Micro - Entreprise Cybersecurity

MECyS

Report Learning Hurdles

3rd Part of Training Plan

Co-funded by the European Union

Point of Contact	Bernd Remmele
Institution	Pädagogische Hochschule Freiburg (PHFR)
E-mail	Bernd.remmele@ph-freiburg.de
Phone	+49 761 682 625

Project Acronym	MECyS
Project Title	Microenterprise Cybersecurity
Funding	Erasmus+/Movetia
Project start date	31/12/2022
Dissemination level	Public
Date of submission	30/08/2023
Lead partner	PHFR
Main Authors	Jessica Peichl (PHFR), Bernd Remmele (PHFR)

Contents

1 Purpose and Approach of this Report

This report is part of the Workpackage 2 ‘Backgrounds and Training Plan’ of the MECyS Project (Micro-Enterprise Cybersecurity). Together with the reports on VET-Systems in the partner countries of the project and on given training tools in the field of cybersecurity (see appendix: Report VET Training) the Learning Hurdles Report forms the basis for the development of adequate trainings.

The purpose of the Learning Hurdles Report is particularly the identification and compilation of effective starting points for training in concern of different Cybersecurity issues.

Many MSEs are not sufficiently informed about the threat posed by cyber attacks and do not know their own risk profile (BMWK 2021). This leads to companies not investing enough in protection against cyber attacks. This includes not only investments in internal information technology, but also the consideration of the "human factor" as a protection mechanism against cyber attacks. Targeted staff training can help increase protection against social engineering attacks such as phishing emails. Given that currently phishing attacks are still the most common method of penetrating internal networks (ENISA 2022), human behaviour is a significant lever.

The Learning Hurdles report will consist of three parts:

- conceptual clarification of the concept of learning hurdle or threshold concept
- a specification in concern of its application to Cybersecurity and the desiderata thereof
- a presentation of preliminary research approaches in relation to learning hurdles in Cybersecurity.

2 Learning Hurdles – Threshold Concepts

Learning hurdles refers to the concept of conceptual change, which captures domain-specific barriers to learning and corresponding learning pathways to achieve conceptual change. The focus in the literature so far is on teaching and learning in the natural sciences (e.g. (Vosniadou et al. 2008, DiSessa 2008, Chi 2008). In addition, there are works on learning and teaching in the humanities and social sciences (e.g. history: Leinhardt/Ravi 2008; philosophy: Arabatzis/Kindi 2008). In the domain of cybersecurity and data protection, the state of research on conceptual change is still very limited (Chan/Wei 2008, Scheponik 2016). Likewise, there has been little research on data security concepts and learning barriers among IT laypersons.

In general, Learning hurdles or threshold concepts are subject specific developmental steps that are not just an incremental growth of knowledge but represent a specific before and after. From a didactical point of view it is of high importance to reflect these specific developmental conditions.

Meyer and Land (2003) explained a threshold concept as "akin to a portal, opening up a new and previously inaccessible way of thinking about something. It represents a transformed way of understanding, or interpreting, or viewing something without which the learner cannot progress" (p. 1). Meyer and Land (2003) identified five characteristics of a threshold concept. They stated that a threshold concept is (likely to be) transformative, (probably) irreversible, (potentially and possibly inherently) troublesome, and contains the capacity to be integrative and bounded. This list was later extended (https://www.ee.ucl.ac.uk/~mflanaga/thresholds.html):

Concerning the Learner

> Transformative: once understood, a threshold concept changes the way in which the student views the discipline.
>
> Irreversible: given their transformative potential, threshold concepts are likely to be irreversible, i.e. they are difficult to unlearn.
>
> Reconstitutive: Understanding a threshold concept may entail a shift in learner subjectivity, which is implied through the transformative and discursive aspects already noted.

Concerning the Process of Learning

> Liminality: the crossing of the threshold is like a 'rite of passage', which has a certain duration and complexity.
>
> Troublesome: threshold concepts are likely to be troublesome for the student, because the knowledge can be troublesome e.g. when it is counter-intuitive, alien or seemingly incoherent.
>
> Discursive: the crossing of a threshold will incorporate an enhanced and extended use of language.

Concerning the Subject Discipline

> Integrative: threshold concepts, once learned, are likely to bring together different aspects of the subject that previously did not appear, to the student, to be related.
>
> Bounded: a threshold concept will probably delineate a particular conceptual space, serving a more specific and limited purpose.

2.1 Didactical Perspective

A starting point for subject didactic development research is the assumption that educational efforts are most efficient when they focus on the specific learning hurdles, otherwise systematic further learning processes are hindered.

The orientation of teaching towards the desired change in learners' conceptions is central in a constructivist understanding of learning and teaching. This is expressed in conceptual-change approaches (for an overview see Vosniadou et al. 2008), domain-specific theories of teaching and learning that capture the domain-specific learning obstacles and the path of the necessary conceptual change and its determinants. It is now known that the initiation of a cognitive conflict is particularly relevant for stimulating conceptual change (Birke 2013 - However learning methodological questions are not part of this report).

As long as learning takes place on lower conceptual level it is not sure that further progress is going into the right direction. Intentional training should therefore focus on such structural conceptual development or on reaching the sphere beyond the (next) threshold.

Overcoming learning hurdles thus also facilitates self-directed or incidental learning processes. This is what makes the focus on threshold concepts so efficient: also the non-intentional training and learning will happen on the advanced level.

3 Desiderata in the Field of Cybersecurity

Both managers and employees show an insufficient risk assessment with regard to data security. Related to this is the assumption that there is often no corresponding position within the company that takes responsibility for the development of competence for data security. The question also arises, especially among young people, concerning what influence their (private) handling of data has on possible concepts for data protection and their behaviour in the work environment.

Overall, there is uncertainty in the area of data security within small companies, which is also an obstacle to the digitalisation of small companies (Brockhaus et al. 2020). Even at management level, there is often a lack of awareness of the correlations and risks of the use of IT technology (NACD - 2021). Similarly, employees, who represent the biggest gateway for cyber attacks in companies, are often not aware of their company's vulnerability (Kemper 2019). Conversely, managers in German companies often consider employees in home offices to be a low IT risk (Deloitte 2021).

In terms of data protection, employees are also often unclear about the company's data protection strategy (if it exists), which is associated with an increased risk of breaches (Chua et al. 2018). In addition, micro-enterprises are often still embedded in a family environment, in which responsibility for IT security is even less clearly regulated.

Above all, among the IT security measures least considered by MSEs are employee training and corresponding IT security strategies (Mitrofan 2020).

The German Federal Office for Information Security (BSI) has found that around two-thirds of people are aware of security recommendations, with 12% implementing them fully and around one-third partially. One of the reasons why implementation fails is that the measures seem too complex or are not understood (BSI 2021). This is where educational measures can come in and increase not only awareness but also understanding of security measures. For successful education measures for MSEs, there is a need for corresponding curricular specifications and prioritisation, because curricula for data security are primarily aimed at experts, e.g. in the professional environment of IT technology topics, and thereby disregard the need for laypersons - especially in MSEs (GEIGER 2020).

3.1 Previous Considerations in GEIGER

The GEIGER curriculum (Remmele/Peichl 2021) maps the development of competences via a level structure, which, however, is oriented towards different company learning scenarios and the target groups dealt with in the project as examples.

	Cyber-security awareness, incl. cyber-secure behaviour (general and SME specific)	Knowledge, application of main features of GEIGER, incl. functional equivalents	Exploitation: kinds of interaction with other (potential) users of GEIGER
Level 0 – Random Cyber-Security Knowledge	Limited, random everyday knowledge of some issues of cyber-security	n.a.	n.a.
Level 1 – Basic Cyber-Security Literacy	General knowledge of a relevant set of cyber-security issues and of basic rules of cyber-secure behaviour	n.a.	n.a.
Level 2 – GEIGER Beginner ("Educated Security Defender"	SME-specific knowledge of a relevant set of cyber-security issues and of basic rules of cyber-secure behaviour	General knowledge about GEIGER	Ability to communicate cyber-security and the general relevance of GEIGER for it within an SME context
Level 3 – GEIGER Advanced ("Certified Security Defender")	SME-specific understanding of a coherent set of cyber-security issues and application of principles-based rules of cyber-secure behaviour within typical SME environments	Detailed knowledge about GEIGER and its application within a (one) specific SME	Ability to explain (mentor) the specific cyber-security aspects of the given SME and how GEIGER works in it
Level 4 – GEIGER Multiplier (educational and other? provider)	SME-specific understanding of a coherent set of cyber-security issues and analysis of cyber-secure behaviour	Detailed understanding of GEIGER and its application within most SME usage environments	Ability to train for level 3 as well as 1 and 2 respectively

4 Hypotheses for the Field of Cybersecurity – with Focus on MSE

With a view to possible learning hurdles in the field of cybersecurity, we assume that the protection of private data, as one major function of cybersecurity in the given context, in a relevant way is counter-intuitive for IT laypersons. This is because the everyday handling of private data is characterised, among other things, by sharing it 'generously', e.g. in social media. Likewise, forgetting personal information appears impolite in private dealings, whereas it is a principle of action within the framework of the General Data Protection Regulation (GDPR) - the same applies to data minimisation, i.e. you can find a hunter-gatherer attitude to private data.

