Echo e-Skill and training Toolkit user experiences regarding user vulnerabilities

Rasmus Päärni

2023 Laurea

Laurea University of Applied Sciences

Echo e-Skills and training Toolkit user experiences regarding user vulnerabilities

Rasmus Päärni
Safety security and risk management

Thesis May, 2023

Laurea University of Applied Sciences

Safety, Security and Risk management

Bachelor's degree

Rasmus Päärni

Abstract

Echo e-Skills and training Toolkit user experiences regarding user vulnerabilities

Year 2023 Number of pages 32

This thesis report presents user experience study for ECHO e-Skills and training Toolkit application that provides skills gap data in the work community. The Toolkit was created by Laurea University of Applied Sciences bachelor's degree student as a thesis project in the ECHO project which has an objective to raise information- and cybersecurity knowledge and skills within the European Union. The objective of this thesis was to find out the user experiences of the Toolkit and if the output data is useful in identifying user-vulnerabilities and to give feedback of the Toolkit's output data and its usefulness for the further development of the Toolkit.

The theoretical framework goes over related information security theories, gap analysis data and its hypothetical usefulness in user-vulnerabilities, what are user-vulnerabilities and how they tie to information security, the qualitative research methods for this thesis as well as the relevant ECHO project's documents that work as a baseline and inspiration for this thesis. This thesis gathered answers regarding the user experience from participants in a qualitative questionnaire, which was gathered from the same group that piloted ECHO Toolkit previously.

The analysis of the results revealed that ECHO Toolkit could be used at least as a part of user-vulnerability identifying process when scanning for risks and vulnerabilities in information security risk management process. While the Toolkit itself might not be enough as is to be the singular source of user-vulnerability data, it could work as a truthful output for participants to self-assess their skills and therefore provide data for information-and cybersecurity practitioners to source their risk management process in right places. Further testing of the ECHO Toolkit in combination with other qualitative methods that support the participants, in real-life settings, could increase the reliability and usability of the output data.

Keywords: Gap analysis, E-skills, User-vulnerabilities, User Experience, ECHO

Contents

1 Introduction

During this thesis Laurea University of Applied Sciences was a part of a bigger European Union -wide project called ECHO - European Network of Cybersecurity Centers and Competence Hub for Innovations and Operations. One of ECHO project’s goals was to develop information-and cybersecurity training, to understand better and reduce the skill gaps between the demand and talent supply (Varbanov 2021, 4). ECHO project has multiple partners and universities that it cooperates with. Laurea University of Applied Sciences was one of those cooperative partners. As ECHO partners, universities have produced research on the topic of cyber- and information security and this has created innovations, research data, and applications by both students and teachers. One of Laurea’s contributions was ECHO paper D9.15. It has produced a web application toolkit for measuring information and cybersecurity related skills, which is called ECHO e-skills and training toolkit. The research paper D9.15 is a collaborative effort by both Laurea university teachers and students. The ECHO toolkit was created by another student as a thesis project, after which Laurea teachers then conducted a piloting study for that Toolkit and how it works in a close to real-life setting. The piloting study authors then concluded that the ECHO toolkit needs more research for the user experience and on the usefulness of the output data the toolkit produces (Frisk, Tikanmäki, Ruoslahti, 2022). This thesis studies the output data of said ECHO web application toolkit in the domain of information and cybersecurity. The objective during this thesis was to research how useful the data from the ECHO toolkit is in a real-life setting, focusing on the possible toolkit applications to information security and specifically in finding user-vulnerabilities. This thesis study goes over the necessary information security literature for the thesis, the thesis process itself, research methods, and the relevant findings. For making the text easier to read and for consistency, the official name ECHO e-skills and training toolkit, will be shortened in this thesis to ECHO toolkit or toolkit depending on the sentence or context. The conclusion part of this thesis, section 5, can be used as potential feedback for the ECHO Toolkit to improve its user experience, output data, and the input data and to contribute to ECHO project’s successor project.

2 Information security and gap analysis

This section of the thesis goes over the theoretical and literary basis for this thesis study. The purpose is to go over the most relevant information security literature to the thesis topic that affects how user-based vulnerabilities could be identified, why identifying them is important, and how the gap analysis and radar chart data from ECHO Toolkit could be tied to identifying said vulnerabilities. Paul Oliver (2012, 10) claims that there needs to be an indication of the relevant research literature that enables the reader to understand the context of the research. Gap analysis, information security and vulnerability identifying literature, and ECHO project’s literature related to this topic was read in the earliest stages of this thesis study to establish and demonstrate the theoretical understanding and professional command of the background theory in order to establish the context for this thesis.

2.1 Information security

ISO 27000 (2020) defines information security as the retention process of confidentiality, integrity, and availability, which is also called information security triad or short, CIA-triad. How the triad works is that every information asset has some version of the triangle shaped out. The lengths of the sides of the triangle may vary based on the information asset that is being used. For example, if an organization wants to advertise a service, the advertisement information asset triangle would have longer sides for integrity and availability since the advertisement would not be confidential information and shown to the world publicly. On the other hand, a retail organization with a personal customer information asset would have an isosceles triangle shaped out, since all the triad aspects are equally important in that context. An example of an isosceles CIA-triad can be found from figure 1.

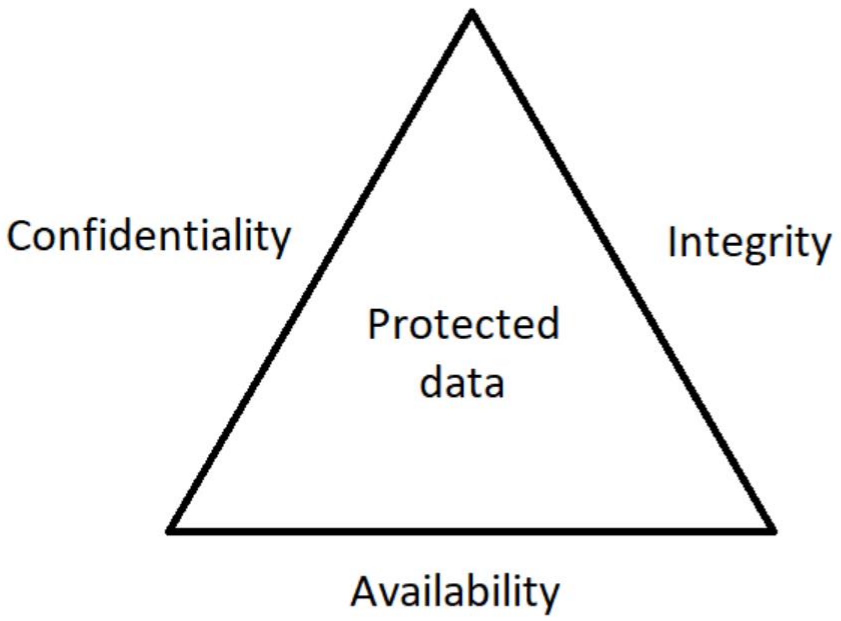


Figure 1: CIA-triad

Confidentiality means that the information that is classified information should only be available to people who need that information for processing it legally. Integrity means that the information should always be stored in the way that it is available to use in legal ways for those who are entitled to use that information, to for example, process an order by a customer (SFS-ISO 27000. 2020.) For this thesis study to be justified, the information security aspect must be explored in the literature review, as it is an integral part of how information is handled and how user-based vulnerabilities are related to information security.

Business continuity, business impact analysis, and risk management are an integral part of information security, and they will be explained more thoroughly in chapter 2.4, but it is important to sate in this chapter that since business continuity, business impact analysis and risk management are meant to discover and analyze potential disruptions for business processes and the information that it uses, human errors, lack of knowledge and know how, and negligence can cause disruptions to the confidentiality, integrity, and availability of the information (Death, Rai. 2017, 167-169.) If any of the key aspects in the information security triad are compromised, it can cause not only legal problems but damage to the business' clients and to the integrity of the company and its reputation.

In information security there are major categories that need to be included into the information security risk management: threats, vulnerabilities, assets, and impact. Threat is a possibility of an incident happening. Finding and analyzing threats should always be a process which produces realistically possible threats to the organization. For example, an employee who has almost no experience in an information system, with a high level of access or allowance to change system's structure, is a threat. Taylor, Alexander, Finch, and Sutton (2013, 19-20) claim that threats should be categorized as accidental or deliberate threats which both contain two further categories: internal and external threats. One of the conditions for accidental threat is human error which can also be called user-based vulnerability.

