A Model to Evaluate Digital Safety Concerns in School Environment

Birgy Lorenz[1,2(✉)], Kaido Kikkas[1,2], Mart Laanpere[1,2], and Edmund Laugasson[1,2]

[1] School of Digital Technologies, Tallinn University, Narva Road 25, 10120 Tallinn, Estonia
{Birgy.Lorenz,Kaido.Kikkas,Mart.Laanpere, Edmund.Laugasson}@tlu.ee
[2] Estonian Information Technology College, Raja St 4C, 12616 Tallinn, Estonia

Abstract. In cyber security of a modern information society, digital safety is becoming more and more important regarding governance and schools as well as well-being of common people, especially children. There are models to evaluate cyber-attacks and technical risks in institutions and ICT services, but there are no good models yet to help understanding the concerns and issues of everyday e-life of commoners, including students and teachers - especially the ones that can be encountered at schools (from primary to upper secondary). This makes digital safety an essential part of innovation and cooperation at schools as well as in teacher training. The aim of this paper is to propose a model that helps to build up internet security training and other activities that will improve children's and teachers' safety skills and resistance to security threats.

Keywords: Digital safety contextual model · Internet safety · Security risks at schools · Security training · Innovation and cooperation in teacher professional development

1 Introduction

Our society allows having online connections with nearly anyone or any device. This has developed new types of crimes - cybercrime, cyber-bullying, online social manipulation etc. Despite the rules and regulations to enhance safe online behavior it has not been sufficient. For example, according to the Eurostat 7.02.2011 newsletter 21/2011, Estonia belongs to top 3 countries using secure software in EU; the EU Kids Online II [15] study stated that it is one of the top countries where children are facing online threats whereas most parents don't have a clue about the online life of their child. The situation has not changed since. The wider use of cloud services, social and automated software solutions (Internet of Things) at schools also brings larger risks and misuse of technology. In addition to their intended targets, attacks and abuse can also influence third parties (institutions, but sometimes even the whole country).

In this article, we define digital safety as a branch of cyber security that deals with people and the levels of online comfort, privacy and reputation, especially in the educational context. Earlier Estonian studies used the term "internet safety", but we feel

P. Zaphiris and A. Ioannou (Eds.): LCT 2016, LNCS 9753, pp. 707–721, 2016.
DOI: 10.1007/978-3-319-39483-1_64

it being too narrow - as we are also talking about the use of mobile technology and other parts of wider digital context. The cyber security approach has been mostly focusing on technological and institutional aspects, the laws and regulations prioritizing critical infrastructure of the government and businesses. At the same time, commoners including children and teachers lack necessary support, as this task has been relegated to voluntary workers or NGO-s. Luckily, political support and interest to develop this field has been growing. It has recently been stressed that commoners are an important part of information warfare [17] - e.g. as reflected by Estonian strategic documents Cyber Security Strategy 2008–2013 [7] and follow-up documents like the same strategy in EU 2013.

1.1 Cyber Security Related Strategy and Policy Documents in Estonia

We have looked at the strategy and educational policy documents in Estonia to propose a cyber-security model for schools. There are not many documents related to digital safety and cyber security (only the Cyber Security Strategy and Defense Strategy), but there are documents that mention digital literacy skills of commoners.

The new Cyber Security Strategy 2014–2017 [8] highlights understanding and discovery of cyber threats and finding ways to ground them. This document emphasizes the rise of digital threats and cybercrime targeting modern technologies, at the same time it is pointed out that the weakest link can be also be human itself. This means that training and digital security related life skills should be taught not only to specialists but also every citizen (including children) that can be targeted in cyber war through social manipulation. The Information Society Development Plan 2020 [11] forecasts the rise of different technologies, suggesting that the added value from using ICT and mobile technologies can only be achieved by enhancing digital literacy skills, including safety skills in this area. The Local Authority Information Society Development Plan 2015 [16] and the Internal Security Development Plan 2015–2020 [13] suggest that the awareness about needed skills for a digital society is a big issue. At the same time they state that as important as the skills are, the values and attitudes that affect our security behavior in this technology rich and global world would be even more important. And finally the National Defense Strategy [22] mentions again the need for better psychological defense: prevention of panic, influencing and containing hostile mindset spread, as well as ensuring trust to the state and defense activities from the commoners' view. It will be also important to ensure that traditional media channels would work in a case of attack; informing population in an emergency situation would be of prime importance. Finally, an important strategy is to eliminate economic incentives for cybercrime.

