One Size Does Not Fit All

Toward Contextualized Security Awareness Training Through User-Centred Design

Master Thesis MOT

B.C.P Zuurbier



TU Delft

One Size Does Not Fit All: Toward Contextualized Security Awareness Training Through User-Centred Design

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

Management of Technology

Faculty of Technology, Policy and Management
Delft University of Technology

Student name:	Bente Zuurbier
Student number:	4995120
Thesis defence date:	8 July 2026

Graduation committee

Prof.dr. M.J.G. van Eeten, Organisation & Governance	Chair
Dr. S.E. Parkin, Organisation & Governance	First supervisor
Dr. K.L.L. van Nunen, Safety & Security Science	Second supervisor

TU Delft

Preface

This research paper on security awareness training marks the end of a seven year journey here at the TU Delft, where I have been able to explore a wide range of interesting topics. From in-depth knowledge on algorithms and programming during my Bachelor's Computer Science, to creative problem solving during my minor at Industrial Design, ending with a year of exploring cyber security during my Master's in Management of Technology.

I am incredibly grateful for the many people I have met on my educational journey, and would like to thank some people specifically for the support during my thesis. First of all, I would like to thank Simon Parkin for all of the guidance and, most of all, the interesting discussions we have had, both during the elective courses and during the course of this research project. Your enthusiasm and knowledge in many different areas motivated me and piqued my interest to continue in the cyber security field in the future. I would also like to thank Karolien van Nunen and Michel van Eeten for being a part of the graduation committee, giving feedback and providing fresh perspectives. Giving me the space to make my own choices, but also reassuring me that the progress was looking good gave me the confidence to keep going.

I also want to thank my company supervisor for always making time for me and helping me find my footing in the company. It was fun to get a look at what a security team does during the weekly and monthly meetings, and you helped in making clear what the company would like to get out of the project, but also giving me the space to define it myself. I also want to thank all of the participants for taking the time to participate and for all the interesting conversations that followed because of that.

Last, but not least, I would like to thank my friends and family for the support during this period. Thank you to my parents and sisters for checking in on the progress and also planning fun things to sometimes take my mind off the project. Thank you to my friends who did the thesis project at the same time, for the many days together on campus, sharing all the doubts, but also celebrating all the milestones together.

Bente Zuurbier
Delft, July 2026

Executive summary

As cybercrimes rise, companies increasingly invest in security awareness training to protect themselves, but the effectiveness of the training is being called into question by researchers. Vendors sell one-size-fits-all training, yet these programmes fail to take the routines and needs of employees into account. This results in low engagement, wasted resources and, most importantly, little change in actual behaviour. Research has explored the relation between training and behaviour, identifying several factors that influence behaviour change. The resulting advice however often remains highly abstract. As such, this research explores how security awareness training can be made more effective by involving employees and designing or modifying it to align with their primary work tasks. It offers a structured approach and practical examples for practitioners to learn from.

The research was conducted as a case study in a large engineering company spread across Europe, focussing on the offices in the Netherlands. The pseudonym IECC was given to the company, as it was an International Engineering and Consultancy Company. Qualitative research methods were used, which included semi-structured interviews with employees from three departments and external experts, brainstorming sessions with employees and an expert validation session with IECC's CISO and change manager. The main research question was: *"How can security awareness training be designed or modified to align with employees' existing work routines and needs?"*

Co-design was used to answer this research question, as each step in the approach used employee input. First, employees were involved in defining their needs and routines from their primary work tasks to answer SQ1, the first sub-question. Three departments of IECC participated in the research, which included the finance department, the Business Unit Living Environment (BULE) and the fieldworkers from Field Lab Consultancy (FLC). The next step in the approach was to evaluate the current training for SQ2, in which employees were also involved. This helped determine which parts of training aligned with their needs and routines and which parts did not. For the last step, employee and expert input was combined to address the misalignments found, thus answering SQ3. This led to practical and example supported advice, targeting the factors that influence the effectiveness of security awareness training on secure behaviour.

The findings for SQ1 demonstrated how employees' primary tasks are accompanied by digital secondary tasks, which in turn shape their security needs. Finance employees, for example, have to do financial checks of projects and handle invoices. This means they have to be able to handle phishing in high-volume email environments, share sensitive files securely within legal constraints and protect their laptops against threats as they contain sensitive financial data. BULE employees, on the other hand, manage projects and create designs for clients, so they need to be able to securely share files with external parties and want clear company guidelines on how to manage these files. Employees from FLC conduct measurements out in the field and felt the need to protect their laptops against physical threats in uncontrolled environments.

The second sub-question examined how current training aligns with the identified needs and routines. The vendor-bought training was found to align only with the generic needs and routines, but more specific needs were left unmet. For example, it did not align with the routines of FLC employees, as they do not work in an office environment where completing e-learning modules is practical.

The final sub-question explored how the identified misalignments could be addressed. The findings were structured around the factors that influence behaviour change, from which prerequisites and training building blocks were developed. Where prerequisites are things that must be in place, but cannot be addressed by training, and building blocks are findings that can be addressed by training. The factors were grouped into two categories, simplicity (the behaviour should be easy to perform) and motivation (people need to be motivated to change their behaviour). Advice for improving simplicity included reviewing policies for feasibility, where a structured feedback loop is recommended to identify high friction policies. The frequency of training should be evaluated as well. It should not exceed employees' resource constraints, yet still be often enough so employees are reminded and do not forget. Different training methods should be offered to fit employees' routines and learning preferences. Advice for improving motivation targeted two factors, concordance and self-efficacy. To improve concordance, information on actual threats should be shared to improve risk perception. There also needs to be clear communication about what the training entails and why it is being done. It is also recommended to have multiple difficulty levels with an intake test to determine the appropriate starting level for an employee. The last piece of advice to improve concordance is by promoting interaction between colleagues on security topics. To improve self-efficacy, more actionable advice based on identified needs needs to be given.

These findings outline an approach to better align training with the needs and routines of employees. The first step in the process is to gather employee input on their primary tasks, needs and routines. The next step is to evaluate the current training in order to determine how well it aligns with the needs and routines found, identifying what needs to be changed and what is already working. The third and final step is to modify or design training using the identified building blocks, to promote actual behaviour change. By involving employees early on in the process, organisations not only gather the input needed to make targeted training, but also build concordance with them, meaning people are committed, which is needed for lasting behaviour change.

Contents

Preface ii

Executive summary iii

Acronyms list viii

1 Introduction 1

2 Background and related work 3
- 2.1 Security awareness training and security behaviour . . . 3
  - 2.1.1 Defining security awareness training and security behaviour . . . 3
  - 2.1.2 Relation security awareness training and security behaviour . . . 4
  - 2.1.3 Factors influencing the relation between training and behaviour . . . 4
  - 2.1.4 Visualizing the factors influencing the effectiveness of security training . . . 4
- 2.2 Designing security awareness training . . . 6
  - 2.2.1 How adults learn differently . . . 6
  - 2.2.2 Aiming for long-term effects . . . 7
  - 2.2.3 Concordance building instead of compliance . . . 8
  - 2.2.4 The role of co-design in making training role-specific . . . 8

3 Methodology 9
- 3.1 Research approach . . . 9
  - 3.1.1 Research setting . . . 9
  - 3.1.2 Research design . . . 9
  - 3.1.3 Sampling and recruitment strategy . . . 11
- 3.2 Research methods . . . 13
  - 3.2.1 Interviews within IECC . . . 13
  - 3.2.2 Interviews outside of IECC . . . 14
  - 3.2.3 Brainstorming sessions . . . 15
  - 3.2.4 Expert validation session with change management . . . 16
  - 3.2.5 Literature review . . . 17
- 3.3 Data analysis . . . 17
  - 3.3.1 Coding for interviews . . . 17
  - 3.3.2 Thematic analysis for brainstorming sessions . . . 17
  - 3.3.3 Framework analysis for expert validation session . . . 18

4 Primary tasks shaping routines and needs 19
- 4.1 Primary tasks, needs and routines finance . . . 19
  - 4.1.1 Primary and secondary tasks finance . . . 19
  - 4.1.2 Security needs finance . . . 20
  - 4.1.3 Routines finance . . . 20
- 4.2 Primary tasks, needs and routines BULE . . . 21
  - 4.2.1 Primary and secondary tasks BULE . . . 21

4.2.2 Security needs BULE . . . 21
4.2.3 Routines BULE . . . 21
4.3 Primary tasks, needs and routines FLC . . . 22
4.3.1 Primary and secondary tasks FLC . . . 22
4.3.2 Security needs FLC . . . 22
4.3.3 Routines FLC . . . 23
4.4 Similarities between departments . . . 23
4.4.1 Similarities in needs . . . 23
4.4.2 Similarities in routines . . . 23
4.5 Summary paragraph . . . 24

5 Current training alignment with routines and needs 25
5.1 Description of training at IECC . . . 25
5.2 Alignment with security needs and routines finance . . . 26
5.2.1 Alignment security needs finance . . . 26
5.2.2 Alignment routines finance . . . 27
5.3 Alignment with security needs and routines BULE . . . 27
5.3.1 Alignment security needs BULE . . . 27
5.3.2 Alignment routines BULE . . . 28
5.4 Alignment with security needs and routines FLC . . . 29
5.4.1 Alignment security needs FLC . . . 29
5.4.2 Alignment routines FLC . . . 30
5.5 Summary paragraph . . . 31

6 Designing training to fit with routines and needs 32
6.1 Simplicity and ability . . . 33
6.1.1 Time and effort . . . 33
6.1.2 Routine . . . 37
6.1.3 Culture . . . 38
6.2 Motivation . . . 39
6.2.1 Concordance . . . 39
6.2.2 Self-efficacy . . . 46
6.3 Summary paragraph . . . 48

7 Practical implications 51
7.1 Practical implications for IECC . . . 51
7.2 Practical implications for other companies . . . 52

8 Discussion 53
8.1 Discussion of results . . . 53
8.1.1 SQ1: Primary tasks, routines and needs . . . 53
8.1.2 SQ2: Alignment current training with routines and needs . . . 54
8.1.3 SQ3: Designing training to address misalignments using employee and expert input 55
8.1.4 Main RQ: designing or modifying training to align with primary work tasks . . . 57
8.2 Relevance and contributions . . . 59
8.2.1 Academic relevance and contributions . . . 59
8.2.2 Societal relevance and contributions . . . 59
8.2.3 Relevance with the MOT programme . . . 60

8.3 Limitations . . . 60
8.4 Future research . . . 61

9 Conclusion **62**

10 Appendix **66**
10.1 AI usage . . . 66
10.2 Dutch interview protocol . . . 66
10.3 Brainstorm session plan . . . 67
10.4 Expert validation session plan . . . 70
10.5 Codebook interviews in IECC . . . 74
10.6 Codebook interviews outside of IECC . . . 79
10.7 Brainstorming whiteboards . . . 81
10.8 Framework analysis expert validation session . . . 84

Acronyms list

Table 1: List of abbreviations

Abbreviation	Definition	Explanation
BISO	Business Information Security Officer	Role bridging security and business, held by an external interviewee.
BULE	Business Unit Living Environment	One of the three IECC departments studied. Manages projects and creates designs for clients.
CISO	Chief Information Security Officer	Role leading the security team, held by external interviewee and participant validation session.
FBM	Fogg Behaviour Model	Behaviour change model that looks at ability, motivation and triggers.
FLC	Field Lab Consultancy	One of the three IECC departments studied. Conducts measurements out in the field.
iCPS	Integrated Creative Problem Solving	European creative problem solving approach used to structure the brainstorming sessions.
IECC	International Engineering and Consultancy Company	Pseudonym for the case study company in which the research was conducted.
ISO	International Organization for Standardization	Standards body behind certifications (e.g. ISO 27001).
KAB	Knowledge Attitude Behaviour	Model linking training to knowledge, attitude and secure behaviour.
MFA	Multi Factor Authentication	Security measure requiring an additional verification step.
MOT	Management of Technology	Master's programme within which this thesis was completed.
RQ	Research Question	The main question guiding the research.
SAM	Security Awareness Manager	Person responsible for security awareness training.
SAT	Security Awareness Training	Interventions aimed at improving security knowledge and secure behaviour.
SQ	Sub-Question	The sub-questions that together address the main research question.

1 Introduction

In an age where cybercrimes are on the rise, companies seek to protect themselves by investing in secure systems and training their employees [19]. The phrase 'users are the weakest link' has been around for some time now, referring to the fact that users are seen as the reason systems fail, due to them making mistakes [25]. As a result, companies invest in training their employees to raise security awareness, assuming this will also increase secure behaviour. A full two decades later users are still seen as the weakest link however, casting a shadow of doubt over current security practices.

These doubts about the effectiveness of security awareness training are well-founded, as results from large-scale, long-term research in real-world settings demonstrate. While Lain, Kostiainen, and Čapkun [20] sought to determine whether employees could be used as a detection mechanism for company wide phishing attacks, they also found unexpected results regarding phishing training. They found that phishing training was ineffective and even led to increased click rates on phishing links. They surmised that this may stem from a false sense of security, with participants feeling overconfident in their ability to spot a phishing email. Ho et al. [15] investigated this further, setting up an eight month long experiment in the healthcare sector with over nineteen thousand participants. While a small improvement was found between those who received the training and the control group, the effect was deemed negligible compared to the effectiveness of different types of phishing lures. They also found that very few people who were presented with the phishing training actually spent time completing it.

Still, most companies assume employees simply need more security awareness training in order to get them to behave securely [12]. This is likely related to the fact that Security Awareness Managers (SAMs) often have to rely on Security Awareness Training (SAT) vendors, as they do not have the time or knowledge to create the training and measures themselves [12]. The SAT vendors provide both the product for raising security awareness and the metrics for measuring success of that product [14]. This creates an information asymmetry, making it difficult to know if the training is actually effective. It creates an environment where companies are unsure how effective their current training is and feel the need to do more to protect themselves, which the SAT vendors capitalise on by selling more training. SAMs often have to rely on them regardless, as they are pressured to report to higher management and adhere to legislation and standards set by certificates such as ISO 27004 from the International Organization for Standardization.

Important to note here is that the training those vendors sell is generic training which they sell to all companies [14]. This so-called 'one-size-fits-all' training leads to lower engagement and less actual change in behaviour, compared to more role-specific training [27]. Without taking into account different primary tasks or security needs that employees have, advice becomes less actionable [6]. Such training is generic on multiple levels as it has generic content, a generic way of teaching and generic end goal behaviour without taking existing routines into account. For example, employees in the financial department need to be able to discern a genuine invoice from a fake invoice, but employees from another department could simply discard any invoices they receive, as they never handle genuine ones [6]. Finance employees would benefit from more in-depth guidance, whilst other employees would likely lose interest going through advice irrelevant to their work.

The problem with companies relying on large amounts of generic training to protect their assets is that employees lose motivation and do not gain the skills or knowledge they specifically need for their tasks. This means not only a loss of the money spent on the training, but also a loss of the time employees spend on ineffective training. Without taking employees' perspectives and needs into account, training is unlikely to achieve behavioural change.

This research thus explores how security awareness training can be made more fit for purpose by including the users in the design process and taking their primary tasks into account. The current 'state of the art' is often too generic, simply copying what others do without accounting for the differences in employees' primary tasks and needs and routines related to those tasks. As the effectiveness of such training is being called into question, a fundamentally different approach to designing training is needed.

Following from this, the main research question is:

How can security awareness training be designed or modified to align with employees' existing work routines and needs?

With the following sub-questions:

1. How do employees' primary work tasks shape their routines and information and skill needs?
2. To what extent does current security awareness training align with these routines and needs?
3. What concrete adjustments to security awareness training can address the identified misalignments based on input from employees and (external) experts?

Together, the sub-questions address the main research question. SQ1 first looks at how employees' primary tasks shape their routines and needs, using employee input. To learn from what is already there, and thus find out what is and is not working, SQ2 looks at how employees evaluate the current security awareness training. Lastly, SQ3 looks at how gaps between the needs and training can be addressed, using both employee and expert input.

2

Background and related work

This chapter is divided into two main sections, section 2.1, which explains the theory behind security awareness training and security behaviour, and section 2.2, which explores how security training can be designed and what to take into account.

2.1 Security awareness training and security behaviour

This section defines security awareness training and behaviour, explains the Knowledge Attitude Behaviour (KAB) model which is used to justify using training to change behaviour, explains the factors that influence the relation between the two and concludes with a visual overview.

2.1.1 Defining security awareness training and security behaviour

This subsection begins by defining what security awareness training and security behaviour are. Security awareness training is a widely used term, referring to a host of activities. This includes activities such as phishing simulations, knowledge quizzes and having users read prepared materials. Other activities include face to face conversations, company wide emails or intranet announcements [12]. Alnajim et al. [3] categorised the training methods into two categories. The first category is conventional training, which includes lecture-based, text-based, video-based and web-based training. With these methods people are given knowledge and it is usually not interactive. Examples include posters, emails, intranet posts and e-learning modules. The other category is the simulation category, which includes any method with which users can practice in a simulated environment. This includes phishing simulation emails, game-based learning and virtual environments. In order to capture both categories, the definition from Hielscher et al. [14] will be used. Namely that security awareness training is "any intervention, online or in-person, to increase employees' security knowledge and/or to change their behaviour" (Hielscher et al., 2024, p. 2667). The other concept to be defined is secure behaviour. Generally speaking, it means to perform one's tasks in a secure way, such as checking emails for potential phishing attacks. Hielscher and Parkin [12] looked at some industry standards, such as ISO 27004, which states employees should be trained against social engineering through phishing simulations. Companies have policies on what employees should and should not do to be secure, as well as general topics they want people to keep in mind [12][24]. As such, security behaviour is defined as performing one's tasks in a secure way, according to company policy.

Based on these definitions, effective or successful security awareness training means that, after following the training, the security behaviour of people is improved. Examples would be that people are now creating secure passwords, using the phishing report button or changing settings in applications to be more privacy minded.

2.1.2 Relation security awareness training and security behaviour

Research into the effectiveness of security awareness training often looks at the relation between security awareness training and behaviour. Alkhazi et al. [2] state that as over two thirds of security awareness training is not effective, it is important to find out why that might be the case. Companies spend large amounts of money on training their employees, but often do not properly measure if the training was successful. Through the use of the Knowledge Attitude Behaviour (KAB) model they hypothesised training has a positive effect on knowledge, which in turn leads to a better attitude towards security policies, leading to improved security related behaviour. While they did find significant positive relations between each of the steps, a gap between reported attitude and behaviour was also found. When they analysed the answers of those participants, they found most reported wanting to behave more securely, but not having the time to do so. A similar study was done by Sas et al. [23], as they also made use of the KAB model. While they did find knowledge and behaviour to be significantly related, attitude and behaviour were not. They indicated that other variables may be at play, such as organisational culture. This means that the KAB model does not provide the whole view of what must be kept in mind when designing security awareness training.

2.1.3 Factors influencing the relation between training and behaviour

A possible explanation for the gap between attitude and behaviour comes from behavioural economics. It is based on the idea of bounded rationality, meaning humans have constraints, such as cognitive, time or knowledge constraints, with which they must make their decisions [6]. Expecting resources to be used for security might mean a loss somewhere else, such as productivity. The security training in this case will not be effective if it does not fit within the capacity and resources available to employees. If too much is asked from users, they will try to circumvent the policy instead [11]. A part of the problem here is that companies do not check if their policies and training are actually fit for purpose, yet ask users to follow them regardless [17]. As users start making compromises between following the policies and getting their jobs done, a form of shadow security arises. Finding out how to make training fit the different primary tasks users have can help prevent this and make the training more effective.

In a similar vein, Sasse et al. [24] state that for behaviour to change, the policy must actually be feasible for users, doable routines have to be created, primary tasks of users must be protected and the user must be engaged. This leads to a number of factors that influence the effectiveness of training. First, the environment must be conducive to change. This includes the organisational culture and the time allotted to users. Second, the user has to actively want to change behaviour and believe they have the ability to do so. Third, and last, the trigger for the old behaviour must be replaced with a trigger for the new behaviour to happen. These factors closely relate to existing behaviour models, such as the Fogg Behaviour Model (FBM), which states that for behaviour to change the person has to be motivated, find it simple to do, have the needed abilities and be triggered to perform the new behaviour [9]. While the culture and trigger have more to do with change management within a company, security awareness training can be used to improve motivation and ability.

2.1.4 Visualizing the factors influencing the effectiveness of security training

A visualisation of factors influencing the effectiveness of training as described above can be seen in figure 2.1. The factors are grouped into categories from the behavioural change model as created by Fogg [9]. They are arranged in the order in which factors should be addressed, as explained with the maturity curve by Sasse et al. [24]. The first category is simplicity and ability, as a person needs to be able to do the behaviour and it needs to be simple to do so. If a behaviour is not simple, the barrier to adoption will become too

high. As stated by Kirlappos, Parkin, and Sasse [17], resources such as time and effort are limited, which means a behaviour requiring little time and effort would make it easier to do. These factors should thus be addressed first, as motivating a person to do something that takes too much time or effort is considerably more difficult. Routine is also a factor in this category, as people are creatures of habit and prefer to stick to known routines [24]. Last in this category is organisational culture, as it can also influence people. If the culture is to behave securely and take your time for it, the barrier to that kind of behaviour becomes lower.
The second category is motivation, as people have to be motivated to actually change. The factors in this category come from Sasse et al. [24]. They include concordance, meaning people are committed to change, self-efficacy, which means people feel confident in their ability to change, and rewards and sanctions, which are external motivators. These factors are also in order, as people should first be committed to change before being taught the necessary skills. Teaching people who do not want to learn is not effective after all. Also, before going for external motivators, internal motivators should first be attempted.
The last category is the trigger or opportunity, as knowing when to display the new behaviour and nudging people to do it can also be a factor in whether people change behaviour or not [24, 9].

As the focus of this research is on security awareness training, a divide was made in the factors. Figure 2.1 shows the distinction that was made between factors that can be addressed through making security awareness training align with the primary tasks of users and ones that have to be addressed outside of that.

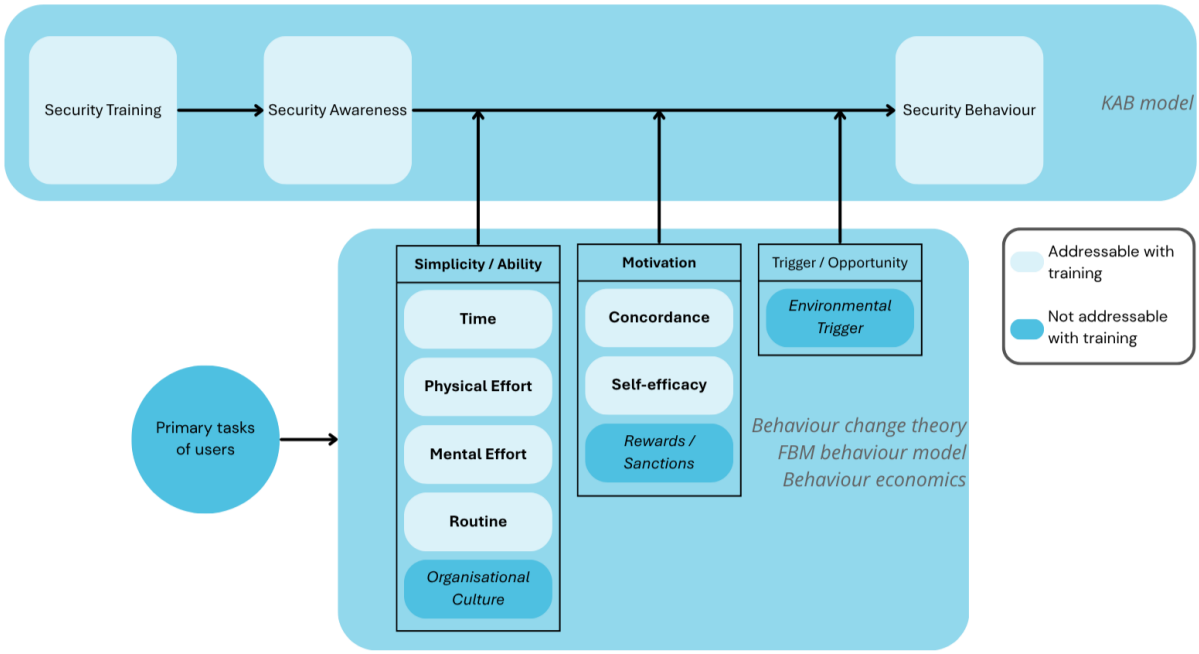

Figure 2.1: Overview of the factors influencing security awareness training effectiveness

All of the factors above are also expected to be influenced by the primary tasks of users. The amount of time and effort something takes, depends on how well it fits with their job. The routines a person has are also dependent on their job and co-workers likely influence the organisational culture they come in contact with. The motivation a person has can also be influenced by their primary work tasks, as someone who has to deal with frequent threats might be more motivated to do something about it than someone whose tasks are further removed from it. Depending on their work they also likely have different needs in terms of skills and information, which impacts their self-efficacy. The kind of rewards or sanctions can also change depending on their

job, as a manager likely faces different sanctions than someone working an operational job. As their primary tasks also influence which kind of applications you work with, environmental triggers also have to be different.

Now, to understand the overview of figure 2.1, consider the example given before, how generic phishing training is not effective as users have very different roles. If phishing training is not seen as one-size-fits-all, but instead made more specific to employees' roles, multiple factors influencing the effectiveness of security training can be improved.

More contextualised training could mean a reduction in time, physical effort and mental effort. Instead of asking users to complete large amounts of training that might not be relevant for them, for which they have to decide what is and is not relevant, they are only given training that is relevant to them. The routine factor can also be targeted, as the workflow of people can be taken into account better when the training is made for smaller groups. To spend thirty seconds on deciding whether an email is malicious is feasible for a person who receives three emails a day, but not for someone who receives a hundred a day. In the training, people can also be made more aware of what consequences could arise from falling for a fake invoice, influencing the concordance factor. A final factor that can be improved is self-efficacy, to improve people's confidence in their skills by giving information actually relevant to their job. For instance, by teaching people in the finance department how to spot fake invoices.

The other factors have to be improved through change management instead. The organisational culture has to be steered in such a way that people adopt the secure behaviours, which a change manager can help with. Part of this is the amount of time people are allotted to complete the training and to behave securely, which management has to make room for. Other aspects that have to be discussed with managers include which rewards employees get for completing the training, or which sanctions they get for failing to complete it. The last factor is the environmental trigger, a trigger for an employee to do the new behaviour instead of the old. These triggers could be implemented by the IT team, in the relevant application. This is again not a part of security awareness training.

2.2 Designing security awareness training

Now that it is clear which factors need to be targeted, the next step is to consider how training can actually be designed to address them. As such, this section builds towards an approach this research uses to accomplish that. First, it discusses what needs to be taken into account when teaching adults new things. Then it addresses how results can be sustained over time and how concordance can be built instead of forcing compliance. Together, these sections point towards co-design as an approach that can take these considerations into account simultaneously.

2.2.1 How adults learn differently

One of the things to take into account when designing security awareness training is the fact that it is for adults, who are not a blank slate like children are, but instead already have a frame of knowledge, experiences and beliefs that shape how new information is perceived [28]. According to Transformative Learning Theory, adults learn new things by reflecting on and challenging their knowledge, experiences and beliefs, to ultimately transform their perspective and understandings [21]. There are ten phases to this transformation, which begins with a disorienting dilemma, where the current frame of reference is disrupted as it failed to explain a new situation. This dilemma does not have to be dramatic or singular, but can also be cumulative. Other phases include self-examination, exploring new action, acquiring knowledge and skills and experimenting with new behaviours [28, 21].