Social engineering attacks also take advantage of such lay approaches. Another problem is the habit of implicitly delegating IT-related competence limits to IT services; people expect Google etc. to take care of everything somehow. The insight into one's own responsibility takes a back seat to this.

The GDPR represents a change in principles (such a historical learning process is an indication of a probably necessary individual change in concept) from selective data protection to the fundamental right to one's own data, which regards every data processing as an exception requiring legitimation - and only against this background are the data protection principles valid for business practice understandable. A misconception would be that one can process personal data in a way that is not (yet) legitimate, e.g. because it does no harm or one is even doing the data subjects a favour.

There are different aspects in the field of data protection that could imply a salient conceptual change. On the one hand, the everyday handling of one's own private data is often characterised by sharing it 'generously' e.g. in social media. Data minimisation as a basic principle (in giving and receiving/hoarding) data, on the other hand might need training. Also experiencing data protection not as a daily nuisance but as the gradual advancement of fundamental rights, e.g. in the view of cookie banners, does not seem trivial.

Also more technical issues of cybersecurity could imply conceptual changes. This might apply for the nature of 'digital assets': from passwords as a way of robbing the person concerned (e.g. money) to passwords as a way of using the identity of the person concerned for attacks on completely different targets. A main question is what is considered a risk: am I or is my company too small to be of interest; do I feel safe because I recognize ‘current’ phishing strategies, do I fell safe because I delegate my security problems to my big tech provider; do I feel safe because I use a long password …

5 Interview Study with German Lay Persons from MSEs

Based on the theoretical considerations concerning potential learning hurdles PHFR started a small interview study (already before MECyS and partly funded by the internal PHFR research support). For the interview guideline (see Appendix) the most promising issues were selected.

Overall, 4 persons working in MSEs were interviewed. The interviews lasted about 40 - 60 minutes and were conducted either in presence or via Zoom. In both cases the sessions were recorded. After transcription, the data was analysed using the Software MAXQDA 2022. Due to the very small sample size the statements cited below have to be taken with interpretative caution.

5.1 Results

The results presented in the following are exemplary and preliminary. Overall the interviews show a quite differentiated understanding of everyday and business cybersecurity; however, the human rights aspect of data protection seems to be conceived more superficial – expectably as it is much more abstract concept.

There is awareness of the goals and features of phishing attacks:

> "… they are becoming more creative. That is to say, they often offer business in the areas [of one's business] or simply you get an order here or we now have the possibility to offer you this and that software. So they are really clever. I have to say, sometimes I have to look two or three times, can it be you, can it be development. And so. It's sometimes very difficult to recognise that."

Also the understanding of login safety is up to date, as there is no particular focus on password length and overall a rough understanding of 2-Factor Authentication:

> "I have no idea if it's safe if you have a long password. It is certainly helpful if you have other characters in it, e.g. letters, numbers and characters."
>
> "Okay, so it's actually also a problem where we're back to the effort, how long does it take me to log in, do I get blocked or then I don't get in at all, and so on."
>
> "The added value, I think, is that there is the security in the sense that two devices would have to be hacked at the same time to get access, so to speak"
>
> "I must also say, now and then I refuse. These two. There are offered to me about two security levels would like. Sometimes I turn it down because I'm just okay weighing that Is it that important for this area now?"

The perspective on data protection is not proactive but rather disenchanting, e.g. when it comes to cookies etc. on the on hand and their handling of data protection issues in their companies:

> "So somewhere we are already so transparent anyway and I have probably already clicked on accept often enough. (...) And it is personally Yes, the effort is not worth it for me to protect my data."
>
> "I think it's totally important. ... It's troublesome in that sense. I think it's much too late. We started to take care of data protection and now we have platforms where a lot of data is collected."
>
> "I know it from us, too. It would be ultra difficult now to store this data, which I get all through reservation requests etc., in a somehow protected way."

6 International Online-Questionnaire Survey

Based on the impression from the interview study the general idea of learning hurdles and the interview guideline were discussed during the Kick-Off-Meeting of MECyS in Freiburg (April 2023). The discussion lead to development of a multi-lingual online-survey pilot-questionnaire (see Appendix).

This questionnaire was also tested and reflected during the MECYS Staff Workshop in Paris. Afterwards the participants filled out the questionnaire themselves, so their answers are part of the following results.

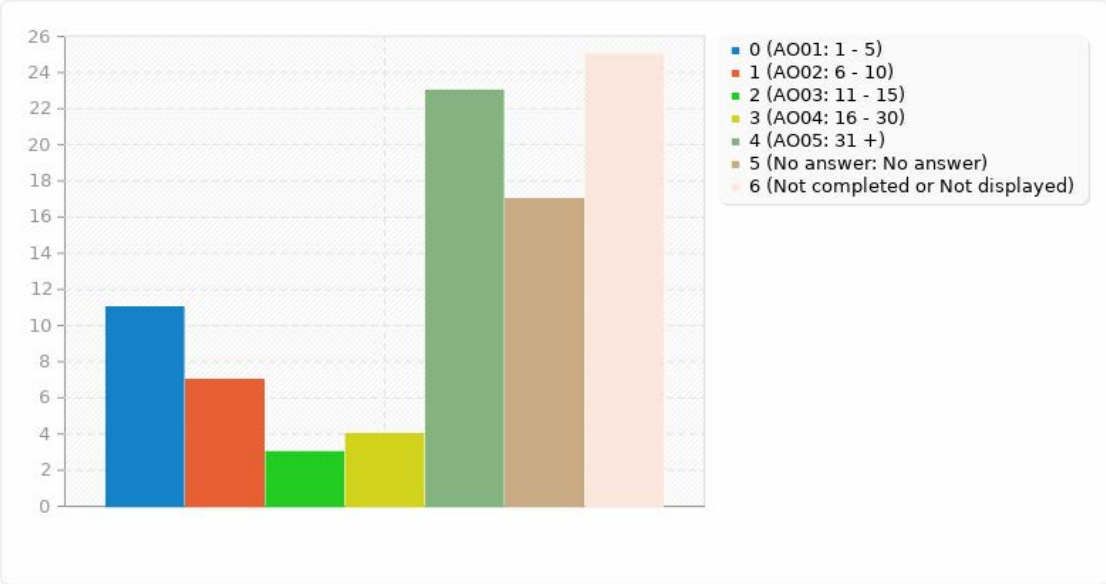
It has to be stressed that the questionnaire is not to be considered a proper research instrument. It is rather a tool to guide further didactical considerations, as it only gives some indication about the validity of potential threshold concepts in the field of cybersecurity.

6.1 Results

Accordingly, as the questionnaire is a pilot one and the sample is rather heterogeneous it is not appropriate to draw any deeper conclusions. Nevertheless, there are some interesting preliminary descriptive results that can help to develop training offers in the further process of MECyS.