In Estonia there are many different institutions and companies that deal with digital security in every day basis. As up to 2014 the main issues and campaigns were related to the project "Be smart online!" [1] that had its limitations in focusing on internet only. From 2014 on, the ICT companies have started their own campaign "Connected with mobile safety" [5]. These projects help to promote the discussion in the society - e.g. parents are increasingly demanding that schools should take action, as parents themselves lack necessary knowledge to support their child.

Based on the strategies, we conclude that the most important is to train citizens who cannot be manipulated, can detect when someone attempts it, and can deal with digital crime or difficulties. At the same time they should preserve good attitudes towards technology, be enthusiastic about present and future developments and keep up the trust in authorities. These goals are expected to be delivered by the teachers and education system.

1.2 Education Strategy and Guidelines

The problem with digital safety in education is that it is not considered important enough. Proper educational use of technology is still lagging behind its social use, there is also opposition from older teachers who think that "school and teaching should be free from digital intervention". Such attitudes may stem from diverse reasons, such as lack of skills, learning aids or devices, or even slow connection speed. At the same time the younger generation and lot of innovative schools are up to the task regarding needs of the modern society. The problem with security is that while digital skill standards have not been implemented yet (they are optional), there is less consensus about whether digital safety should be a responsibility of school or parents - while parents provide the students with devices, the students usually learn most of the skills and develop attitudes "by themselves" or "through social media and real life experience".

We find that our educational strategies that strive to include everyone from the kindergarten to university actually support only the digital skills needed by the labor market. Guidelines that influences schools doings are national curricula (evaluated in the Digiturvis study as explained below) and International Society for Technology in Education (ISTE. NETS) [14] standards that are also optional. As Teachers Professional Standard V [26] also points to ISTE, it is the most important document to understand which problems should be solved through education in digital safety. ISTE standards were introduced to Estonia 2013–2014 when the governmental NGO called the Information Technology Foundation for Education (HITSA) started to implement in in its trainings to teachers and programs for students. The main 5 focus areas are: overall ICT competences in every level of educational; specific competences in vocational and higher education; ICT specialist training; teaching and learning in a digital age; information system in education. Digital safety areas are scattered between every section, e.g. understanding internet safety trends; choosing secure devices to surf online; recognize potential insecure behavior or threat; know how to act when something bad happens or seek help when needed; understand your own and others online behavior; knowledge about account maintenance; help students to learn how to act nice and consider others online. A parallel can be drawn with cars - a good car in the hands of an inexperienced and/or ignorant driver can pose a major danger.

We also looked at the national curricula (from kindergarten to university level), but could find only a fraction of what is really needed. For example, to effectively prevent cyber-crime, students should keep up with the changing technology in education, communities in personal and institutional life. The whole Digiturvis [9] study results can be found here in Estonian: http://1drv.ms/1N7KmtZ.

In conclusion, digital safety topics and areas are mentioned in different strategies. Usually the development is focused on positive aspects – developing services, accessibility, raising awareness and develop skills and competences. Drawbacks are less mentioned, but we see a lot of hints that suggest that future documents will deal with the issue more thoroughly. However, at the moment the documents contain no clear goals to be reached. This means that digital safety area has not been fully understood and this makes it really hard for teachers and schools to understand what is or is not their responsibilities.

1.3 Related Studies in Estonia

As mentioned, the digital safety research done in Estonia so far has mostly been focusing on the positive – overall evaluation of the situation where the youth nowadays live in (social media, online communication). Specifically, no one yet has fully focused on digital safety as it is often hard to separate from its context. The most important study that dealt with the issue on European level was the 2009 EU Kids Online II [15] that gives some insight to young people's online behavior (online habits, exposure to threats, parental supervision). Internet safety issues for the EU countries have been also focused through European Union project InSafe (In Estonia Safer Internet SIC) [12] and European SchoolNet gives out award E-Safety Label [10], that sadly focuses only in the management level and collecting some cases (e.g. cyberbullying and privacy-related issues).

In Estonia we can also refer to international studies like PISA [24] and PIAAC [23] or TALIS [25] that ask some interesting questions about technology. Estonian adults tend to have good basic e-skills, but as the workplace does not value these skills directly, they will deteriorate. At the same time, Estonian schools lag behind the rest of society. The digital literacy level of students almost uniformly exceeds that of teachers - but unfortunately, this does not apply to digital safety skills.

The CreativeClass [6] and "Conceptual framework for increasing society's commitment in ICT" [6] studies point out the autonomy of the schools to interpret the curricula and also reveal different priorities. The digital literacy is one of the main goals/challenges for the Ministry of Education, but it is not always so for the schools. This means that not every school has computer labs, technology lessons, or e-learning. The results show that schools have a lot of autonomy at primary and secondary school level – every school did something differently, but some of them supported it through optional or mandatory courses or extracurricular lessons.