Vulnerability is a weakness in the information systems that can be exploited and used. If maliciously or accidentally exploited, it can cause a sequence that can disrupt the information security triad. To further continue the example in the previous paragraph, if the information systems do not have some sort of hierarchical system in place that categorizes its users and gives or removes accesses to information assets based on that category, so that they have full access to every information asset, is a vulnerability in the system itself and how its build in the first place. If the organization utilizes domain-based controls, such as Microsoft's Azure Active Directory, giving admin privileges and access to an employee without any training or education, and that employee then would accidentally give access to confidential information to someone outside the company policies, is a human error caused by the lack of training, awareness, and knowhow and therefore a vulnerability that has been accidentally exploited. Vulnerabilities can be put into two categories: general vulnerabilities and information specific vulnerabilities. General vulnerabilities include basic weaknesses in software, hardware, premises, people, and processes and procedures. Information specific vulnerabilities consists of unsecured endpoints and mobile devices, unsecured servers and patched operating systems and applications and unsecured connections. (Taylor et al. 2013, 20-21.)

Asset is always the target of the impact of an incident. It might be multiple assets that can be affected, and the asset might not always be tangible such as a computer or a building, but it can also be intellectual property such as research and development secrets or a service that is being produced. It has also been discovered that when an asset is stolen, lost or damaged in any way, the organization will very likely have negative consequences as a result, which in some cases is unrecoverable damage to the asset, the organization’s reputation, and to the client or customer. (Taylor et al. 2013, 21.)

If a risk ends up happening, impact describes how severe the consequences of that risk are and what asset was the target of the impact. Taylor et al. (2013, 21) argue that impact is the most important concept out of all in information security management. The impact always has an effect on the information security triad, possibly compromising one of them which then can impair the organization’s abilities to function partly or even fully. In chapter 2.3, user-based vulnerabilities and their impact are elaborated more thoroughly. It can be argued that risk management is paramount to finding possible threats and weaknesses to information systems and prioritize those risks and risk categories that are the most dangerous for the organization. To conclude, there is a clear indicator, backed by previous research and evidence, that user-based vulnerabilities, their detection and having it part of a risk management process does have benefits and that user-vulnerability is a risk category on its own.

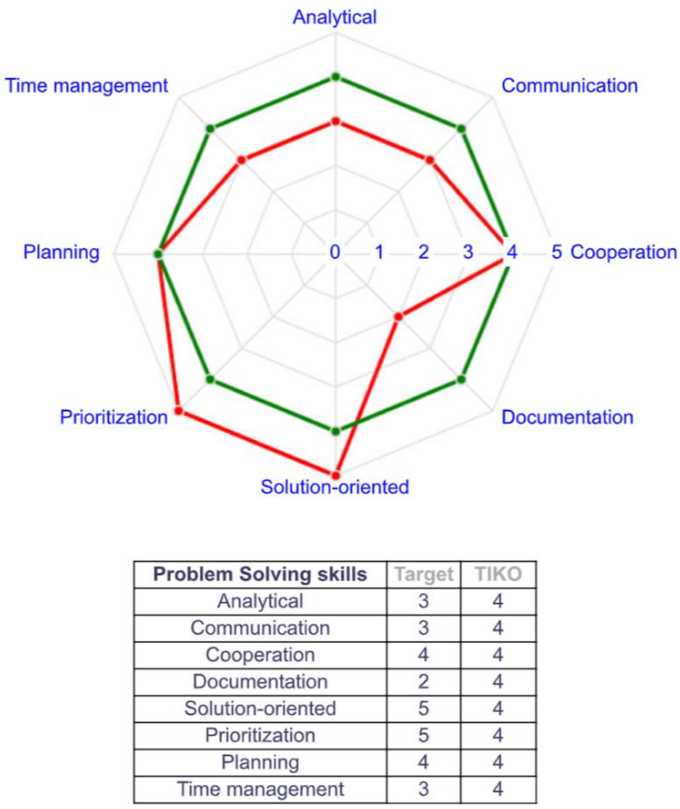
2.2 Relevant ECHO project frameworks and gap analysis

The ECHO (European network of Cybersecurity centers and Competence Hub for innovation and Operations) project was a part of four larger projects initiated by the European commission. “The project ECHO aims to deliver an organized and coordinated approach to improve proactive cyber defense of the European Union, allowing the block to act in anticipation, defending against an attack on computers and networks. ECHO is developing a network through which the EU’s Cybersecurity and Competence Centers can be best coordinated and optimized” (The European Commission, 2019.) One of ECHO project’s deliverables is the piloting study of ECHO toolkit and this thesis study aims to find out if the tools gap analysis information could be post-processed and further use that information to advance or support the user-vulnerability identification in an organization.

D2.6 ECHO Cyber skills framework is the basis for the creation of the ECHO toolkit as well as this thesis study. The framework aims to provide a foundation and guidelines for identification of skills gaps as well as the development of education and training programs to address those gaps. Cyber skills framework aims to provide practical tools for the design and development of learning outcome-based training programs. To accomplish it, the ECHO Cyber skills framework aims to address the needs and skills gaps of cybersecurity professionals by aligning with know-how from existing frameworks (Varbanov 2021, 12.) Based on the European Commission's stated need for digital knowledge and ECHO project's framework for training and growing the knowledge base, the purpose of this thesis study, the research of the ECHO toolkit and how its input could be further processed in information security, aligns with the ECHO project's goals.

The word gap in gap analysis refers to a space between the current level of skill and the expected or desired level of said skill. Gap analysis is based on the subjective truth from the participant and how they perceive their proficiency and competency in a specific skill. If the participant does not answer truthfully, the gap analysis data can get obscured for that participant and partly for the team. When the answers do reflect reality and are as close to the truth as possible from the participants point of view, gap analysis can produce reliable data that shows a clear gap between the needed and desired competency and proficiency (Frisk et al. 2022, 170). After the skill gaps are identified they can be represented in many ways visually.

Radar chart was used in the ECHO toolkit piloting study as a competitive analysis to represent a set of chosen parameters (Frisk et al. 2022). A number scale of 1-5 can be used to describe the level of said parameter. Five being the highest and one being the lowest. This thesis uses gap analysis data as a background information from part of the ECHO D9.15 case study, where a group of people in academic information technology areas were testing out the new ECHO toolkit that provides radar charts based on the self-assessment done as gap analysis. In the Toolkit, the study authors with a supervisor determined three major categories that were tested: technical skills, situational awareness skills, and problem-solving skills. Within those larger categories were 15-22 skills from which team members chose 5-8 skills for self-assessment. (Frisk et al. 2022, 169.) Before the self-assessment, the team supervisor chose the target value, or desired value, for each skill on the scale from 1 to 5. After a team member completed the self-assessment part, they got the results in the form of a radar chart. The radar chart showed two different graphs, one had the supervisor's set target values and the other represented the participant's own self-assessment values of the chosen skills. The toolkit provides both individual radar charts for each team member of the teams and a chart which shows the average level of skill for the whole team. The radar chart that the toolkit provides based on the set target values and individual asset skill values, produces a chart that looks like figure 2, in which the red line shows the desired level of proficiency and green line shows the result from the test group.



Problem Solving skills	Target	TIKO
Analytical	3	4
Communication	3	4
Cooperation	4	4
Documentation	2	4
Solution-oriented	5	4
Prioritization	5	4
Planning	4	4
Time management	3	4

Figure 2: ECHO toolkit radar chart (Frisk et al. 2022, 171).

In the piloting of the toolkit, it was discovered that the toolkit "provides evidence from a real work life setting that shows the Toolkit can be useful for organizations that wish to assess their e-skills and training gaps" (Frisk et al. 2022, 170.) Although the authors of the ECHO toolkit piloting study mention that the categories of skills could be better defined for future use, with the conclusion of the ECHO toolkit pilot study, it can be argued that there is a strong argument for studying if gaps in digital skills (e-skills) and the toolkit can be used to identify user-based vulnerabilities and how adequately ECHO toolkit suits for that purpose as a part of the information security management process. The list of skills that the participants were able to choose from and assess is in table 1.

Technical skills	**Situational awareness skills**	**Problem solving skills**
Architecture	Audit criteria	Analytical

Automation related	Built in security	Communication
Configuration of devices	Common security tools	Cooperation
Databases	Critical infrastructure configurations	Coordination
Development of testing and internal tools	Cybersecurity training experience	Decision making
HW related	Cybersecurity experience	Documentation
Industrial related	Data protection legislation	Interaction
Information system expertise	Infection mapping	Negotiation
Data protection and public sector legislation	Information security	Networking
Management related	Network security	Performance
Scrum and agile methods	Pressure resistance	Planning
Network related	Privacy protection	Practical
Programming	Public sector legislation	Prioritization
Information systems' security	Risk assessments	Punctuality
Optimization and maintenance solutions	Web app security	Self-driven
SW related		Service attitude
Usability		Solution-oriented
		Stress tolerance
		Systematic
		Teamwork

		Testing
		Time management

Table 1: List of skills in the ECHO Toolkit (Frisk et al. 2022, 169).