The Transformative Learning Theory reinforces why one-size-fits-all training is not effective. Generic training makes the assumption that the users are a homogenous group, while they actually have differences in digital literacy, experience, cognitive capacity and knowledge [28]. Not taking their existing frame of reference into account leaves the training at risk of being irrelevant or inaccessible. Whitty [28] instead proposes to create cyber security training informed by transformative learning and thus recognise that adults interpret risks and learn through personal experiences. Training should allow users to critically reflect on their own assumptions and create meaning that is personally relevant. Another aspect to this is that people often discount risks, as they think it will not happen to them or does not happen close to them [26]. They might know it happens to one in ten people, but they do not think that they will be that one person. A disorienting dilemma might help shift this perspective, by showing for example that it did happen close to them. It can help nudge people towards secure behaviour, as they are more likely to employ prevention strategies when a threat is perceived to be harmful or likely to happen to them [7].

Whitty [28] gives an example of how phishing training can use transformative learning. The approach begins with a disorienting dilemma by showing that experts fall for phishing as well, followed by asking them to reflect on how they assess emails for legitimacy. This can lead to a group discussion where new information is introduced and where users can try out the strategies in a safe environment. It gives users a chance to reflect on their current frame of reference, and if needed, adjust it.

This implies that for training design, a single generic intervention is unlikely to trigger meaningful reflection. Even training that is tailored to the individual raises the challenge of ensuring effects do not fade over time.

2.2.2 Aiming for long-term effects

When designing security training it is also important to aim for long-term effects, as the goal is for users to always behave securely. Zhang [30] found that within a month of providing the users with training, the knowledge was forgotten. Especially more technical knowledge, beyond application level knowledge that is needed to use IT, was quickly forgotten. As such, they stressed the need for reminders, which Burke et al. [5] examined in the financial sector. They set up an experiment to see if training could decrease the chances a person invests in fraudulent opportunities. They found the effects of the training decayed over time, but a reminder intervention could prolong the effects for at least three more months, significantly raising the chances of retaining the knowledge for six months after the initial intervention.

To aim for long-term effects, it is thus recommended to include reminders, instead of a singular training moment. Reinheimer et al. [22] searched for the kind of reminder that performs the best, looking at a short text reminder, a video reminder or an an interactive example. They found that without any reminder, after six months no improved performance was found in distinguishing phishing emails from legitimate ones. After rolling out the reminders, the video and interactive examples were found to perform the best, with the effects lasting for at least six months after roll-out.

These reminders and exposure can extend the knowledge retention, but meaningful behaviour change needs more than keeping information fresh in people's minds. As can be seen in figure 2.1, employees must also be motivated to change behaviour in the first place.

2.2.3 Concordance building instead of compliance

As such, concordance is an important factor to address, as without it people are unlikely to stick to new behaviours. Ashenden and Lawrence [4] took inspiration from the medical field on how to reach the shared understanding and agreement needed for concordance. By co-designing the treatment plan, patients were much more likely to stick to it. A similar approach can be taken with security awareness training to improve concordance. Instead of forcing compliance, in effect mandating employees to follow policy which takes a lot of resources due to the need for constant monitoring and enforcement, the security team should aim for concordance [13]. Behaviour change is more likely to happen when people are given the option to commit to change themselves, instead of being forced to comply.

How to actually build concordance in practice, while also addressing the need for tailored and repeated training as discussed in sections above, is thus something that is essential for the chosen approach to address. Co-design offers a way to pursue all of them.

2.2.4 The role of co-design in making training role-specific

Since feeling ownership over the training they must follow helps improve concordance for users, the design process itself can be used for this. Involving employees in the process then becomes not only a methodological convenience, but a way of building concordance as well. Co-design offers this, as it is a structured way of involving employees in developing the training they have to follow.

Specifically, co-design can be used to make training align with the primary tasks that users have, by involving users in the creation of the training. Insufficient communication with users is often what leads to a lack of user-centred design [1]. To understand how co-design can be used for developing training, let us first define it. Kleinsmann and Valkenburg [18] state that in co-design actors share their knowledge in order to create the shared understanding needed to design the final product. This is done with the goal of creating new knowledge and integrating findings. Zamenopoulos and Alexiou [29] state that the idea behind co-design is that as no single person has the knowledge and skills needed to solve the problem, people need to come together to solve the problem for a better future reality. As people collaborate and connect, a synergy is created. As such, co-design is the practice where people collaborate and share their knowledge, skills and resources in order to design a final product [18, 29].

Kaur et al. [16] found that most researchers do not consult users before designing the artifact, which can lead to misalignment between actual and imagined requirements. Co-design can prevent these problems, as users are part of the design process early on. The different factors from figure 2.1 can also be targeted through co-design. By including users, they can make their existing routines clearer and help find ways to fit security into them. The concordance and self-efficacy factors are also taken into account, as part of co-designing involves acceptance finding, which is explained in more detail in the methodology chapter in section 3.2.3. In essence, by involving users early on they are more accepting of the solution and more motivated to actually do it [10].

Co-design is therefore not only a method for tailoring training, but also how this research addresses its main research question. Employees are directly involved in identifying needs and routines for SQ1, by exploring with them how their primary tasks shape those. Current training is also evaluated with them, in order to find out what is and is not working for SQ2. Finally, employee and expert input are combined to address the gaps and redesign training for SQ3.

3 Methodology

In this chapter, the research approach is discussed in section 3.1, which includes the case study setting, research design and sampling and recruitment strategy. In section 3.2 the research methods are discussed, along with their protocols. This includes protocols for the interviews within an engineering and consultancy company, the interviews with external experts, the brainstorming sessions and the expert validation session. Finally, in section 3.3 the data analysis methods are described.

3.1 Research approach

3.1.1 Research setting

The research took place both within an engineering and consultancy company and with participants from other companies large enough to have a security team. A case study was chosen as it allowed for richer data collection and made it possible to discuss the actual implementation feasibility of the findings. By doing the research within a company, it was possible to try to close the gap that currently exists between literature proclaiming that training must be tailored and how companies can actually do this.

The case study setting was within an international engineering and consultancy company. For ease of writing the company will be given a pseudonym hereafter, IECC (International Engineering and Consultancy Company). The focus of this research was within the Netherlands. The existing security awareness training within IECC consists of multiple approaches. They have previously organised a security week to raise awareness, have FAQ pages with information, send phishing simulations every two weeks and make use of a platform which has new training modules for employees every three weeks.

3.1.2 Research design

For this research qualitative methods were used to co-design security awareness training in order to improve the effectiveness of training. This included semi-structured interviews and brainstorming sessions. Where the interviews allowed for in-depth conversations, the brainstorming sessions allowed for group synergy, to generate more novel ideas and validate findings found in the interviews. As such, short interviews were held with people from three different departments within IECC, the results from which were used to hold brainstorming sessions. The interviews outside of IECC were also used as input for the brainstorming sessions, in the sense of 'at company X they do ...'. The results from the brainstorming sessions and interviews were then discussed in an expert validation session with the Chief Information Security Officer (CISO) and the change manager to look at actual implementation within IECC. Figure 3.1 shows which

sub-question each method aimed to answer and table 3.1 shows which sub-questions correspond to which abbreviation.

SQ	Full question
SQ1	How do employees' primary work tasks shape their routines and information and skill needs?
SQ2	To what extent does current security awareness training align with these routines and needs?
SQ3	What concrete adjustments to security awareness training can address the identified misalignments based on input from employees and (external) experts?

Table 3.1: Sub-questions overview

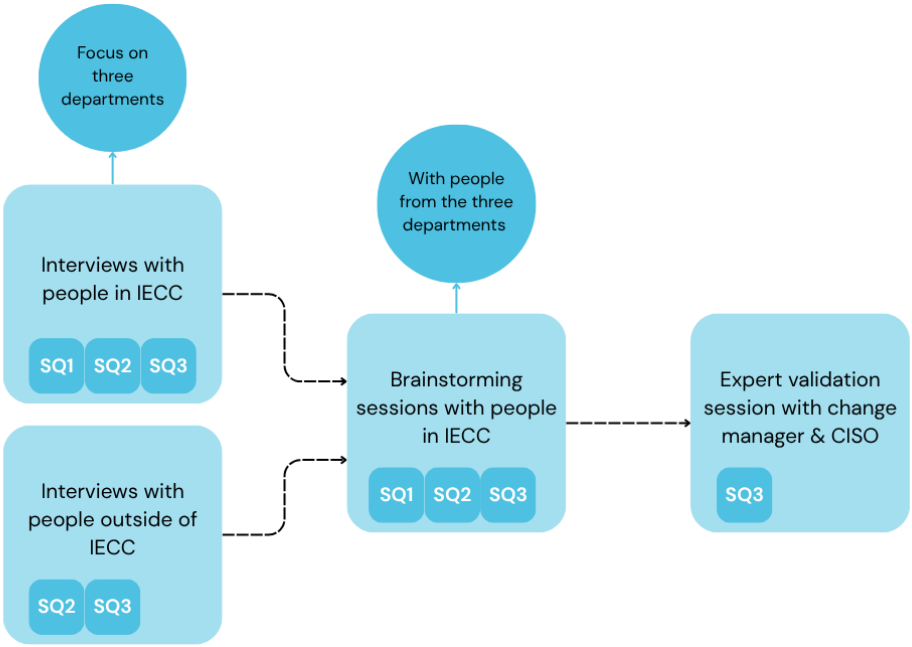

Figure 3.1: Research design

Through the interviews with people in IECC, data was gathered to answer SQ1, SQ2 and SQ3. It helped to answer SQ1, as employees were asked what their primary work tasks are, what their work environment looks like and how security fits with these tasks. Employees were also asked what their opinion is on current security awareness training within IECC and how they feel that it fulfils the needs they have. This helped to answer SQ2. The last question it helped to answer was SQ3, as people were also asked which kind of training methods they prefer.

SQ2 and SQ3 were answered with data gathered from interviews with people outside of IECC. They were asked if they had made their training more role-specific and if so, for which reasons. This helped answer SQ2. They were also asked which kinds of training they had deployed and for which reasons. In particular, participants were asked if they did so as it better fitted within the routines and needs employees have, which is related to SQ3. They were also asked how they make use of employee input, which was used to answer SQ3.

The brainstorming sessions served two purposes, to validate findings found from the interviews and to come up with ways in which training could address the identified needs. As such the brainstorming sessions were used as input for SQ1, SQ2 and SQ3.

The last step in the research design was to conduct an expert validation session with the change manager and CISO within IECC. This session served to determine how the employee input could realistically be used to tailor training to different primary work tasks, to validate findings found for SQ3 and to inform the practical implications chapter.

3.1.3 Sampling and recruitment strategy

The sampling and recruitment strategy is explained in this section, with figure 3.2 showing the number of participants for each method. The interviews were held with three to four people per department, ideally the same group of people would have been in the brainstorming session together. Due to planning issues, the finance brainstorming session was attended by two people and the one from BULE with three people. The finance brainstorming session was held fully online, as people could not be in the same physical location at the same time. The session with BULE was hybrid, with one person joining online and two people being there in person. The session with the people from FLC could not be planned, as it was not possible to find a day during which all the fieldworkers could be in the office at the same time. For the interviews with people outside of IECC, three people were interviewed.

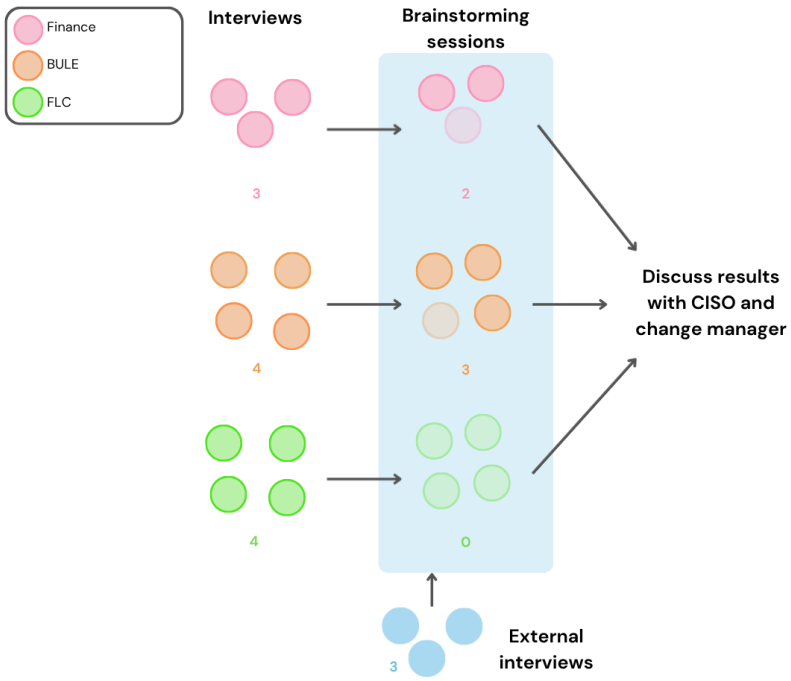

Figure 3.2: Participants

All participants were informed prior to participating what kind of data collection would take place, what would happen to the data afterwards and that participation was voluntary and could be stopped at any point during the research.

Sampling and recruitment strategy interviews and brainstorming sessions within IECC

The chosen sampling strategy is purposive judgement sampling, where participants had to fit within the profile described below. The recruitment was done through the CISO, who contacted team

leads and managers of the departments to ask them if they knew people who they thought would be a good fit to participate. This was done for multiple reasons, first of which was so that people were given approval to spend time on this research from their manager. As participation would take them at least two hours, this way people could feel assured it was okay to spend time on it. Another reason was to make it easier to find a good spread of people in different roles. It is important to note that participation was still stressed to be voluntary, as evidenced by some people declining to participate.

The interviews that took place in IECC were held in different departments in order to get participants with diverse primary tasks. Considering time constraints, the scope was set to three departments. The finance department was chosen as it was deemed a high-risk department, the fieldworkers (Field Lab Consultancy, FLC) were chosen as they had an entirely different work environment and the Business Unit Living Environment (BULE) was chosen as it was the last department from the three main business units IECC has. This also helped to validate any findings contrasting people working in an office environment or in an outside environment, as a second department working in the office was added. It also helped with contrast between working in an internal environment and working with clients. The participants had to have different roles, in order to get a wider view of task diversity. Aiming to create training relevant for a department, instead of relevant for only one specific role or small set of primary tasks, also made it more realistic for a company to actually do. Ideally, however, there were two participants in similar roles, or with similar primary tasks, to validate the findings and better protect the anonymity of participants. Participants were asked about the training, so they needed to be somewhat familiar with it. As they should be familiar with their tasks, security needs and training, participants should be in their role for at least six months already. Summarizing this, the inclusion and exclusion criteria were as follows:

- **Participants should be either working in the finance department, out in the field (FLC) or in BULE. A somewhat even split between departments should be kept.**
- **Participants should have diverse roles, where some overlap is encouraged, but if too many similar roles already participate they should not be included.**
- **Participants should be aware of the security awareness training of IECC, though it is not necessary they completed it.**
- **Participants should have been in their role for at least six months, so as to have a good grasp on primary tasks and security needs.**

Following from this, three people from finance participated, four from BULE and four from FLC. The participants from finance were given the codes F1, F2, F3, the participants from BULE were given the code B1, B2, B3, B4, and participants from FLC were given the codes FLC1, FLC2, FLC3 and FLC4.

Sampling and recruitment strategy interviews outside of IECC

The same sampling strategy, purposive judgement sampling, was used for the interviews outside of IECC, for which participants had to fit the profile as outlined below. The participants were recruited through the researcher's personal network. Two companies came from more IT oriented sectors, which gave an understanding of how training might be done in companies where employees are more digitally mature. One company came from a sector more similar to IECC as it was an engineering sector with people who also work out in the field. Participant E1 works at a company in the ICT sector, as it is a company that handles the IT service desk and application management for clients. Participant E2 works in a similar sector, as they work for a company that gives cyber security advice. Lastly, participant E3 works for a company active in the energy sector, as the company is a wholesaler in that industry. Prior to that they also worked as CISO for a shipping company and engineering company in the energy sector.

The interviews that took place outside of IECC were done at multiple companies. These interviews were not done with users, but instead with people who have designed or decided on the training used at the company. They all had some relevant experience in security awareness and ideally had experience with incorporating user feedback. As participant E1 is the BISO (Business Information Security Officer) of the company they work for, participant E2 is a cyber security consultant who organised the training sessions for their company and participant E3 is the CISO for their current company and had been for two other companies in the past. This led to the following inclusion and exclusion criteria:

- **Participants should be active in a role related to security awareness training**
- **Participants should have experience with designing security awareness training**
- **Participants should be from different companies**
- **Participants would ideally have experience with co-design or practising user-centred security**
- **Participants should be able to speak Dutch or English.**

3.2 Research methods

3.2.1 Interviews within IECC

The semi-structured interviews were held with people from different departments within IECC, where semi-structured interviews were chosen to allow for further exploration of interesting topics that came up. This was also done as the primary tasks and needs were not yet clear before the interviews started, as such the freedom to explore them as the interview went on was needed. Participants were asked what their primary tasks are, the information needs they have, how current training is fulfilling those needs and which kinds of training they prefer. These interviews took place over Teams, as it helped with transcribing the interviews. Participants were informed of this beforehand and signed an informed consent form or gave verbal consent before the interview took place. They were also again informed that participation was voluntary and they were free to not answer any question they did not want to answer. As most employees are not confident in their English skills or cannot speak English, the interviews and brainstorming sessions in IECC were held in Dutch. The full interview protocol in Dutch can be found in appendix 10.2.

The interview protocol can be found in table 3.2. First, in order to answer SQ1, the primary work tasks, information and skill needs and routines had to be known. Next, for answering SQ2 participants were asked if they have followed training, what their opinion is on it and how it fulfils their needs as identified before. Lastly, to answer SQ3, interviewees were asked which training methods they prefer and why they prefer them. The protocol was slightly revised after the first interview, as the question was "Which kinds of security issues do you encounter in your daily work?", but the word issues seemed to be too closely associated with actual incidents happening and thus something going wrong, which led to a strong denial that anything happened. As that was not the purpose of the question, it was changed to "How do you feel that security is a part of your daily work?" as it was a more neutral way of asking and people were more enthusiastic to show their knowledge, instead of feeling like they were expected to have done something wrong.

In these interviews the connection between the primary tasks and factors addressable through training were found. People were asked about their primary work tasks, which kind of needs they have, connecting to self-efficacy, and their routines in relation to each other. Other factors were also discussed as their opinion of current training and general training preferences was explored, connecting to the time, effort and concordance factors.

Table 3.2: Interview protocol interviews in IECC

Sub-question	Measure/variable	Interview question
SQ1: How do employees' primary work tasks shape their routines	Primary work tasks	Could you briefly introduce yourself, such as your role and which department you work in? What are your primary work tasks?
and information and skill needs?	Information and skill needs	How do you feel that security is a part of your daily work? * Which cyber risks do you feel you are exposed to during your work? Do you ever run into issues in your daily work for which you need more knowledge or training?
	Routines	How does your daily work environment look like? Think for example of where you work, what the environment looks like, which technologies you use, etc.
SQ2: To what extent does current security awareness training align with these routines and needs?	Knowledge on current training	Which, if any, of the security awareness training have you done at IECC?
	Opinion of current training	What is your opinion on the current security awareness training at IECC?
	Fulfilment information and skill needs	How does the current security awareness training fulfil your skills and knowledge needs?
SQ3: What concrete adjustments to security awareness training can address the identified misalignments	Training approach preference	Which kind of training methods do you prefer? (E.g. e-learning, physical workshops, short videos).
	Fit training approach and routine	Can you explain why these are your preferred training methods?
based on input from employees and (external) experts?	Training inspiration	Which kind of education or training method did you like outside of security training, and why did you like it?

3.2.2 Interviews outside of IECC

The semi-structured interviews with people outside of IECC were used to determine if and how other companies take primary tasks of users into account. The interviews also served to find out if and how they took user input into account, as well as which types of training they deploy. By conducting these interviews at multiple companies, real-life examples of role-specific training were found. These interviews also took place over Teams and these participants also signed informed consent forms and were reminded that questions could be omitted and participation was voluntary.

The interview protocol for these interviews can be found in table 3.3. For SQ2 questions were asked in order to find out more about the current training and if it takes different needs into account. Next, for SQ3, ideas for different types of training approaches were gathered, as well as the fit with employees' routines. Interviewees were also asked how employee input is incorporated in order to find out feasible ways of doing so.

These interviews also helped to gather data on how to address the factors from the framework, but without the connection to primary tasks. Some questions targeted factors more explicitly, for instance questions on training fitting with routines relate to the routine factor, while those on the training and needs relate to the self-efficacy factor. Other questions depended more on the answers gained, effective training might be because people are motivated or because people find it easy to do. The training preferences, highlighting moment and employee incorporation could address any of the factors, depending on their motivation behind their answers.

Table 3.3: Interview protocol outside IECC

Sub-question	Measure/variable	Interview question
SQ2: To what extent does current security awareness training align with these routines and needs?	Effectiveness	What is the wanted secure behaviour for employees that you are aiming for? How close do you think your security awareness training brings you to the wanted behaviour? Prompt: How do you know that is how effective it is?
	Training & needs	Which kinds of content do you include in your trainings and why? Do you take information and skill needs of different employees into account when deciding on the content? If yes, how?
SQ3: What concrete adjustments to security awareness training can address the identified misalignments based on input from employees and (external) experts?	Creation training	Do you buy your training from a vendor or do you create it yourself? Follow up: (If they have created training themselves) Can you tell me more about X training, what was your process for creating it?
	Training approach preference	Which methods do you make use of for your security awareness training? Follow up: What was the main driver for choosing X method?
	Fit training approach and routine	How do you think these kinds of training fit with employees' routines?
	Highlighting moment	Can you give me an example of training that you implemented that did not work? Why did it not work? If you had to pick one of the training methods that we have discussed, which one do you like the most and why?
	Employee input incorporation	Do you take employee input into account when developing security awareness training? If yes, how? Have you asked employees for feedback on the security training? If so, what did they feel about it?

3.2.3 Brainstorming sessions

Another method used was hosting a brainstorming session with participants. These sessions were held with people from the different departments to validate the findings from the interviews and facilitate a group discussion on security needs and training methods. One session was done hybrid and one fully online. In the same informed consent statement signed for the interviews, participants were also informed about the

data collection and time needed for the brainstorming sessions. These sessions were based on the Integrated Creative Problem Solving (iCPS) approach, which was created by Heijne and van der Meer [10] as a European version to the American Creative Problem Solving approach. iCPS includes project management, information finding, acceptance finding and content finding. A visual overview of this approach can be seen in figure 3.3. The full session plan can be seen in appendix 10.3. This session addressed the factors of the framework in a similar way to the internal interviews, by taking the primary tasks into account as well.

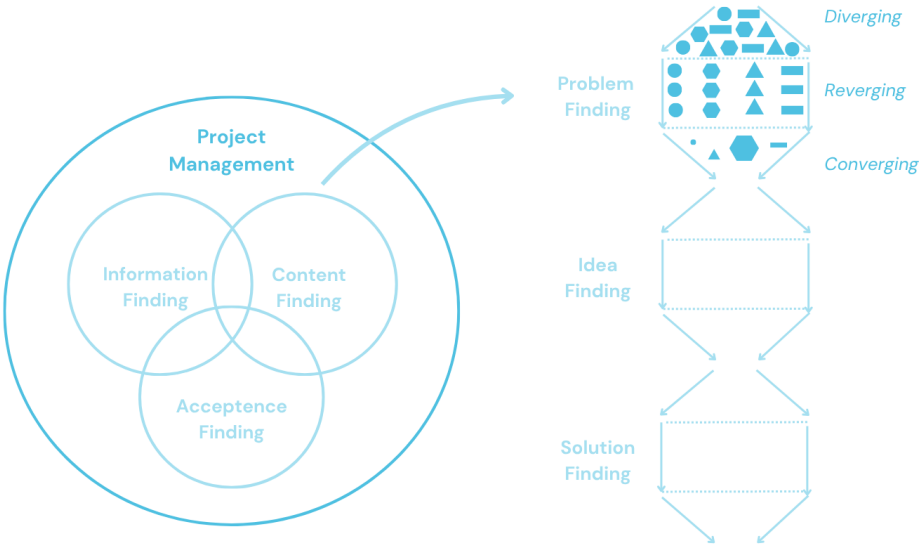

Figure 3.3: Overview of the Integrated Creative Problem Solving approach

Project management is seen as the basis, as part of the process is creating the right settings for the creative session to take place in. Next is information finding, which includes gaining a deeper understanding of the topic beforehand, in order to guide the session properly. Acceptance finding is important to ensure all stakeholders agree on what the problem is and which solution will work, it is essential for the co-creation process. The actual creative session is what content finding is about. It includes problem finding, idea finding and solution finding, which ensures the right problem statement is found, novel ideas are generated and eventually a usable solution is created.

The steps are divided into three streams of thinking, diverging, reverging and converging. During diverging as many ideas as possible are created. During this step group members are asked to postpone judgement, hitch-hike on the ideas of others, to write as much as possible as quantity breeds quality and to let the mind wander freely. During reverging people are asked to be jointly active, listen to each other and move iteratively, as it is okay to change things later. Lastly, during converging people should try to protect original ideas, trust their gut response and have action in mind, namely the problem being addressed.

3.2.4 Expert validation session with change management

As a final step to validate the findings and as input for the practical implications, an expert validation session with the change manager and CISO from IECC was held. During this session the findings were discussed, both from the internal interviews and external interviews where applicable, as well as from the brainstorming sessions, after which participants were asked to discuss the feasibility of the advice given and to give any other commentary they might have.

The session started with an introduction to the building blocks of the training, based on the factors found in literature. Then each building block was discussed, guided by PowerPoint slides summarising the findings and advice. Participants were sent the protocol in advance to read through, to save time during the actual session. The full protocol can be found in appendix 10.4. This session addressed all factors of the framework and is also structured along those factors of the framework.

3.2.5 Literature review

To ground the findings and advice in literature, a literature review was done. Platforms such as Google Scholar, Scopus and the TU Delft library were used to find research papers. Search terms included 'relation security awareness training and secure behaviour', '"security awareness training" AND (generic OR "off-the-shelf" OR "vendor")', 'co-design in security training', 'long term effects of security awareness training' and 'review of cyber security training methods'. Some papers were also found through snowballing from key references.

3.3 Data analysis

3.3.1 Coding for interviews

The analysis method used for the interviews was a middle ground approach to coding. Some codes were created beforehand with the measures and research questions in mind, while others emerged during coding. Coding was performed on the interview transcripts using ATLAS.ti. Two separate codebooks were made, one for the interviews with participants from IECC and one for the external interviews. For the interviews held with people from IECC, the codes created an overview of primary tasks, needs, routines, feedback on current training and preferences for training methods. The codebook created from the interviews held with people from different companies, provided an overview of different security practices in use, how those fit with user needs, how they are developed, what is in the training, why companies do the training and how they gather employee input.

The codebooks were roughly made through three different rounds of coding, starting with open coding to create a long list of codes. Next axial coding was done to create code groups and merge many codes, after which selective coding was done to create themes and delete any codes which were not deemed relevant. This was however a very iterative approach, so each of the rounds were done multiple times. As the codebook for the interviews within IECC had become extensive, the codes were divided per sub-question. The codebook for the interviews outside of IECC was for only three interviews and had remained smaller as it was only meant to help answer SQ2 and SQ3. The full codebook for the interviews within IECC can be found in appendix 10.5 and the codebook for the external interviews can be found in appendix 10.6.

3.3.2 Thematic analysis for brainstorming sessions

A thematic analysis of the brainstorming sessions was conducted, partly done in collaboration with the participants. During the brainstorming session the technique brainwriting was used, which involves writing out the ideas on sticky notes. Another technique was clustering, which is used to sort the ideas into different categories. These categories are sometimes given a name as well to clarify the grouping further. This was done for all of the sticky notes, leading to themes. The clustering was done by having participants move the sticky notes or at times the facilitator moved sticky notes. Placing the notes was an iterative process and the placement of each note was discussed until a consensus was reached. Participants were asked if they agreed with the placement of the notes, and if not where they would like to place them instead. Sticky notes that were given a new placement were the ones going into more detail

on primary work tasks for the BULE session. These were first placed along the notes that were considered the main work tasks, but were later placed in a category of their own called 'communication methods'.

