in *Table 2* the second item, examining log data, is somewhat like this, even if it is not such a novelty to students. The top item of *Table 3* is not that new either, but the students had to make and interpret interviews of family members or acquaintances. A lot of work with this within several tasks certainly had an effect on learning. Our surveys are too simple to evaluate whether the learning extended (as intended) to a wider understanding of InfoSec situation of

Table 3. Awareness



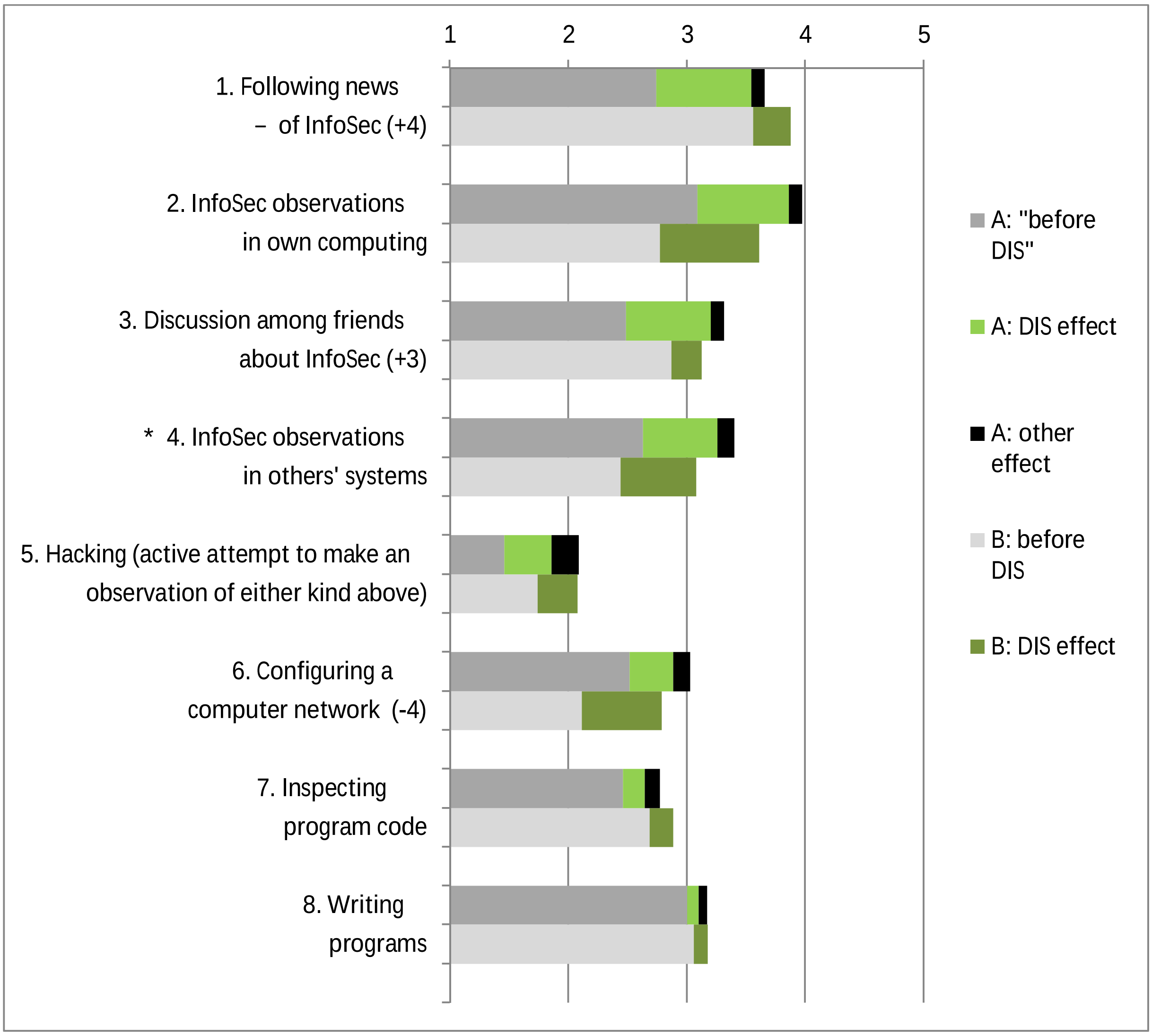
citizens – in the sense of the report [10] that was published on the basis of DIS interviews. Finally the "tweeting" task of InfoSec news repeated 24 times during the course, whence it should induce some learning outcome. Surprisingly the students of survey B had their level so high already in the beginning that their DIS effect would not take the top position in *Table 4*.