An interesting study in terms of digital safety was the Mobile/Smart Security study carried out by the ICT industry representative Look@World Foundation in 2014 [21] that gives overview of mobile technology use among Estonian adults and children (usage, attitudes and security knowledge). The results show good access to mobile technology which will increasingly be the focus of personal technology use. Unfortunately, the safety awareness is again rudimentary and practical defense skills are low - usually, people are aware of dangers in general, but do not know specific threats. For example, only 2 out of 5 people locked their phones. And importantly, parents are unable to support their children, as they are helpless themselves.

The issue is also that in digital safety, people rely on "friends" more than they rely on official help [19]. Principals really think that technical limitations will help [20]. Depending on the school's traditions, these regulations will be developed by principal, teachers or involving students, parents or outside experts. Importantly, the effectiveness of these regulations depends heavily on the level of cooperation - authoritarian rulesets will be much more likely ignored by students.

In conclusion, in the "Education Guidelines to Schools" there are some mention of digital safety and digital literacy skills, but it is still unclear who is responsible and how it is being implemented. Schools' freedom in organizing education and applying curricula makes this really difficult task, as there is no clear understanding what the cases that education should concur. For example, considering things like phishing, seeing/sharing inappropriate content, trust to government, reputation, illegal content, technology over usage, cyber bullying, harassment, public data, identity theft – are they issues that should be dealt with as they appear, or after turning 18 when the youth enter workforce? Would the questionable attitudes (internet is a no-man's land; do but don't get caught) that can foster in the heads of youngsters easier to counter when they are already grown up and have their own opinions how the digital society really works?

Thus, there seems to be a need for a model that education sector could use to understand and teach digital safety issues on the commoners' level rather than in cyber security level that already involves criminal acts. The low-level pranks and disturbances can be dealt with by the educational sector, to raise more responsible and aware people that can really stand up to social manipulation and solve low level situations by themselves, not always seeking help immediately when e.g. somebody sends a spam e-mail. The model should help to detect, explain, solve and choose an awareness training for different low level cases that happen in the schools and usually go unnoticed. This should be a basis in the teacher professional development training regarding digital safety issues.

2 The Model and Its Evaluation

2.1 The Model

We have developed a model based on the research done about students' and teachers online behavior. The digital safety contextual model is based on the school as a smaller-scale model of society dealing with digital world risks on institutional and personal level.

The model is divided into zones, types, challenges and levels, and solutions.

2.1.1 Zones

The model involves different stages. The first is Zones that "people are concerned or not or how much" are divided into two: public and private. For common people (including students) the public zone is something that is not part of the person's immediate interest; school, online friends, acquaintances and society. The private zone includes family, friends, but sometimes even really close online friends (see Fig. 1).

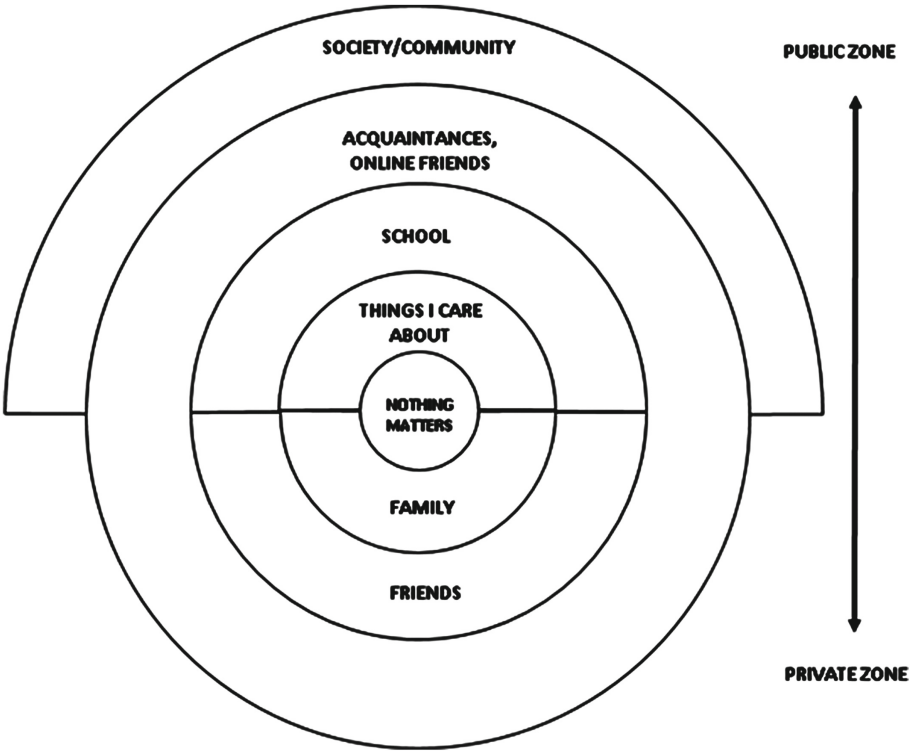

Fig. 1. Personal zones of concerns in digital safety

For a teacher as a representative of an institution (school), the public zone includes his/her classroom, school board and expectations from society. The private zone includes colleagues, students and their parents. In the center there is a zone of ignorance called "nothing matters" (see Fig. 2).