The whiteboards were digitalised and can be found in appendix 10.7, which includes what the whiteboards looked like before the session and after the session. Before the start of the brainstorming sessions the whiteboards were already prepared with some sticky notes with findings from the interviews. Participants all agreed with the notes already on there, usually adding more notes similar to it and thus validating what was already there. They also added completely new ideas which then formed their own categories during clustering.

3.3.3 Framework analysis for expert validation session

The expert validation session was used to gain insights into feasibility and to validate the findings gained from the interviews and the brainstorming sessions. These findings were mapped to the factors of the framework developed in chapter 2, which can be seen in appendix 10.8. For this the codes from both the internal and external interviews were merged into the same ATLAS.ti project and were connected using the network builder to the different factors. From this analysis, different prerequisites and building blocks were created. Prerequisites are things that have to be addressed outside of training, while building blocks are things that can be addressed with training.

The advice or comments gained through the session were directly mapped to those training blocks and prerequisites and the feasibility of implementing them was discussed. During the session a transcript was generated through Teams, from which notes were made. These notes were mapped to each building block, which can also be seen in appendix 10.8.

4

Primary tasks shaping routines and needs

This chapter presents the results gathered to answer SQ1: **"How do employees' primary work tasks shape their routines and information and skill needs?"**. The results were gathered through interviews with participants from three departments and brainstorming sessions. As such, the results are presented in three different sections, with section 4.1 discussing the finance department, section 4.2 discussing BULE and section 4.3 discussing FLC. For each department the primary tasks and accompanying digital secondary tasks are explained first. Then the security needs connected to them are presented and finally the routines as shaped by their primary tasks are described. Section 4.4 discusses the similarities found between the departments and finally section 4.5 provides a summary of the chapter. This chapter discusses the self-efficacy and routine factors of the framework, specifically their connection to the primary work tasks of employees.

4.1 Primary tasks, needs and routines finance

4.1.1 Primary and secondary tasks finance

Through interviews and a brainstorming session with people working in the finance department, the primary tasks were found. These tasks were found to be doing financial checks and handling invoices. These correspond to the tasks as identified in the codebook, which can be seen in table 10.1.

In order to do the financial checks properly, participants noted they have to get access to the right financial files and hours that have been worked on the project, which are all displayed in various dashboards and applications. These files contain sensitive financial information that is stored on the laptops of employees or in shared environments. They also mentioned having many meetings with colleagues in order to explain the story behind the numbers and that most of their communication is internal.

> *"I also speak with team managers, but also the country directors, and to get everyone on board with the story, also behind the numbers, you know?"*
>
> — Interviewee F3

During the brainstorming session, participants noted that secondary tasks that accompany handling invoices include creating invoices, checking the hours worked on a project, sending the invoices to clients, and dealing with a high volume of internal and external emails. Received invoices also have to be booked properly and paid.

> *"Well, the majority is just that I make invoices. That's what I'm mostly busy with."*
>
> — Interviewee F1

4.1.2 Security needs finance

The security needs were identified from both the interviews, as seen in the codebook, and from the brainstorming session. As finance employees have to handle invoices and do the financial control, they are dealing with a lot of financial data, which is sensitive data. As such participants noted they feel the need to protect their laptop against threats. Both in the interviews and in the brainstorm session it came up that this included aspects such as being able to deal with tailgaters and knowing how to make and manage strong passwords.

All participants noted that they have to communicate with people, mostly internally, and share files with them. When sharing these files they also expressed a need to know which files are allowed to be shared and which are not. They want to be able to help people do their work, but also have to comply with privacy laws and regulations. Finding the right balance there is important. This came up during the interviews and was again stressed during the brainstorming sessions. Participants also noted they still wanted to be able, and be allowed, to trust colleagues.

> *"You are then still too easily inclined to share things. But I think, yes, people just need to move on [with work] right, so to what extent do you share things or not?"*
> — Interviewee F3

Another need comes from the multiple different programs being used to collect and store data. Participants wanted to know how to manage their files properly, in terms of storing them in the right places. One participant in particular had a combined wish of safety and efficiency for managing files.

> *"That balance between File Explorer and having everything in SharePoint or in the cloud, how do I manage that most optimally. For me, there would definitely be a win-win in that."*
> — Interviewee F2

Lastly, due to the large number of emails they receive participants also wanted to be able to spot phishing. A related need to this was being able to judge if an email was legitimate or not, and otherwise knowing which steps can be taken to determine the legitimacy. An invoice might be legitimate, but it could also be phishing. The email cannot be ignored, as if it is an actual invoice it needs to be paid. Especially during the brainstorm it was discussed how participants need to know the different steps that come with deciding whether an email is legitimate or whether it is phishing.

4.1.3 Routines finance

The primary tasks and accompanying digital tasks shape the routines and work environment of finance employees in multiple ways. These routines and work environment can be seen under the theme of 'work context' in the codebook. While at times participants said they preferred reading things from paper, they mainly work digitally in applications such as Excel, Outlook and Teams. They also have more specialised applications, such as Maconomy, which hold financial data.

> *"We have Maconomy, that is [...] our financial tool."*
> — Interviewee F3

Participants noted they receive and send a lot of emails on a daily basis, on busy days this is usually around sixty emails. Even though they receive many emails, they very rarely get actual phishing emails. They did note that they thought finance is an attractive target for criminals.

In terms of work environment, participants mostly worked hybrid, with some days working at the office and some days working from home. When at the office they work in a separate wing for which special access is needed.

4.2 Primary tasks, needs and routines BULE

4.2.1 Primary and secondary tasks BULE

Interviews with four people working in the BULE department were conducted, after which a brainstorming session was held. Participants held roles such as project manager and designer. From these roles the primary tasks were found to be managing projects and designing and modelling, as can be seen in the codebook.

Both during the interviews and during the brainstorming session participants noted that managing projects included preparing them by making financial quotes, managing colleagues and most of all a lot of file sharing, communicating and meeting with both internal and external people.

> *"My work basically consists of nothing but meetings, emailing and calling."*
> — Interviewee B3

Tasks that accompany designing and modelling were found to be working with applications to create the designs, storing those in shared environments and sharing those with external people. These are large files that have to be shared, which is done both by emailing links and setting up shared environments. These findings mainly came from the interviews.

4.2.2 Security needs BULE

Project managers said they have sensitive documents on their laptops, which includes framework agreements. As such they need to protect their laptops against threats. During the brainstorm participants noted that for them this includes things like knowing to lock the screen, being extra careful when working at a client office and being able to create strong passwords.

As designers are making 3D designs for clients, they have to manage many large documents in internal and external environments, which has to be done securely. Project managers also have to manage many files in both local and external environments as well as share them with people. For both it is important to share the right files and understand how to do so securely, as found both from the interviews and the brainstorming session. Multiple participants said there is also variation in what the shared environment looks like, meaning they have different environments they need to know how to work securely in.

> *"Maybe we can do something with that, also with sending documents? Yes, I am not much of an expert in it, I have to be honest about that, I like to be informed by my somewhat more digitally mature colleagues."*
> — Interviewee B3

Lastly, all participants from BULE noted that they have a lot of email communication, either to discuss things or for sharing documents. Designers noted that they usually send emails with attachments and links for larger files. These can be from many different applications or platforms, as different ways of working are currently used. One participant summed it up:

> *"Yes, links to SharePoint environments. Sometimes it goes to an intranet, to a WeTransfer. Sometimes it is a OneDrive link. Sometimes it is a SharePoint link, sometimes it is an Autodesk Forma link. They are all from different providers."*
> — Interviewee B2

As such they found it important to know how to handle phishing, both in terms of spotting it and reporting it.

4.2.3 Routines BULE

The routines and work environment for the employees from BULE were also shaped by the primary tasks and digital tasks, the codes for which can be seen under the 'work context' theme. Where the work used

to be on paper, that has all shifted to being digital. Designs are made digitally in CAD applications and communications are done mostly through Outlook and Teams. As they often have to communicate with clients, they get quite a lot of emails, one participant noting he got hundreds a week. All participants did say they very rarely got actual phishing emails, but that it was difficult to spot as they often had to click on links or open files from external emails for their daily work. As everything is now digital, they did think there would be large consequences from a hack, as without a laptop they could not do any work.

> *"we assume that everything works. But if it does happen once that we get hacked or something, you can, yes then, I also cannot do anything without my laptop."*
> — Interviewee B3

Their work environment is also shaped by their tasks, as participants said they work at the office, at home or at the client. For their primary work tasks, they must work together which was usually done in the office or at the client, or focus on creating designs which was done at home.

4.3 Primary tasks, needs and routines FLC

4.3.1 Primary and secondary tasks FLC

As mentioned before, due to people working in the field, only interviews were held and no brainstorming session was done with this group. The primary tasks and needs were clearly found and applicable to all four participants. Their main tasks were found to be doing measurements out in the field and storing the data from these measurements digitally, as seen in the codebook.

For the measurements in the field, participants noted multiple things must be done. The measurements have to be done at the client, which sometimes includes installing measuring equipment to be there for longer periods of time.

> *"The main task of my position is to go to clients to perform emission measurements there."*
> — Interviewee FLC4

Related to this task, they have to record the measurements digitally. Participants said they store this locally first, as they do not always have a network connection out in the field. The transfer of data is done through physical means, such as an SD card, or through methods such as Bluetooth. Once the measurement is completed, the data is put on a shared data disk.

> *"We do have to do a lot with data transfer, we have to get the data that is collected on the equipment onto the laptop. We often do that either with cables, or with Bluetooth, or with SD cards."*
> — FLC1

As the data is stored locally and they have access to the shared data disks, participants also said they feel they have sensitive data on their laptop:

> *"There is also data on it from other clients and that is in principle simply sensitive data, if a client, say, has a very high exceedance of a certain substance for example."*
> — Interviewee FLC4

4.3.2 Security needs FLC

As the fieldworkers are storing measurement data on their laptops and have access to data of multiple clients, they feel the need to protect their laptops. Participants noted this as the biggest security risk they encounter, as they are mostly out in the field and not in a trusted office environment, they have to be extra careful to protect their laptops against physical threats. They mainly spoke of needing to lock their laptops, as clients might take a peek at the data.

*"Someone thinks, oh, I am curious, and looks at my laptop and goes to my data folder and thinks, oh, what has *** actually emitted most recently?"*

— Interviewee FLC4

Another part of storing the data is managing the documents well to ensure accurate information is sent to the labs. This includes putting it in the right folders in the shared data disk and bringing the physical samples back to the lab.

Participants also noted they make little use of Outlook, as they rarely send or receive emails. They understood phishing that can still be sent to them, but they felt the heavy focus of training on the topic did not match their actual risk exposure.

"But I do not really have email contact otherwise, but that is also because I do not really [...] work with external people."

— Interviewee FLC3

4.3.3 Routines FLC

The primary tasks and the relative absence of digital tasks shape the routines and work environment for employees from FLC in multiple ways. These can be seen under 'work context' again, and specifically under 'field work laptop use'. As they have to take measurements, they mostly work out in the field. Some participants did work at the office at times, as they had to do preparatory work. As such, their work environment is not a typical office environment, meaning they use weather-resistant laptops, have to connect to the internet through a SIM card and might be working in very loud environments.

Another way their tasks influence their routines can be seen in the applications they use. As they mainly do measurements, transfer the data to their laptops and upload it to a shared data drive, they rarely make use of Teams or Outlook. Participants said they check their email as little as a couple of times a month, as they receive only a couple of emails a week. They also reported seeing very few or no actual phishing emails.

4.4 Similarities between departments

Not only were differences found between the departments, similarities were also identified. More similarities were found between the two office based teams, but some were also found between all three departments.

4.4.1 Similarities in needs

Across all three departments participants expressed the need to secure their laptop, which included practices like locking their laptop or using passwords to log in to accounts. Regardless of job or work environment, participants felt they had sensitive data on their laptop that needed protecting. This was also seen with participants feeling they needed to manage their files securely.

Aside from the universal needs, the office based departments, finance and BULE, shared additional needs. As they both often have to share files with colleagues and external parties, both expressed the need to know which files can be shared and how it can be done securely. Both departments also felt the need to be able to spot and handle phishing emails well, as they received a high volume of emails daily.

4.4.2 Similarities in routines

A similarity found across all three departments was that participants used a laptop to do their work, as all of the work has gone from analogue to digital.

The two office based departments again have more similarities together compared to FLC. Participants from both groups work in office environments only accessible with an entrance tag and where they are surrounded by trusted colleagues. They also both receive a high volume of emails daily and rely on applications such as Teams or Outlook for daily communication.

While BULE and FLC differ in many aspects, one aspect they share is that both regularly work at client sites, meaning they often do not know everyone who walks around. Participants also noted that they often connect to the internet through a SIM-card rather than a Wi-Fi connection.

4.5 Summary paragraph

A summary of the findings can be found in table 4.1.

Table 4.1: Summary of primary tasks, secondary tasks, security needs and routines per department

Primary task	Secondary tasks	Security needs	Routines
Finance: Financial check Handling invoices	Storing sensitive documents on laptop Using multiple communication systems Sharing files internally Managing files in local and shared environments Getting data from multiple applications	Securing laptop against (physical) threats Handling phishing Sharing files securely Knowing which files can be shared Handling files securely	Work in the office or at home Use Outlook and Teams a lot Rarely see actual phishing Use specialized financial applications
BULE: Project management Designing and modelling	Storing sensitive documents on laptop Using communication systems Sharing files internally and externally Managing files in local and external environments	Securing laptop against (physical) threats Handling phishing Sharing files securely Handling files securely	Work in the office, at home or at client Use Outlook and Teams a lot Use CAD applications Rarely see actual phishing
FLC: Measurements in the field Saving data from measurements	Managing files in local and shared environments Storing sensitive documents on laptop	Handling files securely Securing laptop against (physical) threats	Work mostly outside (not typical office environment), but sometimes in the office Use Outlook and Teams very little Rarely see actual phishing
		All: Secure laptop (ex. lock and password) and handling files securely **Finance&BULE:** Sharing files securely and handling phishing	**All:** Work digitally **Finance&BULE:** Trusted office environment, many mails and Teams and Outlook used **BULE&FLC:** Work at client and use SIM-card internet

5

Current training alignment with routines and needs

This chapter presents the results gathered to answer SQ2: **"To what extent does current security awareness training align with these routines and needs?"**. These results came from the interviews with the three departments and the brainstorming sessions. The current training was analysed to see how well it aligned with the needs and routines identified in chapter 4. Section 5.1 describes the training at IECC, after which the results are structured per department, with section 5.2 for finance, section 5.3 for BULE and section 5.4 for FLC. Each section first looks at the alignment with needs and then at the alignment with routines. The chapter ends with section 5.5, which summarises the chapter. This chapter also connects to the self-efficacy and routine factors of the framework, in addition to touching upon the time, effort and concordance factors. A deeper discussion of all factors can be seen in chapter 6.

A general remark to be made, was that across all departments participants noted that it was important to behave securely, as the consequences of an incident could be great. Many attributed that to growing news coverage on the topic. Most also said, although some did so somewhat begrudgingly, that training was important to do because of this and that it did help with their general awareness. As can be read below, this did not always mean that it also aligned with more specific needs people had.

5.1 Description of training at IECC

To better understand the responses of participants when asked about the current training, the bronze level of the training was reviewed. Only this level was reviewed, as all participants were still on this level. The bronze level consisted of eleven lessons and two tests, starting with why security awareness is important. The next lesson tests the learner's current level of security awareness, but regardless of the outcome you must do all remaining lessons. The following lessons contain topics such as social engineering, how security risks are also present at home and about online privacy. An interesting thing to note here was that some advice was given in these lessons, such as using strong passwords, yet the lesson on making strong passwords is lesson 9. As there are three weeks between each lesson, that means employees have to work at IECC for about six months before they are taught how to make a strong password. Other lessons include how to deal with AI generated content, how to deal with phishing and general security terms. A lot of the advice is not actionable, however, and at times it even states that this is how they recommend doing things, but to always adhere to company policy. A final thing to note is how the questions are phrased. At times it makes it incredibly clear what the right answer is, making it almost irrelevant what the actual content is.

An advantage of using the platform is that it has dashboards in which you can see when emails were sent to whom and whether they clicked on anything. This was used to check findings from the interviews as people noted how many phishing simulation emails they felt they had received. Every participant had received roughly the same amount of phishing emails, as that was set to every two weeks by a company wide policy.

5.2 Alignment with security needs and routines finance

5.2.1 Alignment security needs finance

For the finance department, multiple needs were identified. The first was to protect their laptop against threats, digitally or physically, to protect sensitive data on the laptop. During the brainstorm session participants noted having learned things such as locking your laptop or the clean desk policy, meaning not to leave financial documents open on their desk. They also noted however they felt they should be able to trust colleagues and did not always remove all paper documents when walking away from their desk. Something that came up during the interviews however was the gap people experienced between knowing and doing. They knew that they should talk to people who tailgate them into the building, especially as the finance department has an extra locked entrance, but doing so in practice was not something they felt confident in.

> *"It is actually a bit like a fire drill. You know what to do, but what if the alarm actually goes off?"*
> — Interviewee F1

Another part of keeping your laptop safe was found to be using strong passwords and managing those securely. Multiple participants found it difficult to remember the many different passwords by heart, but were afraid of using a password manager. They were afraid they would no longer remember the passwords themselves and if the technology failed them, they would not be able to log in any more. As such they decided to write the passwords down on paper or in a Word file, as those felt more reliable. Training had not helped them understand a password manager well enough to use it.

> *"there are perhaps many more tools and means to manage those passwords much more easily and yes, to store and remember them, so to speak. Only, there is also immediately the danger in that [...] every time it goes automatically and then all of a sudden that automatic, that falls away and then it is [...], what was that password again?"*
> — Interviewee F2

Another need that came up was associated with sharing files. As they mostly share files internally, they found it difficult at times to know which files can and cannot be shared with colleagues. This came up during the interviews and was again validated during the brainstorming session. They had received training in the past to know how to comply with privacy regulations and laws, but were uncertain now which files could and could not be shared. This also came from a conflict of wanting to help colleagues do their work, not having the time to ask everyone which exact information they needed and being unsure what even was allowed.

> *"Yes, and also with documents that we distribute internally with certain data. Yes, I also find that difficult sometimes, because everyone, yes, they have it then, right? The person you send it to, they do need it too, right?"*
> — Interviewee F3

Being able to manage files securely and efficiently was a need that seemed to not be met, but it was a need that could not entirely be met by training regardless. For the finance department, files have to be collected from many different sources and dashboards with reports are found in multiple applications. During the

brainstorm session this was noted as something that simply had to be done, but they felt they knew how to handle it well enough. The need to be able to handle the different applications better was however brought up in the interviews by one participant.

The final need that was found for participants working in the finance department, was the need to handle phishing, as they receive up to 60 emails on a busy day. Part of that was addressed by current training, as participants noted during the interviews that they felt they could spot a phishing email due to the e-learnings and the simulation phishing emails. In the brainstorming session it did however come up that they felt they did not know how to fully handle phishing, particularly for emails that might be legitimate and for which they could not discern themselves if it was fake or not. They felt some advice or guidelines were missing on what to do in such situations.

5.2.2 Alignment routines finance

For the finance department, their work takes place in a stable and indoor working environment. They often work on their laptop in a relatively quiet office or at home, both environments that offer a reliable Wi-Fi connection and a desk to sit at. Participants found that e-learnings align well with this, as they could sit down and focus somewhere to do the training.

Another aspect as to why participants liked the e-learnings was that it worked well with the high work pressure that they experience. They find they have little time for other things. The e-learnings are delivered in short and easy to understand training blocks, which participants felt they could fit into small gaps in their schedule without disrupting their workflow too much. When asked during the brainstorming session if they would prefer many small blocks of training over the year or only a couple larger blocks, they preferred the current way it was done stating that reason.

> *"I find it, like now, I find it fine just once in a while something short, so to speak, that does not take too long."*
>
> — Interviewee F1

The second training method used by IECC is the phishing simulation emails. These also aligned with their daily routines, as participants from finance spend a considerable amount of time in Outlook for their day to day work.

> *"So phishing emails and trainings like that. Yes, I think that it is fine. Only at some point you know it and that you should get a check once in a while I think that is also only good."*
>
> — Interviewee F2

5.3 Alignment with security needs and routines BULE

5.3.1 Alignment security needs BULE

Participants from BULE also noted that their laptops contain sensitive documents and that they therefore wanted to protect them against threats. Another aspect is that they sometimes work at the office of a client, where they must be extra careful. One aspect of protecting the laptop was by having strong passwords and managing them well, but here participants also noted that they did not know how to use a password manager. Another aspect is while they did all know they had to lock their screens, one participant said they do not always lock it, as it takes too much time and effort. People were not aware that facial recognition is an option if they did not want to use a PIN code, which is thus somewhere that training was found to be lacking.

"I do not do it every time, I have to be honest. [...] having to enter your code to start up again. And now every time I lock it Outlook is somewhat slower when I have opened it again."
— Interviewee B3

Another aspect that was brought up in the brainstorm session was that people can look at your screen, for example when you are on the train or working at a client, for which a privacy screen might be a good option. They also said that they felt a lot of people did not know this was an option.

A different need was being able to share files securely. As they have to share project files or designs with clients, they need to be able to do this safely. While three people all specifically said they knew they could no longer use WeTransfer, none of them knew which way of file sharing should then be used. They also did not know what to do if a client still used WeTransfer. They instead noted that many different ways of sharing files are being used. So this need was not currently addressed by training.

"WeTransfer I know for example, that is completely blocked from within IECC, so you cannot use it. [...] but yes, it can well be that you receive something from a client via WeTransfer. Yes, then you cannot even download it, [...] in any case that clarity is lacking a little."
— Interviewee B2

Another need from BULE was to be able to manage files securely, mostly in a project setting. They felt that some clear guidelines were missing on this, as the set-up of the environment is now mainly dependent on how the project lead wishes it to be. The training is thus either not communicating the guidelines for this at all, or at least not clearly. As one participant noted:

"Setting up a shared environment like that is, I think, somewhat dependent on the project leader or project manager. How they prefer to do it, but there is no real clear guideline on it [...]. I think at least, that is what I often see in practice."
— Interviewee B1

The final need found from participants in BULE is to be able to handle phishing. They felt they could spot phishing, but that it also should not be underestimated how good phishing can be.

"but how sophisticated they are nowadays, you really have to look carefully whether it is real or not."
— Interviewee B3

During the brainstorm people especially noted that spear phishing, such as with personal information or from a client that you are working for, would be difficult to spot. They felt that you are much more likely to click if the phish looks similar to emails you were expecting. This was something they felt was currently still missing from the training.

"If it is something you were already expecting an email about and coincidentally a spam email is sent about exactly that, yes, then you are easily fooled."
— Interviewee B2

5.3.2 Alignment routines BULE

The work environment of participants from BULE is more varied, as participants said they worked either at home, at the office or at a client. In a three week timespan, which is the timespan in which employees are expected to plan the training, they were usually able to find a suitable time to do the training. Doing the e-learning in an office environment in that sense matched the idea that they are nice to do in a quiet environment with a stable internet connection and a desk to sit at. One participant also noted that they think

the online and digital training matches the subject matter itself, as security awareness is largely tied to working behind a computer and working with digital systems.

> *"I think the online environment is also fine, also fitting under the topic it concerns, right? Because it of course takes place behind the computer [...] Only as far as I am concerned it could use a bit more attention, so a bit less in passing, but that we really take a moment to pause and reflect on it."*
> — Interviewee B4

While participants did express they found the e-learnings easy to plan and fit with their routine in that sense, they did not find them particularly engaging in their current form. The same participant who noted the fit between method and content, also mentioned that the training was often done with little attention paid to it, expressing a wish to slow down and be able to reflect more on the content. This sentiment was also broadly discussed during the brainstorm session, where most of the discussion and ideas were focussed on how to make the training more engaging by improving concordance. The results of that are discussed further in section 6.2.1.

Similar to the finance department, the phishing simulation emails aligned well with the existing routines of BULE employees. As Outlook is already used for their daily communication with both internal colleagues and external clients, the simulated phishing emails reached participants in an environment they were already active in. This meant the method fitted smoothly into a routine that was already in place.

5.4 Alignment with security needs and routines FLC

5.4.1 Alignment security needs FLC

For the participants from FLC two main security needs were found. The main need that everyone pointed out was the fact that they have sensitive files on their laptops, which they need to protect. The main risks they saw with that were that they mostly work out in the field, not in a protected office environment. They do not know everyone who walks around and people could look at their screens. The main way of protecting the laptop was by locking the screen and not leaving it behind unattended for long. They noted that this was addressed in the training, but people do sometimes forget, so being reminded is important.

> *"we of course use our laptops a lot outside and I think that is also a risk they run into, that you for example forget to lock a laptop while you are at a client's site. Then they start looking at your screen to check something at the measurements."*
> — Interviewee FLC1

One participant said if the measurement would take multiple days, they would not leave their laptop behind in the mobile measurement station, but take it home with them.

> *"if you are working on a job for multiple days, you leave your measurement setup in place, but I always take my laptop with me. I do not leave it unattended at a client's site, so to speak, because there is also data on it from other clients."*
> — Interviewee FLC4

Another thing they noted was that they have to manage a lot of sensitive files, though mainly in internal systems. They did already know how to do this, as it was part of their way of working from the start.

A final thing to note here is a focus of the training for a need that participants from FLC did not have. They rarely send or receive emails, with most saying they only receive a couple a week, yet a large part of the training has a focus on phishing and simulating phishing. Though some did note that perhaps because you are using Outlook so little, you might be even less alert for phishing.

"Yes if there is a real one in there once, it can easily happen that they still click on it. If you have something like oh, a month ago I received something. Yes like that, they look at their email so infrequently that they do not all pay equal attention to it."

— Interviewee FLC1

This general feeling of training not aligning with their work was shared by multiple participants, as they did not feel they were learning a lot from the trainings and might prefer more concrete advice instead of general knowledge.

"they make those trainings so extensive, while the core is actually just the same. And then I think yes, [...] why do we have to do so many of those trainings?"

— Interviewee FLC2

5.4.2 Alignment routines FLC

The work environment for the participants from FLC stands in clear contrast to those of finance and BULE. While some of the participants spent part of their week in the office, most people in the department work in the field five days a week. This means they usually work in loud environments and participants noted to often have an unstable internet connection. Not working in a typical office environment also means they are not always at a desk or working on their laptops. An e-learning, which assumes a quiet work environment behind a desk with internet connection, does not fit well in the environment of FLC employees.

Another mismatch found was in the phishing simulations. Participants reported to rarely use Outlook, meaning that phishing simulations are not the best way to reach them. Multiple participants also felt they were being sent phishing simulations multiple times a week, even though after checking the platform it was seen they were being sent every two weeks, the same frequency as other departments.

Another aspect of e-learnings not fitting with their needs, was the difference in educational background of the fieldworkers and office workers. While those working in the office usually had a higher theoretical educational background, those working in the field usually had more practically oriented educational backgrounds. Their way of learning things had always been by doing things, not by self-study. Having to plan the e-learnings themselves was not always seen as a positive thing, in contrast to other departments.

"In fieldwork you also have some variation in the education level of people. Then you have people who [...] are more highly educated, but also people who have done an MBO education as environmental officer or something and then you are again heading towards a different kind of people who, well, are not really waiting for it and have something like well, I don't know, I just won't make it."

— Interviewee FLC4

Lastly, while all participants expressed that a high work pressure meant that security training was not always seen as a priority, participants from FLC described how small blocks to plan did not fit within their daily work routine. They often drove to the client early in the morning, spent all day doing measurements out in the field, had to fill in data on their laptops and drive back to the office to deliver the samples to the lab. This left them with no clear gaps to plan the training as was expected of them, leaving them feeling it would have to be done in their own time.