2.3 User-based vulnerabilities and their impact on information security

As stated in chapter 2.1, in information security, vulnerabilities are weaknesses in a system that can be used as a point of attack for malicious entity or individual. Leaving that vulnerability open and unchecked is called a risk. (Taylor et al. 2013, 20-21) One of the most common user-based vulnerabilities are very often tied to the lack of know-how of the information system, negligence, and lack of awareness of weaknesses or risks. Especially the risks that arise from not having proper knowledge of the information systems and how they are structured for the organization.

Munir Ahmed, Lukman Sharif, Muhammad Kabir, and Maha Al-Maimani (2012, 82) argue that the impact of human error in security practices make up two-thirds of security incidents based on reported incidents. Even with advanced information technology created, human factors are not yet excluded from the technological factors when investigating information and cybersecurity incidents. Meaning that information security must take into account the possibility of user-based vulnerabilities and possible human errors in the risk management process. Furthermore, in the risk management process and mediating or removing user-based vulnerabilities, demands building new information technology and digital skills as well as knowledge of the current and new solutions and technology. The European Commission has acknowledged this from a point of view of competitiveness and equality and the EU has started programs that would cater to the need of digital and e-Skills in Europe. According to the European Commission more than 90% of professional roles require basic digital knowledge in Europe. (EU. 2022.) Therefore, it can be argued that since information technology and human errors are inseparable, and 90% of professional roles require basic digital knowledge, user-based vulnerabilities are prevalent and bound to happen in every industry in roles where computers are used to any extent. For that reason, this thesis approaches the gap analysis as a possible solution to identify user-based vulnerabilities or to help identify which areas need more focus in the training of said digital skills and therefore possibly lowering the impact of human errors or the possibility of identifying user-based vulnerabilities before they fully become risks. Since the ECHO Toolkit piloting study authors conclude that the toolkit can be useful in assessing the e-skills and training gaps, and the study also took into consideration that the self-assessment in a skill might vary subjectively from individual to individual (Frisk et al. 2022, 170.), studying if the toolkit results are useful in risk analysis and vulnerability identification from the participants point of view, can produce useful information to the ECHO project and its successor and the information security community.

2.4 Risk management and business impact analysis

According to the ISO standard 31000 (2018), risk is an effect of uncertainty on objectives, which is a combination of risk sources, possible incidents and their consequences and the probability of the incident happening. Risk management then, is a coordinated process where different risks are being detected, analyzed, and controlled to best suit an organization's needs. It is a vital part of any organization's functions to identify possible vulnerabilities, threats, and risks in order to mitigate, transfer, remove or accept them. Part of the digitalization and the rise of IoT (Internet of Things), employees and their devices have become more risk inducing. Not only are there business secrets behind an employee account, but especially in retail businesses, almost endless lists of customer data and information that is protected and regulated by law. As stated in chapter 2.3, human errors make up most of the incidents in cybersecurity field (Ahmed et al. 2012, 82). Since human errors are so prevalent, it should be one of the main targets for vulnerability identification and risk reduction in the information security risk management process. Another part of risk management is business impact analysis. According to Priti Sikdar (2017, 95-96), business impact analysis is a process of studying and analyzing how disruptions affect business functions. The author further states that business impact analysis and risk management should be reported in the same documentation. As mentioned, risks that lead to an incident can be the disruption that impacts the business negatively. Since user vulnerabilities are so common, a disruption by a human error or negligence should be one of the main risk assessment and business impact analysis points in an environment that stores and uses confidential material for is business processes. When the potential disruption is analyzed, usually a few objectives are also established. For example, questions can be answered as how long of a disruption can the organization tolerate? How severe data loss can the company tolerate? How much data should the backups store to restore the system to a point where the business can continue with minimal loss of data? The same questions can be asked when studying how much damage a potential human error or gaps in the team's skills can cause in possible risk scenarios. By studying the ECHO toolkit's user experiences regarding user-based vulnerabilities, it can also provide some information on business impact damage when analyzing the toolkit's output of skill levels from the point of view of the participant.

2.5 User bias

As stated earlier, the premises for the toolkit to be useful, the participants' answers need to be as truthful as possible, meaning that they need to reflect the actual skills level of each participant as close to reality as possible. Given that the answers in the ECHO toolkit cannot identify how bias might affect the results, it is based on the trust in the answers as well as a comprehensive explanation to the participant on how the toolkit collects answers and what each answer category means. Therefore, it is important to explore on a theoretical level how user bias might affect the toolkit. Hence, the questionnaire questions for this thesis are constructed as statements in which it is easier for the participant to reflect the usefulness of the toolkit in a truthful way. As the ECHO toolkit researchers conducted, there is a possibility of participants under-or overestimating their skill in the respective categories (Frisk et al. 2022, 170). To add to it, if the participants don't feel that the toolkit is useful or the user experience isn't pleasant, the bias might increase. Therefore, for the ECHO toolkit to be successful in finding user vulnerabilities, any biases towards the participant's self-assessed skills or the toolkit would have to be minimized. When researching the usefulness of the toolkit and the user experience, it might also be possible to answer whether the user bias in the answers could hypothetically obscure the toolkit's results too much to be reliable data for information security user-based vulnerability identifying process.

Since the ECHO toolkit piloting study participants were from academic background in information technology related fields, it could be that their already accumulated skills and knowledge from IT, information systems, and technical skills caused major bias in answering to the ECHO toolkit self-assessment as well as to the questionnaire done in this thesis. Even though the ECHO toolkit pilot study deliberately chose academic IT-professionals as a group to study, the ultimate purpose of the toolkit's development is to be able to apply it in different fields for different professionals. But, the ECHO toolkit is developed as a cyber-and information security related skill measuring application, so it is possible that the piloting study academic IT-professional hypothetically could either be harsher towards the ECHO toolkit and its utility than necessary or have more positive bias towards it than necessary, for the same reason. In this thesis' questionnaire, of which questions reflect the ECHO toolkit's user-vulnerability application, are fully based on the user experience of the participants and their intuitive opinions of it. This can be defined as response bias that could arise from desirability to answer socially desirable answers in that moment to the questionnaire, even though the participant could have an opposing opinion (Furnham, 1985, 5).

2.6 User experience

Because this thesis and the questionnaire goes over the user experience of the participant, from a user-vulnerability point of view, it matters how the participant views the overall user experience of the ECHO toolkit and which can influence how the participants answer the qualitative questionnaire. Christian Kraft (2012, 3) in his book says that user experience, be it good or bad, affects the expectations of the product and the overall emotions towards the product. Kraft further states that bad user experience and a negative emotion towards the user experience will ultimately end the patronage of said customer. With this, it is fair to argue that bad user experience or a negative emotion towards the toolkit might cause bias in the ECHO Toolkit answers even if the output data corresponds to the participants inputs in a medium to high degree. The negative emotions or bad user experience also might be reflected in the participants answers in the questionnaire, even if the ECHO Toolkit might have worked the way the Piloting study authors expected in a technical level.

Another Laurea University student thesis studied the user experience of the ECHO toolkit from a technical point of view of the user interface as well as its usability. Using different methods and techniques the thesis author conducted that technically the ECHO toolkit worked as the piloting study authors expected but usability wise, the toolkit had issues. That said, the SUS-score (System Usability Scale) done by the thesis author, still provided more satisfaction than dissatisfaction on the usability user experience of the Toolkit (Arokanto, 2022, 37.) Having the user experience information as a part of the literature review is paramount for this thesis study since it can have a drastic effect on both the ECHO toolkit answers as well as this thesis' questionnaire answers. As said in the previous paragraph, it can increase the bias towards finding out the true skill levels of each participant, and therefore it can also affect the underlying user-vulnerability identification process.