At this point of analysis we have partially "calibrated" the measurement in such a way that the learning outcome was good for the top of each table and not good at the bottom of *Table 4*. What level of DIS effect would indicate a good learning outcome for the remaining items? We arrived at the same answer 0.5 for each category of skills by reasoning in the following way.

First we acknowledged the background assumption that a larger effect means a better learning outcome. Then we ascended each table from the bottom to find the first item where the student output in the AOD's would certainly justify the label "good" as learning from DIS. This judgment was initially made on the basis of survey A results only, before the course instances #3 and #4 were run. While running these recent instances, we were able to see during our teacher's work that the outcomes were not very different. The boundary item (7th, 10th and 4th) in each table is marked with a * in front of the label.

What was left right below the boundaries? The 8th item in *Table 2* concerns securing

Table 4. Practices



the availability of one’s own data. This is certainly well understood by the students, in the sense of the awareness category (*Table 3*), but their reports show that they are not always taking good care of this. Very much the same remarks are due to the 11th item in *Table 3*, which requires compliance to one’s own security policy. The 5th item in *Table 4* is about hacking attitude. This remains disappointingly low by the scores. In the reports students said the exercises were interesting and they would like to continue at another time to go deeper into similar exercises (e.g. hack.me). But it is clear from their reports that very few actually got a spark to this kind of hacking.

We summarize at this point that in 21 items (7+10+4) out of the 35 we can report a good learning outcome. We have dealt with 5 other items: the 3 in the previous paragraph and the 2 from the bottom of *Table 4*.

What should be said of the remaining 9 items? Starting from *Table 4: W*hat we already said of the two programming skills applies partially also to configuring a network (6th item). Even if firewall and WLAN settings, which have a good learning outcome, are very much related to it, DIS did not try to give guidance on how to set up a network.

From *Table 3* we can ignore the two bottom items because they have such a good starting level, and survey B clearly indicates a good outcome for the last item (14th). Similarly survey B puts the 12th item to the good side, unlike survey A. In this item the frontier between “self and non-self” is an important concept in information systems security, but the question may have led the students to think too much on the individual level. This can make the issue a little confusing, especially as DIS did not explicitly deal with it.

From *Table 2* we can ignore the four bottom items in the same way as we did above for *Table 3*. That is, these mainly have a good initial level, and the least good one, the 12th in survey B, shows good DIS effect in survey B. Continuing in *Table 2* the item “9. Protection of your privacy” deserves attention. It appears it should as such have reached a higher level. Perhaps the adjacent (also in the questionnaire) 10th item on sensitive private data took a share of the responses and left general privacy a little more “public”. On the other hand, privacy indeed seems something that the young are not so interested in practice because it makes the sociomobile life clumsy. This may be true also for students of InfoSec, even though their AOD contributions tried to emphasize the importance of privacy.

We still need to explain a couple of items that seemed to enter the list of good outcomes without justification from survey B. In *Table 2* the 4th and 7th item are such. Even if these have their DIS effect well below 0.5, their final levels exceed survey A levels, whence misclassification is not likely. A similar argument holds in *Table 3* for the 4th item, partially for the 6th item, but not at all for the 9th item. For the latter two we look for support from the non-corrected effect of “declining skills” for course instance #4. This involves three students for the 9th item, and making an “auto-correction” we get the DIS effect to 0.56. The same procedure with two students for the 6th item leaves us at 0.42, but this raises the final level above that from survey A. It is worth noting that the 6th and 9th item are related to one another and they are both needed for hacking attitude to be efficient. Good results in them makes the observed lack in hacking attitude feel less ultimate.

4 DISCUSSION

Students should spend 107 hours on a course of 4 ECTS. This is also close to the time the teacher needs *during* DIS, assuming two 7-member groups of students (as in 2015–2016). This is roughly 8 hours per student. Some of the teacher's work during DIS is not directed towards the current students but to preparing for the following instance, with the help of the current students' output. Regardless of the often anticipated content of this output there is always something new, which makes giving this course rewarding.