5.5 Summary paragraph

Table 5.1 shows a summary of the chapter.

Table 5.1: Summary of needs, routines and training alignment per department

Department	Needs (N) / Routines (R)	Training alignment
Finance	*N:* Securing laptop against (physical) threats	*Does:* locking laptop, clean desk policy, strong passwords *Does not:* how to deal with tailgating and set up password manager
	N: Handling phishing	*Does:* spot and report phishing *Does not:* what to do when unsure if legitimate or not
	N: Sharing files securely	*Does:* how to share files *Does not:* which files are okay to share
	N: Knowing which files can be shared	*Does:* previously told *Does not:* unsure now
	N: Handling files securely	*Does:* — *Does not:* how to handle them efficiently and securely
	R: Working in office environment	E-learning nice to plan and to do
	R: Often using Outlook	Phishing simulation aligns with routine
BULE	*N:* Securing laptop against (physical) threats	*Does:* locking laptop, secure passwords *Does not:* facial recognition option, set up password manager, privacy screen widely known
	N: Handling phishing	*Does:* spot and report phishing *Does not:* handling tricky phishing, like spear phishing
	N: Sharing files securely	*Does:* do not use WeTransfer *Does not:* outline policy of which tool to use instead
	N: Handling files securely	*Does:* — *Does not:* clear guidelines on how shared environment should look
	R: Working in office and at client office	E-learning nice to plan and fits digital theme, but in current form not very engaging
	R: Often using Outlook	Phishing simulation aligns with routine
FLC	*N:* Handling files securely	*Does:* — *Does not:* —
	N: Securing laptop against (physical) threats	*Does:* locking laptop, do not share pin code with colleagues, not leaving laptop unattended for long *Does not:* —
	N NOT: Handling phishing	*Does:* focus on phishing *Does not:* —
	R: Working outside (and sometimes in office)	E-learning does not match an outside environment and difficult to plan in day
	R: Rarely using Outlook	Phishing simulation do not align with routine
	R: Practical learners	E-learning not working, self-study is not how they usually learn

6

Designing training to fit with routines and needs

This chapter presents the results gathered to answer SQ3: **"What concrete adjustments to security awareness training can address the identified misalignments based on input from employees and (external) experts?"**. The results were gathered through semi-structured interviews with employees from three departments within IECC, semi-structured interviews with security professionals from other companies, brainstorming sessions with employees and an expert validation session with the CISO and change manager of IECC. The results are structured according to the factors identified in the background research as addressable through security awareness training. As such, section 6.1 first discusses the factors of the simplicity and ability category, after which section 6.2 discusses the factors related to motivation. Section 6.3 shows a summary of the chapter. For convenience, an overview of the factors is shown below again in figure 6.1.

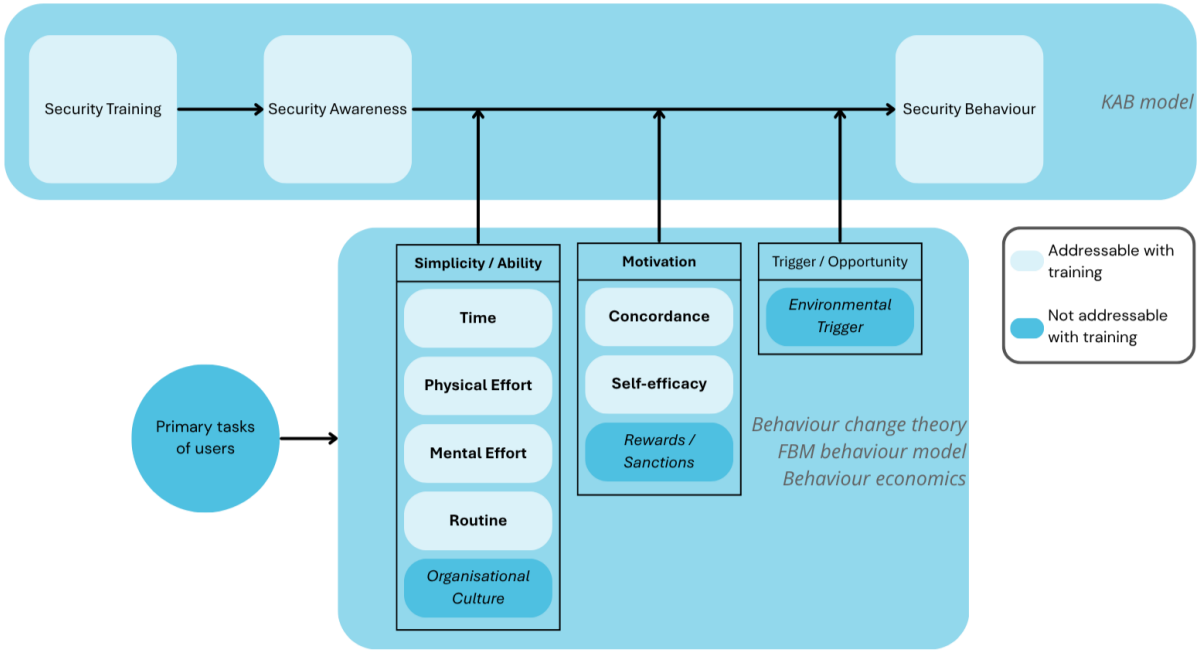

Figure 6.1: Overview of the factors influencing security awareness training effectiveness

The codes gained from the interviews were connected to these factors, as can be seen in appendix 10.8. From this analysis, combined with insights from the brainstorming session and literature, building blocks and prerequisites for each factor were formulated. These were then discussed with the CISO and change manager. A distinction was made between building blocks and prerequisites, as the blocks are something that training can do or address, while the prerequisites have to be taken care of with something other than training. Both of them start with a statement which is first grounded in literature, followed by the findings from the interviews and brainstorming sessions, after which the comments from the expert validation session are presented to reflect on feasibility and what has already been tried within IECC.

The order in which the factors are discussed is intentional, as each factor can act as a blocker for the ones that follow. It makes little sense to motivate people to perform a behaviour that is not yet feasible for them to do, so the factors related to simplicity and ability are addressed first. Only once the behaviour is doable is it productive to focus on motivation. While factors such as time given to spend on security, culture, rewards and sanctions and environmental triggers are not directly addressable through training, time and culture are discussed here as they were very explicitly mentioned in the session with change management.

Something that is already interesting to note is the motivation for companies to even do training. Multiple reasons were given, such as improving awareness and improving behaviour, but the main reason was that they wanted to keep or obtain an ISO certification. To have training that complies with these standards, most companies made use of vendors to get their training, as within resource and time constraints it was not possible to create the training themselves.

6.1 Simplicity and ability

This section starts with a prerequisite, namely to make the policies easier to follow and reduce friction. Then two building blocks are discussed, one on the frequency of training and one on how to make training better fit with people's routines. It closes with a prerequisite on company culture influencing secure behaviour.

6.1.1 Time and effort

Prerequisite: *Review policies on feasibility, try to reduce friction to stay within compliance budget*

From literature research

As found in literature, companies often do not check their policies for feasibility [17]. Without ensuring the wanted behaviour is doable, people will find ways to circumvent them instead, refuse to comply at all or set up shadow security, which might still be insecure while they believe they are behaving securely [11, 17]. People make decisions within a bounded rationality, they have limited resources to spend and will not spend them on security if it means too great of a loss in productivity [6].

From internal interviews and brainstorming sessions

Through the interviews and brainstorming sessions an overarching problem was found, namely that many policies currently in place at IECC were found to be undoable by the participants. This mainly came from the policies being in the way of normal workflows, taking up too much time.
Something a participant from finance noted was that in order to do the financial checks of projects they had to get permission from many different people in order to access the documents needed. This was done so no one account has too many access rights at all times, but it meant a lot of additional time and effort on their part.

"But yes all those things that cost extra time and energy, because that is maybe, well we talk about time and about money, but it is particularly the factor of energy. You notice that immediately comes under pressure with people."

— Interviewee F2

Others from finance also noted that the current advice for how to deal with phishing does not always work well for their department. They get many emails a day, on a peak day they once received a hundred emails, and it is not realistic to call for each email they are unsure about. Another option they then wanted was to be able to ask a colleague for their opinion, but the advice was to not send potential phishing to others. This left them feeling stuck on what to do.

Some policies were also in conflict with each other, as shared by participants from FLC. They have to work on the same laptop sometimes, due to the application they must use. At the client they should lock their laptop whenever they leave, for example when taking a measurement, but they are also told not give their PIN code of their laptop to colleagues. They then had to decide which they think is less bad by themselves, and decided to share the PIN code.

Some policies were also found to be undoable due to conflicts of interest from different departments. During the brainstorm with BULE, people noted that the security advice is to not use public Wi-Fi and instead use their mobile data and create a hotspot. When people did this, they would get comments from finance however to use their mobile data less, as the data bill was getting too high. Some would instead use their private data plan, in order to avoid the reprimand from finance, but still comply with security policy. This then led to a different conflict in policies, however, as they are meant to keep work and private devices separate. This conflict also came up in the finance brainstorm, albeit in a different manner. Participants noted that they have to use Multi Factor Authentication, but this has to be done on their personal phone, as they did not have a work phone. So whereas IT asks employees to use their personal device for things, security wants employees to keep them separate.

All of this led to employees ignoring or working around the security policies they had found to be too time intensive to do, as many stated they already have a high work pressure to deal with and little time left for secure behaviour.

From external interviews

From the external interviews the advice given was to avoid overwhelming users, so as not to slow them down too much.

"So, if you, yeah, keep your employees up to date with everything and keep them sharp, but yeah, you don't want to slow [them] down with [...] everything about this."

— Interviewee E2

In order to review feasibility and get input from employees, the participants had set up multiple ways of receiving feedback. Some were more informal, such as being open for direct conversations and making that known to colleagues. Other ways of receiving feedback were through engagement on posts on the intranet, teams, WhatsApp or other communication channels. More formal feedback was also gathered through surveys and reporting of incidents. One participant noted that they were in the process of setting up tooling to deliver training, but also to create a feedback loop.

"So I hope [...] I can get the feedback loop started and understand what people are desperate for."

— Interviewee E1

From session with the change manager and CISO

From the session with the change manager and CISO, they said they recognised several of the problems that had come up. They also said that they had already tried to resolve the conflict between the security advice to use a mobile hotspot and the complaints from finance about the resulting data costs. They acknowledged that while this had been discussed previously, it had apparently not led to a lasting resolution, as participants were still encountering the same friction. The more specific policy conflict found for FLC, where employees had to choose between locking their laptop and sharing their pin code with a colleague, was acknowledged as a real issue, though it was noted that this was a kind of niche issue that might not get addressed immediately.

For future identification of high friction policies, a feedback loop was seen as a valuable addition by both the change manager and CISO, as it would make it easier to identify such policies without having to rely on a research project to find them. The idea of having a structural channel through which employees could flag such pain points was considered as a feasible thing to implement. During the session, it was suggested the existing safety reporting infrastructure could be repurposed for reporting security incidents. Security incidents could indicate policies not yet properly working.

One point the change manager made was that some of the behaviours found in this research, such as employees not locking their screens because it slows down their laptop, might have a deeper cause than it only costing time and effort. The suggestion was that for some employees there may be underlying reasons why certain secure behaviours are not adopted. Reviewing the feasibility of the policy might not solve those problems, for which other interventions might be needed.

Advice and fulfilment criteria

In literature it was found that companies often do not check for feasibility, but how can the check then be done and how can the feasibility of policies be checked? From the internal interviews and brainstorming sessions it could be seen that there were multiple ways policies could be seen as infeasible, for example by taking too much time, disrupting workflows, not working for specific departments or conflicting with advice from other departments. External interviewees had set up multiple ways of collecting feedback to find out such friction points. Synthesizing these observations, feedback loops in multiple communication channels, casting a wider net to different people, can help identify high friction policies.

Without regular communication with people, the issue might have been assumed to be resolved or it might be assumed that there is no issue, as was seen from the session with the change manager and CISO. People not reporting issues might also come from them simply not following the policies anymore, not knowing the policies exist or not knowing who to talk to about it. Drawing these findings together, only with proper feedback loops set up and without negative feedback can this prerequisite be considered fulfilled.

Building block: *Review the frequency of training and adjust if needed*

From literature research

From the literature it was found that more is not the answer, simply asking people to always do more training is not a realistic solution and it does not take into account the limited resources people have [6, 11].

It is also important to note however that it was found that repetition is needed. Without repetition, people forget the knowledge as quickly as within a month [30]. A single reminder was found to help people retain the information for at least three months [5], so a reminder within that time period can help keep the

knowledge fresh in mind for people.

From internal interviews and brainstorming sessions

Almost every participant that was asked about their opinion on the current training thought the frequency of the phishing simulations was too high. Some felt that they were being sent multiple of them a week, but checking the platform revealed that everyone had been sent more or less the same amount of emails. The single person who was fine with the frequency said they had no complaints as they had not received a single simulation email yet. After checking in the platform reporting dashboards, the participant had received a similar amount of simulation emails as everyone else, but had simply not noticed any of them. Some people did explicitly state that they liked this kind of training, just not the frequency.

> *"I do actually find it fun that they send those phishing emails. Only it is sometimes a bit much."*
> — Interviewee F1

Others were less enthusiastic about the simulations, seeing risks from doing them so often. They noted that they might become paranoid, not trusting any emails they come across. Another problem that had already happened to people was missing legitimate emails, as they no longer trusted any emails with links.

> *"other colleagues said, you have to be careful not to have an overkill of fake emails, because then you start to distrust everything."*
> — Interviewee B3

It is important not to exhaust the compliance budget of people, as people might get really fed up with training. One participant noted he had heard of people who had started clicking on the links in the simulation emails on purpose, as a way to protest.

> *"I already hear that people just deliberately click on those phishing emails. They deliberately just click because they get so tired of it. Yes, that is truly serious."*
> — Interviewee FLC2

All employees are also asked to follow an e-learning every three weeks, taking from 5 to 10 minutes to complete. Few people had complaints on this frequency, some did say they wait a couple of lessons and prefer to knock them out in one go. Multiple participants noted that simply by getting the reminder email to do the training and doing any kind of training, they were again reminded of security, which they found to raise their awareness as well.

From external interviews

The participants from the external companies all used much lower frequency training, especially for the phishing simulations. They did those simulations usually once or twice a year, where the main purpose of those simulations was to test people, not to use it as a form of training in itself.

One participant also mentioned they are planning to introduce e-learnings through a platform, in which they plan to introduce weekly challenges that take a couple minutes, in which employees have to answer questions until they have everything right. Every new employee also has to follow a one-time onboarding training on security awareness. They also mentioned having a security community meet-up every two months which is voluntary to join.

Another participant noted they like to use multiple training methods as it helps with repetition. Through repetition they felt people would understand the material better and remember it better as well.

> *" I think repetition gets everything done, so I do not favour one security awareness training "*
> — Interviewee E2

Multiple training sessions were also found to be needed as the threat landscape constantly changes, introducing new threats that people have to be aware of. Where a decade ago USB-sticks were seen as the biggest threat, it is currently phishing which is seen as the largest risk.

From session with the change manager and CISO
When the frequency of phishing simulations was discussed, the CISO and change manager understood how employees might become overwhelmed by the volume of simulation emails. They also recognised the risk of employees becoming distrusting of every email rather than improving their ability to spot phishing, which would be counterproductive to what they are trying to achieve.

One suggestion that was brought up was to improve the feedback given to employees after they report a simulation email. Currently, reporting a phishing email does not result in much informative feedback, it only opens a ticket with IT, which is automatically closed. By providing more meaningful feedback on how the email could have been identified as phishing, they thought it could become a learning moment.

A slight apprehension to lowering the frequency was also noted, as it may not be the only, or even the primary, problem. They said the reason employees are becoming fearful of their emails rather than more confident in handling phishing, could be that they do not yet feel equipped to handle phishing well. This aspect of the problem is discussed further in the self-efficacy section.

Advice and fulfilment criteria
Literature states that people have limited resources available, as such the frequency of training should not be too high. Do it too often and negative effects might occur, such as distrust, people refusing to do the training or people protesting in other ways as noted by internal participants. Literature also states that the frequency should not be too low, as people often forget information over time. With the changing threat landscape, new training is likely needed over the years, as noted by external interviewees.

A reminder was found to be effective for at least three months in research and adapting training quicker than that to the changing landscape was found close to impossible to do within resource constraints by external participants. Combining these insights, the frequency should be as low as possible, while still getting the needed information across to users. This should remain lower than what people are okay with, to stay within their resource constraints.

6.1.2 Routine

Building block: *Have different options of training methods to fit with people's routines*
From literature research

From literature it was found that adults learn differently than children, they have their own experiences and preferences in which they like to learn things [28]. This means that a single training method is unlikely to work equally well for everyone, offering multiple ways of engaging with the content is more likely to reach a broader group of employees. It is again important to note that more is not the answer, simply giving more training without removing anything risks further exceeding the compliance budget of employees.

From internal interviews and brainstorming sessions
From the interviews it was already clear that people preferred different training methods, which stemmed both from a need to fit their work routine better and because they had different ways they liked to learn. Participants from finance liked the plannability of e-learnings, while people from FLC prefer live sessions as

that fits their schedule better. One participant noted, which was validated by people during the brainstorming sessions, that they would like to be able to choose which method they wanted to do.

> *"that you can sign yourself up for something, so to speak [...] and then everyone can choose for themselves."*
> — Interviewee FLC2

From external interviews
Participants from the external interviews said they also prefer to use multiple different training methods or ways to reach people, as people have different learning styles which they want to accommodate. They did note that it is not realistic to accommodate everyone perfectly, but that they could try at least.

> *"That's because people are different, right? So nobody reacts same to everything. People learn differently too. Some people enjoy reading books. Other people want to have their hands, get their hands dirty. [...] We of course have to pick our battles because we can't do everything [...] We can get as close to it as possible. "*
> — Interviewee E3

Many different ways of training people or getting information across were mentioned across participants. From posters with the 10 golden rules on the wall, to intranet posts and having c-level give announcements. They also made use of onboarding training, e-learnings, phishing simulations and giving presentations to specific departments.

From session with the change manager and CISO
The change manager and the CISO agreed that accommodating different learning preferences and routines would likely improve how well employees engage with and retain the training content. They had actually already attempted to plan security sessions with employees from FLC, but finding the time to actually organise and hold these sessions had proven to be difficult. Part of this was also because they had been trying to expand the security team with another member, but hiring someone had proven to be difficult. As such, other things were taking precedence.

With that in mind, they also stressed the importance of finding the balance between accommodating people and feasibility. Trying to offer something for everyone can quickly become resource intensive for the security team. As such, they found it was needed to make it clear what training is meant to achieve and then determine the most effective method for that goal.

Advice and fulfilment criteria
As people have different routines and different ways they would like to learn, it is recommended to have multiple training methods available. Employees of IECC had two main favourites, an online option that can be planned in their own time and a longer, but less frequent, live in-person option. Some people like to learn on their own, while others prefer learning together with people. Do then give people the option to choose between them, instead of simply stacking more upon them.

As said by an external interviewee, it is impossible to accommodate everyone fully, but it can at least be attempted in some form. Building on these findings, a singular method is unlikely to fit with everyone's routines, while two methods already have a better chance of accommodating more people.

6.1.3 Culture

Prerequisite: *Company culture promotes secure behaviour*

While organisational culture cannot be quickly addressed through training and was therefore deemed out of scope for this research, it was explicitly noted by the change manager as a crucial prerequisite for behaviour change. As such it is discussed in this chapter, but without input from employees on it, as they were not asked about it.

From literature

Demjaha, Parkin, and Pym [6] looked at how to better support people in behaving securely, keeping in mind that people have to make their decisions with limited resources, often leading to sub-optimal decisions. If there is a tendency for herd behaviour in an organisation, culture can have a large influence on the decisions people make. A security minded culture can then lead to decisions being made in favour of security, instead of against it.

From external interviews

Underlining the difficulty of changing culture, one external interviewee noted that organisations might try to improve culture with training, but it is something that largely takes shape naturally over time.

> *" It's always hard for organisations to have an impact on culture, because most of the times there is culture. You can't do anything about it, because it's something natural, it's something organic."*
> — Interviewee E2

Two external interviewees found that c-level and management commitment was needed, both in order to get the resources needed for security and for setting an example to everyone else.

> *" [...] and of course commitment from, from the CEO and from everybody also management, even though everybody's busy and everybody has their own mindset and their own jobs, of course. So yeah, it's hard."*
> — Interviewee E1

From session with the change manager and CISO

In the session with the change manager and CISO they gave two dimensions of company culture that can promote, or block, secure behaviour. The first dimension is that leadership and managers have to be on board, meaning they have to find it important to spend time and money on security. They actively have to ensure that employees can spend time on training and secure behaviours. Ideally managers should set the example and behave securely themselves, so employees feel comfortable doing the same. Which leads to the other dimension of culture that was mentioned, setting the example for each other and holding each other accountable. An example of this would be that they not only lock their own screen, but also address colleagues who forget to lock theirs.

6.2 Motivation

This section shows the ways in which motivation can be improved by targeting the concordance and self-efficacy factors. Concordance has four building blocks, including sharing actual threats and numbers, improving communication, having multiple difficulty levels to training and promoting interaction. Self-efficacy has one larger building block about giving more concrete advice to people.

6.2.1 Concordance

Building block: *Share actual threats and numbers of incidents with people to improve the risk perception and need for secure behaviour*

From literature research

From research it was found that people often discount the risks, as they think it will not happen to them

or does not happen close to them [26]. Showing the actual threats, and thus risks, can help shift this perspective. Researchers also found that if a threat is perceived as more harmful and more likely to happen, people are also more likely to employ prevention strategies [7].

Additionally, concordance building is shown to help people actually change behaviour instead of trying to force compliance [4]. Especially as it takes a lot of resources to force compliance, it is better to spend those resources on building concordance.

From internal interviews and brainstorming sessions

During the interviews multiple people in BULE noted that they would like to hear more about actual threats that IECC faces, as it paints a clearer image of the kind of risks there really are.

> *"they mentioned I think also some numbers or how often we now.. yes, it is simply interesting that you know like hey it is not occasionally or sporadically. We deal with it day in day out."*
>
> — Interviewee B3

This was then also brought up in the brainstorming sessions and everyone there agreed that it would help people better understand why it is so important to behave securely. Hearing 'it can happen to everyone' is a lot different from seeing actual numbers of attacks that IECC faces daily or weekly.

A participant who was also involved in safety policy noted that it was possible to report safety incidents through a tool that is present on everyone's laptops. This could perhaps also be used for reporting security incidents, to get even better insights.

It should also be noted that not everyone was interested, as two participants from FLC noted that they would rather just get the practical advice on what they should do instead of the why surrounding it.

> *"Bluntly put, but do I really care what they can get from it? So to speak, you just should not click on it [a phishing link]."*
>
> — Interviewee FLC2

From external interviews

Participants talked about how when sharing the kind of threats they face or the results of the phishing simulation, they found that people were engaging with the topic a lot. Either by talking about it in person, discussing it on the intranet or coming up to the security team to talk about it. Something they stressed was to avoid shaming people, so to remove any names and not use the experience in a negative way.

> *" For the phishing campaign, of course, we discussed the results with the complete organisation. To show how many clicks there were, but we're not putting any employee in the negative daylight. "*
>
> — Interviewee E2

From session with the change manager and CISO

The CISO and change manager agreed that sharing actual threat data and incident numbers could help employees better understand the risks they face and why secure behaviour matters. Making this information available was seen as practically feasible, as the security team already collects the relevant information. What needed to be figured out would be finding a suitable way to present and share them with employees on a regular basis.

This was when the safety dashboard already in use at IECC was brought up, through which safety incidents are communicated to employees. The security team could look to how that dashboard is set up in order to do something similar for security incidents and threats. As this set-up already exists within the company, building on it instead of needing to figure it out themselves was seen as a realistic and relatively

low-effort way of making threat information more visible to employees.

Advice and fulfilment criteria

Research found that people often discount risks that have not happened to them, as it feels far away. Actively sharing the kind of risks, threats and attacks a company faces can help improve the risk perception. Internal participants expressed an interest in hearing about the actual threats and external interviewees found that it helps with engaging people. Both stressed not to name and shame people however, as that would create a negative experience instead. During the session it came up that this kind of information can be shared through things like dashboards or intranet posts, for which the infrastructure might already exist.

Translating this to criteria, not sharing any information on it would mean this building block is not being fulfilled, while sharing any information that is already being gathered by the security team can go towards fulfilling the building block. It would still need to be checked if that way of communicating it is actually reaching people. Using infrastructure that shows the amount of views can help with that.

Building block: *Have clear communication on what the training is, what it is for and the timeline of the training*

From literature research

As people have limited resources with which they must make decisions, they must be helped to reach the 'good enough' decisions under the knowledge and resource constraints they have [6]. When the delivery of training is not done right it can lead to it not reaching people, people not understanding the training or people simply ignoring it.

From internal interviews and brainstorming sessions

Some examples that came up from the interviews indicated a problem with the communication of the training. Multiple people thought the training was only about phishing, as the platform the training sessions were held on had phish in the name. One participant even said they thought the first invitation to start doing the training was phishing, as they did not expect the training and found the mail suspicious. Only when colleagues said it was legitimate did they start doing the training.

> *"[...] also those security courses, just those trainings. Then I thought yes, but I do not know that either. That was also not IECC, well, then you hear from others: No, you just have to, that is that party, you have to do the trainings there. [...] then I will do it."*
>
> — Interviewee F3

As this seemed to be an issue, it was also brought up during the brainstorming sessions. They validated that the communications were not always very clear, and that they would like to see other things being communicated as well. They would like to know more about the schedule of the training, how many e-learnings would they be expected to do and what were the reasons for doing them.

From external interviews

Participants had multiple ways they tried to improve communications. One participant said they try to make sure the layout, colours and tone of the email and training match the company style to make it more familiar for people. They also noted the importance of doing it in the local language, as the topic is already difficult to understand, language should not be an additional barrier.

> *"the basic thing you can do is do like graphical representations, themes, colors, logos to kind of make it feel [company 3]-ish. That will go a long way in making people both trust it, but also make*

it feel familiar. ”

— Interviewee E3

Another participant said they chose to use communication channels that everyone already uses daily, both to make it more convenient and make it easier to reach everyone.

“People like convenience, right? They want to have, yeah, channels which they use daily. So for example, Teams they use daily and also WhatsApp they use daily. ”

— Interviewee E2

One participant also noted they had problems reaching everyone in the company, as not everyone read the intranet posts or was actively involved with the company culture as they worked at a client five days a week. They hoped to be able to reach them with the new training platform they were about to introduce.

From session with the change manager and CISO

The change manager and CISO acknowledged that communication around the training was an area that needed improvement, noting that information is often out there or has been shared before, yet employees still do not know about it. They found the way things are currently being communicated is not working.

Several examples of communications that had not landed as intended came up during the session. Anything sent in English rather than Dutch was found to be frequently ignored, as people did not understand it. An attempt had also been made to involve managers by asking them to inform their teams in advance when new training or communications were coming, but in practice many managers forgot to do so.

The confusion around the platform being more than just phishing training was also recognised. Employees had been told that the platform would have more than just phishing training, but this had apparently not stuck, as multiple participants still mainly associated it with phishing.

The issue of communications only being sent once also came up explicitly. Employees who joined IECC after a particular communication was sent, such as the introduction of the phishing report button, were simply never informed about it. Onboarding training was seen as a possible way to address this, both by ensuring that all new employees receive the same information and by making it clear from the start who they can turn to if they have questions about security. This would help prevent the situation where employees are expected to know and follow things they were never told about in the first place.

Advice and fulfilment criteria

Without clear communication and proper delivery of training, it might not reach people. Examples from within the company showed that communication sometimes failed to land, suggesting it is important to use channels that are used by everyone. This might mean using multiple channels, and keeping track of which information was sent only once and thus not reaching new employees. The change manager and CISO found that such information could possibly be included in the onboarding training to address this issue. Some other ways of improving communications, as found by external interviewees, were using channels that everyone uses daily, making sure the layout is familiar and using the local language.