3 Methodologies

Helen Simons (2009, 3) argues that case study is an approach, which indicates if a study has the research intent and methodological purpose, which affects the methods chosen to gather data. The purpose of the research for this study derives solely from the client's need of researching their developed gap analysis ECHO toolkit. The piece of research done in this thesis study is limited to the client's ECHO toolkit research results as well as the questionnaire done in this thesis. In the client's own case study (Frisk et al. 2022), they performed a gap analysis for two IT-teams consisting of 16 participants. Mentioned in chapter 2.2, the gap analysis toolkit provides a radar chart which is shown in Figure 2. In this thesis' case study, the same group that piloted the how ECHO toolkit were given a questionnaire afterwards to reflect their experience and the outcome of the toolkit. By joining the knowledge that the ECHO toolkit can work in optimal setting (Frisk et al. 2022, 170) and the supposition that the toolkit could be used as a potential user-based vulnerability identification method and because of the limitation and the usefulness of the information produced by the toolkit that is being researched, it can be argued that this study is unique enough to be called a case study.

3.1 Research methods in information security

As mentioned earlier, part of risk management is risk analysis. It is a process where all the risks, their probability and impact severity are analyzed in order to choose which ones are mitigated, transferred, removed or accepted. This analyzed data is gathered through various methods that are usually either, or both, quantitative and qualitative. An example of quantitative would be a questionnaire that produces numerical data and qualitative could be interviews that produce more specific answers to well-tailored and thought questions or tasks. The piloting study of ECHO toolkit used a qualitative method of gathering data by collecting individual assessments of the toolkit test users' skills, which then together with the supervisor set target skills produced specific radar chart data. Part of this thesis process was to collect data from toolkit pilot users after the piloting day as a Likert scale questionnaire. The questionnaire data will be analyzed as is in the further sections of this thesis to derive a conclusion for the research question.

Bill Gillham (2008, 2) in his book "Developing a questionnaire" says that questionnaires are a structured way for the researcher to ask a range of pre-selected questions or statements and answers. The author further states that the point of pre-selected possibilities of answers to the pre-selected questions, is to know which answers are selected by the participants. Which also makes the analysis easier for the researcher. The qualitative data that is gathered is done by Likert scale, with open-ended statements, that all had five answer possibilities: strongly disagree, agree, neutral, agree, strongly agree. As stated earlier, the self-assessment of individual skills can identify underperforming e-skills which in turn can cause vulnerabilities and risks. The statements in the questionnaire were targeted towards the toolkit and how the test individuals for the toolkit perceive the usefulness of the toolkit and the data that it produces for both the individual participant and the whole team. It is important for the self-assessment in the toolkit to be as truthful as possible since the test individuals subjectively assess their own skill levels, minimizing the individual bias. The individual bias and its contribution to the toolkit is more thoroughly explained in chapter 2.5. The point of the statements in the questionnaire are to help the test individuals reflect if the toolkit can be a truthful output for their skill assessments and if it can be used to detect their individual skills that lack competence and therefore could hypothetically cause vulnerabilities or possible risks to the information systems.

3.2 Questionnaire

This thesis used a questionnaire that was sent to the participants the day after the pilot for the ECHO toolkit was done. The questionnaire had nine statements, to which each had an answer possibility, as a Likert scale, ranged from strongly disagree to strongly agree giving a neutral response in the middle. Therefore, the answers give a number scale from 1 to 5, 1 being strongly disagree and 5 being strongly agree. The aim of the statements was to help the participants reflect on the piloting experience of the ECHO toolkit and the data it produces. By asking reflections in a statement form, in a questionnaire, from each individual of the e-Skills and Training toolkit pilot participants, the idea is to help them provoke more the idea of the potential information security application of the toolkit and more specifically, whether they acknowledge that gap analysis is viable method of detecting information security vulnerabilities in their own skillset or in the total skill level that the team produces. If the participants agree that the toolkit has potential viability, the lesser the possible bias is in both the ECHO toolkit answers as well as the questionnaire done in this thesis study. Since user-based vulnerabilities are most often caused by a lack of skill or knowledge, the participant or the team acknowledging their individual or team's lack of skills could help in creating the starting point for further growth for the lacking skills and to raise the lacking skills in the team to at least conversational level which can lead to safer information security environment in an organization. To research this, the statements in table 2, were asked in the questionnaire.

Statement	**Answer possibilities**
Gap analysis helped me to map where I am within my E-skills	Strongly disagree, Disagree, neutral, agree, strongly agree
After doing the gap analysis, I was confident in my current E-skills	Strongly disagree, Disagree, neutral, agree, strongly agree
Gap analysis made me realize that I have inadequate E-skills in some areas of information-/ Cybersecurity	Strongly disagree, Disagree, neutral, agree, strongly agree
Gap analysis made me realize that I have bad or neglective Information-and cybersecurity habits	Strongly disagree, Disagree, neutral, agree, strongly agree
I felt like the Gap analysis wasn't useful in finding out where my E-skills' strengths and weaknesses are	Strongly disagree, Disagree, neutral, agree, strongly agree
I felt that the Gap analysis didn't explain the team's differences in E-skills clearly enough	Strongly disagree, Disagree, neutral, agree, strongly agree

Gap analysis raised the team’s awareness of information- or cybersecurity skills that are inadequate	Strongly disagree, Disagree, neutral, agree, strongly agree
Gap analysis could be used as a tool to identify user-based information security vulnerabilities	Strongly disagree, Disagree, neutral, agree, strongly agree
Gap analysis raised discussion about information security habits and skills within the team	Strongly disagree, Disagree, neutral, agree, strongly agree

Table 2: Questionnaire statements

Since there are unobservable individual characteristics to the questionnaire and the thesis study, Likert scale was used to gather knowledge of the participants' opinions about the ECHO toolkit and data it produces. The main idea of the questionnaire is to gather knowledge from the toolkit piloting group and discover how the user experience and usefulness felt like when considering the information security application of the output data. Given that the questions are in a statement form, and since the idea of the Likert scale is to see which responses are answered the most, the data is then considered as qualitative. Each of the questionnaire statements and their purpose will be explained more thoroughly in the results in chapter 4. The neutral option was added into the answer pool in case the participants did not have any stance on the statement whatsoever, or possibly to find if the statement itself is irrelevant to the research topic. Since the questionnaire yielded only eight participants of the possible 16 that participated in the ECHO Toolkit pilot, the sample size is too small for any statistical analysis and therefore the answers need to be assessed as is. This means that if most participants answered the same answer or if most of the answers were on the disagree or agree side, it could be argued that the answers can either support or take away from the utility of the toolkit, depending on which side of the scale the answers are located.

4 Results

As said in chapter 2.2, in the Piloting study of the ECHO toolkit the participants had to evaluate skills in three larger categories and for each skill the supervisor had set a target level between 1 to 5 and then the participant would self-assess their skill in that scale of 1 to 5. The qualitative questionnaire gathered ended up consisting of 8 answers from the total of 16 people that participated in the toolkit pilot. The answer statistics will be shown in column charts. Since the participants in the ECHO toolkit pilot were both English speaking and Finnish speaking individuals, the statements in the questionnaire were written in both languages although in this thesis they will be shown only in English. As described in chapter 3.2, the answer possibilities range from 1 to 5. These numerical values are used in the summarization and characterization of the results by using the corresponding number of said range in parenthesis. For example, strongly agree would be shown (5).

The First statement, “Gap analysis helped me to map where I am within my E-skills” (figure 3) was pointed towards the understanding of the individual E-skills of the participant. Four of the participants answered that they agree (4) with the statement that the toolkit actually helped them understand what their skill level is. Half of the answers pointed towards agreeing (4), three participants were neutral (3) on the subject and one participant disagreed (2) with the statement.