6.1.1 Company size

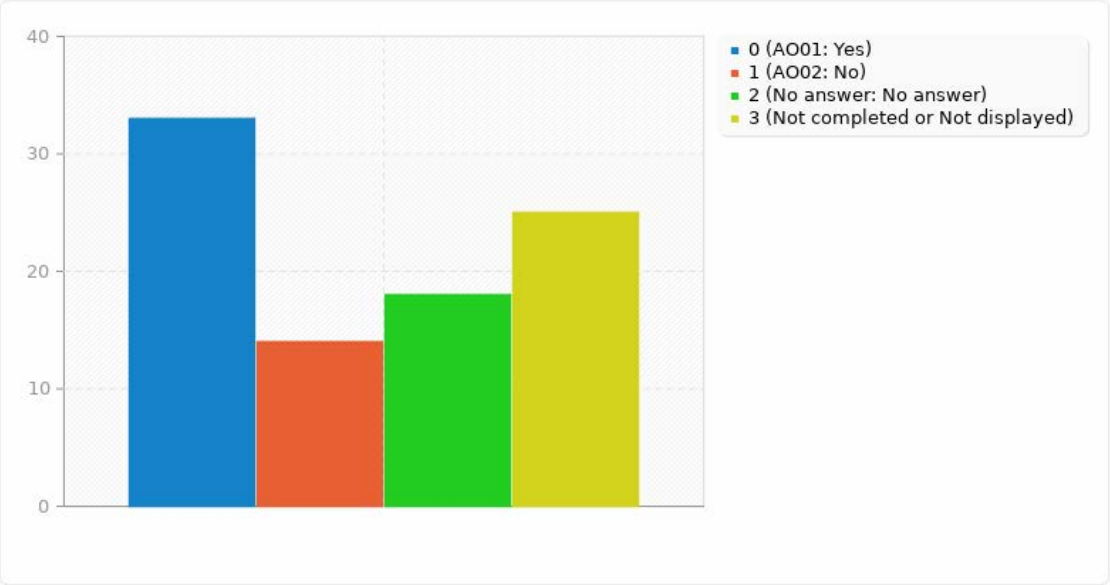
As the result for “How many employees does your company have?” show there is a significant part of persons working in micro-enterprises in the sample:



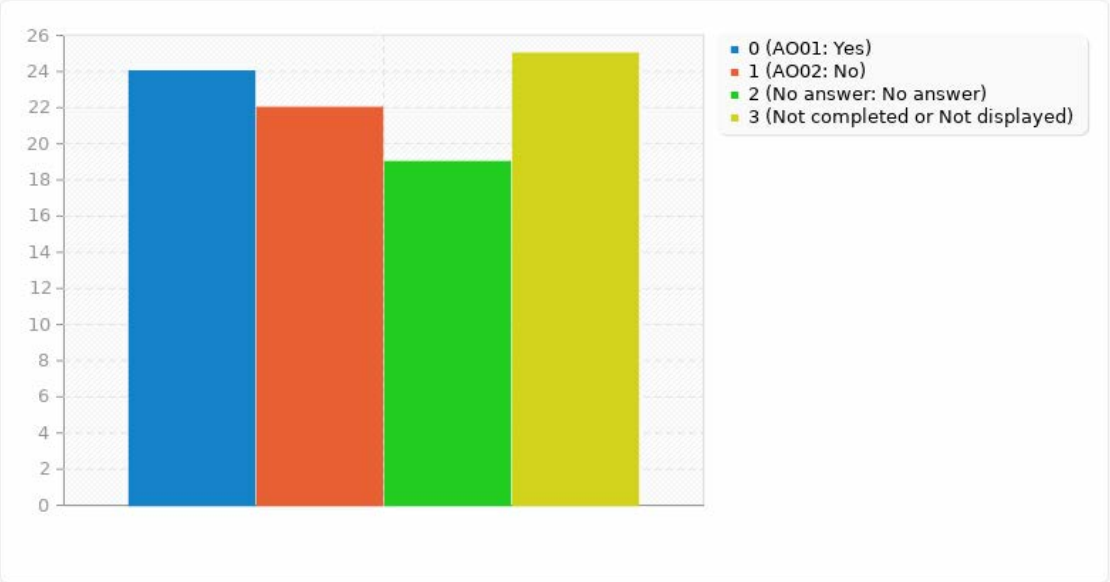
6.1.2 Risk Taking and Awareness

In concern of cybersecurity it is interesting to see that usage of private devices for work and work devices for private purposes is quite common. On the one hand, ease of us beats security.

Do you use private devices for your work?

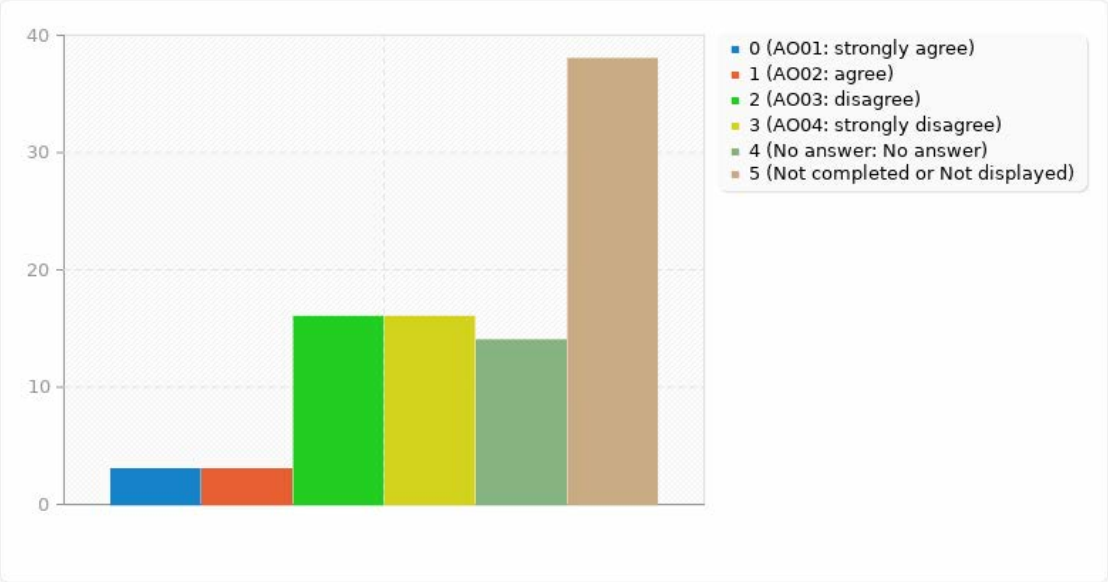


Do you use work devices for private purposes?

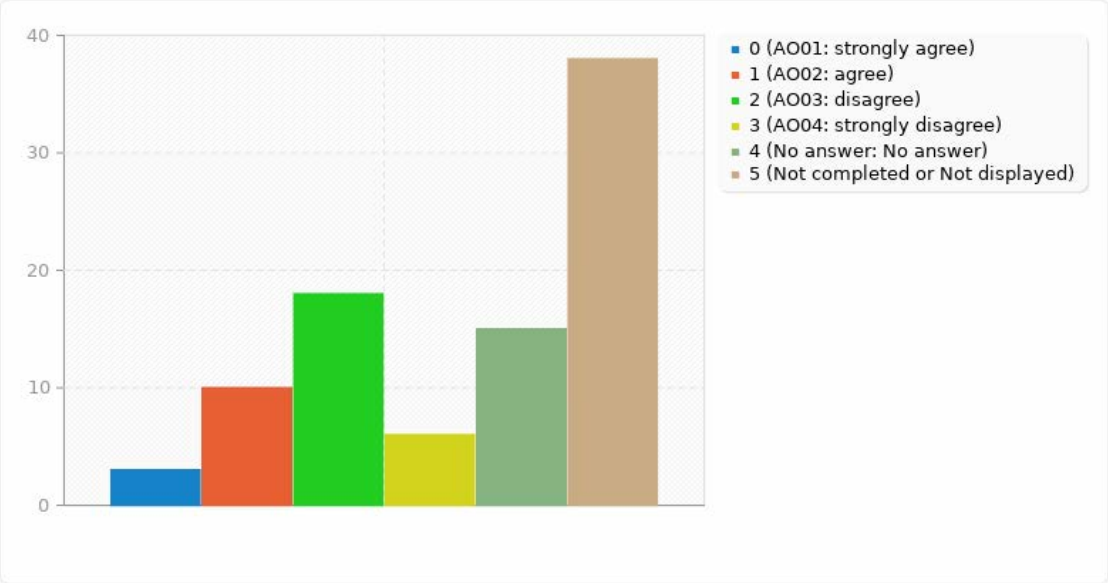


On the other hand, there is clear awareness of the risks also for micro- and small businesses. This might be considered as a typical knowledge-behaviour-gap.