2.1.2 Types

Cyber security and digital safety cases can be divided into two areas based on their nature: a. technical concerns, where the solution involves technical approach (e.g. technical restrictions or monitoring) and b. behavioral concerns, where solutions usually are related to internal procedures, habits, guidelines etc.

At the same time, cases can also divided into institutional and personal (based on "who will solve it"). Yet in digital safety, both categories must be addressed - for example, a person can function well on institutional level (he/she follows secure practices at work) whereas being at serious risk on personal level (disregards security guidelines e.g. on Facebook), especially as the latter can have wider consequences (see Fig. 3).

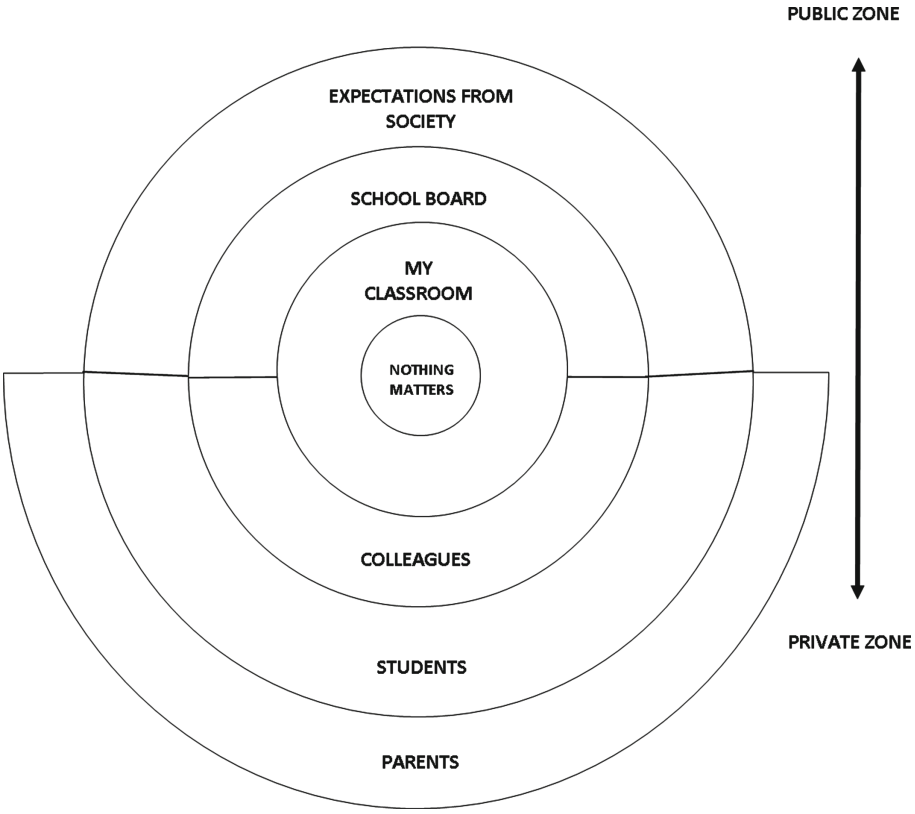

Fig. 2. Institutional zones of concerns in digital safety

2.1.3 Challenges/Concerns

Challenges or concerns of digital safety and security can be divided into 5 categories (reputation, data, fraud, health, freedom) that in turn will be divided into 9 areas of challenges with 7 layers of each. This is the basic conceptual model or taxonomy we are proposing that is inspired from the Concerns-Based Adoption Model (CBAM) (2006).