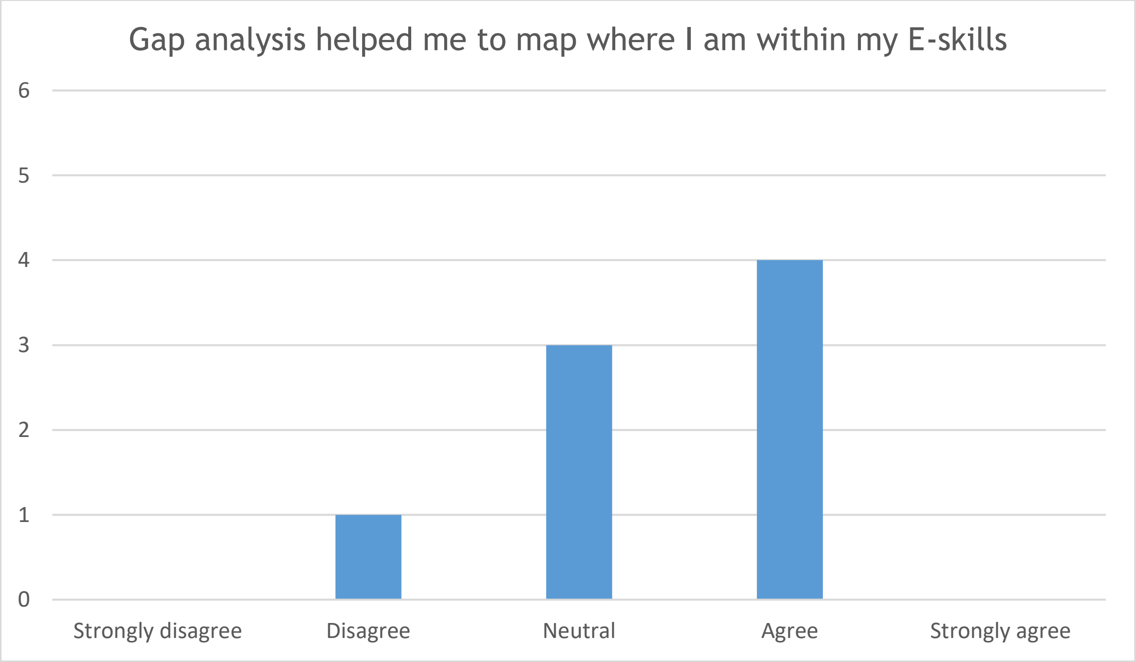


Figure 3: Statement 1 in the questionnaire

Second statement, “After doing the gap analysis, I was confident in my current E-skills” (figure 4), was to provoke the idea of being confident in the skills that were evaluated to discover possible biases in the toolkit answers towards the E-skills of the individual participant. Five answers in total were neutral (3) on this subject, one disagreed (2), and one (4) agreed. The neutrality in the majority of the answers to this statement could have been caused just by having the neutral option in this question or using the ECHO toolkit didn’t change their level of confidence at all.

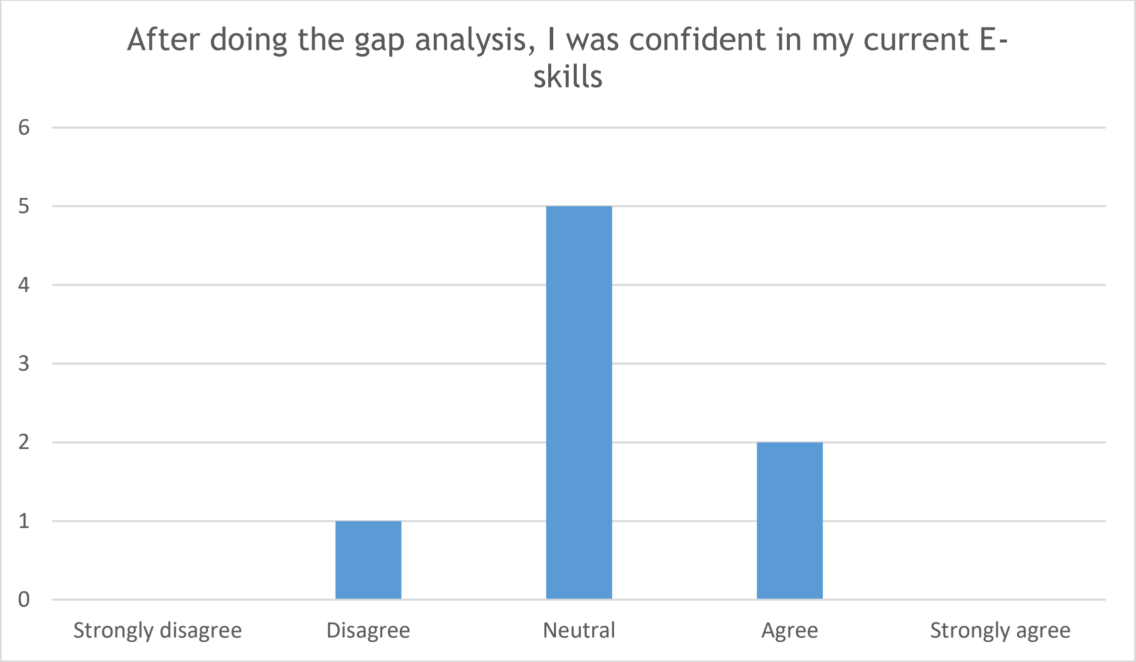


Figure 4: Statement 2 in the questionnaire.

The idea of the ECHO toolkit is to find the adequate and inadequate skills, to figure out the possible user-vulnerabilities and where the individual participant could improve their skills. The statement 3, “Gap analysis made me realize that I have inadequate E-skills in some areas of information-/ Cybersecurity” (figure 5), was asked from the participants to figure out if the output data of the ECHO Toolkit did show them where they could still improve and if they agree with that output. The majority answered the agreed (4) option and one strongly agreed (5). One participant was neutral (3) and two disagreed (2) with the statement.

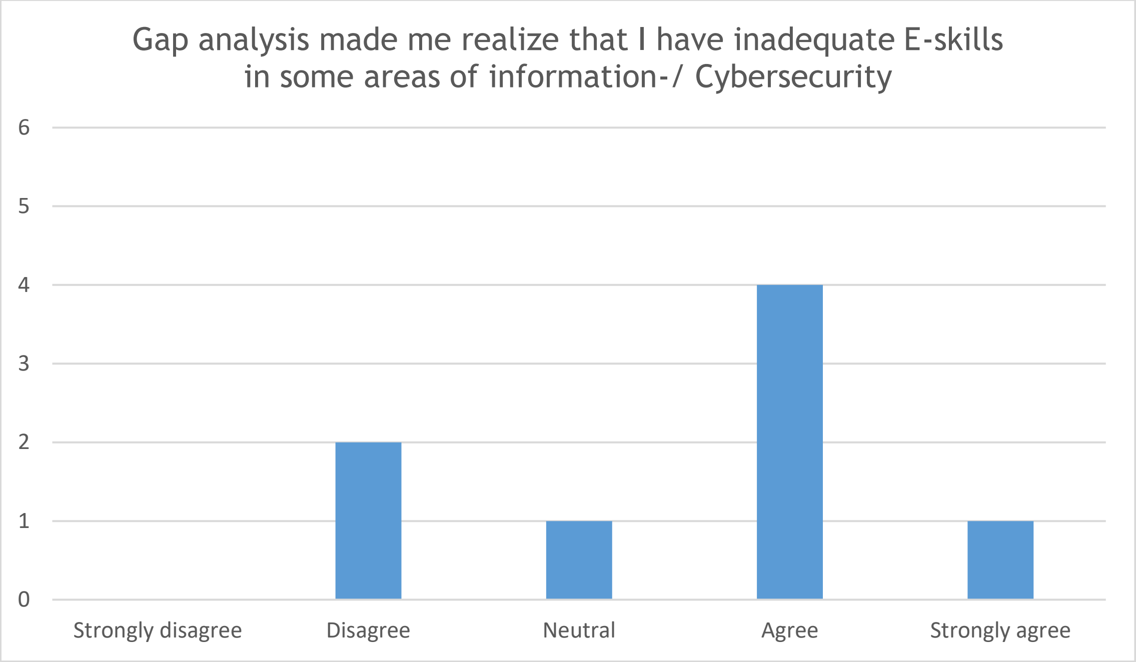


Figure 5: Statement 3 in the questionnaire.

The statement 4, “Gap analysis made me realize that I have bad or neglective Information- and cybersecurity habits” (figure 6), was to provoke the idea of possible neglective or bad habits that the participant might have realized that they have during the ECHO toolkit pilot study. Only one answered the neutral option (3) and six of the answers disagreed (6) with the statement and one strongly disagreed (1). While this kind of statement might have bias in the answers, the idea behind it is that since the ECHO Toolkit does measure the individual skills, it does not have a proper output for neglective or bad habits in the information systems, nor does it properly measure them. Therefore, this statement was put in the questionnaire to see if the participants understood the purpose of the ECHO toolkit and the task that they were assigned during the pilot study.