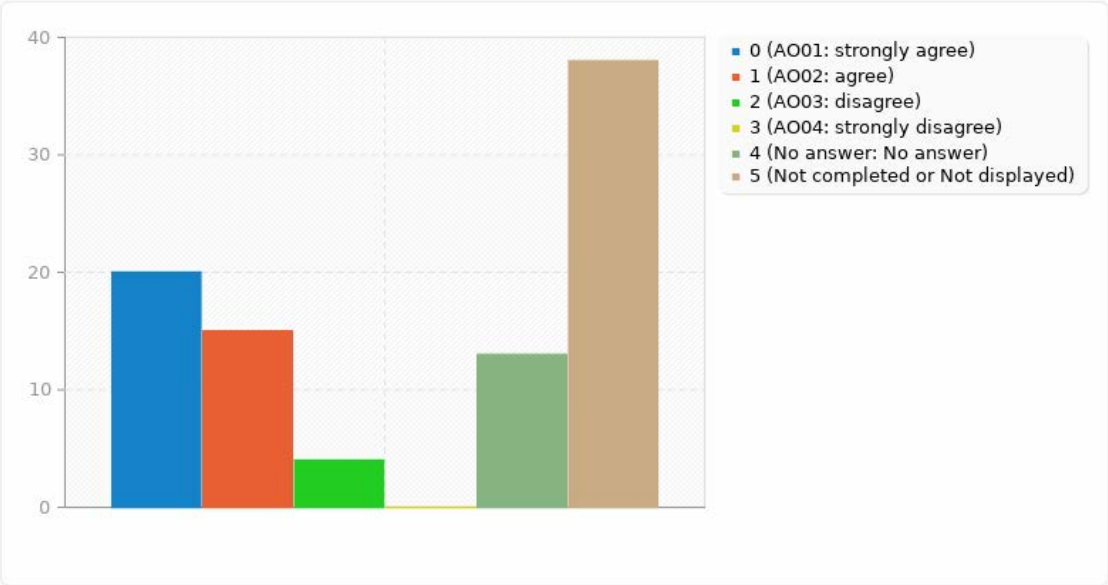
Cyber attacks only target bigger companies



Cyber attacks specialize on lucrative victims



My small company might be a relevant target of cyber attacks

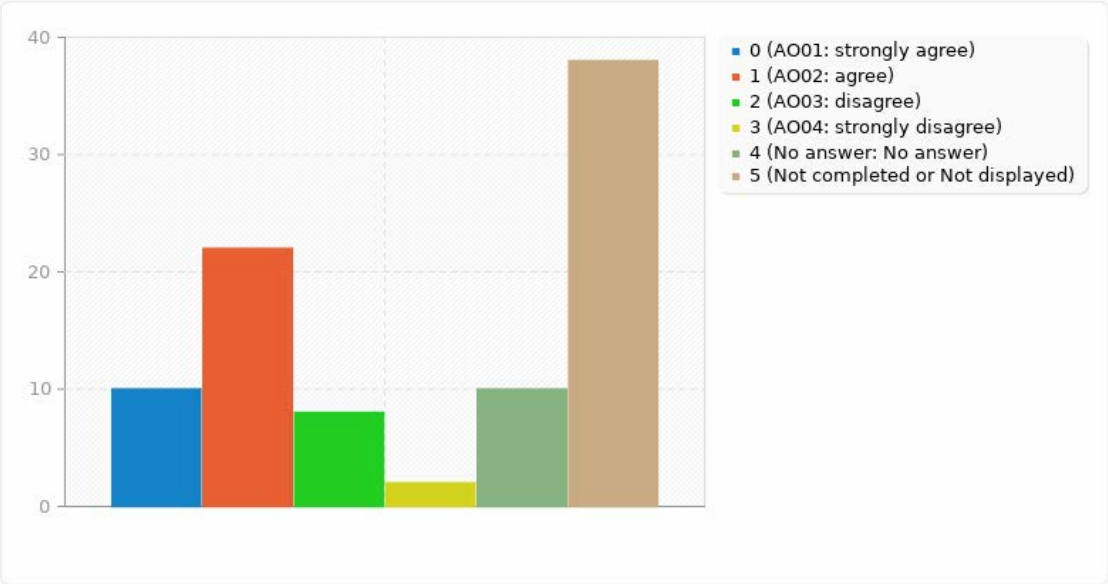


Based on these findings, it can be stated that small and medium-sized enterprises (MSEs) are increasingly conscious that cyber attacks aren't exclusive to larger corporations and that their own company could be vulnerable as well. Despite this awareness, significant risks are still taken, particularly when personal devices are used for work tasks and vice versa. The data underscores a paradox: while MSEs exhibit a clear understanding of the risks, their actions often diverge from this awareness.

6.1.3 Confidence

Even though it can be assumed that phishing e-mails will become harder to detect in the future (e.g. because of better personalisation), the survey participants are quite confident to detect phishing e-mails.

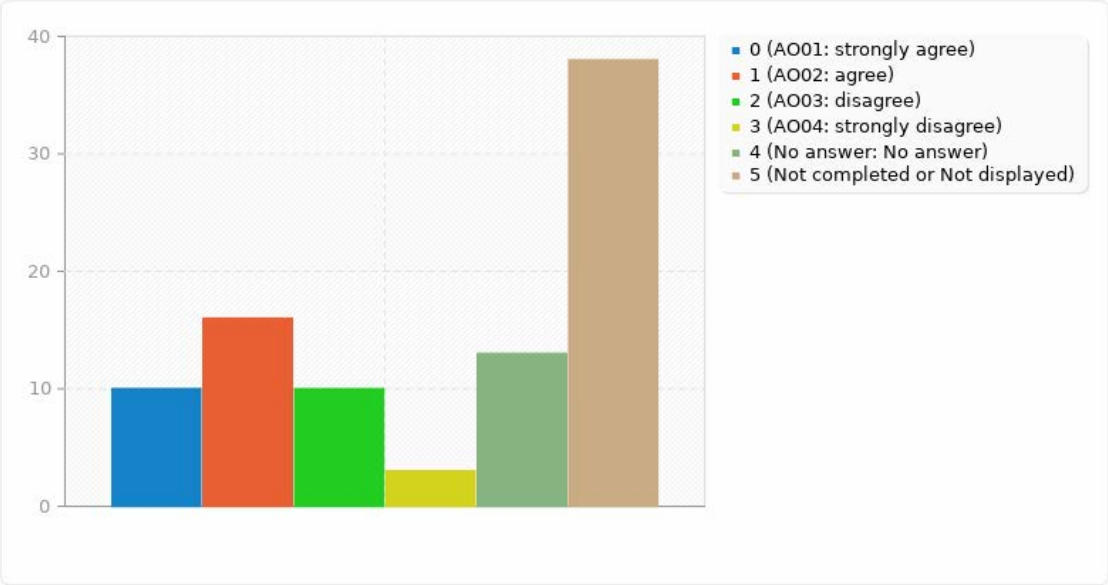
I am confident to detect personalized or KI-based phishing e-mails in the future



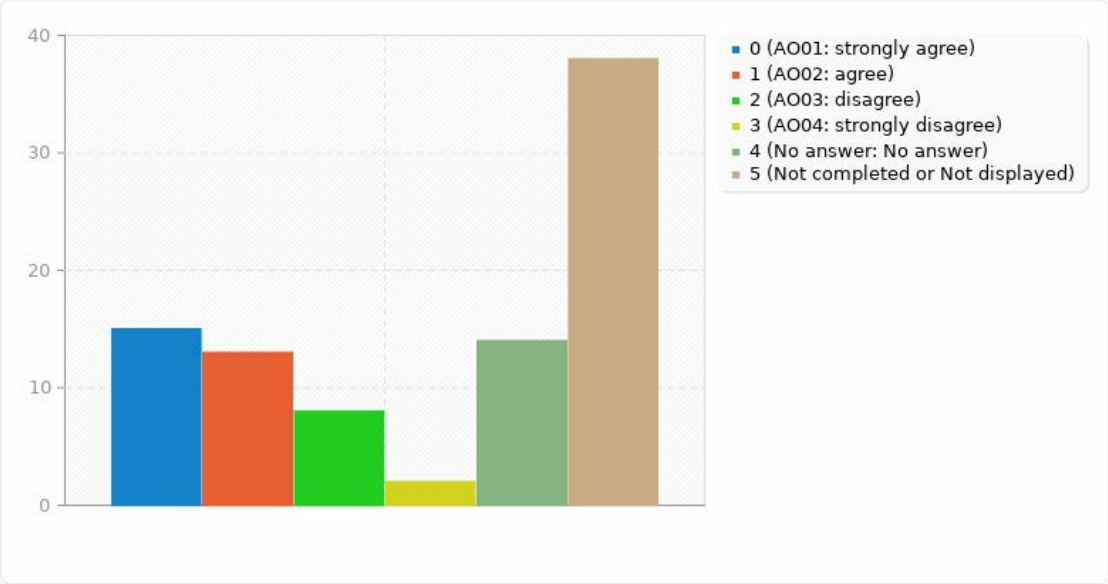
6.1.4 Passwords

Like the result from the interviews 2-Factor-Authentication (a technology that ads a second safety steps in contrast to just using a password as a factor) is in wide use and a understood security measure. Nevertheless, a majority also assumes that a long and complicated password will ensure cybersecurity,