Translating this to practice, finding out whether the information being sent is actually clear can also be done through feedback loops. These could start with counting the number of views and at times asking for engagement on a post to gather feedback. Actively asking for feedback from managers on whether people receive the information can also help. An indicator of communication being lacking could be that people do not make use of certain things, such as a password manager or phishing report button, because they do not

know such things exist. Similar to policies, hearing nothing from people does not mean communication is good, it could very well mean it is not reaching people at all.

Building block: *Have multiple levels of difficulty of the training to challenge the people who would like that and accommodate people who want easier training*

From literature research

Researchers stated that ideally the level of knowledge a person has is assessed before doing training, as they do not need to be taught what they already know. Instead time should be spend on teaching people what they still need to learn. This often does not happen however, leading to wasting time and goodwill of said employees [24].

From internal interviews and brainstorming sessions

From the interviews, it became clear that people had different opinions on the difficulty level of the training. Some found it an appropriate level, while others found it to be too easy. There was no one department that had the same opinion, it only depended on the person. People who found the training to be too easy almost always added that they understood it had to be understandable for everyone, but it had become demotivating for them to do the training.

> *"I do find it very general though, so to speak. I mean, I understand that for 1500 IECC colleagues [...] you have to find something that works for everyone, so to speak, and that everyone can understand. [...] If I am completely honest, most of those trainings I have running in the background while I am just continuing to design."*
>
> — Interviewee B2

They noted that without it being challenging, people started to put on the training in the background while continuing to work. It then became something that just had to be done, but not something they actually learned anything from.

> *"It sometimes challenges, I see that with many colleagues, it sometimes does not really challenge anymore you know. It is often a click, click click, click, click click well, we are done with that one too."*
>
> — Interviewee B4

As such participants offered the possibility of doing a test to test their current knowledge and then being allowed to do training starting from a certain level if they so wished.

> *"I can imagine that you could do a kind of intake test and that you end up at a certain level and that you then receive questions at that level."*
>
> — Interviewee B2

From external interviews

One participant from the external interviews touched upon the difficulties with balancing the level of the training content. While making it understandable for everyone, a risk emerges of people feeling belittled as they think the content is much too easy. Part of that also comes from the way the questions are asked, which makes the right answer very obvious.

> *"Most of the time, security awareness trainings, the answers are easy for most people to get right. And that has both a positive and a negative side. So the positive is it's easy for you to go through the course. The negative side is you might even feel... belittled or talked down to in the training."*
>
> — Interviewee E3

From session with the change manager and CISO
The CISO and change manager agreed that with the current way training was set up, it meant a significant portion of employees were likely not learning anything new from the training. They also noted how frustrating it can be for employees to have to spend time on training with topics they are already very knowledgeable about.

The idea of an intake test that allows employees to skip to a level that actually challenges them was seen by both the CISO and change manager as a possible way to handle this. They compared it to how Duolingo does it, by letting users take the test at the end of a level, to skip over unneeded training and go straight to content that is new for them.

Whether this is realistically achievable would depend on the capabilities of the current platform however. It was noted that this would need to be investigated before any decisions could be made, and that if the platform does not support this kind of approach, it may be worth considering whether the platform itself is still the right fit for what the training is trying to achieve.

Advice and fulfilment criteria
People have different levels of knowledge, which training should take into account. Some employees from IECC found the training to be at the right level, others found it too easy. How an external participant put it, by trying to make it understandable for everyone, a risk emerges of people feeling belittled. Taking all of this together, having multiple difficulty levels and an intake test that determines the level that users should be placed at is recommended.

Only having multiple difficulty levels does not satisfy this building block fully yet, as forcing people to do training far below their knowledge level is demotivating. It should be combined with a test, or other way, determining the level a user should start at.

Building block: *Accommodate and promote interaction (in training) between colleagues to discuss security topics to learn from each other*

From literature research
Research found that adults learn differently than children, as they have their own experiences and frame of knowledge which shapes how they perceive knowledge [28]. They often learn better from personal experiences, as this helps to challenge their frame of knowledge. Interactive training, where people discuss things together, can help with this.

From internal interviews and brainstorming sessions
Participants from all departments thought interactive training would be nice, for multiple reasons. Participants from finance noted there was a gap between knowing and doing, and as such doing a workshop or simulation exercises could help bridge the gap.

Participants from all departments found that interactive training could help bring in new perspectives of people. When people go over training by themselves, they might miss these perspectives.

> *"If you put multiple people together in a group, one person will engage more with one thing and have a question about it and the other more in that other area. Whereas if you do it all individually, yes, then you are just reading [...] Yes, and that is it then."*
>
> — Interviewee F2

Another point people from all departments made, was that this way they simply learned things better. By actively engaging with the subject matter and discussing it with others.

> *"The online tools often work less well for me than just sitting together in a classroom and being able to have a real discussion. Being able to engage in conversation, that usually works better for me."*
> — Interviewee B2

From external interviews

All participants from the interviews said to have tried to make interaction in some way possible between colleagues on security topics. They found this to have the greatest effect on people, in terms of increasing awareness. Promoting interaction was mainly done by making security communities in some way or another. Some did this by creating an online environment where people could discuss topics they had either brought up themselves, or were brought up by the security team.

> *"We created a community, so a security community where people could engage with each other and kind of discuss what their experience was and what they've learned. And then we would have a moderator from the security team that would sit as part of that community and pull out some of this feedback."*
> — Interviewee E3

One participant created a physical environment where people were invited to come together, have a pizza and discuss security topics.

> *" We have a knowledge community about security and that's started I think this year. So we have a pizza session every two months, sometimes even more about the security topic and we just invite everybody who's interested in in the topic."*
> — Interviewee E1

From session with the change manager and CISO

The CISO and change manager were enthusiastic about the idea of promoting interaction between colleagues and thought it could be useful for increasing motivation and developing the skills people reported to currently lack. Two concrete ideas came up during the session. The first was to walk through a potential phishing email together, going through the steps of how to assess it and decide what to do. People could discuss how they usually do it and learn from each other.

The second idea was to discuss an actual phishing incident that had occurred at IECC. This would facilitate a discussion on what happened, what could have happened and what they need to do if they ever do find themselves in a similar situation.

Advice and fulfilment criteria

Employees noted that promoting interaction between people could help them gain new perspectives and ask questions they otherwise would not have bothered with. In the session with the CISO and change manager, this was also seen as an opportunity to help people gain skills they are currently lacking. From the external interviews it was found that both an online or real life environment can be used for it, such as an intranet community or hosting sessions every couple of months.

Translating this to fulfilment criteria, as interaction can be facilitated in multiple ways, it also differs when this building block can be considered fulfilled. It is not fulfilled when no kind of interaction is facilitated or promoted. When hosting live sessions to promote interaction, they should be held regularly and people should be attending the sessions. If the online communities are used to promote interaction, collecting metrics such as views, interactions and comments can help determine the amount of interaction happening.

Measuring the interaction and collecting feedback in this way can also help with other building blocks, such as knowing which topics people want to know more about.

6.2.2 Self-efficacy

Building block: *Give more concrete advice aimed at IECC specific policies and what people actually wish to know*

From literature research

Research found that while people might have knowledge about cyber security and know they should behave securely, without knowing the actual practical strategies to employ, there is likely to be a 'knowing-doing gap' [8]. Even though people know they should do something, they do not do it as they do not know how to. In order for actual action to happen, people need to be able to identify the risks and understand the strategies needed to protect themselves.

From internal interviews and brainstorming sessions

During the interviews, many different needs from people came up that were not all addressed by the current training methods, as explained in more detail in chapter 5. While some people felt they did learn the things they wanted from the training, others found the training to not be very relevant for their work.

> *"They are missing a bit, sometimes they are missing the relevance of it, of what am I actually learning from such a training?"*
>
> — Interviewee FLC1

Participants from all departments found that the advice given as of now was not always very clear or specific enough to be able to do anything after having seen the advice.

> *"A bit more tips, so to speak, aimed [...] at work. [...] how you deal with, I don't know, passwords or whatever and how often you have to change them or whether there is some kind of standard guideline for that."*
>
> — Interviewee B1

A lack of self-efficacy was also found as people were unable to keep up with technological changes. They were not able to understand new technologies by themselves, or when trying felt they were always some steps behind on things.

> *"I am glad that I am making it all my own and learning a bit from it while others are already saying, this is outdated. We are already 3 steps further."*
>
> — Interviewee F2

From external interviews

Participants all said that they think it is a good idea to tailor training to be role-specific. Establishing a baseline of knowledge first and then specializing where needed was how one participant planned to go about it.

> *"And then afterwards, if we, when we have trained everybody, we can figure out if we can tailor make some extra challenges for specific people "*
>
> — Interviewee E1

Another participant noted that at a previous company, they had two people who worked full-time to create the tailored training, but that this was something that was simply too resource intensive to do at their current company.

> *"So what I've seen to be highly effective also requires a lot of resources. So it's something that's tailored to the organisation, something that is that references the language and the themes that are*

in place in the organisation. What we did at [company] is we actually had two full-time employees that created security awareness content. "

— Interviewee E3

One participant did say to be careful to communicate more specific advice to people in a way that it only reaches them, otherwise it confuses people who the advice or warning is not for.

"it's not very useful for everybody, but only for those people to, to have a specialized post for them, right. So I did, I did once I had a post about vulnerability management, [...] it was only meant for people with local administrative rights. [...] But yeah, all the other people were like, okay, what do you want me to do?"

— Interviewee E1

Another way to promote self-efficacy was to have people have confidence in fail-safes, to ensure they would not get too scared to do things. Participants noted it was important for people to be aware and feel like the security team had their back, instead of feeling afraid of a misstep. In that sense they also noted that technology should help people work securely.

"I hope to give people the confidence that we got their back. That's our job as well."

— Interviewee E1

From session with the change manager and CISO

The change manager and CISO both found the knowing-doing gap a real problem and realized people might not know what to do without more specific guidance. The first thought on how to address it was through organizing practical live sessions, where employees could be guided through doing it together. A session where people are invited to set up a password manager was given as an example. Multiple employees had expressed reluctance around using one, as they were unfamiliar with it. A live session would allow people to work through that barrier with support from experts. The underlying idea is that people are perhaps not opposed to adopting a new behaviour, but are held back by the fear of something going wrong.

Another part of giving more concrete advice was to tailor the content of the e-learnings more specifically to IECC policies and departmental needs. The current platform, however, does not allow for modifying individual lessons within an existing level, meaning that tailoring content would require building a level from scratch. However, it was noted that this functionality may become available on the platform in the future, which would make it considerably less resource intensive.

Advice and fulfilment criteria

Literature found that people need concrete advice in order to actually be able to follow it, otherwise a 'knowing-doing gap' is created. It is also important for advice to be about things people actually wish to know. As this research shows, finding out people's needs can be done by asking them one on one or in a group setting. Asking people about their way of working first can help with that, as they can be more easily guided on what is missing or misunderstood when their way of working is understood. The more concrete and targeted advice can then be incorporated in the training.

Translating this once more to fulfilment criteria, advice that does not give step-by-step instructions on how to follow it, or that is not tailored to what the organisations actual policy is, does not fulfil this building block. Advice such as 'use a password manager' is therefore not good enough. How can I make use of a password manager, where can I find it and which one does the organisation use? Fulfilling this building block requires both an analysis of advice from the security team and a feedback loop, as people need to tell the security team themselves whether advice is concrete enough and whether there is advice missing. Ideally, all advice given is easy to follow and covers what people need to know.

6.3 Summary paragraph

A summary of the chapter can be found in table 6.1.

Table 6.1: Summary of findings per building block or prerequisite

Category	Prerequisite (P) / Building block (B)	Findings from literature	Findings from practice	Advice & Criteria
Simplicity and ability Time and effort	**P:** Review policies on feasibility, try to reduce friction to stay within compliance budget	Companies often do not check policies Can lead to people circumventing or refusing to comply	**Internal**: many policies were found to be undoable, leading to circumventing or refusal to comply **External**: avoid overwhelming users, set up feedback loop to find pain points **Session**: had tried to resolve issues before, but apparently unsuccessfully. Think a feedback loop could help identify pain points to find deeper cause of problems	**Advice:** (keep) checking feasibility with feedback loops **Criteria:** fulfilled when only positive feedback received, not when nothing is heard
	B: Review the frequency of training and adjust if needed	People have limited resources, more training is not the answer Repetition is needed however, as knowledge is forgotten otherwise	**Internal**: frequency of simulations too high, clear example of compliance budget being exceeded **External**: multiple kinds of training with different frequencies, needed to have multiple training sessions as threat landscape changes quickly **Session**: understood the frequency was too high, did think other causes of irritation also still existed	**Advice:** often enough to teach everything, not too often to exceed resource constraints users **Criteria:** reminders about every three months, feedback needed if done more often
Simplicity and ability Routine	**B:** Have different options of training methods to fit with people's routines	As adults learn differently, being formed by their experiences, multiple methods are more likely to reach people	**Internal**: people prefer different training methods, as it fits their routines better or learning preferences **External**: prefer and make use of multiple methods to accommodate people **Session**: had attempted to set up special sessions, but due to time constraints had not done so yet. Stressed the need for balance between accommodating and feasibility	**Advice:** ask people about preference and let them choose between methods **Criteria:** every single person need not be accommodated, but have at least two options

Category	Prerequisite (P) / Building block (B)	Findings from literature	Findings from practice	Advice & Criteria
Culture	**P:** Company culture promotes secure behaviour	Within bounded rationality people make sub-optimal choices within constraints. Culture can positively influence it.	**External**: changing culture is difficult, support c-level and management is needed **Session**: without the support of leadership and management, behaviour change will not happen	—
Motivation Concordance	**B:** Share actual threats and numbers of incidents with people to improve the risk perception and need for secure behaviour	People discount risks People are more likely to behave securely if they perceive the threat as harmful Concordance building helps change behaviour	**Internal**: want to hear more about actual threats to understand the need better. Security incidents could be reported the same way safety incidents are **External**: sharing actual threats boosts engagement, but avoid shaming people **Session**: think it would help and already have the data, safety dashboard infrastructure could be used	**Advice:** Share actual threats to improve risk perception, do not name and shame **Criteria:** this is fulfilled if information is shared and it checked that it is reaching people
	B: Have clear communication on what the training is, what it is for and the timeline of the training	People have limited resources to make decisions with, help them by having clear communication	**Internal**: multiple issues with past communication were found, either because it was not sent or people had not noticed it **External**: improve communications by making things look familiar, using the local language and using channels that are used daily **Session**: agreed that improvement was needed, noted other examples of things not landing. Also issue of new employees never receiving past communication	**Advice:** Use channels that are used daily, make lay-out familiar, use local language and include old communications in onboarding **Criteria:** collect metrics and use feedback loops to see if communication is clear. Not hearing anything does not mean it is fulfilled.

Category	Prerequisite (P) / Building block (B)	Findings from literature	Findings from practice	Advice & Criteria
	B: Have multiple levels of difficulty of the training to challenge the people who would like that and accommodate people who want easier training	Current level of knowledge often not tested, leading to wasted time and goodwill on training below their level	**Internal**: different levels of difficulty were wanted, with a test to skip to their level **External**: balancing the level of the content was difficult, as to not belittle people but also not leave people confused **Session**: agreed that it was a waste to have people do training they already know, would have to look into capabilities of platform to address this	**Advice:** have multiple levels of training and a test to determine which level users should do **Criteria:** only multiple levels is not enough, intake test is needed as well
	B: Accommodate and promote interaction (in training) between colleagues to discuss security topics to learn from each other	Adults have their own frame of reference and often learn best by experiencing things	**Internal**: felt it could help close the knowing-doing gap, give new perspectives and make it nicer to learn things **External**: all tried to increase interaction, usually through a security community **Session**: enthusiastic about the idea, think it would be doable to host sessions where people can learn skills and discuss things	**Advice:** promote interaction both online and in real life **Criteria:** feedback and metrics can determine if a good amount of people is interacting
Motivation Self-efficacy	**B:** Give more concrete advice aimed at IECC specific policies and what people actually wish to know	Knowing-doing gap: knowing they should do it, but not how to do it, can happen when people do not understand the actual steps to take	**Internal**: not all information and skill needs were met, advice was not specific enough to follow, had trouble keeping up with technological changes **External**: good idea to make it more concrete and specific, does take a lot of resources to do, also promoted self-efficacy by making people feel the security team had their back **Session**: live session could introduce more practical advice. Platform currently does not support changing lessons, but might in the future making it more feasible	**Advice:** ask people what they want advice on and have step-by-step instructions **Criteria:** untailored or undetailed advice does not fulfil this block, advice needs to be analysed and user tested

7

Practical implications

During the session with the change manager and CISO from IECC it was also discussed when they would be implementing the findings and how they could do so. As such, this chapter first discusses the practical implications for IECC in section 7.1, after which the practical implications for other companies are discussed in section 7.2.

7.1 Practical implications for IECC

During the session with the change manager and the CISO, it became clear that resource constraints have to be taken into account when deciding how to implement the advice. There is limited time or money that can be spent on it. As such, this chapter will start with steps that will immediately be taken and end with steps that will have to be taken in the future after further assessment of feasibility and costs. The steps that will be done first are also based on the awareness maturity curve discussed by Sasse et al. [24], as some steps should be in place before others according to that curve.

The first piece of advice that was deemed feasible to implement in the near future, was to review the security policies in place to try to stay within the compliance budget of people. This would start with the policies that were already identified in this study and more policies could be identified by opening the conversation within the company for people to give feedback on other pain points. A possible way of doing so was identified to be how safety incidents are already being reported, as it could make use of an existing application.

Another step that could immediately be taken was to lower the frequency of phishing simulations, as it had seemed clear from participants that the compliance budget had been far exceeded by doing these every two weeks. The frequency would instead be set to every six weeks.

In terms of improving motivation, sharing actual threats IECC faces was seen as feasible in the near future as well. The numbers, such as the number of phishing emails caught by the filters, were something the security team already has and the way of sharing the numbers could be based on the safety team's existing practices. As the safety team already communicates the monthly incidents through a dashboard, the security team could do it in a similar manner.

Combining two pieces of advice, namely promoting interaction and providing more concrete advice, was also something that was seen as doable in the near future. This would be done by organising live sessions where people, for example, set up a password manager or go through the steps of checking the legitimacy

of an email. This could help with closing the knowing-doing gap participants reported. Other ways of providing more concrete advice, such as during the e-learnings, was something that would be done further in the future, as the platform currently did not easily support this.

Improving the communication was partly doable in the near future and would partly have to be done later on. It would be possible to already communicate more on the timeline of training and why training was being done. During the expert validation session it also became clear that some people likely missed some communications because they had simply not been working at IECC yet at that point in time. A possible way of preventing that in the future would be to include important things in the onboarding training. Another factor to consider is that not everyone looks at the intranet or rarely looks at Outlook, so different means of communication might need to be used, such as bringing it up during the weekly or monthly meeting.

The advice that would have to wait until further in the future was the advice that required finding a balance between accommodating people and it still being doable for the security team. Having different method options available for people and having different levels of difficulty potentially meant considerably more work for the security team, but also could substantially help accommodate the different needs that people have. The feasibility of this depended on the possibilities of the platform, potentially needing to find a different platform and the ongoing process of hiring an additional team member.

7.2 Practical implications for other companies

This research provides practical implications not only for IECC, but also for other companies that want to improve the effectiveness of their security awareness training. While the findings are connected to the context of IECC, the approach can be applied more broadly.

One part of that approach is that companies should start by looking at the work employees do. By first identifying employees' primary tasks, the digital secondary tasks that accompany those tasks and the security needs that follow from them, companies can make training more relevant. This also means that companies should design training using actual employee input, instead of generic assumptions about "the user". Employees in different departments often have different needs and routines. Treating all employees as if they have the same security needs can lead to training that gives advice that is not actionable or not applicable to them.

Another implication from this is that companies should use employee input early in the design process. This does not have to take up much time or resources. Short interviews, focus groups, brainstorming sessions or feedback moments can already provide valuable insight into the needs of employees and how current training aligns with them. This also creates a feedback loop between the security team and employees, which can help bring up other issues or ideas. Having such a feedback loop can also help identify high friction policies which might need to be reviewed and changed.

Finally, the examples from practice discussed both from IECC and from other companies can help other companies translate abstract advice, such as "motivate people", into concrete actions. The factors from the framework, along with the examples from practice that were discussed in the findings, can be used by other companies to inform their own design choices.

8 Discussion

This chapter starts with a discussion of the results in section 8.1, after which the academic and societal relevance and contributions as well as the relevance to the MOT programme are discussed in section 8.2. Next the limitations of the research are reflected on in section 8.3 and the chapter ends by outlining future research in section 8.4.

8.1 Discussion of results

8.1.1 SQ1: Primary tasks, routines and needs

Based on the findings, employees' primary work tasks shape their security needs through secondary tasks associated with the primary tasks. In order to perform their primary tasks, participants had to do a number of secondary tasks which were more closely related to security needs.

While from a primary task such as 'handling invoices' it might be difficult to immediately note all the security needs that come with it, it is easier to do when that is broken up into the (digital) tasks that accompany it. In order to handle invoices, external and internal emails must be sent, sensitive files are stored or accessible through the laptop, these sensitive files have to be shared and they have to work with multiple different applications to get the data required for making an invoice. From these tasks it was easier for participants to express their security needs. With these tasks in mind, they were able to link wanting to protect their laptop to having sensitive files on it, or when sharing sensitive files needing to know which files can and cannot be shared. The need to discern real emails from phishing emails quickly came up as well when the amount of emails they receive and send was discussed. Similar lines of reasoning came up with participants from BULE and FLC as well.

Especially during the brainstorming sessions did participants make these connections, as they were asked which digital tasks accompany the primary tasks they identified and which security needs connect to that. The brainstorming session added a visual overview and it helped participants to be able to discuss it with others.

Primary tasks also shape the routines and work environment of participants. As people from finance mostly work on their laptop and with internal people in order to do their work, they mainly work in the office or at home. Participants from BULE often have to work with clients, as they either design things for them or manage a project with them, they also usually work at the office of clients once a week. Participants from FLC had a very different work environment, as they do not work in a typical office

environment. In order to perform their primary tasks, they have to be out in the field, their laptops are even weather resistant as they work outside. As such it could be said that all departments work digitally, but only some work in a standard office environment. The primary work tasks of participants from finance and BULE also had a collaborative element to them, meaning they often use applications like Teams and Outlook, while FLC employees do not. Working at a client also meant that BULE and FLC employees often use a SIM card to have internet access. Primary tasks thus shape the routines of employees in multiple ways, namely what their work environment looks like and what their digital environment looks like.

From these findings it could also be seen how primary tasks shape what kind of content participants wanted and to some degree which kind of training methods they preferred. Where the security needs shape the kind of content participants want, their routines somewhat shape how they prefer to receive the training. Participants from FLC preferred a physical meetup, as they are rarely in an environment where an e-learning is nice to do. Participants from finance on the other hand liked the e-learnings because they were nice to plan in between work. Part of the method preference also comes from personal preference, as people simply prefer learning on their own or with others.

The findings also show that not everyone has the same needs or routines, emphasizing once more how 'one-size-fits-all' training cannot possibly work. Either more specific needs of people go unaddressed, or if they are addressed but the training is given to everyone, people have to spend time on training that is not relevant for them. This is discussed in more detail in the next section.

8.1.2 SQ2: Alignment current training with routines and needs

Regarding SQ2, the current training was found to align only with needs that were more generic, such as spotting phishing or generally raising awareness. The more specialised needs, such as finance needing to know which files could be shared with whom, were not met. Other examples of needs not being met include participants not using password managers, as they did not know how to use them. Neither did participants challenge tailgaters, as they did not know how to do that in a safe way. They also did not know how to deal with emails that they could not determine themselves whether they were legitimate or phishing. Others also noted that there were many different ways in which files were being managed or shared, but they did not know if there were any company guidelines on how to do it securely. Something else that came up was how participants from FLC felt that the training was heavily focussed on phishing, while they rarely make use of Outlook. A lot of time in the training was spent on things they have little need for. Looking at the training that employees have to follow, it seems logical that more specialised needs were not being met. The vendor-bought training was not adjusted to IECC policy, thus only aligning with generic needs.

In terms of alignment with routines, the current training was found to align mainly with the routines of participants who were working in an office environment, but not with those who work out in the field. An e-learning does not work nicely in an environment that can be loud, have no internet connection and no desk to do the training from. This likely stems from the fact that the training used was vendor-bought, where a vendor assumes that people work on their laptops and make use of Outlook. The same things goes for the phishing simulations, it assumes that people regularly make use of Outlook, which not all employees do. Another aspect of aligning with routines is how a general workday might look for a person, while some might have time to plan a short training in between, for others this might not work well. Participants from FLC felt that small blocks did not fit and they would rather see larger blocks, but less frequent. It was also brought up that those with a practical instead of higher educational background might not see it as a positive thing that they can plan the training themselves and would prefer it to be planned for them.

From these results it can be observed that while participants generally noted that security awareness was important, a clear gap between attitude and behaviour was found due to needs not being met and important factors for behaviour change not being in place. These factors include that people are really motivated to change, find it simple to do, are able to do it and are triggered to perform the new behaviour [9]. As said before, some factors have to be dealt with outside of training, but training can tackle at least the motivation and ability. The different factors that training can, and should, address are discussed in detail in the next section.

8.1.3 SQ3: Designing training to address misalignments using employee and expert input

Regarding SQ3, multiple misalignments and corresponding adjustments were found between training and needs and routines. To present these findings in a structured way, they were mapped to a framework of factors influencing the effectiveness of security awareness training. The factors from the framework identified to be addressable through training were used to categorise findings into prerequisites and building blocks, all of which contain practical examples and advice. While this kind of advice exists in the literature, it tends to remain at a level of abstraction that leaves much room for interpretation, making it difficult for practitioners to know where to start. Without clear guidelines practitioners were left to do things by trial and error, which was evident from the multiple examples where they had tried to implement things, but they had failed to land properly. This research therefore aimed to make the advice more actionable, both by grounding it in the needs and routines of employees and by illustrating it with examples from practice.

Within the simplicity and ability category, the first thing that must be addressed is the feasibility of existing security policies. This was found to be a real problem at IECC, where multiple policies were either in conflict with workflows or in conflict with policies from other departments. This confirms what is found in the literature, namely that companies often do not check their policies for feasibility, which leads to people circumventing them or setting up shadow security [11, 17]. The change manager and CISO recognised the problem and also said that some attempts had already been made to resolve specific conflicts, such as the one over mobile data costs between the security and finance teams. These had apparently not been resolved successfully, as employees were still running into the same problem. This calls for a more structural approach to identifying and addressing high friction policies, such as through a feedback loop that allows employees to flag pain points on an ongoing basis rather than waiting for a research project to surface them. Not hearing anything from people does not mean there are no issues, as people might be ignoring policy or cannot find the security team. Positive feedback is thus necessary for this prerequisite to be considered fulfilled.

The first building block in this category concerns the frequency of training. The frequency of phishing simulations was found to have already exceeded the compliance budget of employees, with some having started to distrust all emails and others deliberately clicking links in protest. This is a clear example of the bounded rationality of employees, as they have limited resources, they will not keep spending them on something they experience as excessive [6]. The change manager and CISO understood this and were open to reducing the frequency of simulations. There is however a need for multiple training sessions every year, both because the ISO certifications demand it and because the threat landscape changes rapidly. It is also needed as knowledge was found to decay quickly without reminders, but remain fresh in the minds of people if reminders were used [5]. As such, training should be done often enough so people do not forget, which is around every three months, but also not so often as to exceed the compliance budget, which can be found through asking for feedback.