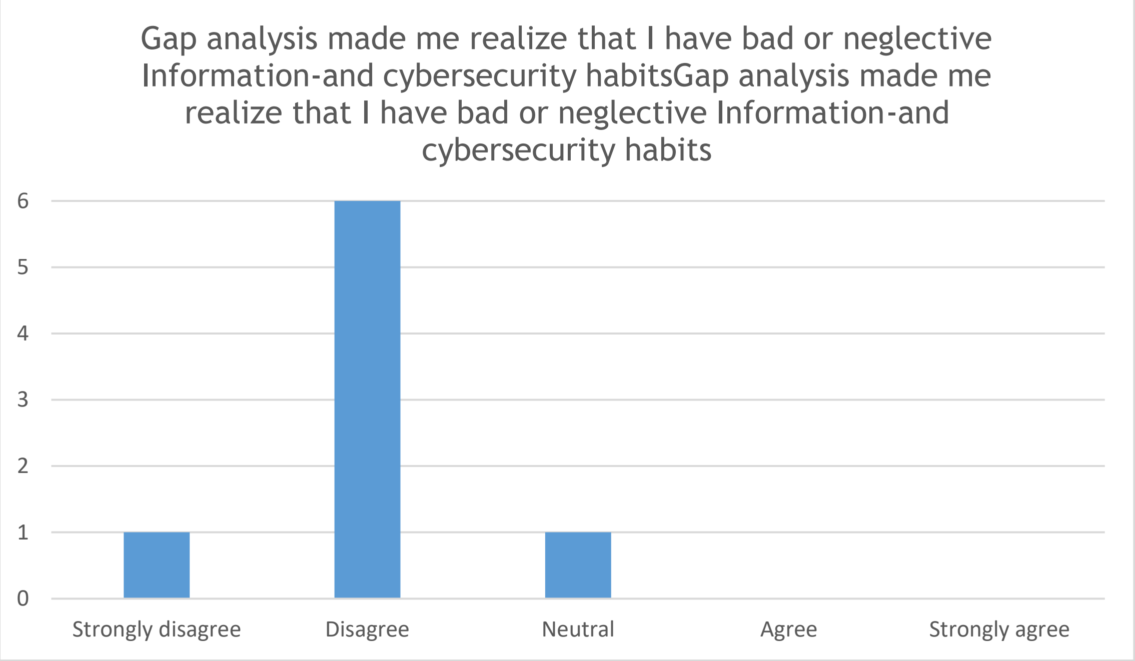


Figure 6: Statement 4 in the questionnaire.

Statement 5, “I felt like the Gap analysis wasn’t useful in finding out where my E-skills' strengths and weaknesses are” (figure 7), is a reversed statement from statement 1 in the questionnaire (figure 3). The idea was to measure if the attitude and usefulness of finding the E-skills in the ECHO toolkit would stay the same or roughly the same by reversing the statement. This helps to eliminate possible biases as well as makes sure that the answers are truthful and, at least to some degree, reproducible and not affected by chance. Three answers were neutral (3), three answers disagreed (3) and two answers agreed (4) with the statement.

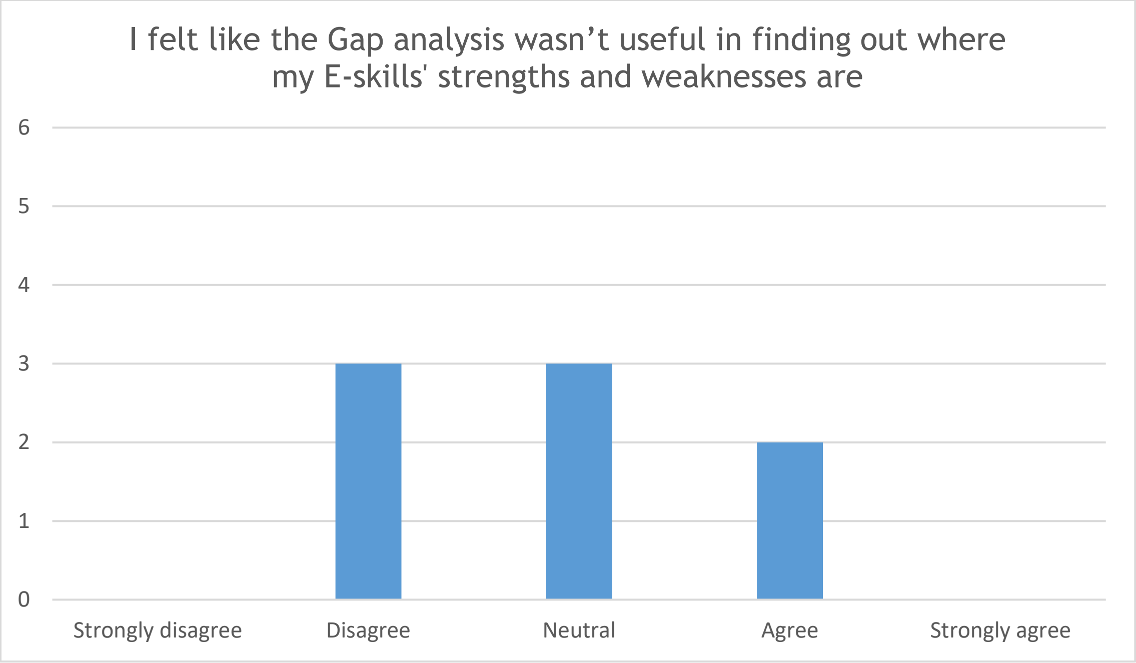


Figure 7: Statement 5 in the questionnaire.

Part of the ECHO toolkit’s output data is a radar chart that shows the average level of a skill for the whole team. This could help the organization as a whole to see where the team is still lacking in skills. Statement 6, “I felt that the Gap analysis didn’t explain the team’s differences in E-skills clearly enough” (figure 8) was to see how useful the participants perceived the toolkit’s output data for the whole team and if it was shown clearly enough to be understandable. Three answers agreed (4) with the statement, one was neutral (3), three disagreed (2), and one strongly disagreed (1). Most of the answers disagreed with the statement.

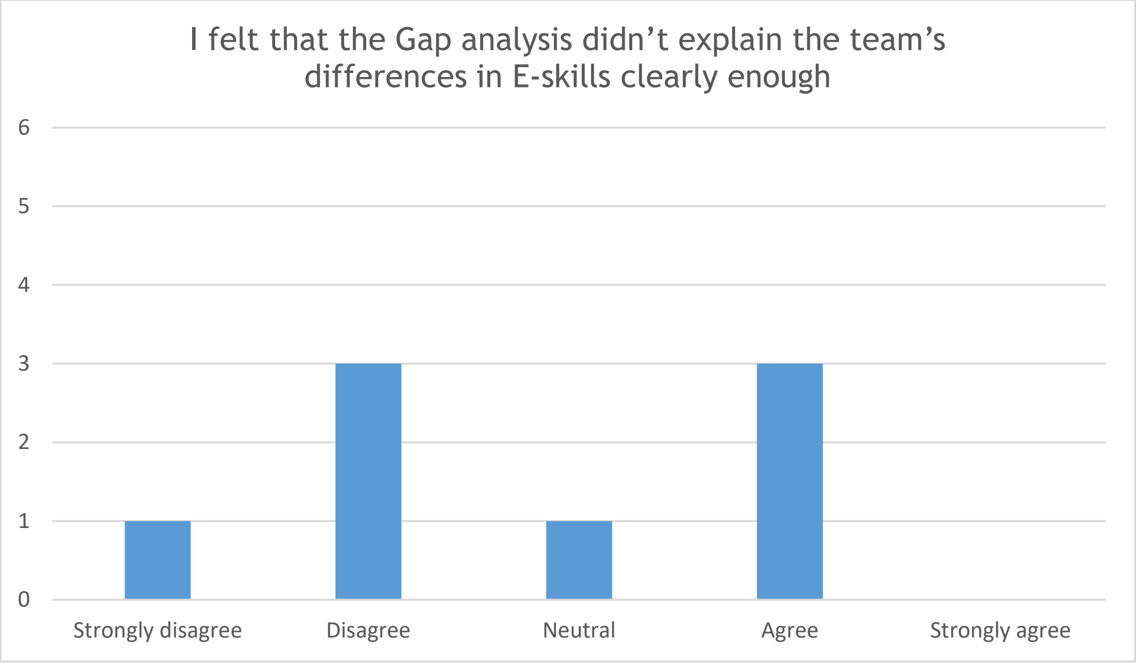


Figure 8: Statement 6 in the questionnaire.

Statement 7, “Gap analysis raised the team’s awareness of information- or cybersecurity skills that are inadequate” (figure 9), continued the idea of the ECHO Toolkit as a possibility to be used for the whole team’s assessment on top of the individual assessment. “Raised awareness” in this statement means that the individual participant would notice and understand from the Toolkit’s output data that there could be skills that need more training inside the team and knowledge that needs to be added to the team. Four of the participants agreed (4) with the statement, one strongly agreed (5), and three answered neutral (3) on the statement.