A long and complicated password will ensure cybersecurity

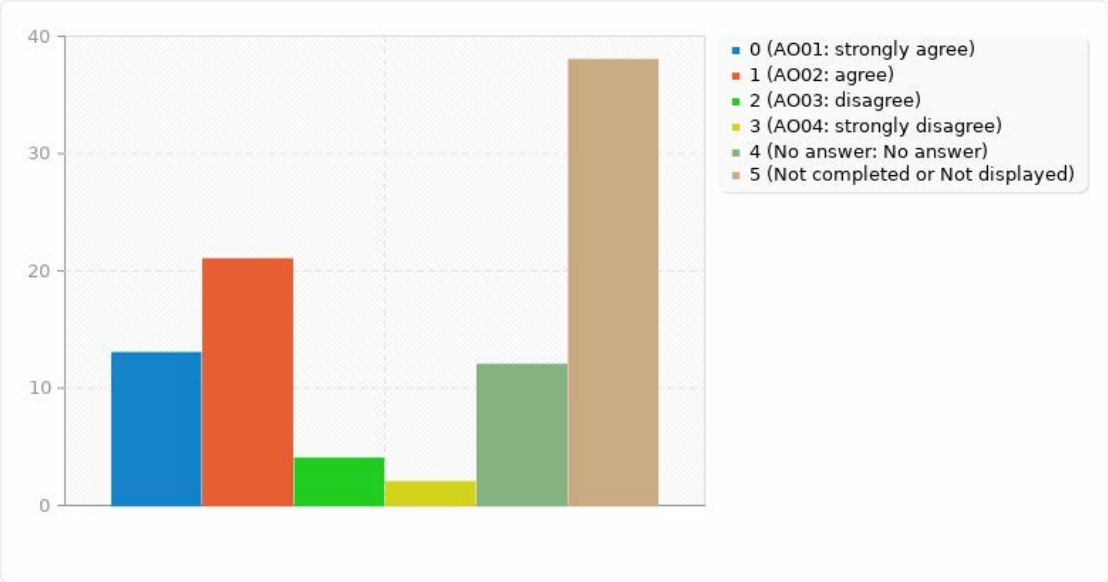


I use 2-Factor Authentication for private online services

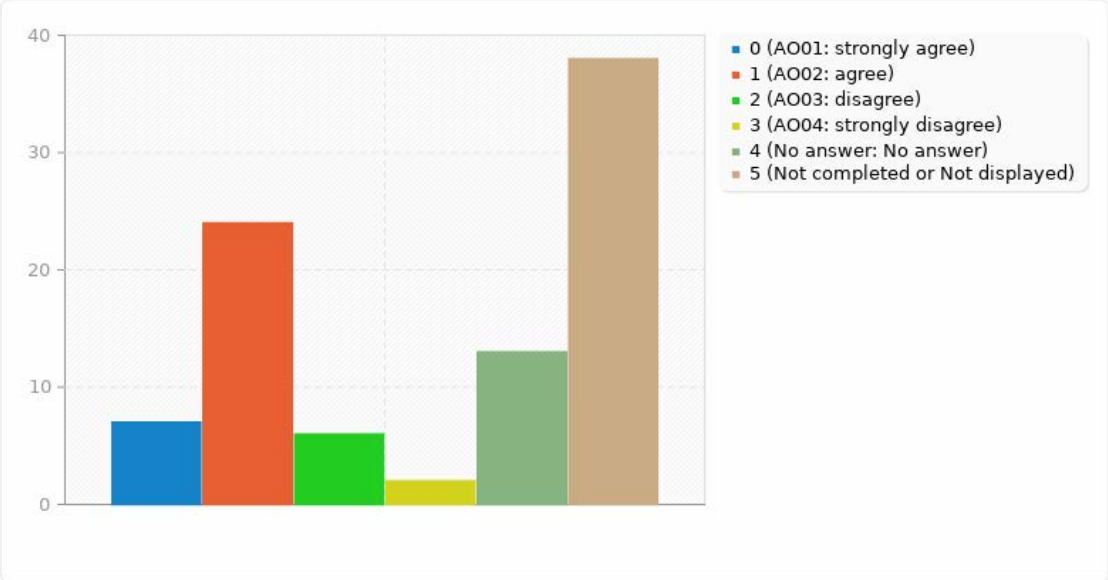


6.1.5 Big Data

I enter different websites via my google or facebook or similar account

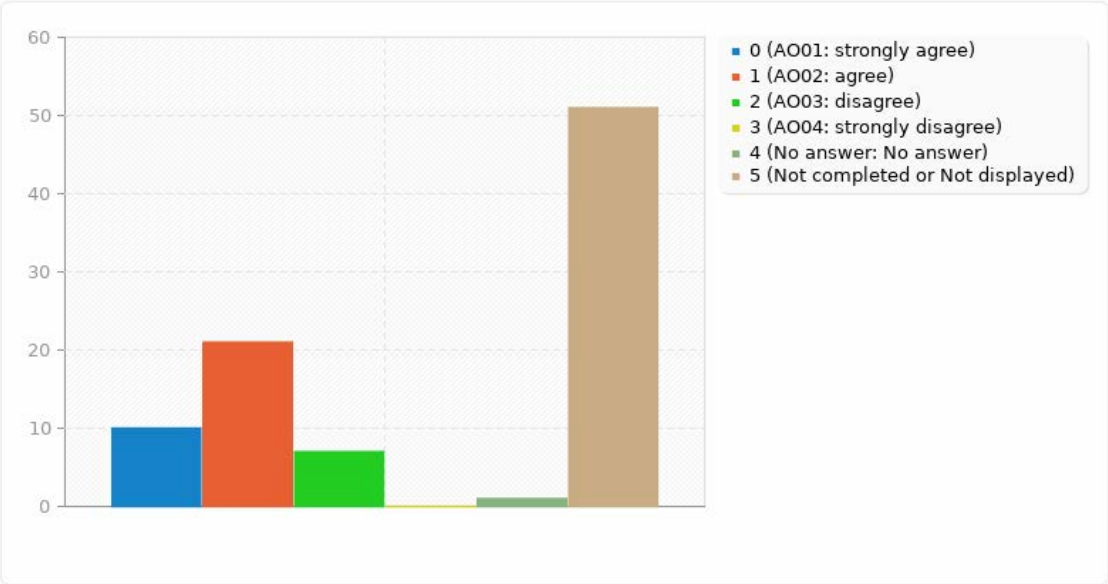


I generally trust bigger companies (e.g. Microsoft, Google, ...) to take my cybersecurity seriously

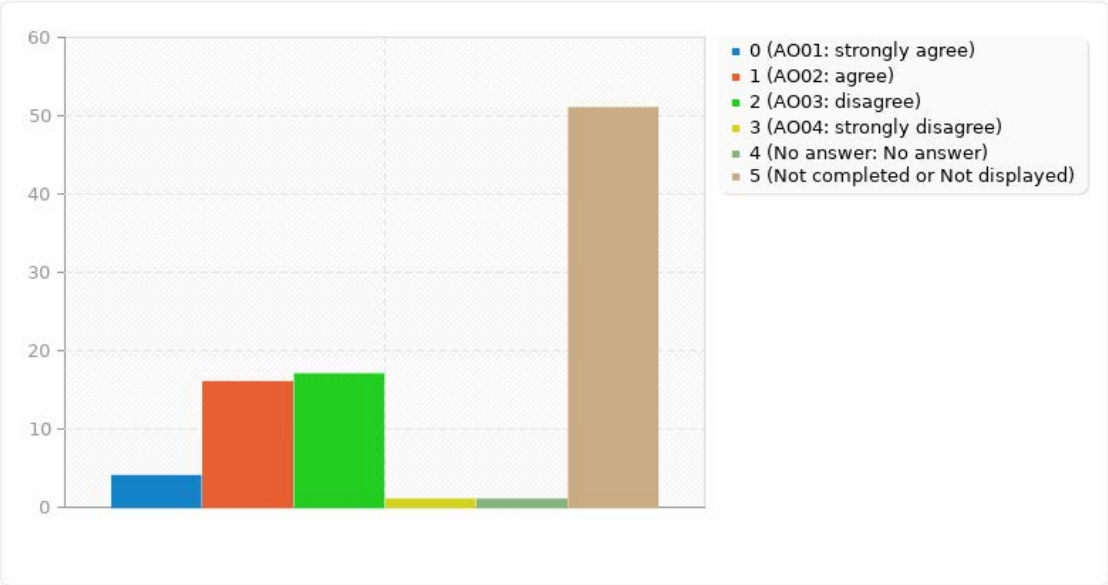


There seems to be a – more or less abstract – reserve against Big Data.