The second building block in the simplicity and ability category is offering multiple training methods to accommodate different routines and learning preferences. This was confirmed as important by both internal and external participants, and is in line with what the literature says about adults learning differently based on their experiences and existing knowledge [28]. In practice, the challenge lies in finding a workable balance between accommodating the different needs and keeping it feasible for the security team. This tension was also reflected in the expert validation session, where the CISO and change manager stressed the need to be clear about what the training is trying to achieve before deciding on a method, rather than attempting to offer something for everyone at once. Fully accommodating everyone will not be possible, but it can at least be kept in mind.

A final prerequisite in the simplicity and ability category is company culture. While this was identified as a factor not addressable through training, it was explicitly mentioned by the change manager how important it was. The security team needs to have the support of c-level and management in order to spend resources on security and employees need to feel supported to spend time on security.

Within the motivation category, the first concordance building block is sharing actual threats and incident numbers with employees. Participants across departments wanted to know more about the real risks IECC faces, and the literature supports this as a way to counter the tendency people have to discount risks that feel distant or unlikely [7, 26]. The expert validation session confirmed this was feasible, as the data already exists within the security team. The existing safety dashboard could be adapted for security, reducing the effort needed to implement this and showing that existing infrastructure might be usable for it. The importance of not naming and shaming individuals, as stressed by external interviewees, is worth keeping in mind when deciding on the format. Ensuring the information actually reaches people is needed for this building block to be considered fulfilled.

Clear communication about the training was identified as a second concordance building block. From both the internal interviews and expert session it was clear things did not always go well. The change manager and CISO acknowledged that the current approach to communication was not working and that something had to change. From the external interviews some ways of doing so had come up. They had ensured the layout of communications was more familiar to people, used the local language when communicating and used channels that were used daily by people to make it more convenient. Gathering feedback, which can be the number of views and engagement on posts, or actively asking people for their opinion on it, can help with understanding if the chosen style of communication is reaching people. Not hearing any feedback on it does not mean it is going well, as it can also mean it is not reaching people at all.

Multiple levels of difficulty were identified as a third concordance building block, grounded in the finding that companies typically do not assess existing knowledge before assigning training, leading to wasted time and goodwill [24]. This was confirmed by participants across departments, with several noting that they were running the training in the background while continuing their actual work. The CISO and change manager agreed this was a waste and the idea of an intake test that allows employees to skip to an appropriate level was received positively. Whether this is achievable on the current platform remains to be investigated, and the question of whether the platform remains the right fit was also raised, should it not be able to support this approach. Interviewees from external companies also said they struggled with balancing the difficulty level of training. The steps to fulfilling this building block would be to have multiple levels of training, followed by having tests that can determine if that level needs to be done by an

employee and allowing them to skip it if is not needed.

Promoting interaction between colleagues was identified as a fourth concordance building block, supported both by the literature on how adults learn from personal experience [28] and by the enthusiasm expressed by participants across departments and external interviewees. External interviewees had done this by setting up security communities. During the session with the change manager and CISO the interaction aspect was considered more in relation to people who were experiencing a knowing-doing gap. Possible ideas that came up were a guided session in which employees work through assessing a potential phishing email together or a discussion of an actual phishing incident that had occurred at IECC. Both combine skill practice with real-world relevance, while promoting interaction. Collecting metrics, such as the amount of people participating, seeing how many messages are sent or how much people are talking during live sessions, as well as asking for feedback from people can help determine how much interaction is happening.

Under the self-efficacy category, the final building block for motivation, is giving more concrete and role-relevant advice to close the knowing-doing gap [8]. Many participants said they knew in theory what they should do, but lacked the specific knowledge or practical skills to actually do it. Here it is important to note that giving more role-specific advice is advised in literature, but how to actually do it is left up to the practitioner. An external interviewee had done so before, but it took a lot of resources. With that in mind, the change manager and CISO pointed to live sessions as the most immediately feasible way to address this, as identified skill gaps could be addressed that way. Tailoring the content of the e-learnings to IECC-specific policies and departmental needs was also seen as something that should be done, but it is currently constrained by the limitations of the platform. Fulfilling this block requires both the security team to analyse the advice and asking people if they think the advice is actionable and role-specific enough.

A comment made by the change manager during the session is worth noting as a final reflection. They observed that many of the issues identified, particularly those related to time and effort, felt interconnected and may reflect deeper underlying dynamics. Issues addressed by one building block might also need to be addressed by another. This reinforces the importance of treating the framework as a whole rather than as a checklist of isolated fixes.
To illustrate what that would look like in practice, let us consider what an ideal training programme might look like when all the blocks are working together. It starts with a foundation of feasible policies, if the secure behaviour conflicts with workflows and takes up too much time, no amount of training will overcome that friction. Once the foundation is in place, training should be structured to accommodate routines and preferences. This can be done by having multiple methods of training with different kinds of frequencies and different levels of difficulty. This can mean giving people the choice to either attend live sessions every quarter that take half an hour to an hour or doing shorter monthly e-learnings that take about 10 minutes. The live sessions can facilitate interaction for those who want it. Employees could take an intake test, allowing them to skip introductory content. In terms of content the training should contain information on actual threats and number of incidents, to improve the risk perception of employees. The advice given in the training should be actionable and role-specific. For all of this to land, it needs to be communicated clearly. None of these blocks operates in a vacuum, and progress on one can create conditions that make the others easier to fulfil.

8.1.4 Main RQ: designing or modifying training to align with primary work tasks

With the insights gained from the sub-questions, the main research question can be answered, namely: **"How can security awareness training be designed or modified to align with employees' existing work routines and needs?"**. The first step in this process is to gather input from employees about their primary

work tasks and discuss with them which kinds of security needs come from those tasks. From the primary work tasks, the routines of employees can also be found. This is preferably an iterative process where the findings and assumptions are also validated with the employees.

The second step, which is applicable for organisations that already have some kind of training in place, is that the current training should be evaluated to see what it does well and what it does not address. Employees should be asked directly how well they think their identified needs are being met and how well the methods fit with their routines. If the current training is generic and vendor-bought, it likely only fits well with employees who have standard office routines and only satisfies more general advice needs. With the knowledge of what the training does well and what it does not, the training can be modified or redesigned using the framework.

For the third and last step, the different factors of the framework should be considered in order. All factors need to be in place for behaviour change to happen, as each factor can act as a blocker. For each of these factors as identified from literature, more actionable security advice from practice was found, some of which were prerequisites and some of which were training building blocks.

The first category to be addressed is the simplicity and ability category, as motivating people for unfeasible behaviour will not work. As such, the policies first need to be given a feasibility check and a structural way of identifying pain points needs to be implemented in the form of a feedback loop. Next, the frequency of the training should be evaluated to see if it is not too often to exceed the compliance budget of employees, but still often enough so people do not forget. Another training building block in this category is to accommodate people's routines and preferences by providing multiple types of training, such as interactive live sessions or independent e-learning lessons. A final prerequisite of this category is culture, where c-level and management should be supportive in terms of resources and by setting the right example.

The other category is motivation, which can be addressed after the first category. It contains two factors addressable by training, namely concordance and self-efficacy. To improve concordance and risk perception, people can be shown the actual threats a company faces. Clear communication also plays a role in concordance, as information can be lost with bad communication. As such, communication channels that are used daily by employees are recommended to use, which might differ per department. Setting up a feedback loop on the quality of communication is recommended, as hearing no feedback might just mean people are not seeing the communication at all. Another way of improving concordance is through having multiple difficulty levels of training and having employees do an intake test to determine what they still need to learn. This prevents wasting resources and goodwill on forcing employees to do irrelevant training. A final way of building concordance that was identified, is to promote interaction between people, as they learn from each other. The other factor in the motivation category is self-efficacy. This can be improved by making advice more actionable and more specific to the needs of employees that were identified earlier.

Ultimately, employee input is not just useful at the design stage, but at every stage of the process. It can be used for identifying needs and routines, to evaluating existing training, to refining the framework over time. This is how security awareness training can be designed or modified to genuinely align with the people it is meant for.

8.2 Relevance and contributions

8.2.1 Academic relevance and contributions

Research is showing a growing consensus that security awareness training in its current form is not effective and that training should be tailored to the needs of users [27, 24]. Most researchers, however, do not consult with users before designing the artifact, as found by Kaur et al. [16]. This leads to much existing work being grounded in theory, rather than in empirical evidence. As such, this research contributes to filling the gap by providing a qualitative, empirically grounded study on how co-design can be used to design or modify security awareness training that is tailored to the primary tasks of users. This provides both the approach that can be followed and practical examples of how to fulfil the advice often given in literature.

A specific contribution that comes from the first step of the approach, lies in how security needs can be derived from primary work tasks. While the literature does say to tailor training to primary work tasks of users, little work specifies how that can be done. This research provides an approach to how primary work tasks can be broken down into digital secondary tasks which can be linked to the actual security needs users have.

The second step of the approach contributes a structured way for practitioners to evaluate existing training before redesigning it, grounding that evaluation in the needs and routines of employees rather than assumptions. The findings from this step also show empirical evidence of what was already found in literature. Namely that vendor-bought training tends to be generic by design, meaning it will typically only satisfy more universal security needs and fit the routines of employees in standard office environments. Employees with more specialised roles or non-standard working conditions are likely to find such training less relevant.

For the third step of the approach, the framework of training building blocks based on the FBM behaviour change model [9], with factors from Sasse et al. [24], offers a practical guideline for both practitioners and researchers to use and build on. It especially gives more actionable advice to practitioners to follow when they are trying to design training that is more aligned with users' primary work tasks. This research demonstrates examples from practice which can help other practitioners decide on how to do things themselves, by seeing what did work and what did not.

8.2.2 Societal relevance and contributions

Cybercrime is on the rise and there are large consequences in case of data breaches [19]. Data breaches lead to financial losses, reputational damage and violations of privacy. While technical measures are important to use to prevent such breaches, the human factor will continue to play a role as well. As such companies invest a lot of money into training, which is expensive, but is being shown to be ineffective. This means there is a need for alternatives.

This research contributes to that need by providing a practical approach companies can follow to improve their training, also within resource constraints. By finding out the different needs of employees that are connected to their primary work tasks and setting up feedback loops, companies can invest time into understanding the needs of their employees instead of buying more training that will not help.

The findings will also be directly implemented in IECC, leading to an immediate practical impact. Concrete examples such as lowering the frequency of training, sharing real threat data, how to review policy feasibility and introducing live sessions can all function as examples other organisations can also learn from.

8.2.3 Relevance with the MOT programme

This research fits in the Management of Technology (MOT) programme, which addresses how technology can be used as a corporate resource to maximise productivity, profitability and competitiveness. Security awareness training can be seen as such a resource, as it is a management decision that shapes how employees make use of technology and how well the company is protected as a result.

The research also connects to the MOT programme through the organisational perspective it takes, by examining stakeholder dynamics and how organisational culture influences how technology is used within the organisation. The involvement of the CISO, change manager and employees from different departments shows the kind of inter- and intra-collaboration as emphasised by the programme.

The elective courses on cyber security also play a foundational role to this research. Those courses introduced the user-centred perspective, where users should not be seen as a problem to be fixed who get no say in how that is done, but instead as stakeholders whose needs should be central and should be accommodated. This focus underpins the entire research design, with the choice of using co-design and using the primary tasks of users as a focal point to design the training around. Behavioural change theory, with frameworks such as the FBM model and theories like bounded rationality, were also encountered through these courses.

8.3 Limitations

For this study there are several limitations to be acknowledged. First of all, purposive sampling was used to select participants with relevant experience, which allowed for in-depth insights. However, this means findings are less generalisable to a larger group beyond the sample. The external interviewees were found through personal connections and internal participants were hand-picked from three departments. The departments were chosen to try to be as representative of the entire company as possible, but there was no company wide recruitment statement. The research was also done with a focus on the Netherlands office of IECC, not with an international perspective. This could also mean a difference in results if the approach was done in a different country, as Dutch people are known to be straightforward and Dutch working culture allows for critical remarks to be made. Another aspect of doing the research in the Netherlands, meant that most of the interviews were in Dutch, with the codes and quotes being translated to English. This could have introduced slight differences in meaning, which were tried to be mitigated through making the translations as close as possible.

Another limitation was the number of people present at the brainstorming sessions. Due to planning issues, no brainstorming session was planned with participants from FLC, as their schedules did not allow for it in the time period the sessions had to be planned. For both the session with BULE and with finance one person was missing due to last-minute personal circumstances. The hybrid session was also more difficult to get the input from the person joining in online, but an effort was made to get input for the whiteboard from the person joining online and they were able to join in on the discussion. The sessions were used to validate the findings and have a discussion between participants, which did not happen for FLC in the end.

Further limitations are biases that could have been introduced in the interviews and brainstorming sessions. These may have resulted from interviewer bias as well as social desirability bias. To combat the bias, it was stressed to all participants that there were no right or wrong answers, their opinions were what mattered. There also seemed to be a culture within IECC where speaking up was desired,

so it did seem that participants were not afraid to share their honest opinions. To further help with this no names were attached to any of the results shared with the company. It was however likely still possible to deduce from some statements who said it, as the sample group of each department was either three or four people. During the brainstorm of finance there was also no manager present, which might also influence whether people feel free to share their opinions. During the session with BULE there was a manager present, but they quickly shared their honest opinion on many matters as well, making it easier for the others to speak up. This is however still a dynamic that should be kept in mind.

A last limitation to discuss is that due to the time planning of the study, some factors influencing behaviour change were deemed out of scope. This does not mean those factors are not important, they should still be addressed. This is however something to be done in future research. Measuring the effectiveness of security training was also deemed out of scope for this study, which limits how well it can be said that designing security awareness training with primary work tasks actually works.

8.4 Future research

To address the generalisability limitations, future research could replicate this study in similar engineering firms to test if the findings hold more broadly. This would also help to collect more practical examples of how training can better align with employees' primary work tasks. To address biases as well, an anonymised survey could be used to avoid possible interviewer bias from leading questions and possibly reduce desirability bias as well.

Future research could look at the factors that were deemed out of scope for this study, by looking at how company culture can be improved to promote secure behaviour. This would include aspects such as management being on board and giving employees time to behave securely. Another aspect could be that people remind each other to behave securely. Other factors that could be looked at are rewards or sanctions as external motivators and implementing triggers to remind people when to display the new behaviour.

Future research could also implement the advice found during this study on how to improve security awareness training and set up feedback loops with employees to continue the co-design process. This could help with evaluating the training and thus further validating how co-design can be used to design training aligned with primary work tasks.

9 Conclusion

This research set out to answer the question: *"How can security awareness training be designed or modified to align with employees' existing work routines and needs?"* Through semi-structured interviews and brainstorming sessions conducted within IECC, semi-structured interviews with external experts and an expert validation session, this research provides the theoretical and practical answers to this research question.

SQ1 asked how employees' primary work tasks shape their routines and information and skill needs. The findings show that digital secondary tasks are connected to the primary tasks, from which the security needs can be extracted. Someone handling invoices must send and receive emails, store sensitive documents and manage files across applications. From these tasks specific security needs follow. This connection was especially clearly seen during the brainstorming sessions, where the whiteboards showed a visual overview of the participants' primary work tasks, accompanying tasks and resulting needs. The work environment and routines are also shaped through the primary tasks, as people work out in the field, in an office environment or at a client in order to do their primary tasks. The kind of applications people use is also dependent on their primary work tasks.

SQ2 asked to what extent the current training aligns with the identified routines and needs. The findings demonstrated that current vendor-bought training aligned with more generic needs, but specific needs were left unaddressed. Employees, for example, did not know which password manager to use, were unclear on which files could be shared under privacy regulations, lacked guidelines on managing files in a shared environment and had trouble knowing what to do with emails they could not classify as phishing or legitimate themselves. Training was also focussed on phishing, whereas some participants barely used their email and had different needs. The training had also assumed an office based working environment in which e-learnings work fine, but did not take into account the routines of people working out in the field.

SQ3 asked what concrete adjustments to security awareness training can address the identified misalignments, based on input from employees and external experts. The findings were structured around factors influencing behaviour change and illustrated with practical examples from both internal participants and external interviewees. The first category, simplicity and ability, needs to be addressed before motivation, as encouraging people toward behaviours that conflict with their workflows will not work. Concretely, this means reviewing security policies for feasibility and implementing a structural feedback loop so employees can flag pain points. Training frequency should also be considered, so as not to exceed the compliance budget of employees. If this is exceeded, protesting behaviour may follow, such as employees deliberately

clicking phishing links. Multiple training methods should be offered to accommodate differences in routines and learning preferences, such as giving employees the choice between quarterly live sessions or shorter monthly e-learnings. The second category is motivation, which contains the concordance and self-efficacy factors. For concordance, organisations should share real incident data to improve risk perception, communicate through channels that reliably reach all employees, and offer multiple difficulty levels with an intake test so employees can skip content they have already mastered. Interactive and live sessions should be held to bridge the knowing-doing gap, for example by working through a real phishing incident together. For self-efficacy, advice should be actionable and role-specific, addressing the actual needs identified per department rather than providing generic guidance.

Combining these findings answers the main research question of how security awareness training can be designed or modified to align with employees' existing work routines and needs. The first step is to gather input from employees on their primary work tasks, the digital secondary tasks that accompany them, and the security needs that follow from those tasks. From the primary work tasks, the routines of employees can also be defined. The second step is to evaluate how well existing training aligns with the needs and routines identified, both by asking employees directly how well their needs are being met and by independently analysing the training as well. If the training is vendor-bought and generic, it is likely to align only with standard office routines and more generic security needs, meaning it does not align with the needs or routines of employees with specialised roles or non-standard working conditions. The third and final step is to design or redesign the training using the framework of factors, working through the prerequisites and building blocks in the order they were presented. First improving simplicity by ensuring the feasibility of policies, adjusting the frequency as needed and providing multiple training methods. Then building motivation through improving concordance and risk perception, and finally strengthening self-efficacy through actionable, role-specific advice.

Co-design serves two purposes throughout this process. It is a method for gathering employee input at each stage, from identifying needs and routines, to evaluating existing training, to refining the framework over time. It also functions as a way of building concordance. By involving employees in the process, they are more likely to accept and commit to behaviour change. Furthermore, it proved to be a way of making abstract advice from the literature more concrete, as employees and external experts contributed practical ideas for addressing the identified factors that would not have emerged from theory alone.

There are some limitations to keep in mind with this research. Due to the use of purposive judgement sampling, the findings should be interpreted within the context of this specific study and may not generalise directly to other organisations. As the brainstorming session with the FLC participants did not take place due to scheduling constraints, the validation of the results for that department is limited. Future research could replicate the study in similar contexts in order to test how well the findings generalise. Other future research could look at implementing the findings and including the factors that were deemed out of scope for this research, namely organisational culture, rewards and sanctions and environmental triggers.

Bibliography

[1] Anne Adams and Martina Angela Sasse. “Users are not the enemy”. In: *Communications of the ACM* 42.12 (1999), pp. 40–46. DOI: https://doi.org/10.1145/322796.322806.

[2] Bader Alkhazi et al. “Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior”. In: *IEEE access* 10 (2022), pp. 132132–132143. DOI: https://doi.org/10.1109/ACCESS.2022.3230286.

[3] Abdullah M. Alnajim et al. “Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches”. In: *Symmetry* 15.12 (2023), p. 2175.

[4] Debi Ashenden and Darren Lawrence. “Security dialogues: Building better relationships between security and business”. In: *IEEE Security & Privacy* 14.3 (2016), pp. 82–87. DOI: https://doi.org/10.1109/MSP.2016.57.

[5] Jeremy Burke et al. “Can educational interventions reduce susceptibility to financial fraud?” In: *Journal of Economic Behavior & Organization* 198 (2022), pp. 250–266. DOI: https://doi.org/10.1016/j.jebo.2022.03.028.

[6] Albesë Demjaha, Simon Parkin, and David Pym. “The boundedly rational employee: Security economics for behaviour intervention support in organizations”. In: *Journal of Computer Security* 30.3 (2022), pp. 435–464. DOI: https://doi.org/10.3233/JCS-210046.

[7] Jacqueline M. Drew. “A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies”. In: *Journal of Criminological Research, Policy and Practice* 6.1 (2020), pp. 17–33. DOI: https://doi.org/10.1108/JCRPP-12-2019-0070.

[8] Jacqueline M. Drew and Lucy Farrell. “Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs”. In: *Police Practice and Research* 19.6 (2018), pp. 537–549. DOI: https://doi.org/10.1080/15614263.2018.1507890.

[9] Brian J. Fogg. “A behavior model for persuasive design”. In: *Proceedings of the 4th international Conference on Persuasive Technology*. 2009, pp. 1–7. DOI: https://doi.org/10.1145/1541948.1541999.

[10] Katrina G. Heijne and Han van der Meer. *Road Map for Creative Problem Solving Techniques: Organizing and facilitating group sessions*. Boom Uitgevers, 2019. ISBN: 9789024401116.

[11] Cormac Herley. “More is not the answer”. In: *IEEE Security & Privacy* 12.1 (2013), pp. 14–19. DOI: https://doi.org/10.1109/MSP.2013.134.

[12] Jonas Hielscher and Simon Parkin. “"What keeps people secure is that they met the security team": Deconstructing drivers and goals of organizational security awareness”. In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 3295–3312. URL: https://resolver.tudelft.nl/uuid:aa1273a2-46f9-4187-9ffe-de09a2a1000d.

[13] Jonas Hielscher et al. ““Taking out the trash”: Why security behavior change requires intentional forgetting”. In: *Proceedings of the 2021 New Security Paradigms Workshop*. 2021, pp. 108–122. DOI: https://doi.org/10.1145/3498891.3498902.

[14] Jonas Hielscher et al. “Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors’ Promises”. In: *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 2024, pp. 2666–2680. DOI: https://doi.org/10.1145/3658644.3690196.

[15] Grant Ho et al. “Understanding the efficacy of phishing training in practice”. In: *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2025, pp. 37–54. DOI: https://doi.org/10.1109/SP61157.2025.00076.

[16] Mannat Kaur et al. “Human factors in security research: Lessons learned from 2008-2018”. In: *arXiv preprint arXiv:2103.13287* (2021). DOI: https://doi.org/10.48550/arXiv.2103.13287.

[17] Iacovos Kirlappos, Simon Parkin, and Martina Angela Sasse. “Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security”. In: 2014. DOI: https://doi.org/10.14722/usec.2014.23007.

[18] Maaike Kleinsmann and Rianne Valkenburg. “Barriers and enablers for creating shared understanding in co-design projects”. In: *Design studies* 29.4 (2008), pp. 369–386. DOI: https://doi.org/10.1016/j.destud.2008.03.003.

[19] Aleksandra Kuzior et al. “Cybersecurity and cybercrime: Current trends and threats.” In: *Journal of International Studies (2071-8330)* 17.2 (2024).

[20] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. “Phishing in organizations: Findings from a large-scale and long-term study”. In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2022, pp. 842–859. DOI: https://doi.org/10.48550/arXiv.2112.07498.

[21] Jack Mezirow. “Transformative learning theory”. In: *Contemporary theories of learning*. Routledge, 2018, pp. 114–128.

[22] Benjamin Reinheimer et al. “An investigation of phishing awareness and education over time: When and how to best remind users”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 2020, pp. 259–284.

[23] Marlies Sas et al. “The impact of training sessions on physical security awareness: Measuring employees’ knowledge, attitude and self-reported behaviour”. In: *Safety science* 144 (2021), p. 105447. DOI: https://doi.org/10.1016/j.ssci.2021.105447.

[24] Martina Angela Sasse et al. “Rebooting IT security awareness–how organisations can encourage and sustain secure behaviours”. In: *European Symposium on Research in Computer Security*. Springer. 2022, pp. 248–265. DOI: https://doi.org/10.1007/978-3-031-25460-4_14.

[25] Bruce Schneier. “Secrets and Lies: Digital Security in a Networked World”. In: *Info - The journal of policy, regulation and strategy for telecommunications* 5 (Jan. 2003). DOI: https://doi.org/10.1002/9781119183631.

[26] Bruce Schneier. “The psychology of security”. In: *International conference on cryptology in Africa*. Springer. 2008, pp. 50–79.

[27] Diana Ussher-Eke. “From Awareness to Action: Designing effective cybersecurity training programs”. In: *International Journal of Science and Research Archive* 16 (2023), pp. 494–504.

[28] Monica T. Whitty. “Transformation Learning Theory for Cyber Security”. In: *The Festschrift Symposium* (2026).

[29] Theodore Zamenopoulos and Katerina Alexiou. *Co-design as collaborative research*. Bristol University/AHRC Connected Communities Programme, 2018.

[30] Tianjian Zhang. “Knowledge Expiration in Security Awareness Training”. In: *Annual ADFSL Conference on Digital Forensics, Security and Law*. Association of Digital Forensics, Security and Law, 2018. URL: https://commons.erau.edu/adfsl/2018/presentations/2.

10 Appendix

10.1 AI usage

For this thesis, AI was used for multiple things. ChatGPT was used to generate the image on the title page, where it was given the title of the study, asked to incorporate co-design and to make it in blue hues. Both ChatGPT and Claude were used for improving the flow of specific sentences, as well as for checking for grammar mistakes. Claude was also used to generate latex formatted tables, as most of the tables were created in Excel or Word, since the Overleaf table interface is not intuitive to work with.

Important to note, interpretations, conclusions and any other idea generation were not done by AI. All original content was my own work, AI was used for language correction and formatting only.

10.2 Dutch interview protocol

Openingsvragen (Warm-up)

- Zou je jezelf kort kunnen introduceren? Denk hierbij aan je rol en op welke afdeling je werkt.

Primaire werktaken en routines

- Wat zijn je belangrijkste werkzaamheden?
- Doorvragen: Denk aan je dagelijkse taken; wat zijn de verantwoordelijkheden die je hebt?
- Hoe ziet je dagelijkse werkomgeving eruit? Denk hierbij bijvoorbeeld aan waar je werkt, hoe de werkomgeving eruit ziet, welke applicaties je gebruikt, etc.

Informatie- en vaardigheidsbehoeften

- Op welke manier is security een onderdeel van je dagelijkse werkzaamheden?
- Met wat voor soort security problemen denk je te maken kunnen krijgen tijdens je werk?
- Loop je weleens tegen security-issues aan waarbij je het gevoel hebt dat je meer kennis of training nodig hebt om ze goed op te lossen?

Huidige trainingen

- Welke security awareness trainingen (indien van toepassing) heb je gevolgd bij IECC?
- Wat is je mening over de huidige security awareness trainingen binnen IECC?
- In hoeverre sluiten de huidige trainingen aan bij jouw behoeften op het gebied van kennis en vaardigheden?

Voorkeuren voor trainingsmethoden

- Aan welke trainingsmethoden geef je de voorkeur? (Bijv. e-learning, fysieke workshops, korte video's).
- Waarom geef je de voorkeur aan deze methoden?
- Welke manier van lesgeven of trainen vond jij buiten security training erg prettig, en waarom vond je het zo prettig?

Afsluiting

- Is er nog iets wat je zou willen toevoegen, wat voor je gevoel nog niet besproken is omtrent cyber security?

10.3 Brainstorm session plan

Goal session

- Check if link primary work tasks and needs is as I think it is from the interviews (to validate results)
- Brainstorm will be on which tasks people have and where there are similarities in needs (to validate and possibly find new ones. Also with the goal in mind that a balance between tailoring and feasibility has to be maintained)

Line of thought: ask people individually what they do in interviews, see which similarities there are, then check in group setting if those are true and if there are more missing

- Idea generation of kinds of training people might like, both in terms of fit with preferences and fit with routine
- With prompting questions to see which ones fit better within routines
- Also use ideas gotten from outside of IECC to keep the flow going and have people create new ideas

Line of thought: if you are looking for ways to design trainings that fit with routines and needs of people, asking them their opinions on it is valuable input.