1. **Reputation**
   a. **Self-inflicted damage** (others think I am incompetent) – as I have no skills to deal with the issue, others see me as stupid. This situation can occur when the person is forced to use technology and there is no or little help available. At school the common occurrence is when people start to use BYOD solutions. In the end there can be issues with technology overuse, misuse and other risks. Without regulations there can be chaos. People can become incompetent when using websites, answering emails, translating digital content or even when the technology is not working properly;

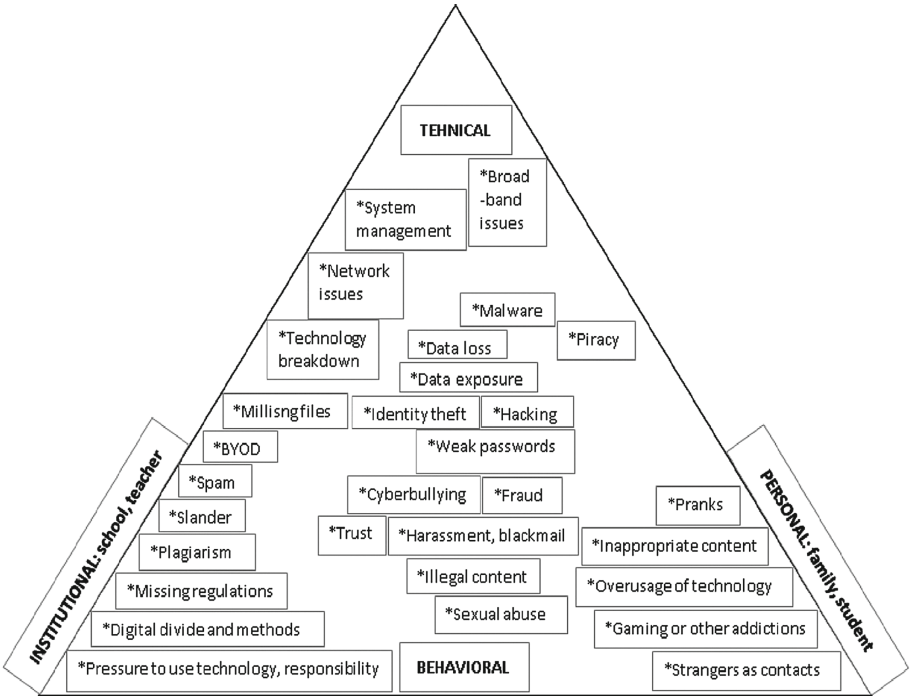

Fig. 3. A model for understanding digital safety incident types (Lorenz 2012b)

b. **Outside damage** – it can result from spreading false information, bullying and harassment. Countermeasures are technical (know how to remove data from the internet) and psychological (raise self-esteem), there might be a need for legal or judicial assistance.

2. **Data**
   a. **Data loss** – the situation can occur on attacks on technology or when we don't have the skills to keep our data secure. A typical example can be sharing one account with more than one person;
   b. **Data exposure** – this is a concern about privacy. Examples include data leak through email, website, losing password, using spyware, hacking, too much contacts online that one does not personally know. There is a need to raise awareness how to make, store and share data in a secure manner.
3. **Fraud**
   a. **Dishonesty** – identity theft, but also spreading false information, prank calls, slandering, plagiarism or other cheating. This will often result in people becoming disillusioned as they lose trust to the society and people's honesty;
   b. **Money loss** – fraud involving material (including monetary) loss. Examples include fake bills or paid but undelivered services. These acts can often result in legal actions.

4. **Health**
   a. **Physical risk factors** – this involves technology misuse or overuse or even addiction (gaming, communicating etc.);
   b. **Mental risk factors** – includes exposure to inappropriate data (sexual abuse, child pornography, torture of animals etc.).
5. **Freedom** – various diverse issues: obstructive malware, connection and usage monitoring by others, manipulation how one is acting online, restricting freedom of speech.

2.1.4 Layers and Levels

To understand concerns or challenges we can divide them into 7 layers (see Table 1). Personal layers are quite similar to organizational levels (school as an institution). In different layers there are different solutions that can help to evolve into the next higher level of understanding. This means that when person or institution is in a lower level then it is not wise to offer them a high level solutions, or you can just predict that probably they will be stuck in "this kind of situation" that "can be solved with a help of this and this".

More examples can be found at https://goo.gl/HwExq3.

2.1.5 Solutions

Solutions in security field example in aviation safety are tied with the Bowtie model (2009), where the problem is in the middle with its causes and solutions on both sides. On the right there prevention tactics that include identifying the case, reasons and effectiveness for the tactics to solve the case before it will occur; on the left there are collected tasks that are related to damage detection, minimization of the effect and finding helpers/responsible persons to solve the bad situation (see Fig. 4).

This model gives us tools to find ways to solve one or another concern and at the same time raise awareness level and develop skills (see Fig. 5).

Example of different levels understanding we can use this simple case where teacher asked primary students to send her their email passwords to make another environment users (see Table 2).