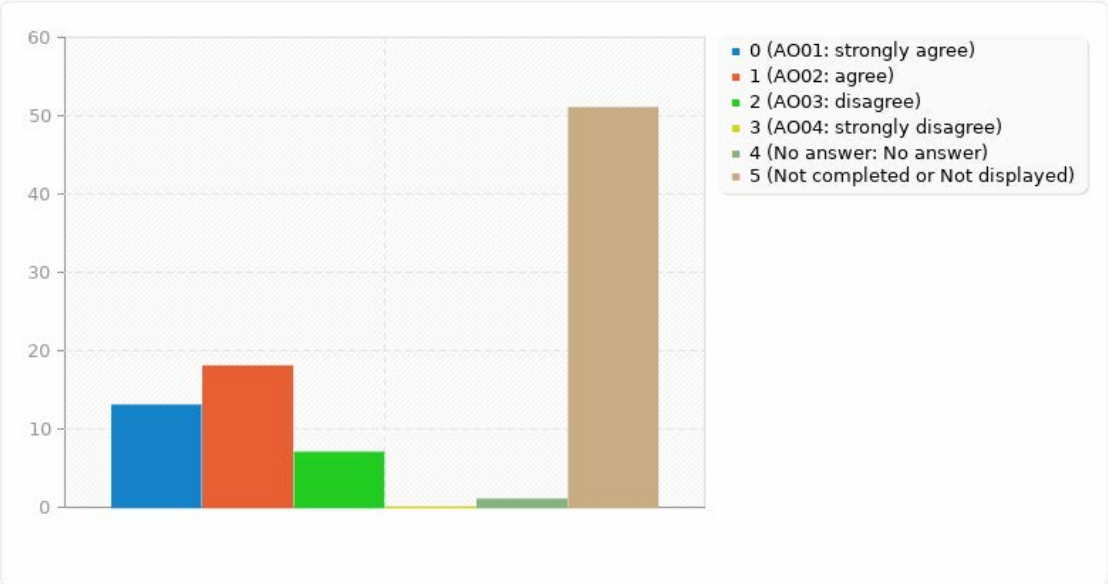
I do not trust companies in the internet to process my data responsibly



It is fair that companies track my online behaviour to improve their services



Personal data should be protected, because otherwise big companies could steer our behaviour.



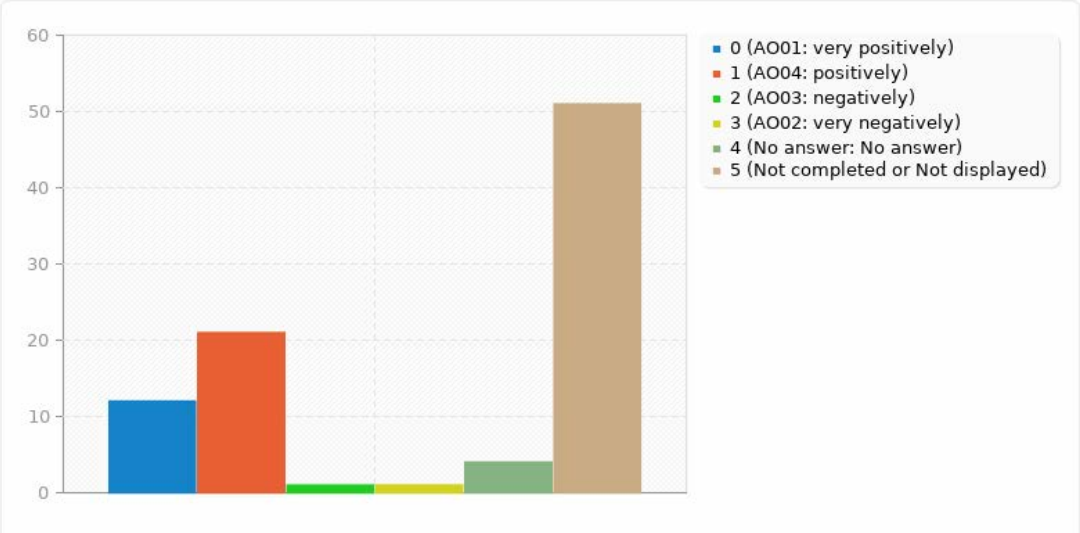
Taken together it can be stated that concerning the data handling of big companies there are salient inconsistencies. There is a tendency to trust bigger companies in terms of cybersecurity but nevertheless a distrust in terms of data protection, even though these two factors cannot be clearly separated in practice. Furthermore, a relevant number of participants agree with being tracked online for service improvements. In contrast, a majority of participants stated that personal data should be protected.

It needs to mentioned that these inconsistencies can also be (partly) due a possible acquiescence bias, that participants are in general more likely to agree to statements than to disagree.

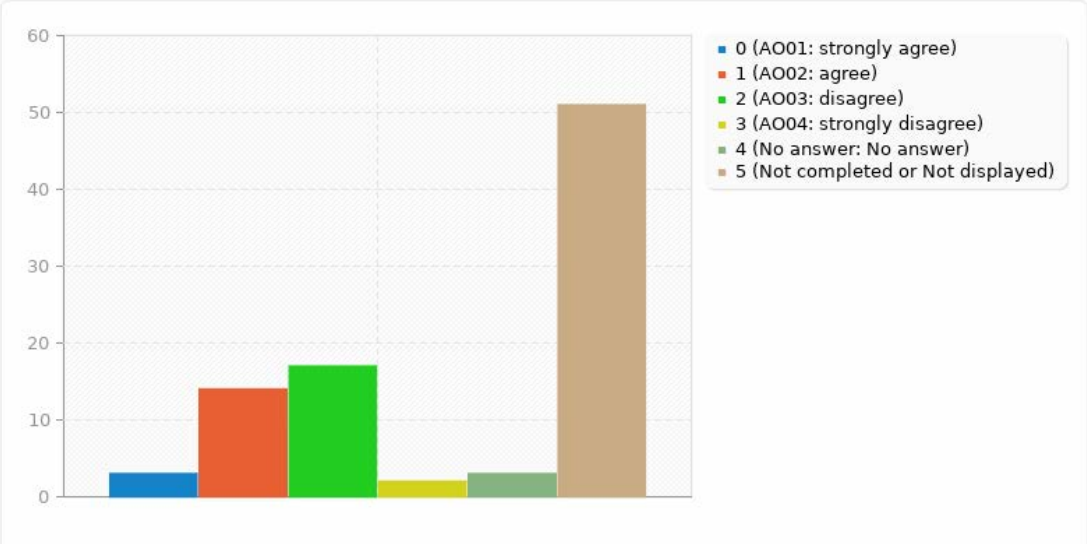
6.1.6 Data Protection

Overall, data protection is a contested field; people want (for themselves), but are annoyed by (current) way handling it, i.e. mainly consent.

In general, data protection impacts me



Data protection makes my daily working processes more difficult



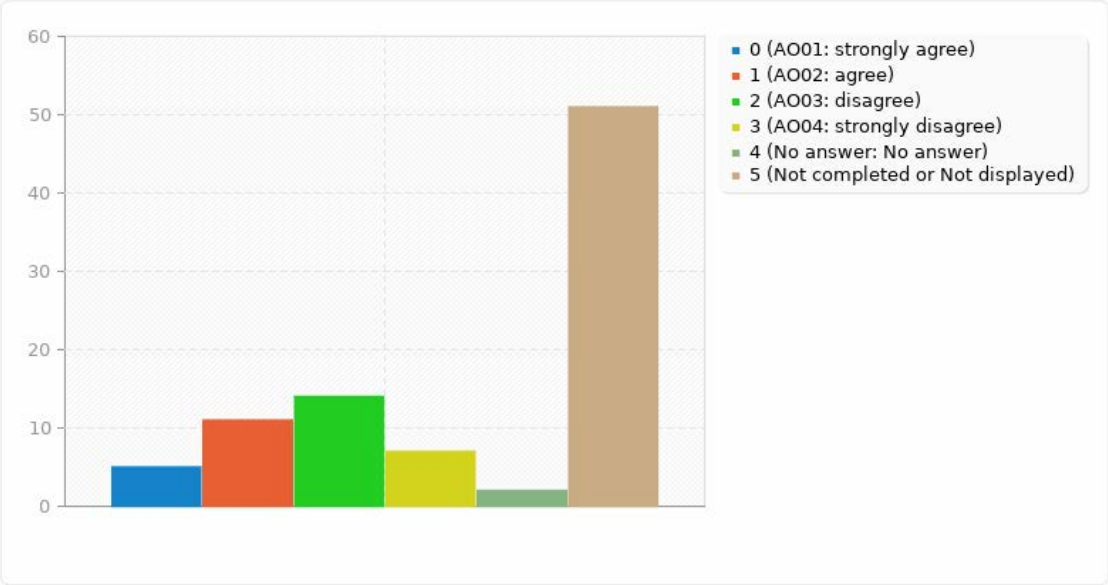
There have also been an open question concerning positive and negative impacts of data protection. Participants clearly state a positive impact of data protection. However, participants also express negative impacts, such as insecurities on data protection measures and bureaucratic efforts. For example, consent forms are considered as a negative impact of data protection, further examples are.