Session outline

- Introduction (10 minutes)
  - Introduce session outline and goals
  - Explain some concepts
- Validation and Idea generation on primary tasks and needs (45 minutes)
  - *Explain brainwriting (5 minutes)*
  - **Brainwriting**: Check and add primary work tasks (8 minutes)
  - *Explain clustering (2 minutes)*
  - **Clustering**: primary work tasks (5 minutes)
  - **Brainwriting**: Check and add digital work tasks (8 minutes)
  - **Clustering**: digital work tasks (5 minutes)
  - **Brainwriting**: Check and add security needs (8 minutes)
  - **Clustering**: security needs (5 minutes)
- Validation and Idea generation on types of training (35 minutes)
  - Brainwriting: check and add training methods (20 minutes)
  - Clustering: training methods (8 minutes)
  - Explain and do hits and dots (7 minutes)

Introduction

- Show session planning
- Explain that the goal is to gather security needs from primary work tasks and ideas for training and validate what was already found
- Show the creative diamond:
  - **Diverging**: coming up with as many ideas as possible
  - **Reverging**: organizing the ideas generated to prepare for converging
  - **Converging**: choosing which ideas we like best
- Each of these steps has methods we can use and certain rules and mindsets that accompany them. I will explain those as we get to each step.

Problem statements

(these statements were used to guide people when coming up with ideas)

How can we directly link our primary daily tasks to our security needs so training can address this?
Hoe kunnen we onze dagelijkse hoofdwerkzaamheden direct koppelen aan de veiligheidsbehoeften zodat training zich daar op kan richten?

How can we create training experiences that match our daily work routine / are exciting to participate in / match my learning preferences?
Hoe kunnen we trainingservaringen creëren die aansluiten bij ons dagelijkse werkroutine / enthousiasmerend zijn om aan deel te nemen / passen bij hoe ik graag kennis tot me neem?

Diverging: brainwriting

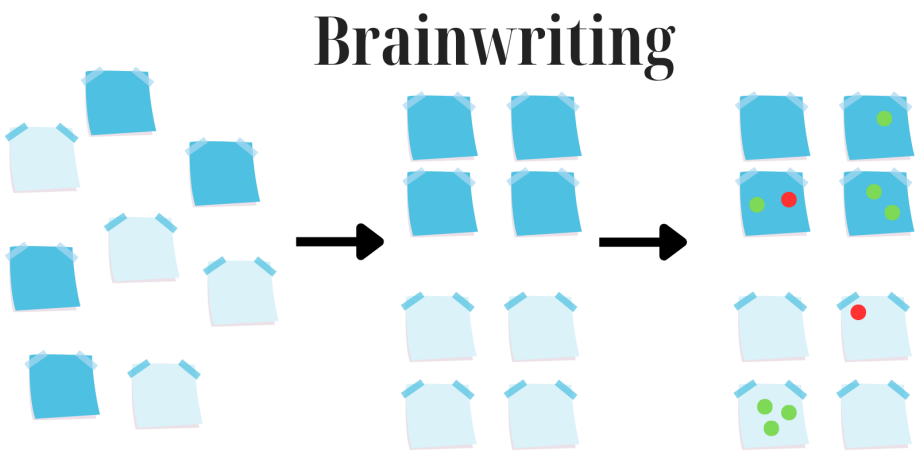

Figure 10.1: Visual of creative technique brainwriting, clustering and hits and dots

We are going to use the technique of brainwriting with post-its for the diverging on the problem statement. How does that work?

- Everyone gets post-its to write on, try to write clear and in capital letters (easier to read from a distance)
- Stick the notes in a way everyone can read them
- And keep the rules in mind! (I will guide this part)

Some things are important to keep in mind here:

- **Postpone judgement**: you may judge ideas at some point, but **not now**
  - Makes people more confident and fluent in generating ideas
- Rules:
  - **Quantity breeds quality,** write out everything! You usually have 3 waves of ideas, common > unusual/silly > novel
  - **Hitchhike**, look at other ideas and try to go off that. Use your associative thinking, maybe also combining multiple ideas present
  - **Freewheel**, there are no wrong answers and also do not point out "wrong" things of others. Maybe the spelling mistake between snow and show gives you new ideas!

(Dutch for during the workshop)

- **Oordeel uitstellen:** je mag ideeën op een gegeven moment beoordelen, maar nu niet
  - Dit maakt mensen zelfverzekerder en vloeiender in het genereren van ideeën.
- **Kwantiteit leidt naar kwaliteit,** schrijf alles op! Je hebt meestal 3 golven van ideeën: alledaags > ongebruikelijk/raar > vernieuwend
- **Meeliften,** kijk naar andere ideeën en probeer daarop verder te bouwen. Gebruik je associatieve denken, en combineer misschien ook meerdere aanwezige ideeën.
- **Freewheelen,** er zijn geen foute antwoorden en wijs ook niet op "foute" dingen van anderen. Misschien geeft de spelfout tussen *plan* en *plant* je wel nieuwe ideeën!

Reverging: clustering

We will use the clustering technique, move post-its together that you feel are similar. This is an iterative process, so just move them in a way that feels right. It can always be moved later.

Rules of reverging:

- **Be jointly active**, this is a group process, so everyone should be moving post-its
- **Listen responsively**, understand why people might want to move certain post-its together
- **Move circulatory**, just start somewhere. Post-its might be moved later, that is completely fine

(Dutch for during workshop)

- **Wees samen actief,** dit is een groepsproces, dus iedereen zou dus post-its moeten verplaatsen
- **Luister responsief,** begrijp waarom mensen bepaalde post-its bij elkaar willen voegen
- **Beweeg circulerend,** begin gewoon ergens. Post-its kunnen later altijd nog worden verplaatst, dat is helemaal prima

Converging: hits and dots

We will use the "hits and dots" technique for this step. You are given a certain amount of "hits" to place on ideas you like and think are good/most relevant. Then you are also given one or two dots to place on an idea you find really novel. After we placed all the dots, we take a look at the post-its that got the most hits/dots.

Rules:

- **Protect originality**: you will likely want to go for the more common and reasonable idea, but this can quickly filter away any novel ideas!
- **Trust your gut:** if you like an option, go for it. It does not need a rational reason for it right away!

- **Have action in mind:** keep in mind the problem you are trying to solve, what is this idea supposed to do?

(Dutch for during workshops)

- **Bescherm originaliteit**: je zult waarschijnlijk willen kiezen voor het meer gangbare en redelijke idee, maar dit kan vernieuwende ideeën al snel wegfilteren!
- **Vertrouw op je gevoel:** als je een optie leuk vindt, ga er dan voor. Het heeft niet meteen een rationele reden nodig!
- **Houd actie voor ogen:** houd het probleem dat je probeert op te lossen in gedachten; wat hoort dit idee te doen?

10.4 Expert validation session plan

Factors influencing effectiveness of training

Motivation: *(people want to do it)*

- **Concordance**: people are committed to change
- **Self-efficacy**: people feel confident in their ability to do the new behaviour successfully
- **Rewards/sanctions:** external motivators, where people are rewarded for doing the behaviour and sanctioned for not doing it

Simplicity/Ability: *(make it easy to do)*

- **Time:** amount of time it takes to do the behaviour
- **Physical effort:** amount of steps a person must take to do the behaviour
- **Mental effort:** amount of energy it costs to do the behaviour
- **Organisational culture:** does everyone do the behaviour or is it accepted not to do it
- **Routine:** people have a way of working and like to stick to it

Trigger/Opportunity: *(make it known when to do it)*

- **Environmental trigger:** trigger that reminds people to behave securely

Each of these factors can be an enabler or a blocker, in an ideal world all are enablers.

Some things have to be in place before other blocks make sense to address. Without those being in place, it won't work. Policies must be doable first and fit with how much time can and are willing to spend. Then you have to motivate people to want to do it and only then is it useful to actually ensure they have the skills needed to do it.

Session planning

- Introduce the different training blocks and session (5 min)
- Simplicity / ability (20 min)
  - Time / effort
  - Culture
  - Routine
- Motivation (30 min)
  - Concordance
  - Self-efficacy
  - Rewards/sanctions
- Environmental trigger (5 min)

Simplicity

Time / effort

Review policies on do-ability, try to reduce friction and to stay within compliance budget.

- **From colleagues:**
  - **Finance:** lot of time lost getting permission or documents from people in order to check project finances. Wanting to ask colleagues if an invoice is legitimate, but should not send potential phishing to others.
  - **BULE:** don't always lock screen as Outlook becomes slow when doing so. Should not use public wifi, but finance gets mad when your data bill is too high from using a hotspot.
  - **FLC:** share pin code laptop as they need to work on same laptop, but need to lock it at the client.
- **From external interviews:** advice to avoid overwhelming users, possibly use a feedback loop to figure out where the pain points are.
- **From research:** before secure behaviour can be achieved, you have to ensure the behaviour you want people to do is doable. If you do not, people will find ways around it, refuse to comply at all or set up shadow security, which might still be insecure while they believe they are behaving securely.

Lower the frequency of the phishing simulations to once a month or once every two months.

- **From colleagues:** liked this way of practicing, but not the frequency. Were now sometimes missing legitimate emails out of fear of clicking on phishing or heard of people protesting by clicking on links on purpose.
- **From external interviews:** most companies do it only once or twice a year, and only use it as a form of testing, not training.
- **From research:** repetition is important, but a single reminder helps people retain the information for at least 3 months, so a reminder every two weeks is not needed.

Culture

Not something that can be quickly addressed with training, but a factor which is important for behaviour change. Think of things such as c-level and management support, freeing up time to behave securely, people holding each other accountable to behave securely or the general feeling in the company being that you should behave securely.

An example I heard from some people is that they address people who do not lock their screens, but also heard from some they do not always lock it themselves. I also heard from almost everyone that due to work pressure there is not always time to work securely.

Routine

Have different options of training methods to fit with people's routines.

- **From colleagues:**
  - **Finance:** like e-learning, does not take much time and can be planned when it fits.
  - **BULE:** liked the plannability of e-learnings, but think live sessions can help with motivation.
  - **FLC:** would like live sessions, e-learnings do not fit their work context of working outside all day and they learn better from doing.

- **From external interviews:** make use of multiple methods to better fit the needs of employees with different learning styles and helps with repetition of content to better understand it. (Ex. Posters in building, intranet posts, security community, e-learning, onboarding training, phishing simulations, giving presentations to specific departments and c-level announcements.)
- **From research:** people have different ways in which they learn new things, do be careful as more is not the answer. Give them the option to choose which they want to do instead of only stacking trainings.

Motivation

Concordance

Share actual threats and numbers of incidents with colleagues to improve the risk perception and need for secure behaviour.

- **From colleagues:** interested in knowing what kinds of threats IECC really faces, think it would help with motivation to behave more securely when you know why you should do so. That people currently do not quite understand the kind of risks there are.
- **From external interviews:** when sharing the kind of threats they face or the results of the phishing simulation they found people were engaging with the topic a lot. Either by talking about it in person, discussing it on the intranet or coming up to the security team to talk about it.
- **From research:** people often discount the risks. They think it will not happen to them or does not happen close to them. Showing the risks can help shift this perspective. Also, in general concordance building is shown to help people actually change behaviour instead of forcing compliance.

Have multiple levels of difficulty of the training to challenge the people who would like that and accommodate people who want easier training.

- **From colleagues:**
  - **Finance:** liked how doable the training was.
  - **BULE:** most people found the current level of training too low, resulting in training being put on in the background. Would like it to be able to do a test to skip easier levels.
  - **FLC:** some liked how doable the training was, some got demotivated having to do training that did not feel challenging.
- **From external interviews:** trying to motivate people through interest, for example by making it challenging.
- **From research:** ideally you first assess the level of knowledge a person has before doing training, as they do not need to be taught what they already know. You want to spend time on teaching people what they need to know still.

Accommodate and promote interaction (in training) between colleagues to discuss security topics to learn from each other.

- **From colleagues:**
  - **Finance:** do think that sometimes knowing is different from doing, doing a workshop, case or simulation exercise can thus help with actually being able to do things instead of only knowing you should do it.

  - **BULE:** think a lot of new perspectives come up when you discuss things with people that you would not have thought of otherwise.
  - **FLC:** the way they prefer to learn things.
- **From external interviews:** find it can make waves in helping to improve culture as well. For example have a security community that come together every couple of months to discuss new security topics during a pizza evening. They bring back what they talked about to their teams.
- **From research:** adults learn differently than children, they have their own experiences and frame of knowledge which shapes how they perceive knowledge. They often learn better from personal experiences, which interactive training can provide.

Have clear communication on what the training is, what it is for and the timeline of the training.

- **From colleagues:** they would like to have clear communication on what they can expect in terms of training. Some examples here are that people thought the training was only phishing training due to the name. Or that people did not expect the training and thought it was phishing, so only later when colleagues told them it was legit did they do it.
- **From external interviews:** some companies try to make sure the lay-out, colours and tone of the email and training matches the company style to make it more familiar for people.
- **From research:** delivery of training often goes wrong, which can lead to it not reaching people, people not understanding the training or people ignoring it.

Self-efficacy

Tailor the advice more to IECC specific policies and what people actually wish to know.

- **From colleagues:**
  - **Finance:** want to know how to deal with suspecting phishing emails that could also be legitimate. Also want to know which documents can be shared privacy legislation wise.
  - **BULE:** want to know how to safely share and handle files, felt like some clear company guidelines on this were missing.
  - **FLC:** want to know how to keep laptop safe from physical threats in a way that fits their work processes.
  - **General:** people did feel they could spot phishing emails now. Without making advice explicit however, people find it difficult to follow. Ex. people do not make use of password managers as they do not know how they work and are afraid of it failing them.
- **From external interviews:** do be careful to communicate more specific advice to people in a way that it only reaches them, otherwise it confuses people who the advice or warning is not for.
- **From research:** vendors cannot provide tailored advice, or the price would be so high no one wants to pay for it. Tailoring advice to the organization can however help make actual behaviour change possible, as people need to feel they have the skills and knowledge to do the actual behaviour.

Rewards/sanctions

External motivators can also be used, such as rewards for behaving securely or reporting incidents, or sanctions for failing to do trainings or not behaving securely. You do have to be careful with sanctions, as you might run the risk of having to play police to enforce things.

Some rewards that people mentioned were providing food during trainings to have more people show up or displaying a 'catch' of the week on TVs next to the coffee machines to show how well someone spotted a potential risk.

Environmental trigger

Not directly related to training, but more related to reminding people to behave securely.

Some people from FLC for example noted that as they rarely use Outlook, it can be nice to have a reminder to be careful for phishing, as it is not part of their daily operations.

10.5 Codebook interviews in IECC

Table 10.1: Codebook SQ1

Theme	Category	Code
Primary work tasks	Task: financial check	Giving advice
		Keeping the broad picture of projects
		Checking if hours are well utilised
		Financial control of projects
		Cost price determination
		Discussing finances
		Understanding what lies behind financial figures
	Task: handling invoices	Forwarding invoices to creditors
		Creating invoices
	Task: project management	Solving ad hoc problems
		Communication with external parties
		Registering for tenders
		Helping out with project
		Monitoring and guiding projects
		Writing quotes
		Coordinating project
		Preparing projects
		Preparing outdoor spaces for companies
	Task: Designing and modelling	Making a digital design
	Task: saving data measurements	Data stored on p-drive (shared network drive)
		Data is initially stored locally
		Data from equipment to laptop
		Field measurement reports
	Task: measurements in the field	Installing measurement equipment
		Performing measurements at client
		Preparing measurements
		Bringing samples to the office
		Working process together on one laptop

Theme	Category	Code
Secondary tasks	Secondary Task: sharing files	Sharing files in different ways
		Shared environment with multiple parties
		Data in multiple locations
		Sometimes sending files to externals
		T-drive shared network drive in file explorer
		Fragmented communication places
	Secondary task: email communication	Internal email traffic
		Lab analysis on email
	Secondary Task: managing (sensitive) files	Laptop contains data from multiple clients
Security need	Share files securely	How to share documents securely
		Sloppiness sharing sensitive documents
		Not using WeTransfer
	Handling phishing	Tendency to click if email applies
		Never received phishing simulation emails
		Phishing emails can be very good
		Report phishing emails
		Easily spot bad phish
		Clicking faster when not much involved
		Confidence in being able to spot phishing
		Clicking on a link without thinking
	Secure laptop	Externals who can access laptop
		No client wifi
		Laptop not unattended
		Locking laptop at client
		Less risk when not connected to internet
	Manage files securely	File management
		Shielding sensitive files
Work context	Analog to digital	Important papers in separate container
		Remembering better by working on paper
		Digital files easier to steal
		Meanwhile, all work is digital
	Application	CAD
		Excel
		Maconomy (financial application)
		Outlook
		PowerPoint
		Teams
		Word
	Trusting colleagues	Being able to trust colleagues
		Conflict between helpfulness and security
		Internal financial risk
		Monthly check mitigates risks
	Mail environment	Colleague did receive a real phishing email

Theme	Category	Code
		Many emails daily
		Few real phishing emails
		Few emails
	Roles	Business controller
		Contract manager
		Lead designer
		Project administrator
		Project controller
		Project coordinator
		Project manager
		Team leader
		Team manager designers
		Field worker
		Road designer
	Field worker laptop use	Only entering data on laptops
		Internet connection via data sim
		Opening outlook rarely
		Weather-resistant laptops
	Work environment	At the client's office
		Almost never at the office
		In the field
		Office and home
		Picking things up by being at the office
		More concentration at home
		Always works at the office

Table 10.2: Codebook SQ2

Theme	Category	Code
Importance of training	Importance of security awareness training	Begrudgingly sees need for training
		Experienced incident
		Major consequences of a hack
		Anyone can fall for it
		Not wanting to be the one who clicks
		News about data leaks
Feedback on current training	Communication about training	Communication about training needed
		Feeling supported is important
		Reminder email about existence of training is good
		Info must be easy to find
		No response from input
		Unworkability not shared

Theme	Category	Code
		'Phish' in name makes people think of phishing training
		Better agreements on communication design
	Effect of current training	More observant than before
		Forgot onboarding training
		Training report on bad habits
		Never used phishing report button
		Private and work safe working
		Fright from simulation click makes more observant
		Training helps awareness of multiple issues
	Fed up with training	Bothered by too much training
		Deliberately clicking in protest
	Happy with current methods	E-learning nice setup
		Simulations are good training
	Content of current training	Focus on mail, misses other attack vectors
		Current simulated phish is simple
		Content is obvious
		Training content not focused on work
		Sometimes new knowledge through training
		Obvious questioning
	Motivation for training	Rewarded for doing extras
		No interest in security
		Creating motivation through method
		Motivation through interest
		Remind team to do training
		Mandatory safe working
	Besides content, training helps awareness	Research itself creates awareness
		Training helps awareness
	Risk of phishing simulations	Ignoring while it is legitimate
		Distrust due to too many simulations
	Simple training	Training understandable for everyone
		Doing training quickly
		Training on in the background
		Training to do in between
		Without a challenge, people don't pay attention
	Trainings completed	Doing training because it is mandatory
		Does training on platform
		Did not do training on platform
		Training outside platform
	Design of current training	E-learning matches digital subject
		E-learning possible, but working independently is difficult

Theme	Category	Code
		Interface sometimes does not work
		Too many simulation emails
	Interaction desired	Only presentation is boring
		Curious about others' experiences
		E-learning not interactive enough
		Without interaction, people keep working

Table 10.3: Codebook SQ3

Theme	Category	Code
Why security is ignored	No time for secure working	Balance between workability and security
		Busyness, work comes first
		Security getting in the way of work
		Working securely costs a lot of time and energy
	Little self-efficacy	Fear of losing technological help
		Older people have more trouble learning
		Technology changes quickly
		Not an expert myself
	Ignoring security policy	Not locking screen
		Password impossible to remember
		Ignoring impractical security advice
		Shadow security password management
		Reusing password
Ideas content training	Advice on secure working	Think before sharing
		Calling IT when in doubt
		Not too many side issues
		Not expected, ignore it
		More specific advice
		Password manager
	Case ideas	Targeted phishing email
		Tailgating simulation
	Digital footprint	Email address known on dark web
		Info on internet used to build trust
		Not knowing what is public
		Being careful about what you share
	Practical examples	Current risks
		Sharing real incidents
	Working method unclear	Company policy needed
		No clear guideline for working method
		Difficult to know what to do about tailgating
		Misses training on personal data online
		Unclear what to do after a misstep

Theme	Category	Code
		Unclear what confidential data is
		Procedure for reporting phishing needed
Ideas methods training	Timing of training	Everything live at once instead of split up
		E-learning only possible in quiet periods
		Joint meeting can be scheduled
		Giving choice between e-learning or live
		Live causes bigger interruption to work
	Different learning methods	Multiple forms of training
		Different levels
	Practical assignments	Case, interaction
		E-learning, interactive
		Learning by doing
	Ideas for training methods	Being able to report incidents
		Short to keep attention
		Spear attack simulation
		Training on basics, e-learning for exceptions
	Discuss training live	Discuss training with each other
		Live training
		Live, interactive
		Game with two groups against each other
		Training during the week start

10.6 Codebook interviews outside of IECC

Table 10.4: Codebook

Category	Code
Base level of awareness	After standard training tailor it
	High base awareness
	Mandatory participation
Company aimed behaviour	Be aware of context and situation
	Confidence in failsafes
	Improve click rate phish emails
	Improve security culture
	More secure mindset
	Not afraid but aware
Company motivation to do training	Goal to improve actual bad behaviour
	Laws mandating yearly training
	Shared responsibility security
Content of training	10 golden rules
	AI and deepfake knowledge
	Changing threat landscape

Category	Code
	Phishing simulation content
	Physical cyber threats
	Sensitive data access
	Showcase real incidents
Development of training	Created training themselves
	Platform bought, altered content
	Tooling used, made content
	Vendor bought, no alterations
Effectiveness metrics	Click through rate
	Engagement
	Reported incidents
	Visualize effectiveness
	Vulnerabilities dropped
Fit with needs	Balance difficulty level
	Different learning styles
	Different risk profiles
	Differentiate training between departments
	Engaging employees
Fit with routines	Convenient daily use
	Familiar lay-out
Ineffective training	checkbox security
	Delivery issues
	Little time to do training
	Specialized info given to everyone
	Too many policies
Resources considerations	Expenses considerations
	Time efficient
Training development advice	Avoid overwhelming users
	Avoid shaming
	Follow up is needed
	Interactive training
	Repetition is needed
	Tailored to the organization
	Technology helps security
	Use local language
	Use multiple training methods
Training methods	Awareness through e-learning
	Awareness through phishing campaign
	C-level announcement
	Different ways to make info available
	Gamification
	Give presentation
	Interaction with collegues on topic
	Small gimmicks
Types of employee input	Direct conversation

Category	Code
	Engagement on posts
	Group discussion
	Reporting incidents
	Security community
	Survey
Types of motivation	Explain the need
	Motivation through interest
	Scare factor
Usage of employee input	Allow own sharing of topics
	Alter content training

10.7 Brainstorming whiteboards

For each of the sessions the whiteboards have a before and after version, so it can be seen which ideas already came from the interviews and which ones were brought up during the session. The ideas from the interviews, for which the goal was to validate them, are made bold in the 'after' session whiteboards.

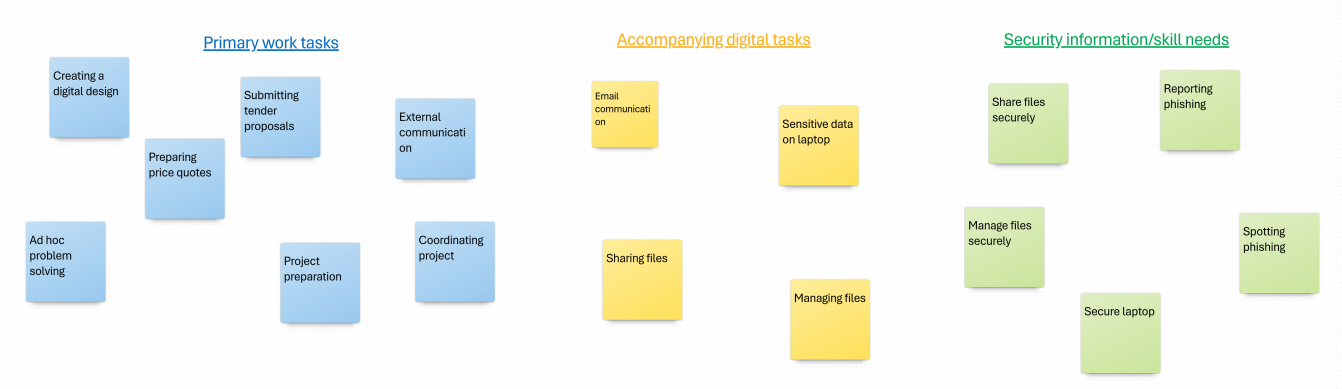

Figure 10.2: Whiteboard of primary tasks BULE before the session

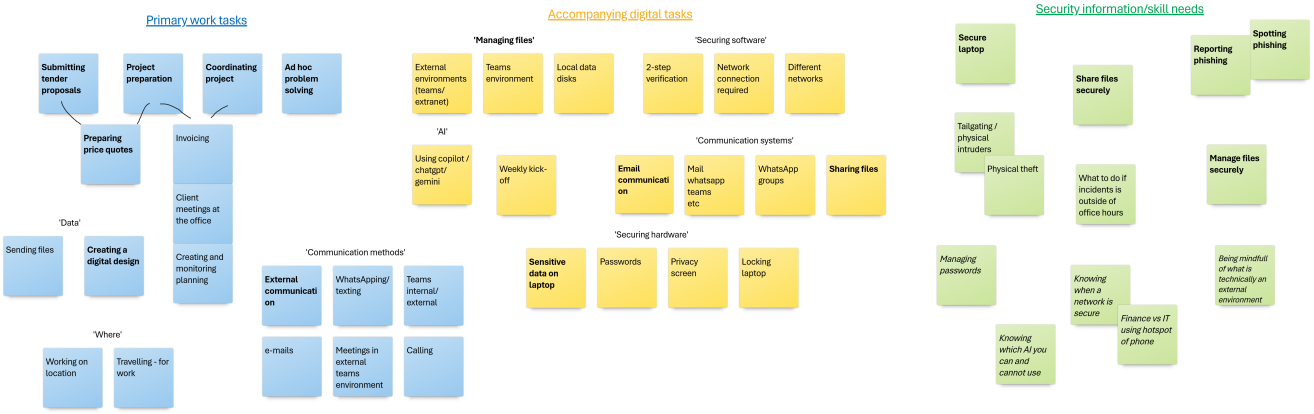

Figure 10.3: Whiteboard of primary tasks BULE after the session

In figure 10.3, it can be seen that some of the notes are in italics. This was done as these ideas were discussed, but not written down as such during the session itself. The session was done with limited time and there was a natural bridge in the session to discussing the training methods. The security needs were already discussed, as such the choice was made to continue before writing everything down.