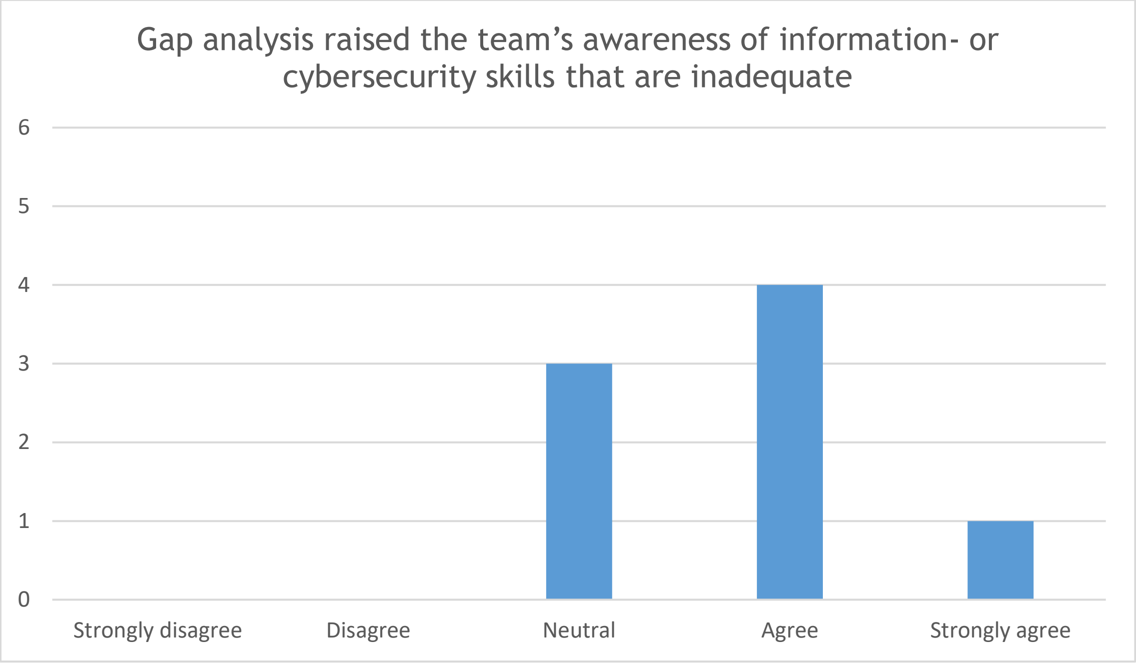


Figure 9: Statement 7 in the questionnaire.

As explained in chapter 2.3, one of the ECHO Toolkit’s output data usages that is being studied is the possibility to find user-based vulnerabilities with skill gaps. Also mentioned in chapter 2.5, user bias can affect the results to either side of the hypothesis of ECHO Toolkit being a viable tool for what it is made for. Statement 8, “Gap analysis could be used as a tool to identify user-based information security vulnerabilities” (figure 10), asks the participant if they could see a potential in the tool for user-based vulnerability identification. The idea is that if the participant agrees with the statement, it could indicate that they have answered truthfully to the ECHO toolkit skill assessment, minimizing the possibility of biases in the answers to the skill gaps. Also, since the participants were from professional academic IT backgrounds, it can be valuable information if the participants see the tool as a possibility for vulnerability identification. Four participants agreed (4) with the statement, two participants strongly agreed (5), one participant was neutral (3), and one participant disagreed (2).

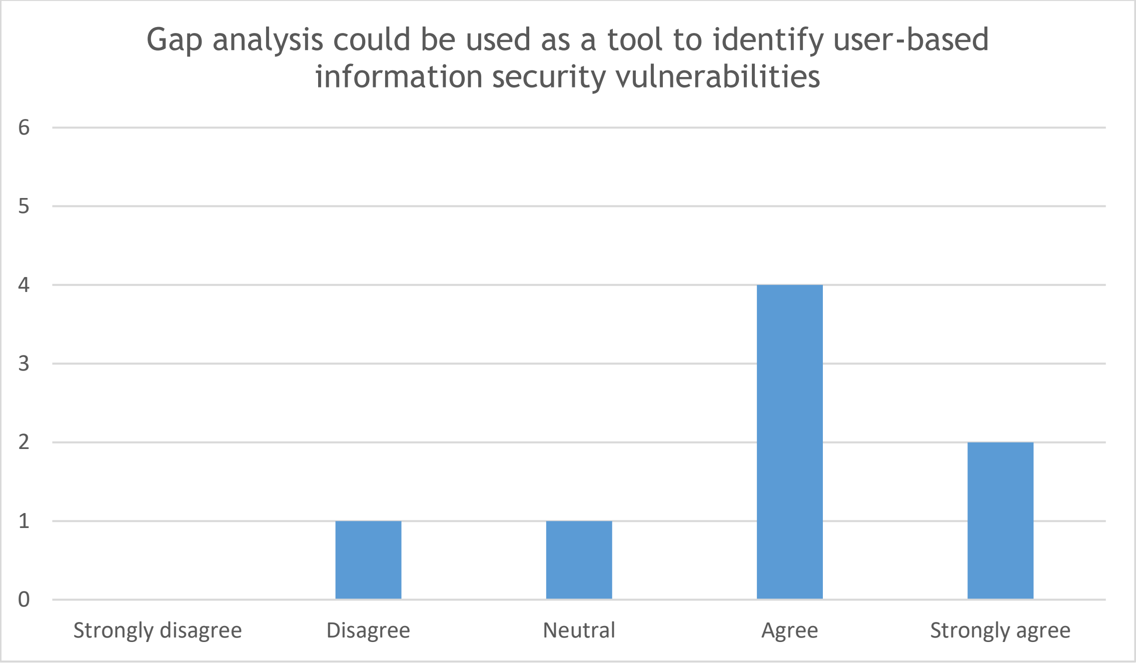


Figure 10: Statement 8 in the questionnaire.

As the authors of the ECHO toolkit pilot study conclude (Frisk et al. 2022), one of the main points of the toolkit is to be a starting point for a discussion within the team. Discussion could also be the starting point to patching user vulnerabilities that stem from a lack of knowledge or know-how of the information systems. In the statement 9, “Gap analysis raised discussion about information security habits and skills within the team” (figure 11), the statement asks the participant if they agree that the ECHO Toolkit can raise discussion towards the skills and habits within the team in the information security context. Four of the answers were agree (4), two were strongly agree (5), one answer was neutral (3), and one disagreed (2).

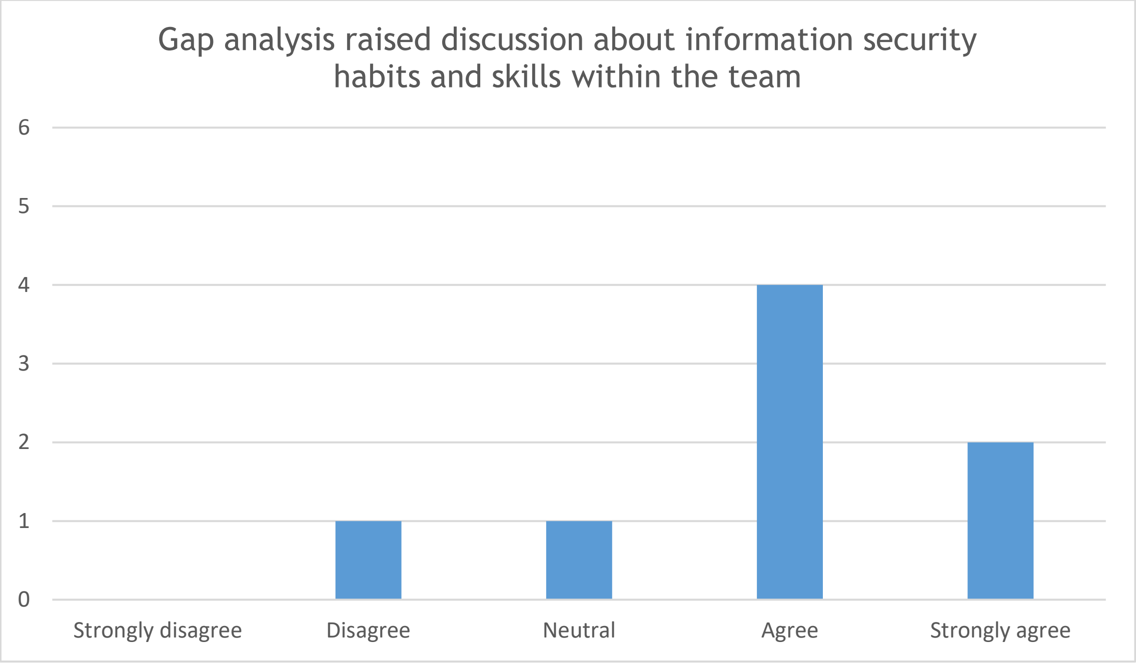


Figure 11: Statement 9 in the questionnaire.