Should there be more assessment? Some students would deserve a good mark and some others the opposite instead of mere "pass". The fine granularity of the tasks may let one think that grading could be built on counting the detailed passes and fails. This would be feasible only by enlarging the proportion of tasks that the students can fail. Instead of introducing individual assessment we have considered it more fruitful to concentrate on guiding each group as a whole. The results we have summarized here tend to show that the current way of assessment is enough to bring about reasonable learning outcome in most areas of the course.

Even if the course contents deal with professional engineering the students can approach most of them from their own daily practices. This may be one enabler for the discussion groups to be successful "teachers" for each student.

5 CONCLUSIONS AND FURTHER WORK

This paper characterizes and evaluates an on-line course, where students are supposed to reach fairly abstract learning objectives by getting involved in asynchronous discussions, after doing also some hands-on home-work. The passing of the course and assessment of learning outcomes are based on requiring the students to pass a large set of small tasks. Together with the teacher's group-based feedback this approach seems to produce reasonable rise in the skill levels – as evidenced by surveys that used self-evaluations.

As further work we consider content analysis. Introducing a moderate set of marking categories will not increase the teacher's ordinary workload very much. This is not likely to lead directly to more reliable results than in this paper. Instead we consider using it together with students' own markings, i.e. self-evaluating some of their writings. More importantly this would mean introducing a new didactic tool into the course. After the next two course instances we would start to know how these two marking-evaluations relate to each other and to the pre- and post- measurements similar to those in this paper.

We intend to keep the pre- and post- measurements in the course, but include the follow-up already in the post-measurement – mainly to assess the phenomenon of "declining skills" better than now. We consider making both measurements a little more like assessment in the sense that besides self-evaluation the students should show some skill in the questionnaires. Because of the tight coupling of the course with its prerequisite and follower, we consider to shift some of the measurements to these from the current course. Both of these adjacent courses have a suitable tool for such – automated examinations with multiple choice questions. Such shift hopefully alleviates the workload of students in our course.

REFERENCES

[1] Klisc, C. (2015), Enhancing Student Learning Outcomes in Asynchronous Online Discussion, Dissertation, Murdoch University. 344p.

[2] Kovanović, V., Joksimović S., Gašević D., Hatala M. and Siemens G. (2015), Content Analytics: the definition, scope, and an overview of published research. Handbook of Learning Analytics.

[3] Ellis, C. (2013), Broadening the scope and increasing the usefulness of learning analytics: The case for assessment analytics, *British Journal of Educational Technology*, vol. 44, no. 4, pp. 662–664.

[4] Kim, D., Park Y., Yoon M. and Jo I.H. (2016), Toward evidence-based learning analytics: Using proxy variables to improve asynchronous online discussion environments, *The Internet and Higher Education*, Vol. 30, pp. 30–43.

[5] Gašević D, Dawson S., Rogers T. and Gasevic D. (2016), Learning analytics should not promote one size fits all: The effects of instructional conditions in predicting academic success, *The Internet and Higher Education*, Vol. 28, pp. 68–84.

[6] Vonderwell, S., Liang X. and Alderman K. (2007), Asynchronous discussions and assessment in online learning, *Journal of Research on Technology in Education*, 39(3), pp. 309–328.

[7] Beckmann, J. and Weber P. (2016), Cognitive presence in Virtual Collaborative Learning: assessing and improving critical thinking in online discussion forums, *Interactive Technology and Smart Education*, Vol. 13 Iss 1 pp.

[8] Koskinen, J.A. and Kelo T.O. (2009), Pure e-learning course in information security, Proc. 2nd Int. Conf. on Security of Information and Networks. ACM, NY, pp. 8–13.

[9] Koskinen, J.A. (2015), E-learning of ethics, awareness, hacking and research by information security majors, 43rd SEFI Annual Conference, Orléans, 29 June–2 July 2015.

[10] Koskinen, J.A. (2015), Surveys of daily information security of citizens in Finland, 14th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, Helsinki, 20–22 August, 2015.