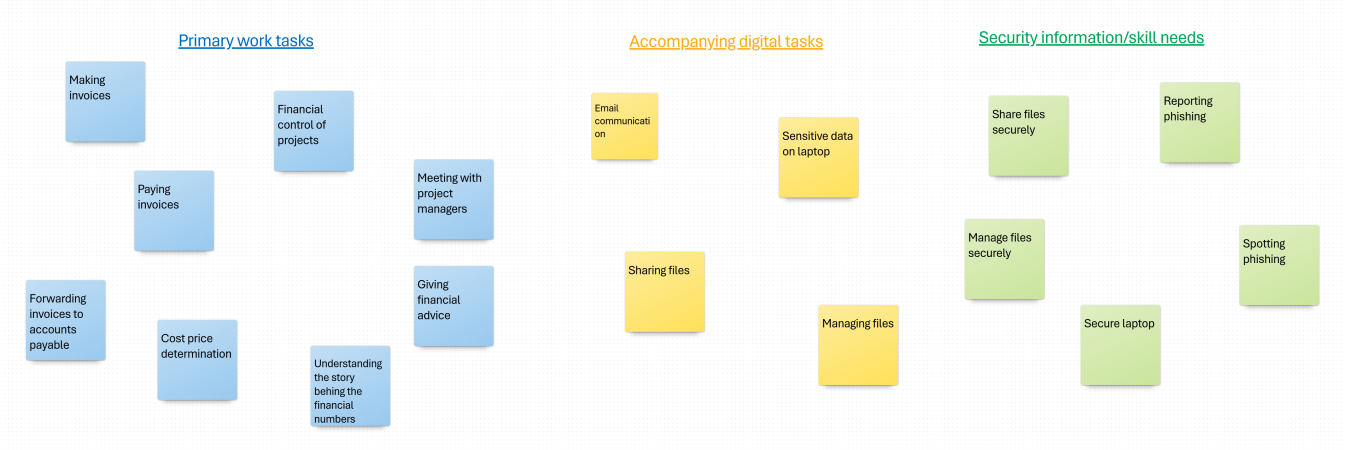

Figure 10.4: Whiteboard of primary tasks finance before the session

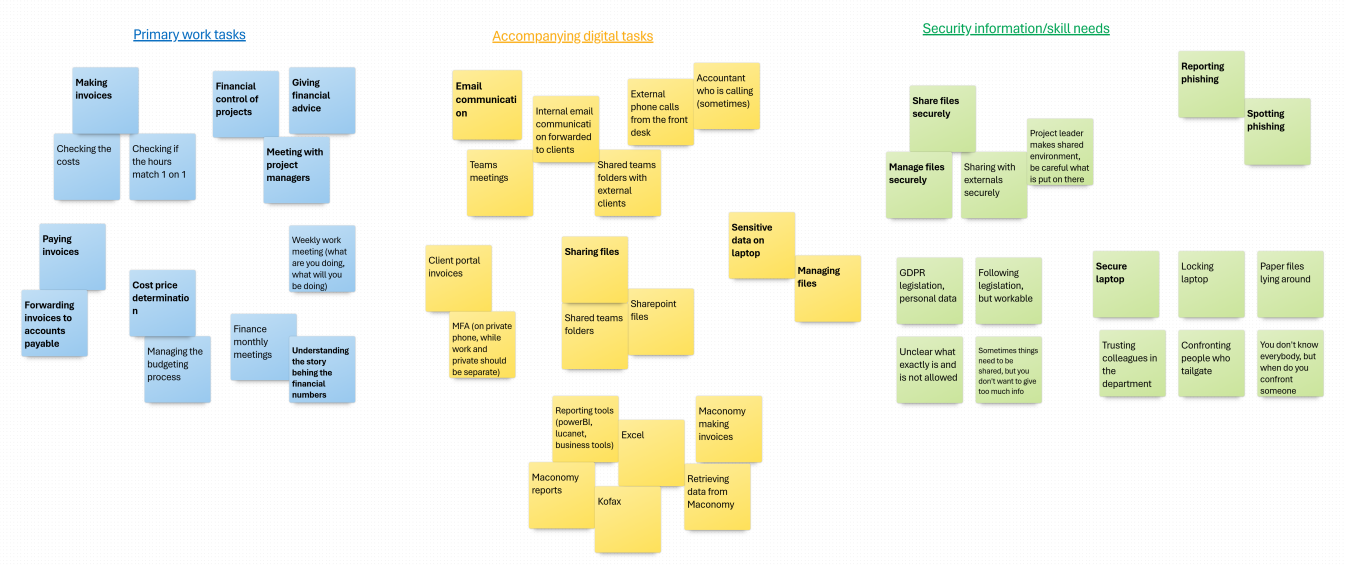

Figure 10.5: Whiteboard of primary tasks finance after the session

To clarify some of the accompanying digital tasks in figure 10.5, Maconomy is the financial application that is used to create invoices, bill hours, register hours and create financial reports. It holds most of the financial data that finance employees have to work with. Kofax is a similar digital financial tool.

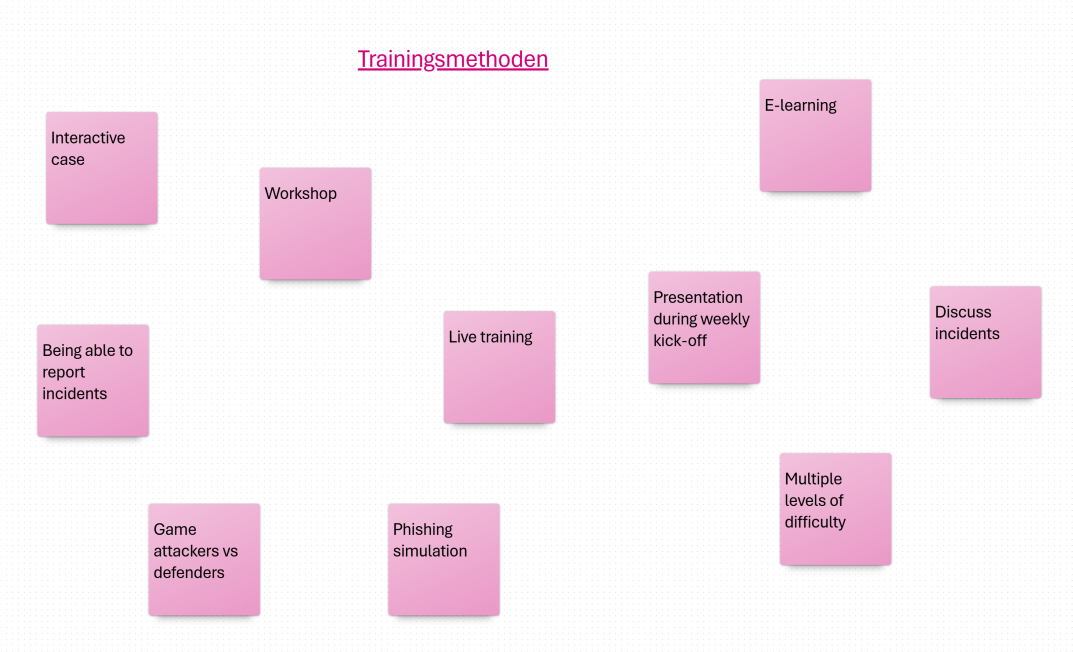

Figure 10.6: Whiteboard of training methods before the session

For the training methods sessions, participants were asked to put hits and dots on the sticky notes. Hits are shown as hearts, which they could put on ideas that just had a gut response of being liked. Dots were put on ideas that they thought would fit their routines or needs best, shown as stars.

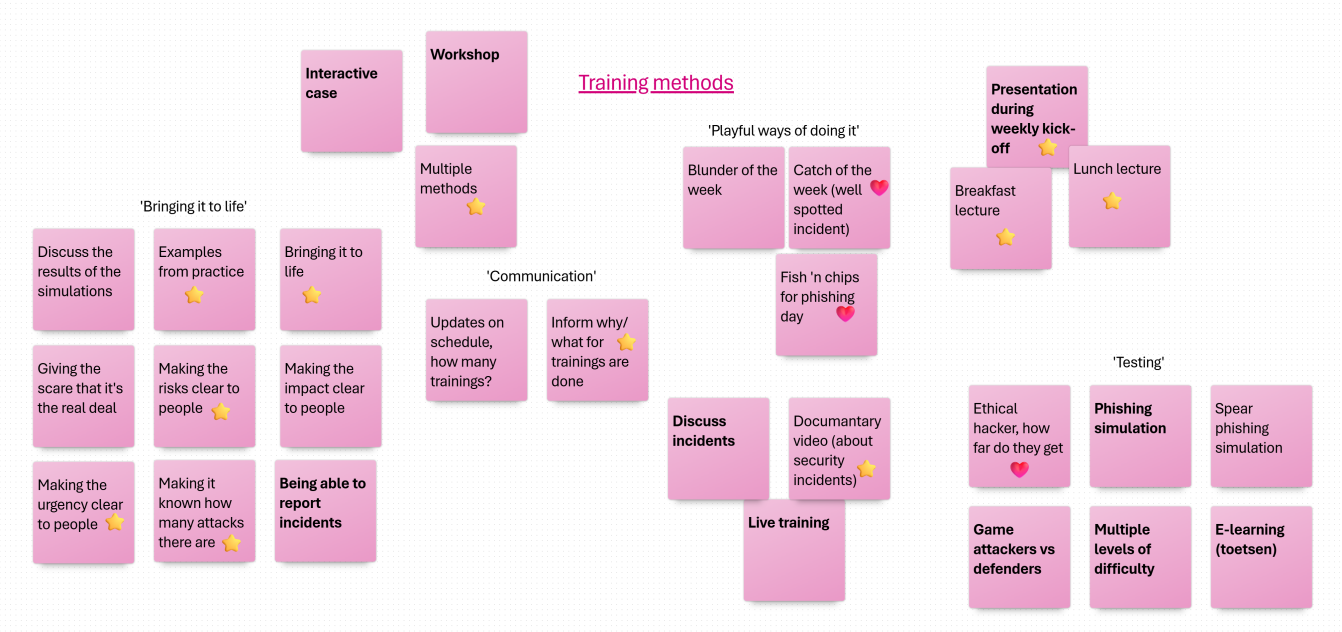

Figure 10.7: Whiteboard of training methods after the session with BULE

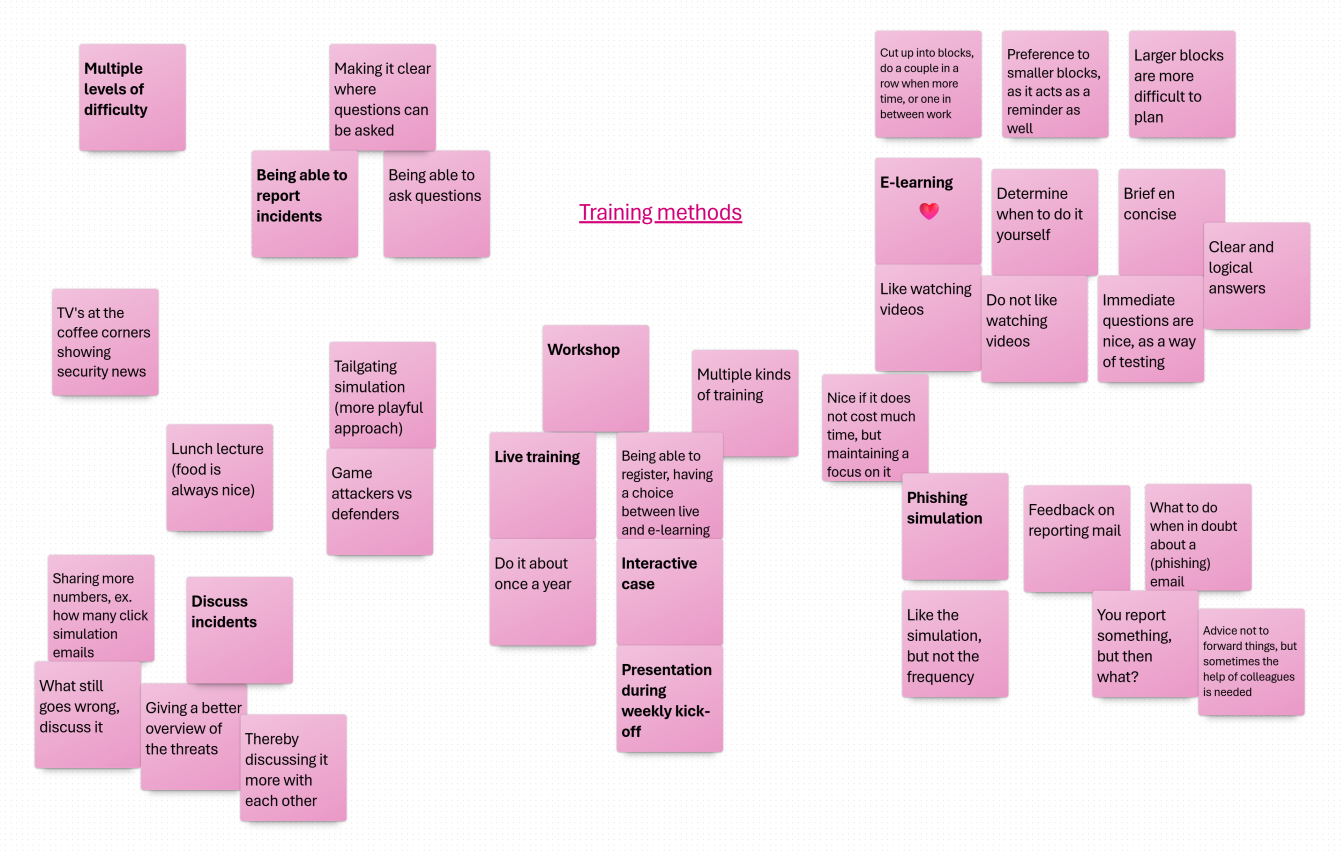

Figure 10.8: Whiteboard of training methods after the session with finance

During the session with finance it became clear they liked e-learnings the best, and as such no elaborate hit and dots session was done.

10.8 Framework analysis expert validation session

First, the figures below show how the codes found from coding the interviews connect to the factors from the framework.

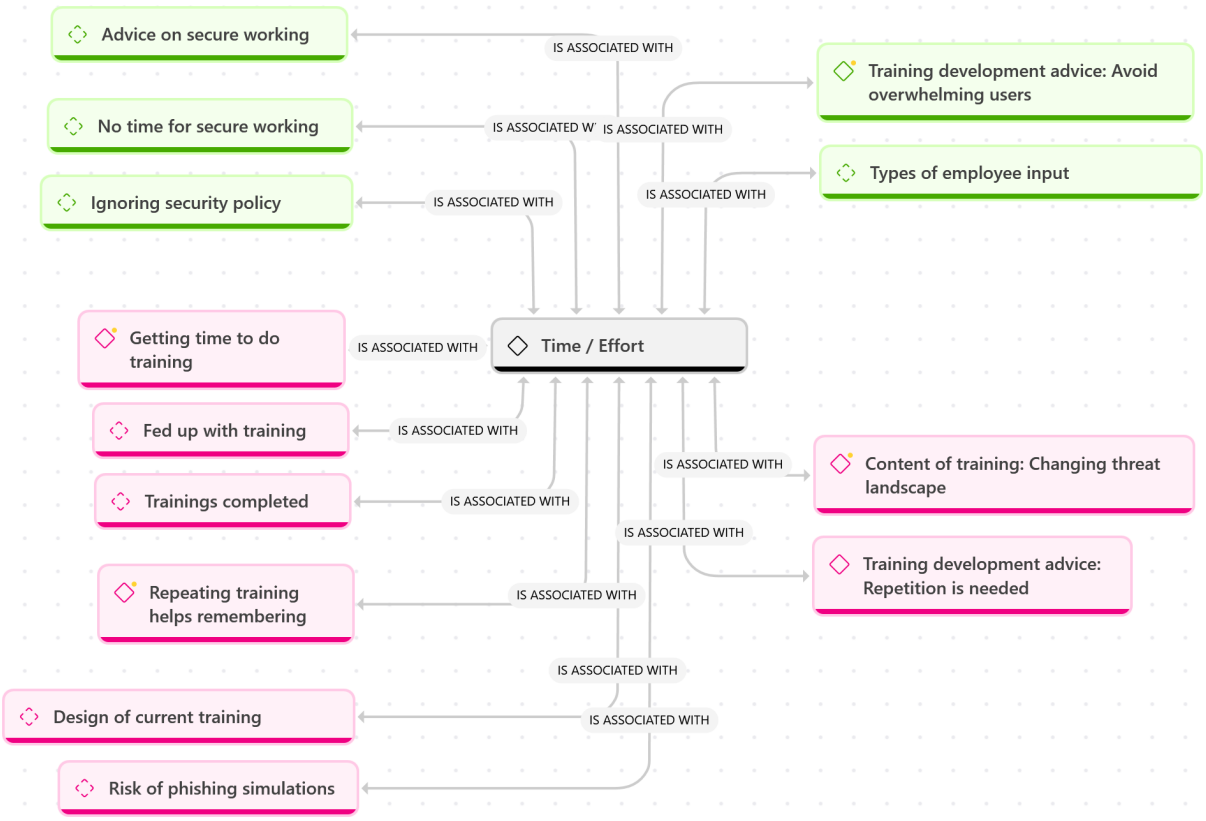

Figure 10.9: Connection of codes (left side internal interviews, right side external interviews) to time and effort

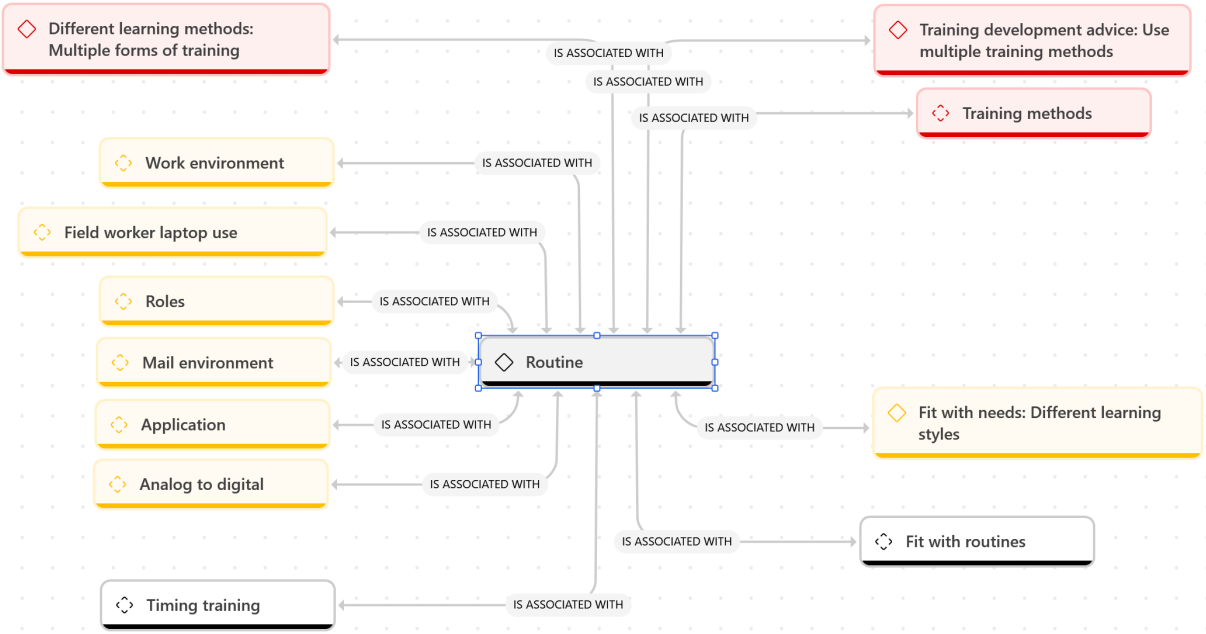

Figure 10.10: Connection of codes (left side internal interviews, right side external interviews) to routine

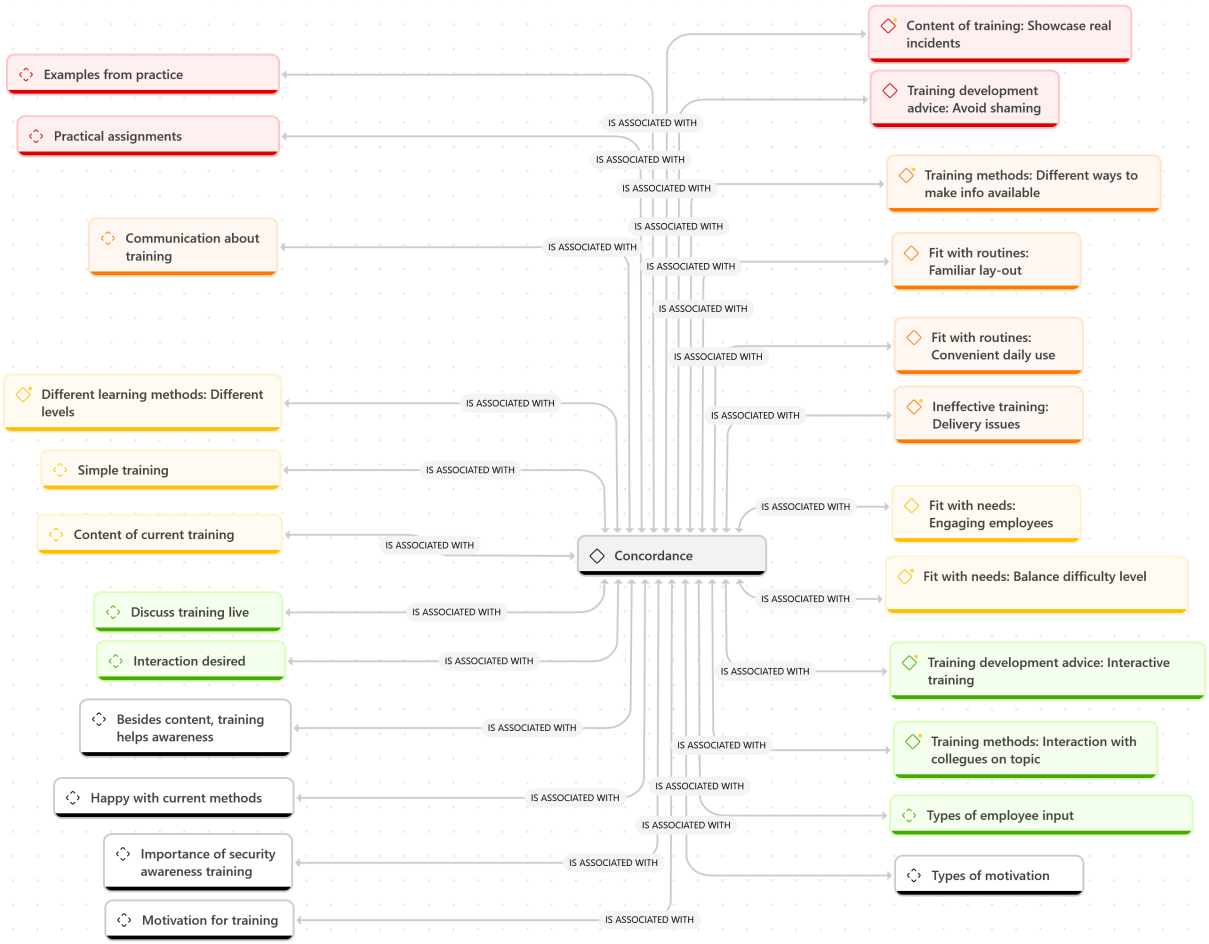

Figure 10.11: Connection of codes (left side internal interviews, right side external interviews) to concordance

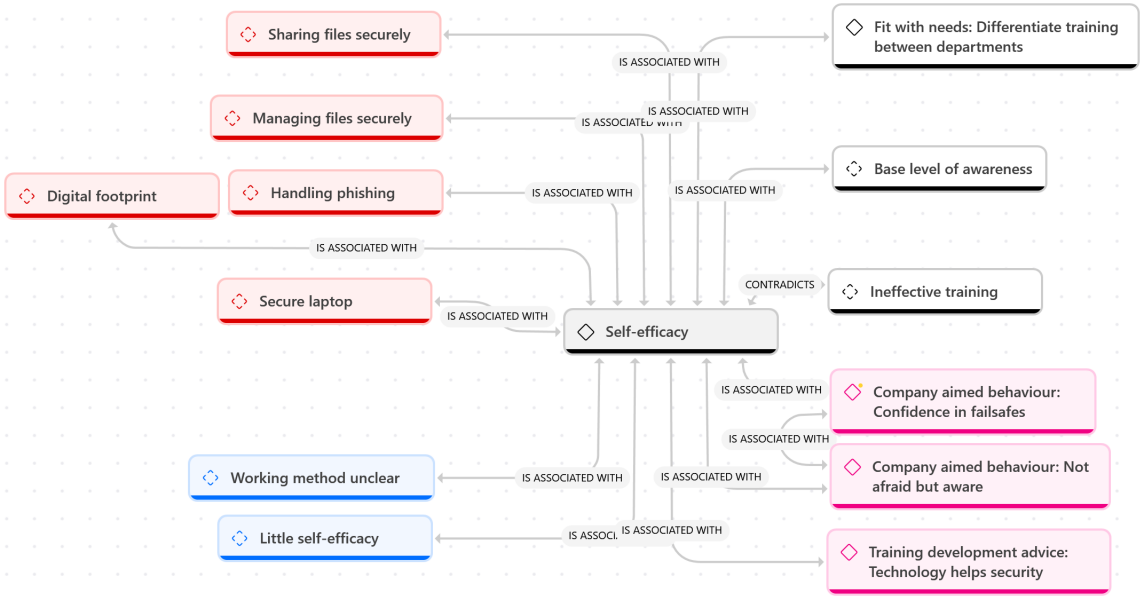

Figure 10.12: Connection of codes (left side internal interviews, right side external interviews) to self-efficacy

Then below here can be seen the advice and other comments given during the session, which was mapped to the training blocks.

Simplicity

Time / effort

Review policies on do-ability, try to reduce friction and to stay within compliance budget.

- Already tried to address some of these problems, such as finance saying the costs for mobile phone usage are too high, but acknowledged that apparently it did not work
- Some policies, such as the one for FLC was very specifically for them, which felt perhaps a bit too niche, but also said that it is something they should deal with
- A feedback loop would be nice, to more easily spot these kinds of high friction policies
- Do think that some things noted, such as not locking screens because it takes a lot of time might have a deeper layer to it as to why people are not doing it

Lower the frequency of the phishing simulations to once a month or once every two months.

- Understood how people might get too flooded with simulations
- People should also not start fearing every email, to help with this there might be a nicer feedback that can be given back when an email is reported to say how you could have seen this was phishing
- Also think the problem is not only the frequency, but also that people do not know how to handle phishing well and are thus becoming afraid

Culture

- Leadership has to be involved
- Managers have to make it possible for employees to behave securely
- Managers should set the example and behave securely themselves
- Without managers being on board, behaviour will not change

Routine

Have different options of training methods to fit with people's routines.

- Have been trying to plan security sessions with employees from FLC, as they already have meetings where they learn essential skills, but never had the time to go through with it
- Agree that people will learn much better if you accommodate those needs, but that there is a balance that must be kept between accommodating and feasibility. Suggest making it clear for yourself what you want to get out of it and what the most effective way of getting there is

Motivation

Concordance

Share actual threats and numbers of incidents with colleagues to improve the risk perception and need for secure behaviour.

- Understand that it can help people

- Making a dashboard with threats and incidents should be doable, as they already have the numbers
- Also, they have a safety dashboard with incidents at the company already, so they could learn from how they do things

Have multiple levels of difficulty of the training to challenge the people who would like that and accommodate people who want easier training.

- Agreed that the current way of training meant that a lot of people were not learning anything new
- Also noted that it can be very frustrating to have to do training on topics you already know
- Having a possibility to do a test and skip to your actual level, likened to how Duolingo does it, would be nice
- It would have to be seen however if that is doable on the current platform and otherwise possibly if the current platform should even be used

Accommodate and promote interaction (in training) between colleagues to discuss security topics to learn from each other.

- Think it could be very useful to do
- Had ideas such as walking through a potential phishing email together
- Also were thinking of talking about an actual phishing incident that happened

Have clear communication on what the training is, what it is for and the timeline of the training.

- Some information is out there or has been communicated in the past already, but people still do not know about it. Something has to change.
- Had some examples of failed communications. Anything sent in English instead of the local language is often ignored. They also tried to get managers to tell people beforehand when things would happen, but many forgot to do so.
- Also said they had told people the platform would have more than just phishing training, but people did not remember
- Also came up that some communications were sent only once and if you have since come to work for IECC, it was never communicated to you. Wanted to look at how onboarding security training might help here, also with making it clear for people who they could ask questions to if needed

Self-efficacy

Give more concrete advice aimed at IECC specific policies and what people actually wish to know.

- To close the knowing-doing gap, have live sessions where people can join to learn the skill. You could have a day where people are invited to join to set up their password manager. People are afraid of the unknown and might need to be helped past a hurdle
- The current platform did not allow for changing part of a level sent to people, you would need to make the level yourself. It might become possible in the future however