In the students' view, there were no problem as the case was not recognized. They were happy that teacher offered this kind of solution where they could use the same password in several places. At the same time it was manipulating them to think this is a good practice. Problems in this case could be lack of privacy or hacking, as now teacher had a list of students' passwords which can be considered a serious offense. A solution for this will be awareness training to students. In the parents' view - as the parent was competent in digital safety, he insisted that this incident would be treated as cyber security expected it to be treated. Even if it was a semi-criminal case, it was not treated in that way, as in education there should be a way to people learn from the mistakes (the school board opinion). In the teacher's' view it was an easy solution as the students forget their passwords all the time, so it had affected the e-learning quality as most of the class time was spent changing passwords or fixing accounts. The solution would be to have a discussion with the school board as the institution needs

Table 1. Personal layers and Institutional levels

Layer/Level	Personal	Institutional
1 Nothing matters	"It does not involve me, I don't care". It can be solved through awareness training – to let people know these things are out there in the world	This concerns me a little or not at all
2 Need for more information	"I should know about this more". In this stage we can offer guidelines like "when you see something like this, you might want to act like that"	It's someone else's concern (parents, ICT manager, students themselves)
3 Attitude	"It is important to me as well". The support will be related to explain cases, discussions in a small group, but also public presentations and mass media influence	This can be dealt with technological restrictions – where there is a regulation that you cannot pass, then the behavior will be more secure (e.g. obligation to use 15 character password)
4 Skills	"How can I do that". There is a need for training, practice	Issues occur, we must start to deal with them with a help of experts (class teacher, psychologist, ICT manager)
5 Trial and error	"I will test it myself". In this stage people are searching for sharing experiences to another, coaching, supervision or other	At school it can be dealt with regulating the field – when it is publicly not visible, there is no problem. Schools involve also external experts like child welfare. Everyone must obey the rules and regulations even when testing the limits
6 Implementation of routines	"I don't think in that matter anymore, it's a kind of elementary, hygiene level to me". In this layer there can be only a shocking cases that can shake the person's mind or he/she has developed a need to give something back to the community, to be asked to be involved making others life easier	This is our concern. We need to discuss and solve it together. If needed there should be an active board to solve cases. Cases are also measured and logged
7 Expert	Future developments, creation of the law, development plans, finding out new threats and reporting it to the community, helping others and taking responsibility of it	We include everyone to the process of agreements and we believe in it. All concerns will be dealt with. There is an action plan. And everyone that is needed are involved in the solution finding process

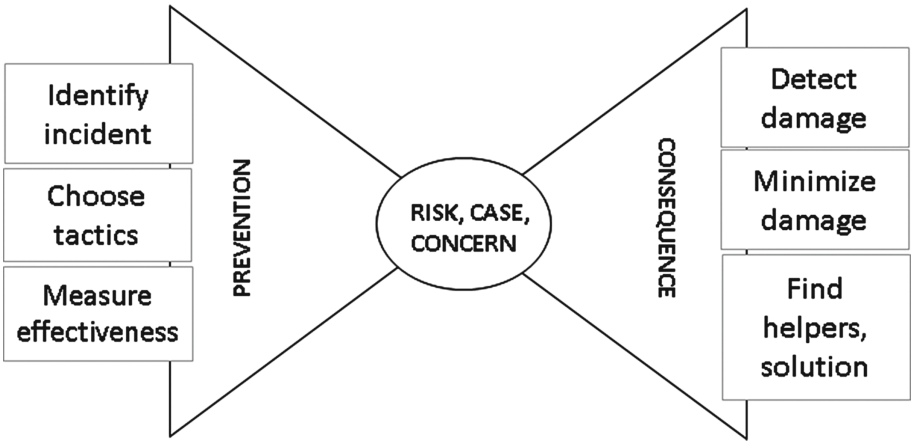

Fig. 4. A simplified bow-tie model for dealing with digital safety risks

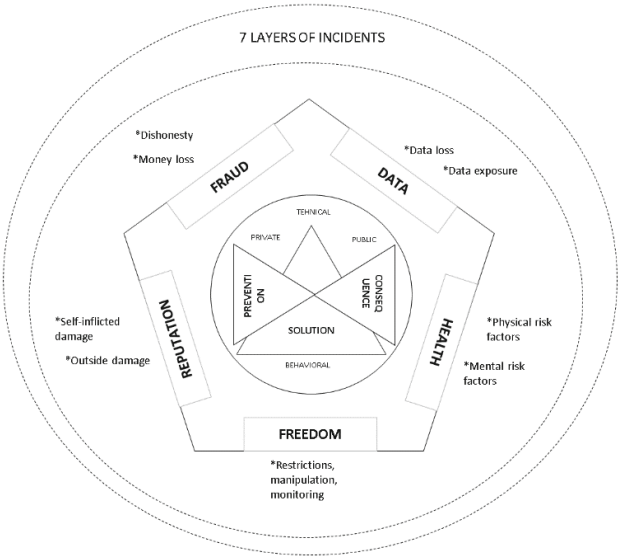

Fig. 5. The complete model to evaluate digital safety concerns of commoners

more clear regulations and understanding responsibilities of different parties, as well as to inform the teacher that this kind of action would not be a good practice.