> “The ads that targeting me and the way all they know about me.”
>
> “Some companies sell or give you contact info and you receive unwanted communications.”
>
> “Annoying cookie banners etc.”
>
> “Pesonalized adds”
>
> “Small associations are insecure about what the can publish or not.”

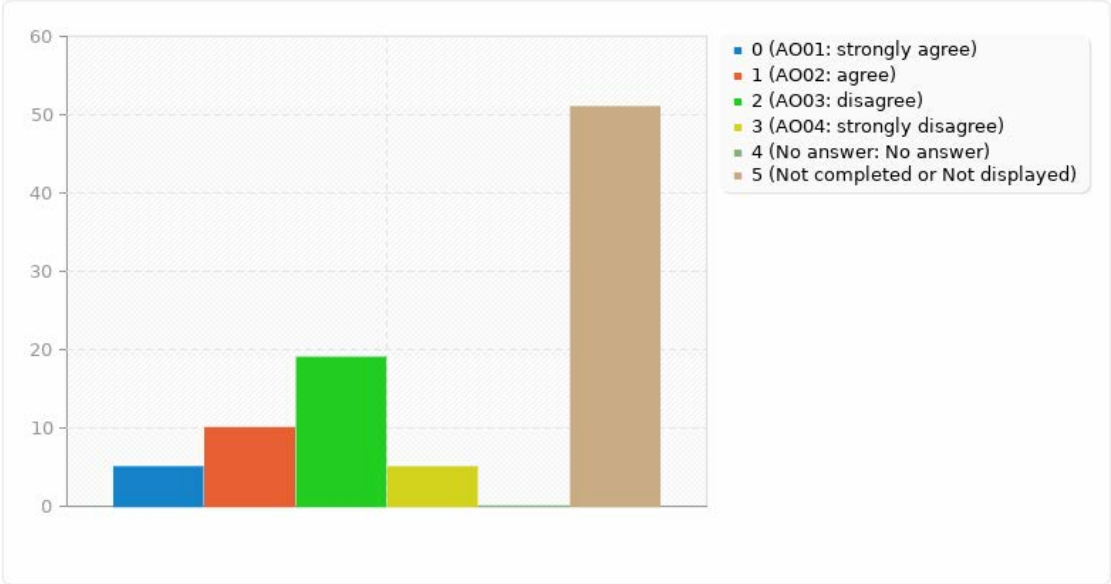
6.1.7 Surveillance

The ambiguous perception of data protection is also visible when it comes to digital surveillance. There are more or less split answers (dis/agreement) in concern of the general attitude to one's privacy and the resignation about inevitability of being transparent for Big Data.

I have nothing to hide.



It's too late to protect my personal data – the big tech companies and intelligence services know everything anyway.



7 Overall Summary and Conclusions

While MSEs exhibit a clear understanding of the risks, their actions often diverge from this awareness. Potentially, this might be due to limited resources hindering the clear separation of private and work devices.

Passwords are considered safe; nevertheless, 2-Factor Authentication is used, possibly due to technological requirements.

There are contradictions concerning trust in bigger companies: They are trusted in concern of cyber security but not in concern for data protection. However, in reality, this issue is more complex and not easy to distinguish.

Participants agree to being tracked online for purposes that only serve the company (and not necessarily themselves), but they also expect their data to be protected from big companies. This results might possibly indicate an acquiescence bias.

There is a perceived positive impact of data protection. Negative impacts concern especially insecurities and added bureaucratic measures. The consent form is perceived as negative by participants.

Overall, there are ambiguities between risk aware knowledge, rather pragmatic behaviour and divergent attitudes to data protection.

8 References

Arabatzis, Theodore/Kindi, Vasso 2008: The Problem of Conceptual Change in the Philosophy and History of Science, in: Vosniadou, S: International Handbook of Research on Conceptual Change, New York, 345-373

Birke, Franziska (2013): Was wandelt sich beim konzeptuellen Wandel? Der Beitrag der Debatte um ‚conceptual change für die wissenschaftspropädeutischen Bemühungen in der ökonomischen Bildung in der Sekundarstufe II, in: Retzmann, T.: Ökonomische Allgemeinbildung in der Sekundarstufe II. Schwalbach/Ts., 87-99.

BMWK - Bundesministerium für Wirtschaft und Klimaschutz (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in. https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.html

Brockhaus, C., Bischoff, T., Haverkamp, K, Proeger, T. Thonipara, A. (2020): Digitalisierung von kleinen und mittleren Unternehmen in Deutschland – ein Forschungsüberblick. Göttinger Beiträge zur Handwerksforschung 46 doi:10.3249/2364-3897-gbh-46

BSI - Bundesamt für Sicherheit in der Informationstechnik (2021): Die Lage der IT-Sicherheit in Deutschland 2021 https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Chan, Y. -Y. and Wei, V. K. (2008): Teaching for Conceptual Change in Security Awareness. in IEEE Security & Privacy, vol. 6, no. 6, pp. 67-69, Nov.-Dec. 2008, doi: 10.1109/MSP.2008.157.

Chi, Michelene T.H. 2008: Three Types of Conceptual Change: Belief Revision, Mental Model Transformation, and Categorical Shift, in: Vosniadou, S: International Handbook of Research on Conceptual Change, New York, 61-82.

Chua, H.; Wong, S.; Low; Chang, Y. (2018): Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics Volume 35, Issue 6, 1770-1780.

Deloitte (2021): Cyber Security Report 2021. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-Cyber-Security-Report-2021.pdf

DiSessa, Andrea A. 2008: A Bird's Eye View of the 'Pieces' vs. 'Coherence' Controversy, in: Vosniadou, S.: International Handbook of Research on Conceptual Change, New York, 35-60.

ENISA 2022: Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

GEIGER (2020): Deliverable D3.1 Training Plan. https://project.cyber-geiger.eu/doc/deliverables/GEIGER_D3.1_Training_Plan.pdf

Kemper, G. (2019): Improving employees' cyber security awareness. In: Computer Fraud & Security, Volume 2019, Issue 8, 11-14.https://doi.org/10.1016/S1361-3723(19)30085-5.

Leinhardt, Gaea; Ravi, Anita K. 2008: Changing Historical Conceptions of History, in: Vosniadou, S.: International Handbook of Research on Conceptual Change, New York.

Meyer, J. & R. Land (2003): Threshold Concepts and Troublesome Knowledge, in: Rust, C.: Improving Student Learning: Improving Student Learning Theory and Practice. Oxford, 1–16.

Mitrofan, A.-L., Cruceru, E.-V., Barbu, A. (2020) Determining the main causes that lead to cybersecurity risks in SMEs. Business Excellence and Management Volume 10 Issue 4, 38-48. 10.24818/beman/2020.10.4-03

NACD - National Association of Corporate Directors (2017): Director's Handbook on Cyber-Risk Oversight.

Remmele, B.; Peichl, J. (2021): Structuring a Cybersecurity Curriculum for Non-IT Employees of Micro- and Small Enterprises. ARES 2021.

Scheponik, T. (2016): How students reason about Cybersecurity concepts. IEEE Frontiers in Education Conference (FIE), 2016, pp. 1-5, doi: 10.1109/FIE.2016.7757363.

Vosniadou, Stella (2008): Conceptual Change Research: An Introduction, in: Vosniadou, S.: International Handbook of Research on Conceptual Change, New York, xiii-xxviii.

9 Appendix

9.1 Interview-Guideline

Interview Guidelines – Learning Hurdles in Cybersecurity / Data Protection

Entry questions:

- What kind of company do you work for? How many employees does your company have?
- What role does IT play in your company? Do you also use private devices in the company?
- How do you organise IT?
- Do you talk informally about cybersecurity and data protection with friends/family and colleagues?

Exit questions:

- What security measures do you implement in your company? Are there any other measures that you have not yet mentioned?
- Anything else you would like to add?