From figures 3,5, and 9 it is clear to say that the ECHO toolkit can have success in finding the information-and cybersecurity related individual skill gaps, which is a positive outcome for the toolkit for finding user-vulnerabilities that would be so called general vulnerabilities. There is a possibility that socially it would be desirable for an academic IT-professional to answer that a newly found toolkit that measures information-and cybersecurity related skills works well just because it is new and exciting in the field, but having the technical user experience data available, as well as the other results from this thesis' questionnaire, such as the agreeable results in figure 5, would indicate that the participants answered mostly truthfully to the questionnaire as well as the toolkit's skill assessments, lessening the bias.

As said, the statement in figure 6 was to find out if the participants had understood the output data and the purpose of the ECHO toolkit. Since seven participants disagreed or strongly disagreed with the statement that the Toolkit provided the participant information about their possible neglective or bad habits, it is fair to say that the participants either understood what the ECHO toolkit measures, or they had bias in the answers to the Figure 6 statement. Even though it is possible, but it is unlikely that academic professionals in IT-fields would not be aware of their possible neglective or bad habits, it is more likely that the assignment of the ECHO toolkit was understood properly, thus supporting the possibility of the toolkit being useful in information security setting.

In figure 8, some of the participants agreed that the ECHO toolkit did not explain the teams' differences clearly enough. This could be just a limitation of the radar chart output that the toolkit has, and some participants could have struggled to understand it, disliked the method of showing, or truthfully didn’t perceive the radar chart as a clear indicator for skill gaps in the team.

Since the participants to the ECHO toolkit pilot study were academic staff in business information technology related degrees, figure 10 was asked. Having the possibility of bias in the Toolkit answers is most likely lower in a group of participants that understand the industry as well as information security and its vulnerabilities better. Therefore, this question can indicate positive feedback to the ECHO toolkit’s ability to scope user vulnerabilities as a part of otherwise established risk management process.

5 Conclusion

The objective of this thesis was to research if the client’s ECHO toolkit data output is useful in an information security and user-vulnerability setting and if it is possible to apply it in a real-world scenario. To put that into test, a questionnaire was done to the participants of how they perceive the usefulness of the toolkit and its output data in a real-life testing scenario that the piloting study authors conducted (Frisk et al. 2022). From a theoretical standpoint, user vulnerabilities and human errors are a real risk that every information- and cybersecurity practitioner should take into account in information security risk management. The ECHO toolkit has some potential in being a qualitative research tool when identifying user-vulnerabilities and scoping out risks in an already established risk management process, being a qualitative research tool in vulnerability and risk scanning. It should be tested how the toolkit’s output data changes, or the participants perception of the toolkit, when used in conjunction with some other method to support the user’s ability to self-assess their skills as well as proper discussions on the team’s strengths and weaknesses. For example, the participant should be made to feel that their answers and participation matters in the larger scale of the project and that it could prove to be valuable in their work or workplace in general, making the infrastructure more secure by finding out the possible user vulnerabilities. This could be done by telling or in writing before the self-assessment. This also could make the toolkit as well as the questionnaire less biased in answers.

Although the questionnaire gathered answers from only half of the potential participants, the pre-selected statements did run their purpose in seeing what answers were selected for the purposes of finding out the possible information security and user-vulnerability utility from the participants point of view, if the answers are assessed as is. Overall, it seemed that the user experience for the participants considering the information security side was more positive than negative. Although the questionnaire yielded some neutral answers for the statements, most of the participants in each statement were either disagreeing or agreeing, which indicates certain success or failure in the different aspects of the information security utility of the ECHO toolkit. In this case, the questionnaire results tilt more to the success side.

From the results, it seems that the output information from the ECHO toolkit has potential in revealing user-vulnerabilities, if used as a part of risk-management identifying process. As the literature review suggests, information security has three main components to it, confidentiality, integrity, and availability, of which all can be disrupted by user-caused vulnerabilities and risks such as human errors or lack of knowledge and skills. Having both gaps in skill levels between employees or teams, and the demand for talent versus the supply, ECHO toolkit has potential in revealing the gaps as a truthful source of qualitative data for both user-based vulnerability identification and overall risk management process. Since the toolkit shows which skills are inadequate, the information security practitioners could use the tool, in combination with other methods, to prioritize patching to the most vulnerable information assets.

The results of this thesis can be affected significantly by the fact that only 8 of the 16 Piloting study participants answered the questionnaire. Since the answer percentage of the initial group size is so small, a total of 50 percent of the potential answers, the data output of the toolkit would need more test studies in real-life scenarios. In each of these test studies, a questionnaire immediately afterwards can give helpful feedback on the usefulness of the toolkit data, which could also be a built-in feature to the toolkit that starts right after the gap analysis part is done. Also, adding the sample size to the toolkit and the questionnaire afterwards, as well as focusing the questionnaire questions to be even more aligned with the skills of the toolkit is recommended. The toolkit should be tested in different organizations, professions, through different professionals, and then comparing the usefulness of the data output and the questionnaire afterwards from each test setting to verify this thesis' results as well as to confirm the validity of the ECHO toolkit as a part of user-vulnerability identification process for different stakeholders with varying levels of IT-skills.

These results and recommendations were shown to the client in a Teams call during the thesis process. The literature basis, research methods, and the results of the questionnaire were presented. The client gave positive feedback on the idea of researching and concluding that the ECHO toolkit could be tested in a risk management scenario as a part of vulnerability identification process. It was acknowledged that with a higher sample size and larger, more heterogeneous test group, the results could vary from the original ones. When the ECHO project ends, the client said that the successor of the ECHO project will use risk management and vulnerability identification as a potential new perspective in developing the toolkit further.

References

Electronic

Arokanto, N. 2022. Usability study of the ECHO e-skills gap analysis tool. Accessed 3.1.2023. https://www.theseus.fi/bitstream/handle/10024/784823/Arokanto_Niko.pdf?sequence=2&isAllowed=y

Death, D. & Rai, A. 2017. Information Security handbook: Implement Information security Effectively As per Your Organization's Needs. Packt Publishing. Accessed 1.3.2023. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=5183382

Frisk, I., Tikanmäki, I. & Ruoslahti, H. 2022. Piloting the ECHO e-skills and Training toolkit. Vol. 53, no. 2 (2022):163-175. Accessed 6.5.2022. https://isij.eu/article/piloting-echo-e-skills-and-training-toolkit

Furnham, A. 1986. Response bias, social desirability and dissimulation. Volume 7, Issue 3. Accessed 15.12.2022. https://www.sciencedirect.com/science/article/abs/pii/0191886986900140?via%3Dihub

Gillham, B. 2008. Developing a Questionnaire. Bloomsbury Publishing Plc. Accessed 19.10.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=1644312

Kraft, C. 2012. User Experience Innovation: User Centered Design That Works. New York: Apress L. P. Accessed 10.10.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=1155991

Oliver, P. 2012. Succeeding with your literature review: a handbook for students. Accessed 15.9.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=863799

SFS-ISO 27000. 2020. Information technology. Suomen standardoimisliitto RY. Accessed 3.11.2021.

SFS-ISO 31000. 2018. Riskienhallinta.Ohjeet/Risk management. Guidelines. Suomen standardoimisliitto RY. Accessed 3.11.2021.

Sikdar, P. 2017. Practitioners Guide to Business Impact Analysis. Auerbach Publishers, Incorporated. Accessed 10.10.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=5050064

Simons, H. 2009. Case Study Research in Practice. SAGE Publications. Accessed 28.5.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=743724

Taylor, A., Alexander, D., Finch, A. & Sutton, D. 2013. “Information Security Management Principles”. BCS Learning & Development Limited. Accessed 10.10.2022. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=1213992

The European Commission. 2022. Shaping Europe’s digital future; Digital skills. Accessed 10.10.2022. https://digital-strategy.ec.europa.eu/en/policies/digital-skills

The European Commission. 2019. European network of Cybersecurity centres and competence Hub for innovation and Operations. Accessed 11.10.2022. https://cordis.europa.eu/project/id/830943

Varbanov, P. 2021. D2.6 ECHO Cyberskills Framework. Accessed 15.1.2023. https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf

Figures

Tables