The validation process shows that the schools still lack understanding about different internet safety issues and their solutions. We also understood that the level of action is related to school culture and the level they are on. Most schools are lagging behind in the level 2–4 depending of the situation as in every school there are teachers that "don't use the internet and so don't see it as his/her problem" and most of the schools have had first entry level training in internet security but see the solution to be

Table 2. Sample cases

Connected persons	Students	Parents	Teacher
Personal/Public	Personal	Personal	Personal
Technical/Behavioral	Technical	Behavioral	Technical/Behavioral
Concern	Freedom	Dishonesty	Self-inflicted damage
Layers/Levels	1	7	2
Prevention	Can't use services that are offered	Understanding the nature of the issue (why it can happen, is it a malicious act or not)	Knowledge about personal data security issues was low
Consequences	Cannot participate in school's activities	Trust in the institution will decrease	Data exposure, hacking
Who will I get help from/What is needed to be done	ICT personnel will help	Web Police, School board, talking to the teacher	Need for rules and regulations in the institution regarding personal data protection and passwords

part of ICT managers, the psychologist's or class teacher's job. Only one school had an idea for a plan where teachers and students would get training once in every three year or had a board to solve the cases. No one had significant written regulations, logging the events and knowing where to turn when they needed external help, except e-police services as this kind of campaign has been going on in Estonia for 4 years by now.

We propose that this model can be used to develop a tool that can collect cases from a everyday life of a student - both personal and institutional. First it helps to reflect to the student itself what she/he can do in this situation, if she/he really is thinking of the solution. Also, as these cases can be collected and refused to give good examples how different ways in different levels people can solve issues. This can be a learning tool, at the same time it can be a tool to also not only understand the cases, but solve them and improve awareness training both in teacher's professional development studies and students.

3 Conclusions

A big problem is that digital safety issues seem either to be of equal importance to the overworked school administration or are dismissed completely as "parental challenge", not an educational one. The biggest security risk in the future is predicted to be "located between the keyboard and the chair", defense always lagging behind attackers and challenges. Training security mindset is not only a workplace and adults challenge, it

should be dealt already on a basic school level, where the school can give students appropriate digital skills and security understanding that can help them throughout their lives.

For different levels of awareness, different solutions are needed. Our model helps to detect low level incidents and disturbances that influence commoners' attitudes. Some students are in the level that they don't know and they don't care, others in the same citations might see lot of things that can go wrong and prepare for it, that the threat will not realize. Model helps also teacher and school leader to understand in what areas they are in a low level position and where they might be already an expert. Model also helps to choose solutions – will we need regulations, awareness trainings, specialist help, technical regulations or other.

Based on the model above, most digital safety issues found at school are related to data, reputation, free will and fraud (people are not honest). When students or teachers act then there is a fine line between ethics and real life regulations as policy and law. Usually at school, even the cases that has a hint of criminal behavior (sharing personal data without permission, weak passwords and password sharing etc.) will not be prosecuted with full intent. Eventually these cases are solved by removing the offending data from the internet and hoping for the best or changing the password and account regulations. Most of the time the issues are not dealt with as the threat is not being recognized or is taken as not so serious that the case might need. Sometimes the case is being noticed but no one knows how to act on it. At the same time most cases can escalate rather quickly to more serious issues that needs police or court attention, depending of the country, school and people. When solving these cases, the solutions fell into the field of awareness training; arguing and discussing with each other and community; implementations of new rules and regulations both technical and behavioral.

So we also propose to develop a tool using our model to let digital safety incidents be simulated - the tool should reflect in which direction should think before acting or when something has already happened, the tool can point you in the right direction to solve the case. So we could call the tool also as "prevention" not only "solution" but definitely both cases are presented. The perspective would be students anonymously tell stories, through which also feedback as solution is given by the model. In this way the model will be enriched with new cases and solutions. This model is for younger people to analyze cases independently or together with teacher and find the solution. For time to time experts will look at the given solutions and correct the model if needed. Also web police and teachers are engaged to develop understanding of cases and its solutions.

The tool based on our model would help to raise awareness and through this also solve problems ("It helped me without having to reveal my ignorance or involve the police!").

Acknowledgements. This study was supported by the Tiger University Program of the Information Technology Foundation for Education.