Data Protection			
Thesis - Hurdle	Vignette	Introductory question	Follow-up questions
From: Data protection as a nuisance To: (long-term) adjustment of fundamental rights	In the office, Peter is once again upset about all the cookie banners, which are simply annoying for him. His office colleague Anja thinks that such banners make sense in principle so that she knows, or at least could know, who knows what about her - it is important to her to be able to claim her basic right.	What is your experience with cookie banners? [explain if necessary]	How are such banners implemented on your company website? Were there any reactions to it - internal/external? How is the right to data protection addressed? Is data protection in general annoying or is it worth the effort in terms of personal data protection?
	Timo has a small shop for computer and mobile phone repairs. He saves the names and contact details of his customers so that he can easily record appointments and invoices. A customer contacts him and wants all of his data deleted.	Is data protection manageable at all for smaller companies?	Does your company store personal data? If yes, which ones? Are there precise responsibilities for this? How is your company prepared for such or similar requests? What or who would it hurt to provide a better service to customers with the data available? What about responsibility for others' data in private, e.g. photo with others - unasked - on social media?
From: when you have nothing to hide, To: even the mere possibility that others know more about me than necessary restricts freedom. From: resignation To: active data minimisation (even on a small scale)	Two colleagues are talking during their lunch break. They use various Google products in everyday life and for work and are also on social media. They agree that it's too late for data protection: they know everything about you anyway. Mareike thinks it's far too difficult - where should you start and how is data protection even possible nowadays? Tanja is of the opinion that she has nothing to hide anyway.	What do you think about the statements by Mareike and Tanja?	What role do google & co play for your company / how do you regulate data protection or similar in this context? Does it still make sense to look after your own data when google and the others know everything about you anyway? Is it worth the effort if you "actually have nothing to hide"? Do you change your 'normal' behaviour if you expect it to be stored somewhere? How does your company handle employee data?
		What does that actually mean, "data protection	

		is a fundamental right"? And how is that supposed to be weighed against other interests and other fundamental rights? (Example: New business data transmission)	

Cybersecurity			
Thesis - Hurdle	Vignette	Introductory question	Follow-up question
From: Social engineering attacks are not aimed at 'little ones', To: automated etc. even the smallest things make a mess or grant access to further resources From: feeling safe recognising phishing strategies, To: the strategies are constantly evolving	Sandra receives a somewhat strange e-mail from her supervisor and is not sure whether it is phishing. Her colleague Martin says that phishing e-mails are very easy to recognise, e.g. because they contain grammatical errors or the sender's address is strange.	How well would you say you can detect phishing emails?	Do you know any examples for such emails? What do you think are common detection features of phishing emails? How do they differ from spam? Have phishing strategies changed?
From: the lack of clarity about possible digital assets, To: even smaller companies can be worthwhile victims	Hans has a small company that supplies special screws to a larger car manufacturer. Hans thinks his company is too small for a cyber attack.	How would you estimate the risk of a cyber attack for smaller companies, such as Hans', to become victims of a cyber attack?	How do you estimate the danger for your own company? What can cyber criminals steal from smaller companies? Is it even worth the effort?
From: (former) focus on password length To: Understanding of MFA principle	Andreas is the manager of a small company and uses particularly long passwords to protect his online accounts. This makes him feel secure. A new colleague points out to him that even a long password does not necessarily guarantee high security. She suggests using multi-factor authentication in addition (such as when logging in for online banking)	Where do you see the added value of multi-factor authentication? (explain if necessary)	Where do you see potential dangers even with long passwords? What security measures do you know and use in your company and privately?
From: Delegation of cybersecurity to system To: Awareness that there may be potential security vulnerabilities and that users can/should take active action (e.g. update etc.)	Anna uses Microsoft products (e.g. Outlook) for her small shop to handle e-mails, appointments, deliveries, etc. She also uses Microsoft services. Since Microsoft is a big company, she assumes that the services ensure cybersecurity.	To what extent do you share Anna's assessment?	Is it enough to rely on services from large providers? What other security measures should be implemented when using programmes like Teams?

9.2 Survey Questionnaire

Data protection and cybersecurity in micro- and small businesses

Thank you very much for your cooperation with the University of Education in Freiburg by taking part in the survey!

The results of the survey will be used for a pilot study to explore education in cybersecurity and data protection for small businesses. The pilot study takes place in the context of the Erasmus+ project MECyS, which designs and implements an educational programme on these topics.

Filling out the questionnaire takes about 15 minutes. Your data will be evaluated anonymously.

There are 24 questions in this survey.

General information

In which sector does your company operate?

Please write your answer here:

Is your company providing services or selling goods via the internet?

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

How many employees does your company have?

Choose one of the following answers

Please choose **only one** of the following:

- 1 - 5
- 6 - 10
- 11 - 15
- 16 - 30
- 31 +

Do you use private devices for your work?

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

Do you use work devices for private purposes?

Choose one of the following answers

Please choose **only one** of the following:

- Yes
- No

What is your role in your company: *

Choose one of the following answers

If you choose 'Other:' please also specify your choice in the accompanying text field.

Please choose **only one** of the following:

- Employee
- Manager
- Other

Cybersecurity

Please rate the following statements:

Please choose the appropriate response for each item:

	strongly agree	agree	disagree	strongly disagree
I know typical goals and features of phishing e-mails				
I am able to detect usual phishing e-mails				
I am confident to detect personalized or KI-based phishing e-mails in the future				

Can you name typical goals and features of phishing attacks?

Please write your answer here:

Please rate the following statements:

Please choose the appropriate response for each item:

	strongly agree	agree	disagree	strongly disagree

Cyber attacks only target bigger companies				
Cyber attacks specialize on lucrative victims				
My small company might be a relevant target of cyber attacks				

Can you name typical goals of cyber attacks?

Please write your answer here:

Please rate the following statements:

Please choose the appropriate response for each item:

	strongly agree	**agree**	**disagree**	**strongly disagree**
A long and complicated password will ensure cybersecurity				
I know the concept of 2-Factor Authentication				
I use 2-Factor Authentication for private online services				

Please name 2 examples for 2-factor authentication

Please write your answer here:

Which examples of personal data do you know?

Please write your answer here:

Please rate the following statements:

Please choose the appropriate response for each item:

	strongly agree	**agree**	**disagree**	**strongly disagree**
I enter different websites via my google or facebook or similar account				
I generally trust bigger companies (e.g. Microsoft, Google, ..) to take my cybersecurity seriously				

I pay attention to my cybersecurity when using these services				

Data privacy

Please rate the following statements:

Please choose the appropriate response for each item:

	strongly agree	**agree**	**disagree**	**strongly disagree**
I know typical functions that cookies have				
I benefit from certain cookies				
It is fair that companies track my online behaviour to improve their services				

Which are the cookie options you typically accept?

Check all that apply

Please choose **all** that apply:

- I accept all
- I only accept necessary cookies
- depends on how much time or patience I have
- Depends on the content of the website

In general, data protection impacts me -

Please choose the appropriate response for each item:

	very positively	**positively**	**negatively**	**very negatively**
as customer				
at my work				
in my leisure time				
as a citizen				

Which is the most negative impact you experience(d)?

Please write your answer here:

Which is the most positive impact you experience(d)?

Please write your answer here:

Please rate: personal data should be protected, because

Please choose the appropriate response for each item:

	strongly agree	agree	disagree	strongly disagree
otherwise big companies could steer our behaviour				
otherwise the state could control us				
privacy is a basis for civil rights				
data protection is part of acting responsible in business				

Please rate the following statements in concern of data protection:

Please choose the appropriate response for each item:

	strongly agree	agree	disagree	strongly disagree
„I have nothing to hide“				
„It‘s too late to protect my personal data – the big tech companies and intelligence services know everything anyway“				
„I actively implement measures to protect my data.“				
“I try to inform myself about data protection.“				
“I do not trust companies in the internet to process my data responsibly”				
”Even small individual measures can in sum make a big difference when all stick to them.”				
If I do not protect my private data it also affects the data of others				

Please rate the following statements in concern of data protection:

Please choose the appropriate response for each item:

	strongly agree	agree	disagree	strongly disagree

My company has a responsibility in protecting personal data of its clients				
My company has a responsibility in protecting personal data of its employees				
My company takes data protection serious				
Data protection makes my daily working processes more difficult				
The formal requirements of data protection are practically impossible to implement				

Please rate the following statements in concern of data protection:

Please choose the appropriate response for each item:

	strongly agree	**agree**	**disagree**	**strongly disagree**
“My company has succeeded in implementing data protection”				
“My company is prepared for deleting personal data when requested”				
“My company asks for consent when legally required for processing data”				
"In business context, I have insecurities in concern of data protection“				

If so, where?

Please write your answer here:

Submit your survey.
Thank you for completing this survey.