References

1. Be Smart Online: NPO Estonian Union for Child Welfare (2012). http://www.targaltinternetis.ee/en/projektist/
2. Bowtie model: Introduction to Bowtie model, Civil Aviation Authority (2009). http://www.caa.co.uk/default.aspx?catid=2786&pagetype=90
3. Conceptual framework for increasing society's commitment in ICT: approaches in general and higher education for motivating ICT-related career choices and improving competences for applying and developing ICT, Tartu University (2015). https://sisu.ut.ee/ikt/
4. Concerns-Based Adoption Model: American Institutes for Research (SEDL) (2006). http://www.sedl.org/cbam/
5. Connected with mobile safety: Look@World Foundation (2013). http://www.nutikaitse.ee/nutikaitse-2017-projektist/
6. CreativeClass: BalticComputerSystems Eesti (2014). http://www.bcskoolitus.ee/creativeclass/
7. Cyber security strategy 2008–2013 in Estonia: Republic of Estonia Ministry of Defence (2008). https://valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf
8. Cyber security strategy 2014–2017 in Estonia: Republic of Estonia Ministry of Economic Affairs and Communications (2014). https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
9. Digiturvis: Tallinn University, Republic of Estonia Ministry of Economic Affairs and Communications (2015). http://1drv.ms/1N7KmtZ
10. E-Safety Label: European SchoolNet (2012). http://www.esafetylabel.eu/web/guest/about
11. Information Society Development plan 2020 in Estonia: Republic of Estonia Ministry of Economic Affairs and Communications (2013). http://www.riso.ee/sites/default/files/elfinder/article_files/infoyhiskonna_arengukava_2020_f.pdf
12. InSafe: European SchoolNet (2014). http://www.saferinternet.org/about
13. Internal Security Development Plan 2015–2020: Republic of Estonia Ministry of Interior (2015). https://valitsus.ee/sites/default/files/content-editors/arengukavad/siseturvalisuse_arengukava_2015-2020_kodulehele.pdf
14. ISTE standards - International Society for Technology in Education: Information Technology Foundation for Education (HITSA) (2012). http://www.innovatsioonikeskus.ee/sites/default/files/ISTE/ISTE_NETS_S%20%28Estonian%29.pdf
15. Livingstone, S., Haddon, L.: EU kids online. Z. Für Psychol./J. Psychol. **217**(4), 236 (2009)
16. Local Authority Information Society Development Plan 2015: Republic of Estonia Ministry of Interior (2011). http://kov.riik.ee/wp-content/uploads/2013/04/KOVIYAK_2012-EGA-l%C3%B5ppversioon.pdf
17. Lorenz, B., Kikkas, K.: Socially engineered commoners as cyber warriors-Estonian future or present? In: 2012 4th International Conference on Cyber Conflict (CYCON). IEEE (2012)
18. Lorenz, B., Kikkas, K., Laanpere, M.: Comparing children's e-Safety strategies with guidelines offered by adults. Electron. J. e-Learn. **10**(3), 326–338 (2012)
19. Lorenz, B., Kikkas, K., Laanpere, M.: Bottom-up development of e-Safety policy for estonian schools. In: Estevez, E., Janssen, M. (eds.) 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2011), 26–28 September 2011, pp. 309–312. ACM International Conference Proceedings Series. ACM (2011)
20. Lorenz, B., Kikkas, K., Laanpere, M.: Exploring the impact of school culture on school's internet safety policy development. In: Stephanidis, C. (ed.) HCII 2013, Part II. CCIS, vol. 374, pp. 57–60. Springer, Heidelberg (2013)

21. Mobile/Smart Security study: Look@World Foundation (2014). http://www.vaatamaailma.ee/nutiturvalisuse-uuring-seitse-last-kumnest-saab-nutitelefoni-kasutada-piiramatult
22. National Defense Strategy: Republic of Estonia Ministry of Defence (2010). https://valitsus.ee/sites/default/files/content-editors/arengukavad/riigikaitse_strateegia.pdf
23. PIAAC Estonia: Republic of Estonia Ministry of Education and Research (2014). https://www.hm.ee/et/tegevused/uuringud-ja-statistika/piaac
24. PISA Estonia: Republic of Estonia Ministry of Education and Research (2012). https://www.hm.ee/et/tegevused/uuringud-ja-statistika/pisa
25. TALIS Estonia: Republic of Estonia Ministry of Education and Research (2008). https://www.hm.ee/et/tegevused/uuringud-ja-statistika/talis
26. Teachers Professional Standard V: Educational Qualification Board (2013). http://www.hm.ee/index.php?popup=download&id=4321